Un " rapprochement curieux de l'algèbre et de la théorie des nombres" : études sur l'utilisation des congruences en France de 1801 à 1850

Jenny Boucard

Université Pierre et Marie Curie

École Doctorale Paris Centre

Thèse de doctorat

Discipline : Mathématiques

présentée par

Jenny Boucard

Un « rapprochement curieux de l'algèbre et de la théorie des nombres » : études sur l'utilisation des congruences en France de 1801 à 1850

---

dirigée par Catherine Goldstein et Pierre Lamandé

Soutenue le 9 décembre 2011 devant le jury composé de :

M. Frédéric Brechenmacher ...	Université d'Artois
M. Christian Gilain	Université Pierre et Marie Curie Paris
M^me^ Catherine Goldstein	Institut de mathématiques de Jussieu
M. Pierre Lamandé	Université de Nantes
M^me^ Jeanne Peiffer	Centre Alexandre Koyré
M. David Pengelley	New Mexico State University
M. Norbert Schappacher	Université de Strasbourg

Institut de Mathématiques de Jussieu
4, place Jussieu
75 005 Paris

Je reviendrai ailleurs sur ce rapprochement curieux de l'algèbre et de la théorie des nombres ; et je ferai voir que les principes généraux de l'analyse mathématique ont leur source naturelle dans la simple considération de l'ordre, ou de la disposition mutuelle qu'on peut observer actuellement entre plusieurs objets : ce qui me paraît le plus haut point d'abstraction et de généralité où il soit permis de porter la science.

Louis Poinsot, 1820

Remerciements

Avec les quelques lignes qui suivent, je souhaite montrer ma reconnaissance envers tous ceux qui, de près ou de loin, m'ont aidée dans l'élaboration de ma thèse... en espérant n'oublier personne.

En premier lieu, je tiens à exprimer toute ma gratitude envers mes deux directeurs de thèse sans lesquels ce travail n'aurait jamais vu le jour. Merci à Pierre Lamandé pour m'avoir accompagnée dans mes premières expériences en histoire des mathématiques, et conseillée depuis ma deuxième année de Master. C'est également grâce à lui que je suis entrée en contact avec Catherine Goldstein, qui a accepté de codiriger cette thèse et qui y a consacré un nombre d'heures incalculable. Merci donc à elle pour sa grande disponibilité, ses encouragements permanents et ses nombreux conseils qui m'ont permis d'avancer dans mes recherches. En particulier, merci à son implication dans ce marathon des derniers mois qu'a été la rédaction de ces quelques centaines de pages. Sans jamais perdre patience malgré mes blocages, oublis, incohérences, fautes d'orthographe, de style, ..., elle m'a soutenue et encouragée jusque dans les dernières heures.

Je tiens également à remercier Jeanne Peiffer et David Pengelley qui ont accepté d'être rapporteurs de cette thèse malgré des délais très courts. Merci également à Frédéric Brechenmacher, Christian Gilain et Norbert Schappacher pour leur participation au jury.

Bien sûr, je suis également très reconnaissante envers tous les membres du projet *Histoire des mathématiques* de l'Institut de Mathématiques de Jussieu qui m'ont accueillie dans leur équipe ces dernières années et m'ont soutenue intellectuellement, moralement et techniquement. Un grand merci également aux doctorants et anciens doctorants qui m'ont souvent remonté le moral en partageant leur propre expérience de thésard : je pense tout particulièrement à Frédéric Brechenmacher, Sébastien Gauthier, Alexandre Guilbaud, Juliette Leloup, Anne-Sandrine Paumier. Plus généralement, merci au personnel de l'UPMC qui m'a aidée dans mes démarches ces dernières années.

Ce travail n'aurait pas pu être ce qu'il est aujourd'hui sans les exposés et discussions des groupes de travail, séminaires, colloques organisés ici et ailleurs, auxquels j'ai participé ces dernières années : merci donc aux organisateurs et participants, dont les questions, commentaires et suggestions ont été très bénéfiques. De même, un grand merci à ceux qui m'ont aidée pour la publication de mon premier article sur Poinsot c'est-à-dire Catherine et Pierre bien sûr, toute l'équipe de la *Revue d'histoire des mathématiques*, et tout spécialement les deux rapporteurs anonymes pour leur relecture attentive et leurs conseils avisés.

Dans le cadre de recherches en histoire des sciences, la possibilité d'accéder aux documents originaux est primordiale : je remercie donc le personnel des différentes institutions qui m'ont permis d'accéder à des manuscrits et autres documents, et tout particulièrement celui des archives de l'Académie des Sciences, de la Bibliothèque de l'Institut de France, et de l'Observatoire Royal de Bruxelles.

À côté de ma thèse, j'ai également enseigné les mathématiques aux charmants élèves du collège de Valence d'Agen jusqu'en juin dernier. Merci à eux qui, sans le savoir, m'ont permis de changer d'air, à mes collègues pour leur soutien et leurs encouragements ainsi qu'au personnel de direction qui a toujours fait en sorte que je puisse me déplacer régulièrement à Paris en m'accordant des emplois du temps adaptés. J'en profite également pour remercier l'équipe du Département Mathématiques et Histoire des Sciences de l'Université Paris 8 qui m'accueille cette année en tant qu'Attaché Temporaire d'Enseignement et de Recherche et qui me permet ainsi de faire mes premiers pas dans l'enseignement supérieur.

Enfin, je suis très reconnaissante envers ma famille, mes amis, et tout particulièrement Laurent, qui ont su, pendant ces dernières années, me soutenir et me conseiller dans mes nombreux moments de doute, et ce, malgré mon manque de disponibilité. Je tiens tout particulièrement à remercier ceux qui m'ont hébergée de nombreuses fois à Paris (Mathilde, Lise et Thomas, Anouchka et Carole, Anne-Sandrine et Pierre, Lucile et Sylvain) et ceux qui ont pris du temps pour relire certaines parties de ma thèse : MicHaël (un grand merci également pour les livres empruntés et les photocopies faites à la BU de Toulouse), ainsi que ma mère et Laurent, qui auraient certainement préféré consacrer ce dernier week-end ensoleillé de septembre à autre chose que l'histoire des mathématiques... Un dernier clin d'œil à Éclipse et Épice qui m'ont souvent inspirée par leur présence plus ou moins discrète dans mon bureau...

Résumé

Résumé

Gauss introduit la notion de congruence en 1801 dans les *Disquisitiones Arithmeticae*. L'historiographie classique relie le plus souvent l'histoire de cette notion au développement de la théorie des nombres algébriques, une histoire construite autour d'un groupe de mathématiciens allemands. Pourtant, d'autres auteurs ont publié des travaux en lien avec les congruences dans la première moitié du XIX^{e} siècle, et ce dans des perspectives différentes. Dans ce travail, nous nous proposons de rendre compte de ces dernières en nous concentrant sur les travaux de la scène française publiés entre 1801 et 1850. À partir d'une première lecture globale des textes de notre corpus, nous montrons d'abord que les congruences n'y ont pas connu un développement autonome mais ont été étudiées dans un lien étroit avec les équations. Toutefois, les différentes pratiques rencontrées sont très variées, que ce soit du point de vue des méthodes, des outils en jeu ou des configurations disciplinaires en jeu. Nous étudions ensuite plusieurs travaux arithmétiques d'Euler, de Lagrange, de Legendre et de Gauss afin de comprendre certaines origines de cette activité multiforme mise en évidence dans notre première partie. Nous nous concentrons enfin sur les travaux de deux auteurs de notre corpus, Louis Poinsot et Augustin Louis Cauchy, qui ont joué un rôle important dans l'élaboration et la diffusion de résultats et de pratiques liés aux congruences, même s'ils ont pratiquement disparu des histoires de la théorie des nombres publiées au XX^{e} siècle.

Mots-clefs

Algèbre, Cauchy, congruences, Poinsot, théorie des nombres, histoire des mathématiques au XIX^{e} siècle.

"A curious encounter between algebra and number theory" : studies on the uses of congruence in France between 1801 and 1850

Abstract

Gauss introduced the notion of congruence in 1801 in the *Disquisitiones Arithmeticae*. The standard historiography connects its history to the development of algebraic number theory, a history built around a group of German mathematicians. However other authors in the first half of the nineteenth century published works related to congruences from different perspectives. We study here some of them while focusing on the French scene between 1801 and 1850. From a global reading of the texts of our corpus, we first show that congruences did not develop in France as an autonomous field, but as one tightly linked to the theory of equations. However, the different practices thus encountered were far from uniform, whether in terms of methods, tools or disciplinary configurations. We then study arithmetical works of Euler, Lagrange, Legendre and Gauss in order to understand some of the origins of the multifarious activity analyzed in our first part. Finally, we focus on the work of two authors, Louis Poinsot and Augustin Louis Cauchy, who played a key role in elaborating and circulating results and practices related to congruences, but who have virtually disappeared from twentieth-century histories of number theory.

Keywords

Algebra, Cauchy, congruences, Poinsot, number theory, history of mathematics in the nineteenth century.

Table des matières

Introduction générale

Le début du XIX^{e} siècle est généralement perçu comme une période de profond changement en mathématiques, dont une des caractéristiques principales serait l'avènement de la rigueur et la mise en place de nouveaux fondements et de nouveaux objets [1] :

> Curiously enough, mathematics and its historiography are rather acutely conscious of the fact that the turn from the 18th to the 19th century marks a decisive turning point full of consequences in the development of science.[...]
>
> [...], the "great upheaval in the sciences" predicted by Diderot seized mathematics as well, and led to new developments of method and object not anticipated. The new style of mathematics, which began to emerge at the turn to the 19th century, is seen, as most historians of mathematics agree, first of all in the tendancy towards rigorous proof, and in a more careful elaboration of the foundations and definitions of mathematics. Analysis sees a foundation of its methods, the nucleus of which is described as arithmetization [Jahnke et Otte, 1981, p. 21].

Parmi les exemples couramment mentionnés, nous pouvons évoquer la construction d'une théorie des nombres complexes au cours de la première moitié du XIX^{e} siècle [2], la redéfinition de la notion de fonction et des concepts associés (continuité, limite), le programme d'arithmétisation de Karl Weierstrass et de Leopold Kronecker visant à la fin du siècle à refonder l'analyse, voire l'ensemble des mathématiques, sur les nombres entiers [3]. Cette période est aussi celle de profondes transformations disciplinaires [4]. Jeremy Gray décrit ces modifications comme une révolution :

> I have argued that there was a revolution in mathematics in the nineteenth century because, although the objects of study remained superficially the same, the way they were defined, analysed theoretically, and thought about intuitively was entirely transformed. This new framework was incompatible with older ones, and the transition to it was much greater than scientists are accustomed to.[...]
>
> The chief aspect of this revolution was ontological, and this shift underlies all the domains of mathematics considered here. Such basic concepts as integer in number theory and straight line in geometry were completely reformulated [Gray, 1992].

C'est dans cette perspective que nous avons commencé à nous intéresser à l'introduction d'un nouvel objet de la théorie des nombres : les résidus et les congruences.

1. Nous empruntons cette citation à une sélection de références intitulée *Sur l'historiographie de l'articulation XVIII^{e}-XIX^{e} siècles en mathématiques* préparée par Christian Gilain dans le cadre de la première séance du groupe de travail *Les sciences mathématiques 1750-1850 : continuités et ruptures*. Notons que ce groupe vise à remettre en cause l'idée d'une rupture radicale et complète pendant la période, nous y reviendrons.

2. Nous pensons notamment aux textes de Jean-Robert Argand, de Carl Friedrich Gauss, et d'Augustin Louis Cauchy : voir [Flament, 2003] à ce sujet.

3. Voir [Grattan-Guinness, 1980], [Grabiner, 1981], [Bottazzini, 1986] et [Goldstein et Schappacher, 2007a, part. V].

4. Voir [Stichweh, 1991], [Guntau et Laitko, 1987] et pour la théorie des nombres particulièrement, voir [Goldstein et Schappacher, 2007a, part. I].

La notion de congruence est introduite par Gauss en 1801 dans les *Disquisitiones Arithmeticae*[5] :

> Si un nombre a divise la différence des nombres b et c, b et c sont dits *congrus* suivant a, sinon *incongrus*. a s'appellera le module ; chacun des nombres b et c, *résidus* de l'autre dans le premier cas, et *non résidus* dans le second.
>
> Les nombres peuvent être positifs ou négatifs, mais entiers. Quant au module il doit évidemment être pris absolument, c'est-à-dire sans aucun signe [Gauss, 1801, art. 1].
>
> [...] Nous désignerons dorénavant la congruence de deux nombres par ce signe $\equiv$, en y joignant, lorsqu'il sera nécessaire, le module renfermé entre parenthèses ; ainsi $-16 \equiv 9 \pmod 5$, $-7 \equiv 15 \pmod{11}$ [Gauss, 1801, art. 3].

Autrement dit, deux nombres a et b sont congrus suivant p si leurs restes après division par le nombre p sont égaux. Les congruences sont donc étroitement liées avec les restes de divisions. Dès 1751, Leonhard Euler avait entamé l'examen systématique de ces restes, qu'il nomme *résidus*, et en avait établi de nombreuses propriétés. Dans les *Disquisitiones*, les premiers chapitres sont entièrement consacrés à ces résidus et aux congruences et ces notions interviennent de manière décisive dans les chapitres suivants, consacrés aux formes quadratiques, à la factorisation des nombres entiers, et enfin à la détermination des nombres entiers n pour lesquels un polygone régulier de n côtés peut être inscrit dans le cercle à la règle et au compas, où la théorie des résidus permet de recoder adéquatement les racines de l'unité. Gauss prouve en particulier une loi considérée comme centrale bien au-delà de la théorie des nombres, la loi de réciprocité quadratique : dans le cas où p et q sont deux nombres premiers impairs, dont l'un au moins n'est pas de la forme $4n + 3$, cette loi dit par exemple que p est congru à un carré modulo q si et seulement si q est congru à un carré modulo p.

Les congruences participent aux évolutions mentionnées plus haut et sont au cœur des *Disquisitiones* de Gauss. Celui-ci en retour est un ouvrage-clé dans l'histoire de la théorie des nombres :

> Gauss's book is now seen as having created number theory as a systematic discipline in its own right, with the book, as well as the new discipline, represented as a landmark of German culture [Goldstein et Schappacher, 2007a, p. 4].

Le thème des congruences semblait donc prometteur pour aborder la question de la transformation des mathématiques entre le XVIII^e^ et le XIX^e^ siècle. Gauss souligne immédiatement la similarité entre congruence et égalité et on pourrait supposer qu'une réflexion nouvelle se soit alors ouverte sur les opérations, les signes, le fait d'opérer sur des classes de nombres ou leurs représentants, etc. L'histoire pourtant semble avoir surtout

5. Toutes nos citations des *Disquisitiones Arithmeticae* sont empruntées à la traduction française publiée en 1807.

pris acte du lien entre les lois de réciprocité et le développement de la réflexion sur la notion d'entier algébrique.

L'historiographie réduit en tout cas le plus souvent l'histoire des congruences au développement de la théorie algébrique des nombres, construite autour d'un groupe de savants allemands. Rappelons-en les grandes lignes. C'est par exemple le cas dans [Bourbaki, 1984] ou encore [Gray, 1992]. Cette histoire débute en 1801 avec la publication des *Disquisitiones Arithmeticae* de Gauss : celui-ci définit donc la notion de congruence, établit la stabilité de la notion par les opérations usuelles, étudie certaines équations aux congruences. En particulier, il élabore une théorie des résidus quadratiques et présente notamment deux démonstrations de loi de réciprocité quadratique. À la suite de ce premier ouvrage, Gauss poursuit ses recherches sur ces thèmes en essayant d'obtenir des résultats équivalents pour des résidus d'ordre supérieur : les résidus cubiques et biquadratiques. Ainsi, entre 1828 et 1831, il publie un mémoire en deux parties sur les résidus biquadratiques, dans lequel il présente une étude détaillée de ce que l'on appelle aujourd'hui les entiers de Gauss, c'est-à-dire les nombres de la forme $a + b\sqrt{-1} = a + bi$, où a et b sont des nombres entiers réels, et les utilise pour établir une loi de réciprocité biquadratique.

Dans le deuxième quart du XIX$^{\text{e}}$ siècle, les *Disquisitiones* deviennent un traité de référence lors de la formation mathématique de jeunes mathématiciens allemands, tels que Carl Gustav Jacob Jacobi, Johann Peter Gustav Lejeune Dirichlet, Ernst Eduard Kummer ou Gotthold Eisenstein, qui prouvent d'autres cas de lois de réciprocité. Là encore, suivant Gauss, ces mathématiciens sont amenés à introduire de nouveaux ensembles de nombres : par exemple, la théorie des résidus cubiques implique la considération de nombres de la forme $a+b\omega$, où a et b sont des nombres entiers réels, et où ω est une racine cubique complexe de l'unité. Les propriétés habituelles des nombres entiers réels, et en particulier la possibilité d'une décomposition unique en facteurs premiers, sont également valables pour les nombres de la forme $a+bi$ et $a+b\omega$, et on peut démontrer ces propriétés de manière tout à fait analogue à celles des nombres réels entiers. Mais lorsque Kummer, en particulier, commence à étudier les entiers cyclotomiques, qui sont composés plus généralement de coefficients entiers et de racines p^{e} de l'unité, il s'aperçoit que l'analogie avec les nombres entiers réels n'est plus valide dans certains cas : la décomposition de ces nouveaux nombres entiers complexes en facteurs premiers n'est plus nécessairement unique. Kummer construit donc ce qu'il appelle les nombres idéaux afin de rétablir cette propriété de décomposition unique ; là encore, les congruences jouent un rôle décisif puisque la construction des nombres idéaux repose sur les propriétés de divisibilité vérifiées par ces nouveaux types de nombres. Même si ses recherches ont pour objectif premier les lois de réciprocité d'ordre supérieur, Kummer utilise également ses nombres idéaux pour démontrer le dernier théorème de Fermat [6] pour un grand nombre de nouveaux cas. La

6. Selon ce théorème, l'équation $x^n + y^n = z^n$ n'admet pas de solutions entières non triviales lorsque n est supérieur à 2. Voir sur les travaux de Kummer [Edwards, 1977].

théorie des nombres idéaux de Kummer est ensuite reprise et modifiée par Kronecker et Richard Dedekind. Les congruences en tant que telles paraissent alors ne plus jouer un rôle aussi important, mais un développement parallèle conduit par ailleurs à la notion de corps finis. Cette histoire de la théorie des nombres algébriques se synthétise dans *Die Theorie der algebraischen Zahlkörper*, publié en 1897, dans lequel David Hilbert adopte et développe le point de vue structural de Dedekind [7].

La discussion épistémologique qu'on pouvait attendre sur le nouveau concept ne semble donc pas avoir eu lieu. Une hypothèse évidente est que les textes où il apparaît étaient considérés comme trop marginaux. Une double remise en question de ce récit traditionnel de l'histoire de la théorie des nombres a eu lieu dans les dernières décennies. D'une part, elle a montré l'importance de prendre en compte l'organisation humaine et matérielle de la recherche pour rendre compte de la diffusion réelle des idées après leur conception : les sociétés savantes, les journaux, l'enseignement, les liens avec telle ou telle communauté, qu'elle soit celle des ingénieurs ou des philosophes. D'autre part, elle a insisté sur les représentations disciplinaires multiples, dont les composantes imposent certaines contraintes sur le développement et aussi sur sa visibilité. Par exemple, les auteurs de [Goldstein et Schappacher, 2007a] montrent que les congruences sont bien au cœur d'une première structuration disciplinaire (au sens de Guntau et Laitko) de la théorie des nombres, mais qu'au milieu du dix-neuvième siècle, celle-ci touche l'enseignement, mais pas l'organisation de la recherche. Ils appellent « *analyse algébrique arithmétique* » le champ de recherche liant les lois de réciprocité, les formes, les nombres complexes ainsi que des outils d'analyses comme les séries infinies, les fonctions elliptiques, qui s'établit à cette époque. Celui-ci ne s'organise pas autour d'un seul objet bien délimité. C'est seulement à la fin du siècle que ce processus de disciplinarisation aura lieu plus nettement, autour d'objets comme les corps de nombres ou les séries de Dirichlet [8]. Certaines filiations, certains transferts ne sont pas perçus simplement quand l'organisation disciplinaire change ainsi radicalement, dans la mesure où on les recherche à partir d'une thématique ou un objet dont, comme le souligne J. Gray plus haut, le mode d'élaboration même est différent.

Un indice supplémentaire qui suggère de prendre en compte ces observations pour étudier résidus et congruences est que certains travaux arithmétiques disparaissent complètement, ou apparaissent comme tout à fait isolés, décrits selon le cas comme précurseurs ou marginaux. Il a déjà été noté que la théorie des formes quadratiques qui occupe aussi une place importance au moins jusqu'à la première guerre mondiale est toute entière marginalisée dans l'historiographie traditionnelle [9]. Les travaux des mathématiciens en théorie

7. Voir [Goldstein et Schappacher, 2007b, p. 88-90] pour une analyse de la place des *Disquisitiones* et de la définition de la théorie des nombres dans cette somme de la théorie des nombres algébriques.
8. Voir [Goldstein et Schappacher, 2007b] pour une étude de ce processus à partir de 1860.
9. Voir [Goldstein, 1999].

des nombres en dehors des centres allemands ont été longtemps ignorés. Lorsque le dernier théorème de Fermat occupe une place importante dans la narration, quelques savants français sont mentionnés, mais en tant qu'acteurs secondaires : Adrien-Marie Legendre et Gabriel Lamé sont cités pour leurs preuves « increasingly difficult », [Gray, 1992, p. 230], des cas particuliers $n = 5$ et $n = 7$ de ce théorème. Lamé et Cauchy sont également considérés pour leurs tentatives ratées de démonstration de l'existence de la décomposition unique en facteurs premiers pour les nombres entiers cyclotomiques. Or, entre 1827 et 1829, Jacobi et Cauchy publient des mémoires contenant des résultats très similaires obtenus indépendamment et qui s'avèrent ensuite fondamentaux dans les travaux de Jacobi, Dirichlet et Kummer. Lemmermeyer, dans son article sur les rôles joués par les travaux de Jacobi dans la construction de la théorie des nombres idéaux de Kummer, remarque effectivement que Cauchy et Jacobi arrivent à des conclusions similaires, puis observe : « Cauchy also studied these sums, but his lack of understanding higher reciprocity kept him from going as far as Jacobi did »[Lemmermeyer, 2009, p. 171]. Les mémoires de Cauchy n'aboutissent effectivement pas comme ceux de Jacobi à l'énoncé de la loi de réciprocité cubique par exemple, et à la considération de certaines formes d'entiers complexes. Mais est-ce parce qu'il ne comprenait pas les fondements des lois de réciprocité d'ordre supérieur, ou est-ce parce que ses objectifs n'étaient pas les mêmes que ceux de Jacobi ? Les jeunes Jacobi et Dirichlet sont particulièrement au fait des recherches de Gauss, dont l'objectif est explicitement d'obtenir des lois de réciprocité d'ordre supérieur. Du point de vue d'une histoire de la théorie des nombres algébriques, le développement qui consiste à introduire des entiers complexes dans les recherches sur les lois de réciprocité apparaît comme naturel. Mais cette historiographie centrée sur des objets (ici : les corps de nombres algébriques) produits à la fin d'un certain développement induit une grille de lecture qui rend difficile la compréhension de l'ensemble des résultats et des idées développées par des savants dont les perspectives sont différentes : l'exemple précédent le montre particulièrement bien pour Cauchy.

Évariste Galois propose d'introduire des solutions imaginaires (complexes) des congruences ordinaires dans le cadre de ses recherches sur la théorie des équations algébriques. L'historiographie tend à en faire un auteur tout à fait isolé dont les résultats ne seront reconnus que lorsqu'ils auront été retrouvés indépendamment par Theodor Schönemann, puis incorporés par Dedekind et surtout par Hilbert à la théorie algébrique des nombres, sous la forme d'une théorie des corps finis[10]. Pourtant, comme nous le verrons, d'autres auteurs basés en France ont proposé d'étudier les solutions imaginaires[11] des congruences dans les années 1820 et 1830.

Dans le *Report on the Theory of Numbers* de Henry John Stephen Smith, publié entre 1859 et 1865, donc avant l'avènement des corps de nombres, l'auteur cite dans son

10. Voir [Frei, 2007].
11. Nous reviendrons sur la notion de racine imaginaire de congruence plus loin.

introduction les savants qui, selon lui, ont participé au développement de la théorie des nombres à la suite de Gauss :

> The arithmetical memoirs of Gauss himself, subsequent to the publication of the ' Disquisitiones Arithmeticae ' ; those of Cauchy, Jacobi, Lejeune Dirichlet, Eisenstein, Poinsot, and, among still living mathematicians, of MM. Kummer, Kronecker, and Hermite, have served to simplify as well as to extend the science [Smith, 1859-1865, p. 38].

Certains noms apparaissent donc, puis disparaissent selon les priorités utilisées pour décrire cette histoire. C'est cette apparente contradiction entre la présence de Poinsot et Cauchy dans le rapport de Smith au milieu du dix-neuvième siècle, et leur disparition de l'historiographie de la théorie des nombres, qui va particulièrement nous intéresser dans cette étude.

Nous avons donc choisi d'étudier particulièrement la scène française avant 1850. Il apparaît nécessaire pour cela de procéder autrement, c'est-à-dire sans une grille de lecture centrée autour de résultats perçus par avance comme essentiels, pour pouvoir mettre en avant les caractéristiques propres des travaux des savants qui ne s'insèrent pas dans l'histoire classique de la théorie des nombres décrite plus haut.

Notre tâche initiale a été de construire notre corpus de travail en rassemblant les publications où les résidus et les congruences sont utilisés explicitement, que ce soit sous la forme développée par Gauss ou non [12]. Nous avons donc commencé par établir une méthode afin de repérer ces textes en dressant une liste de quelques mots, symboles et théorèmes-clés que l'on retrouve dans la majorité des cas des raisonnements avec les résidus et les congruences. Partant de cela, nous avons examiné des synthèses postérieures afin d'obtenir ainsi un premier corpus, puis nous avons analysé chacun des textes ainsi sélectionnés à partir d'un double questionnement : quelles sont les sources données explicitement par l'auteur ? Comment les résidus ou les congruences sont-ils utilisés ? Nous avons enfin complété cette première liste en dépouillant les principaux périodiques scientifiques de la scène française, ainsi que plusieurs ouvrages sur l'histoire de la théorie des nombres du XIX^{e} et XX^{e} siècles, en appliquant notre double questionnement pour chacun des textes retenus. Cette première partie nous permet de situer les auteurs et leurs modalités de travail, et de repérer leurs liens entre eux. Elle est d'abord descriptive (et par là-même parfois répétitive) parce qu'elle vise à donner les éléments concrets disponibles dans la première moitié du XIX^{e} siècle pour notre thème. Nous retrouverons en particulier de manière proéminente les deux auteurs mentionnés par Smith : Cauchy et Poinsot, ainsi que plusieurs autres. Nous reviendrons dans une deuxième partie sur les sources communes de ces auteurs, en particulier les recherches d'Euler et de Joseph-Louis

12. C'est l'objet de notre première partie.

Lagrange au siècle précédent, afin d'être en mesure de comprendre les ruptures et les continuités sur la période 1750-1850.

Nous serons ainsi mieux armés pour revenir en détail sur les deux auteurs que nous avons distingués : Poinsot et Cauchy. Nous étudierons leurs différentes productions autour des résidus et des congruences dans les deux parties suivantes, en considérant des contextes de lecture variés, afin de faire ressortir différents aspects de leur activité. Il est essentiel d'expliciter le plus précisément possible le contexte considéré. Étudiant une tablette mathématique babylonienne dans trois contextes différents, J. Ritter constate :

> Each reader brings to a text an embedding in a larger corpus of texts, one which shapes his or her understanding. This is inevitably the case but can be done on a more or less conscious manner ; I have tried to argue here for the importance of bringing explicitly into play the precise contents of the corpus as well as that of making that corpus as complete as possible[...] Moreover I have underlined the advantages of adopting several different explicit contexts in order to explore the maximum of aspects of the text, many of which achieve visibility only under the changing light of multiple recontextualizations [Ritter, 2004, p. 195].

Chaque lecture est dépendante de différents critères, en particulier du choix du corpus encadrant cette lecture. Ainsi, lire les travaux de Galois à la lumière des écrits de Gauss ou de la théorie de Galois telle qu'elle est présentée aujourd'hui n'implique pas les mêmes conclusions [13] ; un autre exemple a été évoqué précédemment avec la lecture des recherches arithmétiques de la première moitié du XIX^{e} siècle à la lumière de la théorie des corps de nombres algébriques. Étudier un texte, ou un groupe de textes, en le situant dans des contextes variés (et explicités) permet d'en faire ressortir des informations différentes. Les deux premières parties de l'étude fournissent déjà des contextualisations à nos deux auteurs ; nous expliciterons, dans les parties qui leur sont consacrées, des contextes supplémentaires propres à mieux appréhender les caractéristiques de leurs travaux.

Du point de vue de l'histoire encore courante de la théorie des nombres, le développement des congruences semble avant tout une accumulation de résultats nouveaux. La notion de corps finis donne bien sûr une autre légitimation aux résidus et aux congruences, principalement en ce qu'elle gomme les différences conceptuelles entre eux et l'égalité sur les nombres. Comme nous le verrons, la prise en compte d'autres auteurs, et d'autres contextes, montre à quel point ce sont au contraire les jeux de miroir entre nombres et résidus, entre égalités et congruences, parfois à l'intérieur d'un espace disciplinaire commun (la théorie des équations), parfois non, qui sont importants pour que ces notions s'intègrent au cours du dix-neuvième siècle à la pratique courante des mathématiques.

13. Voir [Ehrhardt, 2007].

PARTIE I

Les résidus et les congruences dans les publications de 1801 à 1850

CHAPITRE 1

Construction du corpus : méthode

I Critères de repérage des textes

Afin de construire notre corpus de textes relatifs aux résidus et aux congruences pour la période 1801 - 1850, nous avons défini des critères qui permettent de cerner les textes entrant dans le cadre de notre étude. En effet, selon les auteurs et les époques, ces objets d'apparition relativement récente[1] prennent différentes formes ; les notations et le vocabulaire autour des résidus et des congruences sont loin d'être unifiés sur la période considérée. Ainsi, les *congruences* de Gauss sont des *équivalences* chez *Cauchy* ou encore des *équations* chez Poinsot ou *équations indéterminées* chez Legendre. De même, on trouve des *résidus* dans certains écrits, des *restes* dans d'autres, ou des *nombres de même forme* chez Cauchy.

Du point de vue des notations, là encore, les habitudes sont diverses. Gauss introduit le symbole ≡ et la notion de module dans les *Disquisitiones Arithmeticae* en 1801, mais beaucoup de mathématiciens ne les intègrent pas dans leurs travaux. L'autre type de notation le plus souvent utilisée est le signe = associé à une notation pour désigner "multiple de" ou complété par une expression en toutes lettres. Par exemple, dans la deuxième édition de son *Essai sur la théorie des nombres* publiée en 1808, Legendre écrit parfois une égalité en précisant qu'il « néglige les multiples de n »[Legendre, 1808, p. 167]. Il écrit également la congruence $x^n \equiv b \pmod{a}$ sous la forme $x^n - b = ay$[Legendre, 1808, p. 340] et sous la forme $x^n - b = \mathfrak{M}(a)$[Legendre, 1808, p. 340]. Ces trois expressions traduisent bien sûr le même problème mathématique. Néanmoins, dans le second cas, on voit qu'une variable supplémentaire y intervient : ce sont typiquement les notations adoptées au XVIII$^{\text{e}}$ siècle dans le cadre de l'analyse diophantienne. Dans les deux autres écritures, on ne tient pas compte de la valeur du multiple de n. Cela traduit l'idée de congruence de Gauss : la différence $x^{n-1} - 1$ est divisible par n, mais on ne s'intéresse pas à la valeur du quotient. Ce sont donc les deux formes de notations basées sur la considération d'un multiple quelconque qui sont prises en compte ici.

Les dénominations et notations employées pour désigner les résidus et les congruences diffèrent aussi pour un même auteur selon les supports : ainsi, Louis Poinsot désigne invariablement dans ses publications les congruences par la notation $= Mp$, tandis que dans certains de ces manuscrits, il emploie le symbole ≡ de Gauss.

Afin de grouper les textes où les résidus et les congruences sont présents, nous avons

1. Euler commence à travailler avec les résidus dans les années 1750 et les congruences sont introduites par Gauss en 1801.

systématiquement procédé au repérage de certains mots clés : “congruence”, ou les expressions associées, “résidu” et “reste”. Lorsque c'est l'expression “reste” qui est utilisée, nous avons également vérifié que les raisonnements employés dans le texte en question s'appuyaient sur des propriétés des résidus (opérations sur les restes, propriétés des résidus quadratiques, utilisation du petit théorème de Fermat ou encore considération d'une racine primitive[2], ...). Par exemple, dans un des textes de Cauchy en rapport avec le théorème de Fermat sur les nombres polygones[3], l'auteur utilise à deux reprises les restes dans les trente-quatre pages du mémoire. Ce sont deux remarques de la forme : telle expression « n'est pas un nombre impair dont la division par 8 donne 7 pour reste »[Cauchy, 1818, p. 321], ce qui peut être traduit par “telle expression n'est pas de la forme $8k + 7$”. Ici, Cauchy n'utilise aucune propriété propre à la théorie des résidus et des congruences : nous avons donc écarté ce texte de notre corpus. Pour repérer les congruences dans les textes analysés du point de vue des notations, nous avons systématiquement cherché la notation $\equiv$ ou les notations de la forme $= Mp$, où Mp désigne un multiple de p. Enfin, nous avons également, dans un premier temps, conservé les mémoires où l'auteur aborde un théorème le plus souvent associé aux résidus et congruences : c'est le cas des théorèmes de Fermat et de Wilson.

II Un premier repérage de corpus : les synthèses postérieures

Nous avons d'abord effectué ce repérage systématique de mots et de symboles clés dans trois ouvrages dont l'objectif est de recenser des textes scientifiques. Cela nous a permis d'obtenir une première liste de textes en vue de la construction de notre corpus.

1 - *History of the Theory of Numbers* de Dickson (1919-1923) et la thèse d'A. E. Cooper sur les résidus quadratiques (1926)

La première synthèse analysée est l'ouvrage en trois volumes de Leonard Eugene Dickson, publié entre 1919 et 1923 : *History of the Theory of Numbers*[4]. Dans la préface de son premier volume, l'auteur indique l'objectif de son projet : « This history aims to give an

2. Une racine primitive d'un nombre premier p est un nombre tel que les résidus de ses puissances successives donnent tous les nombres entiers compris entre 1 et $p-1$: c'est ce que nous appelons aujourd'hui un générateur du groupe cyclique $\mathbb{F}_p^*$. D'une manière générale, une racine primitive d'une équation ou d'une congruence engendre toutes les autres racines de l'équation ou de la congruence considérée.

3. Les nombres polygones, ou nombres polygonaux, sont des nombres pouvant être représentés par des polygones. Les nombres triangulaires, par exemple, sont de la forme $1 + 2 + 3 + \ldots$. Plus généralement, si on considère un polygone à c côtés, le n^{e} nombre polygonal est donné par la forme $\frac{1}{2}n\left[(c-2)n-(c-4)\right]$. Le théorème de Fermat sur ces nombres affirme que tout nombre entier s'écrit comme somme d'au plus n nombres polygonaux, lorsque le polygone considéré a n côtés.

4. Della Fenster étudie la réception des *Disquisitiones Arithmeticae* aux États-Unis à travers la construction de cet ouvrage et les travaux de théorie des nombres de Dickson dans [Fenster, 2007].

adequate account of the entire litterature of the theory of numbers »[Dickson, 1919-1923, Vol. 1, Préface, p. vii]. L'ouvrage est basé sur un large dépouillement (par Dickson et ses collaborateurs) de sources variées. Les trois volumes traitent respectivement de la divisibilité et des nombres premiers (*Divisibility and primality*), de l'analyse diophantienne (*Diophantine Analysis*) et de la théorie des formes (*Quadratic and Higher Forms*). Chaque tome est de nouveau subdivisé thématiquement. L'auteur justifie ce choix dans sa préface :

> It is inconceivable that any one would desire this vast amount of material arranged other than by topics. Again, conventional histories take for granted that each fact has been discovered by a natural series of deductions from earlier facts and devote considerable space in the attempt to trace the sequence. But men experienced in research know that at least the germs of many important results are discovered by a sudden and mysterious intuition, perhaps the result of subconscious mental effort, even though such intuitions have to be subjected later to the sorting process of the critical faculties. What is generally wanted is a full and correct statements of the facts, not an historian's personnal explanation of those facts [Dickson, 1919-1923, Vol. 2, Préface, p. xx].

Pour chacune des sections, Dickson reporte toutes les références trouvées en lien avec le sujet en question, indique pour chacune d'elles séparément les notions définies, les résultats énoncés et résume les démonstrations le cas échéant. Cet ouvrage constitue donc un outil incontournable pour avoir une idée précise des différents textes publiés sur un thème et une période donnés.

Néanmoins, le choix de décrire la théorie des nombres par thèmes et sous-thèmes impose déjà *a priori* le choix d'un découpage. Comme indiqué dans [Fenster, 2007], Dickson connaît bien les *Disquisitiones Arithmeticae*, qu'il cite à de nombreuses reprises, et dont il détaille beaucoup de passages, mais il ne se base pas sur l'ouvrage de Gauss pour construire sa table des matières. En effet, si l'on repère les sections dont les titres contiennent les mots "résidu" ou "congruence" ou la notation " $\pmod p$" dans la table des matières [5], elles sont dispersées dans les trois volumes. Dans les *Disquisitiones Arithmeticae*, les quatre premières sections sont entièrement consacrées aux congruences et résidus : les propriétés de ces objets y sont donc regroupées et constituent des théories à part entière. De même, aucune section du traité de Dickson n'est consacrée à la cyclotomie par exemple ; or, ce thème central de la section VII des *Disquisitiones Arithmeticae* utilise les congruences et de nombreux travaux sont publiés à ce sujet. D'autre part, le volume le plus important en nombre de pages est celui sur l'analyse diophantienne et il contient de nombreuses utilisations des congruences. Comme cela est remarqué dans [Fenster, 2007] : « However, in volume 2 (with more than 800 pages the largest of the three), Dickson's interests and prioritites clearly did not coincide with those of Gauss ; many scattered questions of Diophantine analysis find their place in this second volume »[Fenster, 2007, p.

5. Voir annexe, page 446.

469]. Nous avons donc dû dépouiller le traité de Dickson, sa table des matières ne permettant pas un repérage direct de notre sujet.

Il est remarquable et bien connu que la loi de réciprocité quadratique ne fait pas partie de cette histoire de la théorie des nombres[6]. Les travaux sur ce théorème fondamental devaient en fait être référencés dans un quatrième volume qui n'a finalement jamais vu le jour. Un chapitre de ce volume a néanmoins été rédigé sous la forme d'une thèse par un étudiant de Dickson à l'université de Chicago, Albert Everett Cooper, sous le nom *A Topical History of the Theory of Quadratic Residues*. Nous l'avons donc inclus dans notre analyse de l'ouvrage de Dickson.

Dans la liste obtenue à partir de ces deux ouvrages, on compte environ cent trente textes pour quarante-quatre auteurs. Si on se restreint aux textes repérés dans les sections dont les titres contiennent les mots "résidu" ou "congruence" ou la notation " $\pmod p$" dans la table des matières, tous les auteurs apparaissent, sauf cinq d'entre eux. Parmi ceux-ci, quatre ne publient qu'un seul texte consistant en une courte note de moins de cinq pages : il s'agit de Barlow, Clausen, Collins, et Grenoble. Le cinquième auteur est Serret, dont le *Cours d'algèbre supérieure* contient pourtant plusieurs leçons consacrées en grande partie aux congruences et aux résidus[7]. Néanmoins, la première édition de cet ouvrage n'est publiée qu'en 1849, et les références de Dickson concernent la deuxième édition et les suivantes.

2 - Le *Catalogue of Scientific Papers* de la Royal Society de Londres (1867-1872)

Afin de compléter la liste obtenue à partir de l'analyse de [Dickson, 1919-1923] et [Cooper, 1926], nous avons utilisé le *Catalogue of Scientific Papers*. Ce programme de recension est préparé par la *Royal Society* en 1857. L'édition[8] que nous avons compulsée est celle regroupant les travaux scientifiques de 1800 à 1863. Voici la description donnée dans le préface :

> The Catalogue is intended to serve as an Index of the Titles and Dates of Scientific Papers contained in the Transactions of Societies, Journals, and other Periodical Works which have been published from the beginning of the present century to the end of the year 1863[White et al., 1867-1872, Vol. 1, Préface, p. iii].

Pour la période 1800-1863, l'index par auteur se compose de six volumes. Un index par thème est également publié en 1908. Par rapport à [Dickson, 1919-1923], la table des matières pour la théorie des nombres de cet index est beaucoup plus proche de celle des *Disquisitiones Arithmeticae* : une des premières sections est consacrée aux congruences linéaires, puis viennent les résidus quadratiques et les formes quadratiques. Les congruences

6. Voir [Fenster, 1999].
7. Nous revenons sur ce cours dans notre deuxième chapitre.
8. Elle est ensuite complétée par une recension des travaux scientifiques jusqu'à la fin du siècle.

de degré supérieur avec les résidus d'ordre supérieur et les formes de degré supérieur sont abordées dans les sections suivantes. Enfin, une des dernières sections est intitulée *Application of trigonometric functions to arithmetic ; cyclotomy*, avec le sous-titre *Binomial equations*, ce qui correspond à la section VII des *Disquisitiones Arithmeticae*. Cette approche est donc totalement différente de celle adoptée par [Dickson, 1919-1923] et offre une prise directe sur les travaux sur les congruences. Cela nous a notamment permis de repérer des textes d'Eisenstein et Kummer non détectés à partir de notre analyse de la synthèse de Dickson.

3 - Un premier corpus

À partir de ces recensions, nous avons obtenu une première liste de textes, auxquels nous avons appliqué une double grille de lecture [9] : pour chaque texte, nous avons relevé à quels savants l'auteur se réfère. D'autre part, nous avons appliqué notre méthode de repérage par mots et symboles clés pour déterminer si l'écrit en question pouvait appartenir ou non à notre corpus final. Dans certains cas, il n'a pas été facile de trancher : nous avons néanmoins gardé tous les textes où au moins un raisonnement sur les résidus et les congruences (par exemple, des opérations sur les résidus) était mené. Par contre, comme indiqué au début de ce chapitre, nous avons exclu les travaux où est utilisé uniquement le fait de considérer un nombre de la forme $4n+1$ (ou une autre forme de ce type qu'on pourrait être tenté de simplifier par une congruence) si aucune propriété liée aux congruences n'est appliquée. Le corpus ainsi formé est certes hétérogène : dans certains textes, un seul raisonnement en lien avec les résidus apparaît parmi des dizaines de pages, tandis que d'autres écrits sont entièrement consacrés à ce thème. Cela fait néanmoins partie de l'objet de notre étude : repérer quelles sont les utilisations faites de ces objets, y compris celles qui sont élémentaires ou anecdotiques par rapport au reste de la recherche.

Parmi les articles repérés dans les synthèses de Dickson et Cooper à partir des mots et symboles clés définis précédemment, un seul, en définitive, ne contient aucun raisonnement sur les résidus et les congruences : il s'agit d'une question posée par Abel en 1828 dans le troisième tome du *Journal de Crelle* (p. 212) dans la partie *Aufgaben und Lehrsätze*. Dickson annonce qu'Abel demande s'il existe un nombre premier p et un entier a tels que $a^{p-1} \equiv 1 \pmod{p^2}$. Or, Abel n'utilise ni les congruences, ni les restes puisqu'il formule sa question en termes de divisibilité : « Kann $\alpha^{\mu-1} - 1$, wenn μ eine Primzahl ist und α eine ganze Zahl und kleiner als μ und größer als 1 ist, durch μ^2 theilbar sein ? ». Ce type de modification se retrouve assez régulièrement dans [Dickson, 1919-1923] pour

9. Il n'y a que trois publications auxquelles nous n'avons pas pu accéder, respectivement en italien, russe et allemand. Le premier est un mémoire de Libri, intitulé *Memoria sopra la teoria die numeri*, publié de manière indépendante en 1820 ; l'auteur aborde des thèmes de théorie des nombres dans des écrits ultéieurs. Le deuxième est un cours d'analyse algébrique et transcendante d'Ostrogradsky. Le troisième est une note sur les restes cubiques insérée en 1842 dans un brochure d'un lycée allemand.

les références antérieures à 1801 : par exemple, l'auteur attribue à plusieurs reprises des raisonnements sous la forme de résidus ou de congruences à Lagrange alors que ce dernier n'utilise presque exclusivement que des démonstrations en termes de divisibilité.

III Vers le corpus final

Afin de pallier les manques éventuels des synthèses utilisées, nous avons, dans un deuxième temps, réitéré ce travail de repérage sur les ouvrages généraux d'algèbre et de théorie des nombres, ainsi que sur les périodiques disponibles en France durant la période considérée [10]. Puis, nous avons appliqué notre double grille de lecture à chaque nouveau texte ainsi repéré.

Enfin, les articles repérés ont été vérifiés à partir de deux autres synthèses, le *Report on the Theory of Numbers* de Smith[Smith, 1859-1865] et le tome sur la théorie des nombres de l'*Encyclopédie des sciences mathématiques pures et appliquées* d'après l'édition allemande dirigée par Molk [Meyer et Molk, 1904 - 1916]. Nous avons également comparé les textes repérés avec la liste des publications de chacun des auteurs intégrés dans notre corpus à l'aide de l'index par auteurs du *Catalogue of Scientific papers.*Nous avons complété notre corpus en dépouillant plusieurs ouvrages historiques sur l'histoire de la théorie des nombres [11]. Cette dernière étape nous a permis d'intégrer au corpus des rapports généraux (comme [Peacock, 1834]) ou des commentaires publiés dans des périodiques non scientifiques (comme [Poinsot, 1808]) , qui ne sont pas référencés dans les synthèses contrôlées précédemment.

Remarquons tout de suite qu'avec notre méthode, nous obtenons un corpus dont les textes sont majoritairement issus de publications françaises et allemandes, et dont la plupart des auteurs sont également de ces deux nationalités. Il serait donc utile de dépouiller des périodiques d'autres pays afin d'y mesurer la place des congruences et résidus et de déterminer si notre construction de corpus renvoie une image représentative ou non.

Nous analysons dans les chapitres 2 à 4 le contenu général du corpus obtenu à partir des ouvrages et périodiques disponibles sur la scène française entre 1801 et 1850, en nous arrêtant plus particulièrement sur les publications françaises. Nous complétons éventuellement avec d'autres textes de notre corpus en le mentionnant explicitement.

10. Nous présentons les traités généraux et les périodiques étudiés dans les chapitres 2 et 3.
11. Nous avons utilisé [Goldstein et al., 2007], [Lemmermeyer, 2000] et [Edwards, 1977].

IV Dickson *a posteriori*

À partir du corpus final, nous pouvons commenter plus finement les conséquences du choix de la table des matières adoptées par Dickson. Nous avons inséré en annexe [12] la liste des textes de notre corpus final non référencés dans [Dickson, 1919-1923] et [Cooper, 1926]. On y trouve par exemple plusieurs textes d'Eisenstein, Kummer et Cauchy. Les travaux de Kummer sont presque exclusivement traités dans la section sur le dernier théorème de Fermat. Or, comme nous l'avons rappelé dans l'introduction, Kummer travaille d'abord sur la théorie des résidus d'ordre supérieur, bâtit sa théorie des nombres idéaux, puis en donne une application au dernier théorème de Fermat. Dans la recension, les articles de Kummer n'ayant aucun lien avec le dernier théorème de Fermat sont donc écartés définitivement par Dickson puisque les sujets qui y sont traités (résidus supérieurs, entiers complexes, ...) ne font partie d'aucune section de la table des matières. De même, Cauchy, en 1847, publie de nombreuses notes aux *Comptes Rendus* des séances de l'Académie des sciences en relation avec ses recherches sur le théorème de Fermat. La note intitulée *Mémoire sur de nouvelles formules relatives à la théorie des polynômes radicaux, et sur le dernier théorème de Fermat* est référencée dans l'ouvrage de Dickson, mais pas pour ses raisonnements sur les résidus et les congruences. Or, dans ce mémoire, Cauchy utilise les propriétés des racines primitives d'un nombre premier p (c'est-à-dire la racine de la congruence $x^{p-1} \equiv 1 \pmod{p}$) pour corroborer ses affirmations. Enfin, Eisenstein est également cité à plusieurs reprises, notamment pour ses résultats sur les sommes de carrés et la théorie des formes, mais jamais pour ses démonstrations des lois de réciprocité [13]. Or, sur les 19 textes d'Eisenstein de notre corpus, les titres de 10 textes contiennent une expression de la forme "loi de réciprocité" ou "théorème fondamental pour les résidus" ....

Ainsi, ces trois exemples montrent bien que, du point de vue de notre étude, l'analyse d'une synthèse telle que celle de Dickson n'est pas exhaustive puisque les résidus et les congruences sont parfois employés en tant qu'outils et ne sont donc pas mis en avant dans les résumés. Cela justifie les nombreuses sources utilisées ici pour la construction de notre corpus. D'autre part, cela met également en évidence l'importance des contextes : une étude des travaux d'Eisenstein sur la période considérée, d'après les commentaires contenus dans l'ouvrage de Dickson, amènerait à des conclusions très différentes d'une étude des articles d'Eisenstein publiés dans le *Journal de Crelle*, par exemple.

12. Voir page 448.

13. Il est seulement indiqué dans [Dickson, 1919-1923, Vol. 2, p. 771] qu'un savant utilise la loi de réciprocité d'Eisenstein.

CHAPITRE 2

Les résidus et les congruences dans les livres

Dans ce chapitre, nous commentons les passages faisant intervenir les résidus et les congruences dans des livres publiés en France entre 1801 et 1850. Nous analysons tout d'abord la place des résidus et des congruences dans les traités généraux d'algèbre et de théorie des nombres. Les traités explicitement destinés à l'enseignement [1] sont examinés dans la section suivante.

I Les monographies de recherche

Comme nous l'avons indiqué dans l'introduction, les traités de Gauss et de Legendre sont les sources usuelles des mathématiciens pour leurs recherches arithmétiques dans la première moitié du XIX^{e} siècle. Nous y reviendrons donc en détail dans la deuxième partie. Ces monographies mises à part, les congruences ne sont pas traitées dans les autres ouvrages. On retrouve des allusions aux résidus et aux travaux de Legendre et Gauss dans deux traités, dont les statuts sont très différents : l'un est une référence de base en algèbre et fait partie des listes d'ouvrages recommandés pour l'enseignement, tandis que l'autre est marginal et témoigne de la résistance de certains savants à l'introduction des notions de Gauss dans les années 1850.

1 - Le *Traité de la résolution des équations numériques de tous les degrés* de Lagrange (1808)

À l'occasion de la deuxième édition de son traité sur la résolution des équations numériques [2], Lagrange ajoute quatorze notes sur la théorie algébrique des équations [3]. La quatorzième note reprend la méthode de résolution algébrique des équations binômes donnée par Gauss en 1801 ; Lagrange en propose une simplification, qui évite la résolution d'équations intermédiaires, mais il conserve le cœur de la méthode de Gauss : l'utilisation des racines primitives de nombres premiers.

Lagrange commence par un rappel du théorème de Fermat, de la définition des racines primitives, ainsi que de leur propriété fondamentale utilisée par Gauss dans la section VII : une racine primitive a pour le nombre premier p est telle que les termes 1, a, a^2, a^3,

1. Nous désignons ainsi les ouvrages qui contiennent, dans leur introduction ou leur titre, une mention explicite à un public donné d'élèves ou à un établissement d'enseignement.

2. La première édition, intitulée *De la résolution des équations numériques de tous les degrés*, est publiée en 1798 sans additions ; il ne contient pas de raisonnements sur les résidus et les congruences.

3. Lagrange a publié un important travail sur la théorie générale des équations en 1770. Voir [Lagrange, 1772-1773].

$\ldots$, a^{p-2} donnent tous les restes compris entre 1 et $p-1$, dans un ordre différent de celui déduit de l'ordre sur les entiers naturels. Ainsi, les racines différentes de l'unité r, r^2, r^3, $\ldots$, r^{p-1} de l'équation $x^p - 1 = 0$ peuvent être remplacées par les termes

$$r, r^a, r^{a^2}, r^{a^3}, \ldots, r^{a^{p-2}}.$$

Il justifie l'intérêt de ce choix en considérant un nombre premier μ :

> L'avantage de cette nouvelle forme des racines consiste en ce que si dans la série des racines
>
> $$r, r^a, r^{a^2}, r^{a^3}, r^{a^4}, etc., r^{a^{\mu-2}},$$
>
> on met r^a à la place de r, elle devient
>
> $$r^a, r^{a^2}, r^{a^3}, r^{a^4}, r^{a^5}, etc., r\ ;$$
>
> et si l'on y met r^{a^2} à la place de r, elle devient
>
> $$r^{a^2}, r^{a^3}, r^{a^4}, r^{a^5}, r^{a^6}, etc., r, r^a,$$
>
> et ainsi de suite[Lagrange, 1808, p. 332].

Lagrange ne mentionne qu'une seule fois la théorie des nombres dans cette note XIV, mais il indique explicitement l'utilité des racines primitives dans cette méthode de résolution. La suite de la note est consacrée à l'exposé de la méthode de résolution des équations binômes - qui se base sur des outils similaires à ceux de Gauss - et ne contient plus de résultats de théorie des nombres.

2 - . . . et un texte plus tardif et marginal : le *Traité de l'analyse indéterminée du second degré à deux inconnues* de Desmarest (1852)

Un texte sur les racines primitives a été présenté à l'Académie des Sciences en 1845 par Eugène Desmarest, pharmacien de formation. Poinsot donne un rapport favorable de ce travail lors de la séance du 9 février 1846, et propose d'insérer la table des racines primitives donnée par Desmarest dans les *Mémoires des savants étrangers*. Ce texte est repris dans la quatrième partie du traité de Desmarest publié en 1852 ; le titre de l'ouvrage est effectivement suivi de la mention « Mémoire présenté à l'Académie des Sciences et inséré, après rapport, au recueil des savants étrangers » et l'auteur lui-même précise en note au début de la quatrième partie que celle-ci a été présentée indépendamment du traité à l'Académie et qu'elle doit être publiée dans les *Mémoires* des savants étrangers. Malgré la marginalité de son auteur, nous avons pris en compte ce traité à cause de cette

reconnaissance par l'Académie.

Les trois premières parties du *Traité de l'analyse indéterminée du second degré* de Desmarest contiennent des méthodes permettant de résoudre des équations indéterminées du second degré de différentes sortes, comme par exemple $aX^2 + bX + c = kY$ ou $ax^2 + 2bxy + cy^2 = M$. Les résultats sur les résidus, et en particulier sur les racines primitives, sont exposés dans une soixantaine de pages dans la quatrième et dernière partie. Cette section comprend les démonstrations des théorèmes de Fermat et de Wilson, des propriétés générales sur les racines primitives et sur les relations existant entre celles-ci, et des réflexions sur la détermination de ces racines primitives. À aucun moment Desmarest n'utilise les notations et le vocabulaire des *Disquisitiones Arithmeticae* et il s'en explique dès la préface et l'introduction :

> dans les sciences exactes, et surtout dans une théorie sur les nombres, tout néologisme non puissamment motivé, toute innovation, si elle n'est pas impérieusement exigée, doivent être bannis ; or, les notations, les dénominations, introduites par Gauss, nous paraissant avoir en général, à un haut degré ce caractère négatif. Ce défaut explique peut-être, et le petit nombre de lecteurs conquis chez nous par le savant Allemand, et par suite l'idée fausse qu'on s'est fait du progrès de la partie que nous traitons ici[...][Desmarest, 1852, Préface, p. vi]

Desmarest explique ensuite que le lecteur de son traité peut n'avoir que des connaissances en arithmétique, puisqu'il n'utilise pas dans son travail d'outils étrangers à cette discipline :

> [...] suit-il qu'un traité sur un point des sciences exactes doive prendre la forme encyclopédique, qu'un traité sur les nombres, doive chercher ses preuves dans une analyse transcendante ou même simplement dans l'algèbre ? Cet écueil, créé en général par une vanité puérile, nous avons voulu, à l'exemple des Gauss, des Poinsot, etc., etc., soigneusement l'éviter, et nous pouvons affirmer que tout lecteur, familiarisé avec les principes ordinaires de l'arithmétique, pourra lire, comprendre notre travail, et de cette lecture retirer, nous l'espérons, un profit réel[Desmarest, 1852, Préface, p. viii].

Dans son introduction, Desmarest revient sur les ouvrages de Legendre et Gauss :

> Ne parlons des ouvrages que les plus étendus et qui offrent un ensemble de principes sur le sujet qui nous occupe : *Essai sur la théorie des nombres* par Legendre ; *Disquisitiones Arithmeticae* de Gauss. Malgré notre profond respect pour ces maîtres de la science, nous pensons que le premier est un simple recueil, et son titre l'indique, de principes déjà connus ou dus à l'auteur, sur la théorie des nombres, c'est-à-dire sur toute l'analyse indéterminée. Quant au second ouvrage, peut-être est-il permis de reprocher au savant allemand l'emploi de notations particulières, de dénominations nouvelles qui ne paraissent pas indispensables. Remarquons, d'ailleurs, que le travail de Gauss, justement intitulé *Recherches*, est purement théorique, ne donne

aucun moyen pratique de résoudre en nombres entiers les équations du second degré à deux inconnues[Desmarest, 1852, Introduction, p. 1-2].

Desmarest émet donc des réserves sur les ouvrages de théorie des nombres en général, et sur celui de Gauss en particulier : les résultats obtenus lui semblent dispersés et trop théoriques, ne permettant pas souvent des applications pratiques. De plus, l'étude de l'ouvrage de Gauss, et de certains travaux ultérieurs, nécessitent d'intégrer de nouvelles notions, comme les congruences par exemple. Malgré ces réticences, Desmarest cite un nombre important de savants en liaison avec la théorie des nombres : Euler, Johann Heinrich Lambert, Lagrange, Legendre, Gauss, Poinsot et Jacobi. Insistons finalement sur l'exigence de Desmarest de construire un traité fondé uniquement sur les « principes ordinaires de l'arithmétique » : on verra au cours de notre étude à quel point cette volonté d'isoler l'arithmétique des autres domaines mathématiques confirme le caractère marginal de ce livre par rapport aux pratiques des mathématiciens français de notre corpus dans la première moitié du XIX^{e} siècle.

II La place des résidus et les congruences dans l'enseignement scientifique français

1 - Présentation

Les manuels donnent des indications sur les savoirs et savoir faire attendus de groupes d'élèves dans le cadre de leur formation [4]. L'objectif est donc de déterminer ici quelle est la place des résidus et des congruences, dans l'enseignement des mathématiques en France pour la première moitié du XIX^{e} siècle.

Nous nous sommes d'abord appuyés sur les textes officiels liés à l'enseignement, afin de déterminer les ouvrages conseillés officiellement pour l'enseignement de l'algèbre et de l'arithmétique [5]. Le premier programme pour l'admission à l'École Polytechnique est rédigé par Laplace, Lagrange et Monge et paraît le 28 février 1800 ; il reste en application jusqu'en 1854, sans modifications importantes [6]. Dans la partie réservée à l'algèbre et l'arithmétique, il comprend l'étude des quatre opérations élémentaires, de la notion de plus grand commun diviseur, de l'étude des proportions, des progressions et des logarithmes. Le 10 décembre 1802 paraît l'arrêté concernant l'organisation de l'enseignement dans les lycées, qui est donné sous forme de deux séries de classes indépendantes : une pour les mathématiques et une pour le latin. Le 10 avril 1803 est publié le résultat des travaux de la

4. Sur le rôle joué par l'enseignement dans l'histoire des mathématiques, voir notamment [Belhoste, 1998].

5. Nous nous basons ici sur les données contenues dans [Dhombres, 1985], [Belhoste, 1989] et [Belhoste, 1995].

6. Les exigences des examinateurs deviennent néanmoins de plus en plus importantes avec le nombre croissant de candidats.

commission pour les mathématiques composée de Laplace, Monge et Lacroix. Elle fournit une liste d'ouvrages devant servir à l'enseignement des sciences. Pour les mathématiques, ce sont les manuels de Lacroix qui sont choisis. La somme des connaissances contenues dans ces ouvrages dépasse largement le bagage nécessaire pour le passage du concours d'entrée à l'Ecole Polytechnique. L'étude des *Compléments des éléments d'algèbre* de Lacroix est prévue pour les classes de mathématiques transcendantes [7]. Le 19 septembre 1809 paraît le nouveau plan d'étude des lycées. Il restructure l' enseignement sur la base de classes dont le contenu est à la fois scientifique et littéraire. Les classes de mathématiques spéciales, surtout vouées à la préparation au concours d'entrée des écoles spéciales, remplacent les classes de mathématiques transcendantes. Une nouvelle liste d'ouvrages est alors donnée qui comprend les ouvrages de Bézout, Bossut et Lacroix [8]. On retrouve également les *Compléments des éléments d'algèbre* de Lacroix et le traité des équations numériques de Lagrange [9]. En 1814, les *Éléments d'algèbre* d'Euler sont ajoutés. À partir de 1821, les programmes sont de plus en plus détaillés, et ne reposent plus sur une liste de livres imposée, même si le professeur doit s'appuyer sur des manuels recommandés. On n'y trouve aucune référence aux résidus et aux congruences.

À partir des années 1830, à côté des ouvrages de Lacroix, d'autres manuels d'algèbre sont destinés aux candidats à l'entrée à l'École Polytechnique : ce sont les traités de Reynaud, Lefébure de Fourcy, Bourdon [10]. Ces manuels contiennent parfois des notions hors-programme : par exemple, dans [Lefebure de Fourcy, 1833], Lefébure de Fourcy note d'une étoile les notions qui ne sont pas exigées au concours d'entrée à l'École Polytechnique, on y trouve par exemple le théorème de Sturm, dont la démonstration est publiée en 1829 dans le *Bulletin de Férussac* [11].

Dans cette liste d'ouvrages, nous avons cherché les mentions aux résidus et congruences à partir des mots et symboles-clés cités dans le chapitre 1. La majorité des manuels d'algèbre et tous les manuels d'arithmétique abordent des thèmes élémentaires et on n'y retrouve aucune trace des résidus et des congruences. Nous donnons ci-dessous un panorama des extraits contenant des mentions aux résidus ou aux congruences dans les ouvrages restants. Nous commentons également les deux premières éditions du *Cours d'algèbre supérieure* de Joseph-Alfred Serret, publiées en 1849 et 1854, afin de voir quels

7. La création des facultés des sciences date de 1808 et les classes de mathématiques transcendantes visent alors très probablement à pallier cette absence d'enseignement supérieur en dehors des écoles spéciales.

8. Pour une étude détaillée du contenu des manuels de Bézout et Lacroix et de leur influence, voir notamment [Lamandé, 1987], [Lamandé, 2004], [Alfonsi, 2005], [Ehrhardt, 2007].

9. Il existe plusieurs éditions de ce traité ; à partir de la deuxième édition publiée en 1808, l'ouvrage de Lagrange comprend une note mentionnant les résidus et les congruences ; nous l'avons étudiée dans la section précédente puisque ce traité n'est pas explicitement assigné à l'enseignement.

10. Voir [Ehrhardt, 2007, p. 136]. Cette liste est issue du *Manuel des aspirants à l'École Polytechnique*, de Georges Ritt (1839).

11. Le théorème de Sturm est également publié en 1832 dans la première édition du *Traité élémentaire d'algèbre* de Choquet et Mayer. À ce sujet voir en particulier [Ehrhardt, 2007, p. 173-174] et [Sinaceur, 1991, p. 35-36].

résultats autour des résidus et des congruences sont mis en avant à la fin de la période étudiée ici.

2 - Le *Complément des éléments d'algèbre* de Lacroix (1804)

Dès la troisième édition de l'ouvrage de Lacroix en 1804, qui traite principalement de la résolution algébrique des équations, on retrouve un résumé de la section VII de Gauss. Il est inclus dans la dernière partie, dont le titre est *Des propriétés des nombres*. Lacroix commence par y dresser un rapide historique des quelques résultats importants de théorie des nombres démontrés au XVIII^{e} siècle par Euler et Lagrange - comme par exemple le théorème des quatre carrés et le théorème de Wilson - puis poursuit :

> Il serait impossible, sans sortir beaucoup des limites où je dois renfermer cet ouvrage, de développer ici les démonstrations des théorèmes que je viens d'énoncer ; mais pour donner une idée de ces recherches, je vais exposer, d'après M. Gauss, *la théorie des restes* que laissent les puissances d'un nombre, lorsqu'on les divise par le même nombre premier, et qui conduit à prouver la proposition indiquée à la page 92 [Lacroix, 1804, p. 296] [12].

Il donne ensuite quelques résultats sur les résidus des puissances : il liste en premier lieu les restes des puissances de 3 modulo 7, et remarque que les restes obtenus décrivent tous les nombres inférieurs à 7. Puis il énonce ensuite que, pour tout nombre a et tout nombre premier p, il existe un nombre t inférieur à p tel que a^t laisse l'unité pour reste après division par p, et que ce nombre t est un diviseur de $p-1$; il en déduit le petit théorème de Fermat. L'article 156 est la démonstration de l'existence d'une racine primitive pour tout nombre a et diviseur premier p. Lacroix insiste sur le fait que les diverses puissances d'une racine primitive d'un nombre premier p donnent pour restes modulo p tous les nombres compris entre 1 et $p-1$. Ici, il n'utilise ni les notations de Gauss, ni celles de Legendre et ne raisonne qu'en termes de division euclidienne.

Il résume ensuite la méthode de Gauss de résolution algébrique de l'équation $x^n = 1$, où n est un nombre premier. Dans cette version abrégée, même si elle est intégrée dans la partie dédiée à la théorie des nombres de son ouvrage, Lacroix n'insiste pas sur la nécessité d'utiliser des racines primitives, ni sur l'utilité de la théorie des nombres dans la démonstration de ce résultat d'algèbre. Il développe, pour finir, le cas particulier de $n = 17$. Il indique en note que le lien entre la résolution algébrique de l'équation $x^p = 1$ et la division du cercle en p parties égales est présentée dans son *Traité élémentaire de*

12. La propriété énoncée page 92 est le principe de la méthode de résolution de Gauss :

> M. Gauss, dans un ouvrage très-remarquable, intitulé : *Disquisitiones Arithmeticae*, a fait voir que *toute équation à deux termes, dont l'exposant est un nombre premier, peut être décomposée rationnellement en d'autres équations dont les degrés sont marqués par les facteurs premiers du nombre qui précède d'une unité ce nombre premier*[Lacroix, 1804, p. 92].

Calcul différentiel et intégral. Il conclut sa section sur la théorie des nombres, et donc son traité, en renvoyant le lecteur qui voudrait approfondir ce sujet aux textes de Gauss et Legendre.

Dès la quatrième édition de ses *Compléments aux éléments d'algèbre*, publiée en 1817, Lacroix reprend la version simplifiée par Lagrange pour exposer la résolution algébrique des équations binômes, sans la détailler mais en l'illustrant à l'aide de la résolution de l'équation $x^5 - 1 = 0$.

3 - Les ouvrages destinés à la préparation au concours d'admission à l'École Polytechnique

Parmi cet ensemble d'ouvrages, seuls quelques-uns abordent la théorie des résidus et des congruences. Certains renvoient aux traités de Gauss et Legendre. Ainsi, dans la sixième édition des *Éléments d'arithmétique*, Bourdon observe :

> Nous ne pousserons pas plus loin l'examen des propriétés des nombres ; mais nous recommanderons aux jeunes gens qui, déjà familiarisés avec l'analyse algébrique, voudraient étendre leurs connaissances sur cette partie, la lecture de deux ouvrages intitulés : *Théorie des nombre* par *Legendre*, et *Disquisitiones Arithmeticae*, de *Gauss*, ouvrage traduit avec beaucoup de succès par M. *Poulet-Delisle*[Bourdon, 1828, p. 232].

Il en est de même pour [Choquet et Mayer, 1836] et [Francoeur, 1838]. Dans le manuel de Francoeur, qui a enseigné à la Faculté des Sciences de Paris, le cinquième chapitre est consacré aux équations déterminées et indéterminées des premier et second degrés. Il considère notamment les équations indéterminées de la forme $my = x^2 \pm a$, ce qui correspond à la congruence binôme $x^2 \equiv a \pmod{m}$, et raisonne à partir des restes des quotients $\frac{x^2}{m}$; il évite ainsi, consciemment ou non, l'utilisation des notations introduites par Gauss.

Dans ses *Leçons d'algèbre*, Lefebure de Fourcy consacre le chapitre VII à l'analyse indéterminée du premier degré et ne donne pas de résultats sur les résidus et les congruences. Par contre, le chapitre XII, qui est intitulé *Propositions sur les nombres. Grandeurs incommensurables et approximations des racines. Progressions. Fractions continues.* (17 pages), contient une section marquée d'une étoile - et donc considérée comme "hors-programme" pour la préparation du concours d'entrée à l'École Polytechnique - nommée *Continuation. Théorèmes sur les résidus*. L'auteur donne notamment le théorème fondamental de l'arithmétique sur la décomposition unique des nombres entiers en facteurs premiers, puis des propriétés sur les résidus, les résidus des puissances, ainsi que le théorème d'Euler - Fermat. Il en déduit le théorème de Fermat et définit ce que sont les *racines primitives*, en donnant pour référence Euler. Il renvoie le lecteur désireux d'approfondir le sujet à l'étude de l'ouvrage de Legendre.

4 - Le *Cours d'Algèbre Supérieure* de Serret (1849 - 1854)

Ce cours contient des recherches assez récentes et approfondies, en particulier sur la théorie générale des équations. Sept éditions de ce *Cours* ont été éditées entre 1849 et 1928, et il constitue une référence au moins jusque dans les années 1870, comme en témoignent les nombreuses mentions de ce livre dans les articles [13]. Nous avons étudié les deux premières éditions, publiées en 1849 et 1854. La théorie des nombres est principalement développée dans les leçons 23 à 25. Dans les deux éditions, les leçons 23 et 24 sont pratiquement identiques [14].

La vingt-troisième leçon donne des résultats fondamentaux sur les congruences. L'auteur commence par introduire les nombres *congrus*, ou *équivalents*, ainsi que la notation $\equiv$ qu'il attribue à Gauss. Il observe d'ailleurs :

> L'avantage de la notation de M. Gauss, pour représenter les congruences, consiste surtout en ce qu'elle rappelle la grande analogie qui existe entre les congruences et les équations, sans qu'il y ait pourtant de confusion à craindre. Nous allons faire voir que la plupart des transformations que l'on peut faire subir aux égalités peuvent être appliquées aux congruences[Serret, 1849, p. 298].

Comme annoncé, il étudie les propriétés opératoires des congruences, démontre les théorèmes de Fermat et Wilson [15], puis énonce des propriétés des congruences générales. Il donne notamment le théorème sur le nombre maximum des racines pour une congruence donnée, ainsi qu'une méthode pour calculer ce nombre de racines.

La vingt-quatrième leçon a essentiellement pour objet les racines primitives des nombres premiers. Serret part des propriétés sur les congruences binômes, et poursuit avec des théorèmes sur l'existence des racines primitives, leur nombre et une méthode pour les déterminer. Avant de conclure sur des propriétés des racines des équations binômes, il communique une table des racines primitives des nombres premiers inférieurs à 100.

Les sujets abordés dans la vingt-cinquième leçon sont par contre très différents dans les deux éditions. Dans la première édition de 1849, Serret expose des résultats classiques de théorie des nombres, déjà étudiés au XVIII^{e} siècle. Il se réfère à Euler et Hermite pour présenter des théorèmes sur le produit et le quotient de deux nombres d'une forme donnée [16], puis il s'appuie sur des congruences pour obtenir trois théorèmes : tout nombre premier de la forme $4n+1$ peut être mis sous la forme d'une somme de deux carrés, et ce de manière unique ; tout nombre premier de la forme $8n+1$ ou $8n+3$ peut s'exprimer sous la forme x^2+2y^2 ; tout nombre entier peut se mettre sous la forme d'au plus quatre carrés.

13. Se reporter par exemple à [Ehrhardt, 2007] pour des commentaires sur ce thème.
14. Dans la deuxième édition, on trouve de plus un exemple de calcul du nombre de racines d'une congruence et une remarque suivant la démonstration du théorème de Wilson.
15. Il renvoie d'ailleurs à Poinsot pour une démonstration des versions généralisées de ces théorèmes.
16. Par exemple : le produit de deux sommes de deux carrés est une somme de deux carrés.

Dans la deuxième édition de 1854, Serret développe d'autres résultats, démontrés pour certains au cours du XIX^{e} siècle. Il démontre d'abord des propriétés générales sur les congruences irréductibles de degré premier, en utilisant notamment l'algorithme d'Euclide sur ce type de congruences. Il démontre que toute congruence de degré premier est décomposable en un produit de facteurs premiers, et ce, de manière unique. Partant de là, il expose une deuxième section intitulée *Des nouvelles quantités imaginaires qui naissent de la théorie des nombres* ; celle-ci contient un résumé de la théorie des imaginaires de Galois [17], publiée pour la première fois dans le *Bulletin de Férussac* en 1830. Serret étend alors le théorème sur le nombre maximal de racines d'une congruence, démontré dans la leçon 23, aux racines imaginaires des congruences, puis il continue à présenter les résultats donnés par Galois dans [Galois, 1830], en complétant certaines démonstrations [18].

La théorie des nombres intervient également dans la vingt-huitième leçon des deux premières éditions du *Cours d'algèbre supérieure* de Serret [19]. Cette partie traite de la résolution algébrique des équations binômes $x^n = 1$, où n est un nombre premier. Serret développe notamment le cas où $n = 17$ du point de vue de la détermination des expressions des racines et de celui de leur construction géométrique. Serret se réfère à Gauss pour la méthode de résolution algébrique et l'utilisation d'une racine primitive du nombre n, et donne la démonstration d'Abel.

Contrairement à la première édition de l'ouvrage de Serret, la deuxième s'achève avec quinze notes. Les neuvième et dixième notes contiennent des propriétés de l'équation $\frac{x^p-1}{x-1} = 0$ et de la fonction $X = \frac{x^p-1}{x-1}$. Serret y rappelle l'importance des racines primitives et de l'irréductibilité de l'équation $\frac{x^p-1}{x-1} = 0$ dans la résolution algébrique des équations binômes. L'objet de la note IX est de démontrer cette irréductibilité. Dans la note X, Serret démontre l'égalité $X = Y^2 \pm nZ^2$, le signe dépendant de la forme du nombre n. La onzième note contient la démonstration de la loi de réciprocité quadratique donnée par Legendre et Jacobi. Les deux dernières notes ont également pour objet des résultats de la théorie analytique des nombres [20] mais ne font pas intervenir les résidus et les congruences.

Ainsi, même si l'ouvrage de Serret est un cours d'algèbre, il contient une quantité non négligeable de théorie des nombres, avec en particulier des résultats importants en lien avec les résidus et les congruences. L'édition de 1854 développe des théorèmes qui sont d'un niveau bien plus avancé que ce que l'on retrouve dans les désormais classiques *Théorie des nombres* de Legendre et *Disquisitiones Arithmeticae* de Gauss.

17. Nous commentons l'article de Galois correspondant dans le troisième chapitre, à partir de la page 59.

18. La relecture d'une partie des travaux de Galois par Serret dans son ouvrage est étudiée dans [Ehrhardt, 2007].

19. Même si les exposés diffèrent sur certains points, le contenu est sensiblement le même.

20. Elles traitent notamment de la valeur approchée de $x!$ pour un grand nombre x et sur la quantité de nombres premiers compris entre deux nombres donnés.

5 - Des cours non rédigés

Concluons cette section sur l'enseignement en remarquant que l'examen des manuels et des textes officiels à disposition ne permet pas de donner une vision totale de l'enseignement des mathématiques en France. En effet, au moins une école n'est pas soumise à des programmes : les professeurs titulaires du Collège de France élaborent eux-mêmes le contenu de leurs cours, tant que celui-ci entre dans le cadre de leur chaire. Le Collège de France est donc un lieu où les leçons peuvent être très proches des recherches des professeurs [21] et où les étudiants n'obtiennent pas de diplôme. À partir de 1837, Liouville donne des cours au Collège de France, tout d'abord en remplacement de Biot. Il est très difficile de connaître avec exactitude le contenu des cours professés par Liouville au Collège de France. Néanmoins, les auteurs de [Belhoste et Lützen, 1984] ont retrouvé les notes d'un des auditeurs de Liouville, A. Barré de Saint-Venant, pour les deux cours de l'année 1839-1840. Un de ceux-ci traite des intégrales définies. Mais, prétextant que les intégrales définies peuvent être un outil utile à la théorie des nombres, Liouville enseigne cette discipline à ses auditeurs de la dixième à la seizième leçon, en s'appuyant particulièrement sur les travaux de Dirichlet. Il commence par les bases de la théorie des congruences, avec notamment les théorèmes de Fermat et de Wilson, puis expose la théorie des résidus quadratiques en incluant une démonstration de la loi de réciprocité quadratique. Il démontre ensuite les formules de Gauss [22] liant les fonctions circulaires au symbole $\left(\frac{n}{p}\right)$, pour en déduire des formules donnant le nombre de résidus et de non résidus quadratiques d'un nombre premier p, inférieurs à p. Il achève son cours en démontrant un cas particulier du théorème de la progression arithmétique : il existe une infinité de nombres premiers dans une progression arithmétique dont la raison est un nombre premier de la forme $4n+3$ [23]. On voit donc à l'aide de cet exemple que la théorie des nombres est enseignée sans qu'il en découle un manuel dans certains établissements en France.

6 - Conclusion

L'analyse précédente montre que la théorie des résidus et des congruences n'a pas une place autonome et bien établie dans l'enseignement scientifique en France pendant la première moitié du XIX$^{\text{e}}$ siècle. Seule la résolution algébrique des équations binômes donnée par Gauss en 1801 est intégrée dans les *Compléments d'algèbre* de Lacroix et dans le traité des équations numériques de Lagrange. Il faut ensuite attendre le *Cours d'algèbre supérieure* de Serret pour que plusieurs leçons soient consacrées à la théorie des résidus et des congruences, et aucun ouvrage français consacré en majorité aux résidus et congruences (comme les *Disquisitiones Arithmeticae* par exemple) n'est publié pour

21. Nous reprenons l'analyse développée dans [Belhoste et Lützen, 1984].
22. Voir notamment la deuxième partie de notre travail, page 206.
23. La démonstration de ce cas nécessite l'utilisation d'outils analytiques tandis que celle du cas où la raison est un nombre premier de la forme $4n+1$ s'appuie sur des arguments arithmétiques élémentaires.

la période considérée[24]. On peut donc en déduire que les sources d'apprentissage sur ce thème disponibles en français restent les mêmes pendant toute la période considérée : les ouvrages de Gauss et Legendre. À ces deux traités s'ajoutent les articles de recherche insérés dans les publications périodiques : nous étudions ces publications dans le chapitre suivant.

24. Cette situation se prolonge : voir [Décaillot, 1998] pour des commentaires sur les tentatives infructueuses d'obtenir une chaire de théorie des nombres au Collège de France à la fin du XIX^{e} siècle. En revanche, on retrouve ailleurs des traités dans lesquels les congruences ont une place importante : nous pensons par exemple aux ouvrages de Ferdinand Minding et Pafnuti L. Cěbiseˇv publiés respectivement en 1832 et 1849 : voir [Goldstein et Schappacher, 2007a, p. 25-26 et p. 56-57].

CHAPITRE 3

Les résidus et les congruences dans les périodiques

I Présentation des périodiques utilisés pour notre étude

Au XIX^{e} siècle, l'activité mathématique se traduit de plus en plus souvent sous la forme de la publication d'articles de longueurs variées dans des journaux. L'étude des journaux permet ainsi d'obtenir des informations sur l'activité d'une communauté scientifique à un instant donné. Comme le remarque Norbert Verdier [1] :

> Il [un journal donné] constitue en ce sens un corpus intéressant pour faire de l'histoire des mathématiques. Par ses contenus, ses réseaux d'auteurs et sa périodicité, il est un marqueur du temps qui passe sur une période donnée et permet de mesurer des évolutions, de saisir des moments de rupture et de fond, c'est-à-dire de saisir des épisodes de la vie mathématique [Verdier, 2009, p. 6].

Nous repérons dans ce chapitre résidus et congruences en dépouillant systématiquement plusieurs journaux. L'analyse de leur place dans les différents articles publiés nous permet de savoir quels sont les moyens de communication possibles et privilégiés par les auteurs concernés, en fonction de leur position et des thèmes abordés [2]. Nous avons inclus les diverses séries d'ouvrages publiés par l'Académie des Sciences, en nous basant sur la définition du journal donnée dans [Verdier, 2009, p. 6] : « Un journal est un écrit périodique ou, comme le prévoit le législateur, un écrit paraissant "par livraisons et irrégulièrement" d'après l'article premier de la loi du 9 juin 1817 ».

Commençons par une présentation rapide de chaque périodique analysé, en distinguant deux périodes [3] : de 1801 à 1835 puis de 1835 à 1850. Ce découpage n'est pas arbitraire : les journaux scientifiques dont la publication commence avant les années 1830 disparaissent presque tous avant 1835, année à partir de laquelle sont créées de nouvelles publications périodiques, institutionnelles ou non.

1. Pour un ouvrage général sur les journaux mathématiques européens, on peut se reporter à [Ausejo et Hormigón, 1993]. Un programme d'étude des journaux scientifiques a été lancé par Jean Dhombres, voir [Dhombres, 1994] et pour des cas concrets, les études publiées dans *Sciences et Techniques en perspective* et *Rivista di Storia della Scienza* entre 1993 et 1996.

2. Nous renvoyons à [Peiffer, 1998] notamment pour une étude sur une autre forme de communication entre savants : les correspondances.

3. Conjointement aux périodiques scientifiques, d'autres journaux apportent des informations sur les activités scientifiques de la première moitié du XIX^{e} siècle. Ainsi, avant 1835, on retrouve des rapports sur certains événements de l'Académie dans des journaux culturels ou politiques, dans la *Décade philosophique* (publiée de 1794 à 1807) ou dans *Le Globe* à partir de 1825 par exemple.Voir [Crosland, 1992, p. 281 et p. 285] notamment. Dès 1800, des textes écrits par des scientifiques, et non par des journalistes, sont aussi publiés dans le journal gouvernemental, le *Moniteur*. Cela permet de diffuser des textes scientifiques rapidement, parfois avant leur parution dans les *Mémoires* de l'Académie. Nous avons focalisé notre étude sur les périodiques scientifiques et n'avons donc pas intégré ces autres journaux dans notre analyse.

1 - 1801-1835 : les premiers journaux mathématiques

Au début du XIX^{e} siècle, les ouvrages publiés par l'Académie des Sciences de Paris se divisent en deux collections de *Mémoires* : ceux réservés aux académiciens et ceux dans lesquels sont insérés les mémoires proposés à l'Académie par des savants qui n'en sont pas membres, lorsqu'ils ont reçu un rapport favorable par une commission d'académiciens. Ces derniers mémoires sont nommés le plus souvent *Mémoires des Savants étrangers* par les auteurs, et c'est donc ainsi que nous les désignerons ici [4]. Les *Mémoires* réservés aux travaux des Académiciens paraissent généralement tous les ans [5], mais il y a un décalage entre la présentation d'un travail à l'Académie et sa publication dans les *Mémoires* de plusieurs années, ce délai étant encore plus important pour les *Mémoires des savants étrangers*.

Un autre périodique institutionnel paraît à la fin du XVIII^{e} siècle : après la création de l'École Polytechnique en 1794, le *Journal de l'École Polytechnique* [6] est lancé en 1795 et est d'abord destiné à donner des informations sur les enseignements et les activités des élèves. On y retrouve en fait rapidement deux types d'articles : des textes en liaison avec les cours donnés à l'*École* et des travaux scientifiques. Loïc Lamy remarque d'ailleurs l'évolution de ce périodique dès le début du XIX^{e} siècle : « le *Journal* est devenu progressivement, tout au moins dans sa forme, une sorte de recueil académique comme le désiraient Poisson et Hachette dans leur lettre du 5 septembre 1808, c'est-à-dire que les articles publiés étaient plus proches de la science proprement dite que de l'enseignement »[Lamy, 1996, p. 25]. Il ajoute que des mémoires lus à l'Académie sont publiés dans le *Journal* dès 1806. Le *Journal de l'École Polytechnique* peut donc être considéré comme une source institutionnelle supplémentaire, contenant notamment des travaux présentés à l'Académie, mais non publiés dans les *Mémoires*.

Par ailleurs, pour la période étudiée, deux périodiques généralistes publiés en France contiennent une partie mathématique non négligeable. Le premier est le *Bulletin de la société philomathique* [7]. Cette société, fondée par six savants amateurs en 1788, prend rapidement de l'importance en accueillant des transfuges de l'Académie royale des sciences, après sa suppression en 1793. Son *Bulletin* [8] est publié de 1792 à 1826. Ce périodique

4. À partir de 1803, la collection réservée aux non membres est officiellement intitulée *Mémoires présentés à l'Institut des Sciences, Lettres et Arts par divers savants, et lus à l'Assemblée : Sciences mathématiques et physiques*, mais reste connue par le titre antérieur, plus court *Mémoires des Savants étrangers*. Voir [Crosland, 1992, p. 281-282].

5. Les années 1813-1815 constituent une exception, expliquée notamment par la chute napoléonienne et les troubles politiques consécutifs. Voir [Crosland, 1992, p. 282].

6. Voir notamment [Lamy, 1996] pour des indications sur les conditions de la naissance de ce périodique et pour une étude du contenu de ce journal de 1795 à 1831.

7. Les sciences physiques et mathématiques sont néanmoins minoritaires par rapport aux sciences naturelles au sein de cette société.

8. Nous renvoyons à [Taton, 1990] pour de plus amples informations sur la Société philomathique et son *Bulletin*.

ne contient toutefois pas d'articles dans lesquels les auteurs utilisent les résidus et les congruences.

Le deuxième journal généraliste est créé par André d'Audebard, baron de Férussac, un naturaliste reconnu ayant présenté ses travaux à l'Académie. L'objectif de Férussac en imaginant un périodique est de « recenser, décrire et classer tout ce qui se publie dans le monde en matière de "sciences", au sens le plus large possible [...] »[Bru et Martin, 2005, p. 11]. Le *Bulletin général et universel des annonces et des nouvelles scientifiques*, généralement surnommé le *Bulletin de Férussac*[9], paraît de 1823 à 1831. Selon Taton :

> Mais, dès la fin de 1822, la majeure partie de [l'activité du baron de Férussac] fut réservée à la préparation et à l'organisation de son Bulletin. Pendant dix ans, il se consacra à ce travail gigantesque de direction, recrutant des centaines de collaborateurs, obtenant la livraison régulière de quelques 500 revues paraissant dans le monde entier, faisant publier des analyses de tous les articles importants et mettant ensuite ces revues à la disposition de tous [Taton, 1947, p. 102].

Cela donne une idée de l'ampleur du projet de Férussac[10]. En 1823, quatre tomes de douze numéros sont publiés. En 1824, ce journal devient le *Bulletin Universel des Sciences et de l'Industrie*, et est composé de huit sections ; c'est ici la première section, consacrée aux sciences mathématiques, astronomiques, physiques et chimiques, qui nous intéresse. La partie Mathématiques est elle-même divisée en deux sous-sections - Mathématiques élémentaires et Mathématiques transcendantes - jusqu'au tome 10. Dans le onzième tome, Charles Sturm, qui collabore avec Férussac, tente de classer les articles en plusieurs rubriques - Géométrie, Analyse, Mécanique, ...- mais renonce rapidement. Les travaux concernés se retrouvent ensuite tous dans une unique rubrique Mathématiques. Ce périodique retiendra notre attention car il contient des articles en lien avec les résidus et les congruences.

De nombreux collaborateurs participent à la rédaction des différents tomes du *Bulletin*. En ce qui concerne notre thème, c'est principalement Antoine-Augustin Cournot qui rend compte des différents documents disponibles, en signant des initiales C. ou A. C.[11].

Les premiers journaux scientifiques spécialisés dans une discipline commencent à paraître dans les années 1770. Dès 1800, un tiers des journaux scientifiques sont consacrés à

9. Se reporter notamment à [Bru et Martin, 2005] et [Taton, 1947] pour des informations plus détaillées sur ce périodique et son auteur.

10. Notons qu'à côté du *Bulletin*, le salon et la Bibliothèque de Férussac sont également des lieux d'échanges scientifiques importants : les revues et les ouvrages scientifiques commandés afin d'en faire des comptes rendus pour le *Bulletin* sont ensuite entreposés dans la Bibliothèque, et le salon permet aux jeunes mathématiciens d'échanger sur les sciences : ainsi, Abel, Cournot, Dirichlet et Galois participent aux réunions du salon de Férussac et publient certains de leurs travaux dans le *Bulletin*.

11. À ce sujet, voir [Taton, 1947] et [Bru et Martin, 2005]. Nous remercions d'ailleurs Bernard Bru de nous avoir fourni des notes sur ces comptes-rendus de Cournot, avant leur publication dans le onzième tome des *Oeuvres complètes* de Cournot avec ses écrits de jeunesse.

un seul domaine. Le premier journal français non lié à une institution, entièrement consacré aux mathématiques, dont la durée de vie a été conséquente, est publié de 1810 à 1832 : ce sont les *Annales de mathématiques pures et appliquées*[12], fondées par Joseph Diaz Gergonne et Joseph-Esprit Thomas Lavernède, professeurs de mathématiques à Nîmes (et connu sous le nom des *Annales de Gergonne*). L'objectif premier de Gergonne est de publier des mémoires pour le progrès de l'enseignement des mathématiques. En réalité, les *Annales* sont constituées en majorité d'articles sur les recherches mathématiques contemporaines, quelques textes seulement contenant des exposés plus élémentaires. Ce premier journal mathématique ne contient pas de travaux sur les résidus et les congruences.

On peut ajouter à cette courte liste de journaux un périodique d'un genre un peu différent : les *Exercices de Mathématiques*, publiés régulièrement entre 1826 et 1830, mais dont l'unique rédacteur est Cauchy[13]. Comme il est bien connu, cette publication permet au mathématicien de diffuser ses recherches, rapidement et sous forme de mémoires entiers, contrairement aux publications académiques.

Dans son étude sur le *Journal de Liouville*, Norbert Verdier indique l'existence de deux « poussées éditoriales »[Verdier, 2009, p. 13] dans la première moitié du XIX^{e} siècle. La première a lieu pendant les années 1825 et 1826. Plusieurs journaux mathématiques paraissent en Europe et sont étroitement liés entre eux : les auteurs de chacun des périodiques reprennent les analyses, traduisent les mémoires, résument les contenus des autres journaux, ce qui permet une circulation de l'information d'autant plus importante. Parmi ceux-ci, aucun n'est français. D'après notre premier relevé dans [Dickson, 1919-1923] et [White et al., 1867-1872], la *Correspondance mathématique et physique* de Jean Guillaume Garnier et Adolphe Quételet, et le *Zeitschrift für Physik und Mathematik* de Andreas Baumgartner et Andreas Freiherr von Ettinghausen contiennent chacun seulement un article concernant les résidus, où une preuve d'Euler est reproduite. Finalement, un seul périodique strictement mathématique rassemble, comme on peut s'y attendre, la plupart des articles sur les résidus et les congruences avant 1835 : c'est le *Journal für die reine und angewandte Mathematik*, fondé par August Leopold Crelle en 1826 (le *Journal de Crelle*). Les deux tiers des articles y sont publiés en allemand, la majorité du tiers restant, en français ou latin. Ce *Journal* semble être accessible à la population savante de Paris et des grandes villes de province ; des mathématiciens français connus, comme Siméon-Denis Poisson, Joseph Liouville, Antoine-Augustin Cournot, Sophie Germain, y publient d'ailleurs des articles.

Pendant les années 1830, la publication de plusieurs de ces périodiques est stoppée, principalement pour des raisons financières (sauf les *Exercices* de Cauchy, interrompus lorsque leur auteur part en exil). Ainsi, le *Bulletin de Férussac*, les *Annales de Gergonne* ou encore le *Zeitschrift für Physik und Mathematik* cessent de paraître. Le *Journal de*

12. Pour une analyse détaillée de ce périodique, se reporter à [Gérini, 2002].
13. Voir notamment [Belhoste, 1985, p. 93] à ce sujet.

Crelle qui surmonte les difficultés rencontrées fait donc figure d'exception[14]. De 1831 à 1835, les mathématiciens français ne disposent plus d'aucun autre périodique pour communiquer rapidement leurs recherches.

2 - 1835-1850 : le *Journal de Liouville* et les *Comptes Rendus* des séances de l'Académie

La deuxième « poussée éditoriale » évoquée plus haut a lieu entre 1835 et 1836, avec la naissance de deux périodiques consacrés principalement aux recherches nouvelles[15] : les *Comptes Rendus de l'Académie des Sciences* et le *Journal de mathématiques pures et appliquées*, fondé par Joseph Liouville.

Parallèlement aux *Mémoires* de l'Académie dont la publication continue, un autre journal académique voit le jour en 1835 : les *Comptes rendus hebdomadaires des séances de l'Académie des Sciences*[16] sont publiés chaque samedi, à l'issue de la séance du lundi précédent. Ils contiennent des articles assez courts[17] correspondant aux lectures et aux présentations faites lors de la séance en question. Les auteurs peuvent être académiciens ou non (dans ce dernier cas, les notes sont présentées avec l'aval d'un académicien). Ce journal permet ainsi une circulation plus systématique, rapide et large, du contenu des séances de l'Académie[18].

Quant au *Journal de Liouville*, il commence à paraître en 1836. Le premier tome est précédé d'un *Avertissement* où Liouville[19] expose son projet éditorial. Il souhaite que son périodique soit composé essentiellement d'articles de recherche, même s'il ne rejette pas les textes liés à l'enseignement[20]. Une différence majeure avec le *Bulletin de Férussac* est que Liouville n'est pas favorable à la publication de comptes rendus

14. À ce sujet, voir [Verdier, 2009, ch. 3].

15. D'autres journaux contenant des mathématiques paraissent aussi de façon éphémère, notamment destinés à l'enseignement et aux candidats à certaines écoles. Voir par exemple [Verdier, 2009, ch. 5] pour la *Gazette des écoles* et *Le Géomètre*.

16. Se reporter à [Crosland, 1992, p. 281-296] et [Brian et Demeulenaere Douyère, 1996, p. 132-134] pour une explication détaillée de la mise en place et du fonctionnement de ce nouveau moyen de communication, ainsi que pour un aperçu de l'implication de certains savants dans la création de ces *Comptes rendus*.

17. Il est prévu un maximum de huit pages par numéro et cinquante pages par an, par académicien. Cette limite est en fait largement dépassée par certains savants. Par exemple, Cauchy publie dans les *Comptes Rendus* plus d'une centaine de pages en 1840... pour la théorie des nombres seulement !

18. Pour le premier tiers du XIX^{e} siècle, le lecteur d'aujourd'hui peut se reporter aux *Procès verbaux des séances de l'Académie*. Les *Procès verbaux* pour les séances de 1795 à 1835 ont été publiés au début du XX^{e} siècle. Ils contiennent la liste des événements (élections, ...) importants de chaque séance, des travaux présentés à l'Académie, ainsi que certains rapports.

19. Pour une étude détaillée sur le périodique créé par Liouville : voir [Verdier, 2009]. Des travaux sont également consacrés aux recherches mathématiques de Liouville : voir par exemple [Lützen, 1982] et [Peiffer, 1983].

20. Voir [Verdier, 2009, p. 62-63].

d'autres publications. De plus, Liouville affirme qu'en tant qu'éditeur, il ne veut pas laisser transparaître son avis sur les textes retenus : cette attitude est contraire à celle adoptée par Gergonne dans ses *Annales*[21]. La réalité sera toutefois quelque peu différente. Des publications extérieures seront en effet reproduites, parfois traduites. Si Liouville fait appel aux savants français afin de nourrir son *Journal*, il annonce également l'insertion de documents émanant de savants étrangers. On verra effectivement plus loin que des traductions d'articles du *Journal de Crelle* sont insérées dans le *Journal de Liouville*, dans des délais plus ou moins longs par rapport à la publication originale[22].

Une autre caractéristique du *Journal de Liouville* est que l'éditeur n'a pas adopté de classification pour ranger les différents articles. En nous appuyant sur la classification proposée [Verdier, 2009], et sur les résultats ainsi obtenus[23], nous constatons que le *Journal de Liouville* comprend une part non négligeable de théorie des nombres : en effet, dans la première série (1836-1855), la théorie des nombres occupe 10% des articles, et même 15% entre 1846 et 1850. Ce pic de publication s'explique par une activité intensive autour de la démonstration du dernier théorème de Fermat[24], ce qui est également le cas pour les *Comptes Rendus* de l'Académie en 1847.

Deux autres journaux mathématiques apparaissent un peu plus tard. En septembre 1839, Cauchy lance à nouveau un périodique réservé à lui seul, désormais intitulé *Exercices d'analyse et de physique mathématique*. Enfin, à partir de 1842, sont créées les *Nouvelles annales de mathématiques. Journal des candidats aux écoles polytechnique et normale*[25], par Camille Christophe Gerono et Olry Terquem[26]. Ce journal contient des mémoires de mathématiques, mais aussi des problèmes (et leurs solutions) liés aux programmes d'admission aux écoles polytechnique et normale, ainsi que des comptes rendus sur d'autres journaux, comme le *Journal de Crelle*, et sur les séances des Académies de Paris et Berlin. En ce sens, les *Nouvelles Annales* se situent donc dans la lignée des *Annales de Gergonne* et du *Géomètre*. Ses auteurs et ses lecteurs sont majoritairement des professeurs et des étudiants. Ce périodique mathématique constitue donc un espace unique de publication pour certains[27]. Bien que la géométrie ait une place dominante dans les *Nouvelles Annales*, plusieurs textes en lien avec les résidus et les congruences y sont publiés.

21. Voir [Verdier, 2009, p. 63-64].
22. D'après l'étude présentée dans [Verdier, 2009, ch. 14], 70% des articles du *Journal de Liouville* sont originaux.
23. Voir en particulier [Verdier, 2009, partie III].
24. Une analyse du rôle du *Journal de Liouville* dans la circulation des travaux sur le dernier théorème de Fermat à cette période est donnée dans [Verdier, 2009, p. 292-296].
25. L'étude des *Nouvelles Annales* est actuellement menée conjointement par des chercheurs des Archives Henri Poincaré à Nancy et du Groupe d'Histoire et Diffusion des Sciences d'Orsay.
26. Nous nous appuyons sur l'analyse donnée dans [Verdier, 2009, p. 240-260].
27. Norbert Verdier remarque effectivement que la plupart des articles insérés dans le *Journal de Liouville* contiennent des travaux précédemment présentés à l'Académie, et ayant donc dû obtenir son approbation.

3 - Des périodiques plus ou moins rapides

Après 1835, la communication des recherches est donc bien plus rapide avec le *Journal de Liouville* ou les *Comptes Rendus* de l'Académie, et certaines discussions sont ainsi transcrites au fur et à mesure de la publication des fascicules [28]. Par contre, les délais entre la présentation d'un travail devant l'Académie des sciences et son intégration dans les *Mémoires* peuvent être très longs. Voici trois exemples illustrant ce phénomène et rencontrés lors de notre analyse [29] :

- Cauchy présente en 1830 un mémoire de théorie des nombres à l'Académie, celui-ci n'est ensuite publié qu'en 1840 ; ici, ce délai s'explique en partie par les événements politiques qui poussent Cauchy à s'exiler.
- Les travaux présentés par Libri à l'Académie entre 1824 et 1825, pour lesquels les commissions désignées donnent un avis favorable à leur insertion dans les *Mémoires des savants étrangers*, ne seront publiés dans les *Mémoires* de l'Académie qu'en 1838, plusieurs années après l'élection de Libri comme académicien.
- De même, les recherches en théorie des nombres de Lebesgue, présentées en 1836 à l'Académie, font l'objet d'un rapport favorable à leur publication dans les *Mémoires des savants étrangers* : nous n'avons retrouvé cette fois-ci aucune trace de leur publication !

Ces décalages très importants [30] ont un effet historiographique, car ils rendent encore plus difficile la tâche de déterminer quand exactement tel mathématicien a eu connaissance des travaux de tel autre.

II Résidus et congruences dans les journaux : 1800-1835

Nous allons maintenant analyser les travaux publiés dans ces périodiques, en nous concentrant principalement sur les périodiques français, ainsi que sur les recherches de savants français publiés à l'étranger. Nous donnerons également un aperçu global du contenu des articles publiés dans le *Journal de Crelle* : comme nous l'avons vu dans les chapitres précédents, d'ailleurs en conformité avec l'historiographie usuelle, c'est le périodique contenant le plus grand nombre d'articles sur notre thème ; de plus, comme

28. On peut par exemple suivre le déroulement du conflit entre Liouville et Libri en 1843 : voir [Belhoste et Lützen, 1984] et [Ehrhardt, 2011].

29. Nous nous référons ici à l'Académie des Sciences de Paris après 1801 uniquement. Nous verrons dans la deuxième partie que la situation est identique, voire pire, au XVIII^{e} siècle pour les *Mémoires* des académies de Berlin ou de Saint-Pétersbourg par exemple : on peut citer un mémoire sur les résidus d'Euler, [Euler, 1761b], qui est présenté à l'Académie de Saint-Pétersbourg en 1755, puis publié dans les *Mémoires* de cette même institution en 1761 seulement.

30. Notons que ces retards de publication ne sont pas particuliers à la théorie des nombres ni aux mathématiques mais concernent beaucoup de travaux de cette période.

nous le précisons dans ce qui suit, son contenu est commenté, voire reproduit, dans certains des périodiques français. Afin de mieux comprendre la chronologie des recherches, nous respectons ici le découpage précédent en deux périodes, qui permet de garder la trace des lieux réels de parution.

1 - Les *Mémoires* de l'Académie

Entre 1801 et 1835, trois textes des *Mémoires* de l'Académie des Sciences de Paris contiennent des raisonnements en lien avec notre thème.

(a) Poinsot : présentation de ses recherches en géométrie, algèbre et théorie des nombres (1818)

Le premier est un texte d'une douzaine de pages de Louis Poinsot, présenté à l'Académie le 5 mai 1817, puis publié en 1818. Dans cet *Extrait de quelques recherches nouvelles sur l'algèbre et sur la théorie des nombres*, Poinsot résume ses recherches passées et actuelles sur la géométrie des polygones, les permutations et les congruences, objets liés respectivement à la géométrie, l'algèbre et la théorie des nombres. Il relie ces trois études par ce qu'il appelle « la théorie de l'ordre et de la situation des choses sans aucune considération de la grandeur » [Poinsot, 1818, p. 382]. À partir du cinquième paragraphe, Poinsot présente ses recherches arithmétiques, consacrées à l'étude des racines primitives, notion qu'il attribue à Euler : il développe une analogie entre ces racines primitives, qui sont solutions de congruences binômes, et les racines de l'équation binôme correspondante, en tenant compte des racines imaginaires de ces congruences. Remarquons que pour nos auteurs, les racines imaginaires de congruences sont les racines qui ne sont pas entières, de la même façon que les racines imaginaires des équations sont celles qui ne sont pas réelles. Poinsot n'utilise pas dans ce mémoire de notations ou expressions particulières pour désigner des congruences, mais considère les racines primitives d'un nombre premier ou, de manière plus générale, des équations indéterminées : « si l'on a des équations quelconques indéterminées rapportées à un nombre premier dont elles renferment certains multiples, je dis qu'on pourra substituer à leur place les mêmes équations où l'on ferait nuls partout les multiples du nombre premier qu'on y considère » [Poinsot, 1818, p. 389]. Il rappelle néanmoins le vocabulaire introduit par Gauss : « M. Gauss les [les propriétés des résidus de puissance] a étendues et reproduites sous une autre forme, en représentant par de nouveaux signes les équations indéterminées qu'il nomme alors des *congruences*, ce qui veut dire des équations dont les deux membres *s'accordent* à donner le même résidu » [Poinsot, 1818, p. 390]. Il développe ses travaux arithmétiques annoncés ici dans [Poinsot, 1820].

(b) Legendre

Les deux autres textes publiés dans les *Mémoires* de l'Académie sont de Legendre.

Le premier, intitulé *Recherches sur quelques objets d'analyse indéterminée et particulièrement sur le théorème de Fermat*, est présenté en 1823 à l'Académie, puis publié en 1827. Il contient notamment une démonstration du dernier théorème de Fermat dans le cas $n = 5$. Certains des raisonnements produits ici font intervenir des restes, mais de manière assez élémentaire. Nous donnons ci-dessous deux exemples.

Pour justifier que si $x^5 + y^5 + z^5 = 0$ est satisfaite, alors un des nombres x, y ou z est divisible par 5, Legendre observe que la puissance cinquième d'un nombre non divisible par 5 est de l'une des quatre formes $25m \pm 1$ ou $25m \pm 7$. Or : « trois des quatre restes ± 1, ± 7, ne peuvent faire ni la somme 0 ni la somme 25 » [Legendre, 1827, p. 11].

Ou encore, Legendre étudie les conséquences d'une méthode vraisemblablement fournie par Sophie Germain en vue d'obtenir des résultats autour du dernier théorème de Fermat [31]. Cette méthode est basée sur une égalité entre des résidus :

> Pour cela, supposons, ce qui sera prouvé ultérieurement, qu'il existe pour chaque valeur de n, un nombre premier $\theta = 2kn + 1$, tel qu'on ne peut satisfaire à l'équation $r' = r + 1$, r et r' étant deux résidus de puissances $n^{\text{ièmes}}$ divisées par θ, et tel en même temps que n ne soit pas un de ces résidus [Legendre, 1827, p. 15].

En termes de congruences, l'égalité entre les résidus se note $r' \equiv r+1 \pmod{\theta}$. Legendre remarque d'ailleurs un peu plus loin dans une note à propos d'autres égalités où il a omis les multiples de θ :

> Ces équations entre les restes provenant de la division de plusieurs nombres par un même nombre premier θ, se traitent comme les équations ordinaires, sans qu'il soit besoin des signes nouveaux d'égalité ni des dénominations nouvelles assez *incongrues*, dont quelques géomètres font usage [Legendre, 1827, p. 15].

Ce commentaire est clairement destiné à Gauss, et certainement aussi à Sophie Germain qui, de son côté, félicite Gauss pour son heureuse notation.

À la fin du mémoire, Legendre obtient également des résultats sur les équations de la forme $4P = X^2 \pm nY^2$. Sophie Germain s'appuie d'ailleurs sur ces résultats et ceux exposés dans [Legendre, 1830] dans son unique publication de théorie des nombres [Germain, 1831]. C'est également ce thème que Legendre aborde à nouveau dans le second mémoire.

Dans ce dernier, lu le 11 octobre 1830 à l'Académie et publié en 1832 dans les *Mémoires*, Legendre indique une méthode permettant de déterminer les polynômes Y et Z

31. Il crédite d'ailleurs Sophie Germain d'une preuve donnée dans ce texte : voir [Legendre, 1827, p. 17]. Voir également le paragraphe consacré aux travaux de théorie des nombres de la mathématicienne : page 63 de cette partie. Sur le programme de S. Germain à propos du théorème de Fermat, voir [Laubenbacher et Pengelley, 2010] [Del Centina, 2008].

tels que $4(x^n - 1) = (x-1)(Y^2 \pm nZ^2)$, où n est un nombre premier impair [32]. Il utilise ici explicitement la notion de racine primitive et développe des raisonnements à partir des résidus quadratiques. Il note g une racine primitive de n, et note α l'un des termes de la forme g^{2k}, $0 < k < \frac{n-3}{2}$: il obtient ainsi les résidus quadratiques de n. Il note β, un des termes de la forme g^{2k+1}, $0 < k < \frac{n-3}{2}$, puis rappelle que le produit de tous les facteurs de la forme $(x - r^\alpha)$ est égal à $\frac{1}{2}(Y \pm Z\sqrt{n})$ et que le produit des $(x - r^\beta)$ est alors égal à $\frac{1}{2}(Y \mp Z\sqrt{n})$. D'un autre côté, le produit de tous les facteurs de la forme $(x - r^\alpha)$ est également de la forme $x^m + \frac{1}{2}A_1 x^{m-1} + \frac{1}{2}A_2 x^{m-2} + \ldots$, où $m = \frac{1}{2}(n-1)$. Il en déduit ensuite des liens entre les coefficients A_i et les sommes $S_k = \sum r^{k\alpha}$.

Ici, Legendre s'appuie donc sur les racines primitives et sur ce qu'on appelle aujourd'hui les sommes de Gauss pour mener ses raisonnements. Néanmoins, il n'utilise ni ne se réfère explicitement aux recherches de Gauss.

2 - Le *Journal de l'École Polytechnique*

(a) Les *Leçons* de l'École Normale de l'an III (1812)

Dans la réédition des *Leçons de Mathématiques données à l'École Normale en 1795* par Laplace et Lagrange dans le douzième tome du *Journal de l'École Polytechnique*, Gauss est mentionné à deux reprises pour sa résolution générale de l'équation binôme (section VII des *Disquisitiones Arithmeticae*). Laplace note d'ailleurs, à propos des sujets qui paraissent inutiles au premier abord mais qui permettent d'obtenir des résultats importants :

> Depuis la première publication de ces leçons, M. Gauss, célèbre géomètre, a réalisé cette prédiction ; et par une application extrêmement ingénieuse de la théorie des nombres, il est parvenu à des résultats intéressants, entièrement nouveaux, sur la résolution des équations et sur l'inscription des polygones réguliers dans le cercle [Laplace, 1812, p. 24].

On ne trouve pas de raisonnements explicites sur les résidus ou les congruences dans ce texte, en dehors de cette allusion, qui met en avant leurs applications à l'algèbre et à la géométrie.

(b) Les *nombres de même forme* de Cauchy (1813)

Cauchy, alors ingénieur aux Ponts et Chaussées, publie ses *Recherches sur les nombres* dans le *Journal de l'École Polytechnique* en 1813. L'objectif annoncé du savant est de démontrer plus simplement un résultat sur les formes quadratiques déjà prouvé par Lagrange en 1770 : si p est un nombre premier et B, C sont des entiers non divisibles par p

32. Legendre observe au début de ce texte qu'il a déjà donné des résultats à ce sujet dans [Legendre, 1808, art. 512], valables pour certaines petites valeurs de n.

alors il existe des nombres entiers t et u tels que t^2+Bu^2+C soit divisible par p. Pour cela, Cauchy introduit ce qu'il appelle les *nombres de même forme* : ceux-ci sont similaires aux nombres congrus de Gauss, mais ni Gauss ni son ouvrage ne sont mentionnés par Cauchy. Voici sa définition :

> Pour simplifier les énoncés de ces théorèmes, j'appellerai *nombres de même forme*, relativement à un diviseur donné, des nombres entiers qui, étant divisés par ce diviseur, donnent des restes entiers et positifs égaux. Par opposition, j'appellerai *nombres de forme différente* des nombres entiers qui, étant divisés par le diviseur donné, donneront des restes entiers et positifs différents.
>
> Supposons que
>
> $$a_0, a_1, a_2, \ldots, a_\alpha,$$
>
> soient une série de nombres entiers positifs ou négatifs, composée de $\alpha+1$ termes différents ; nous représenterons par a_x le terme général de cette série et nous dirons alors que la formule a_x peut prendre successivement $\alpha+1$ valeurs différentes. Si, de plus, les valeurs particulières
>
> $$a_0, a_1, a_2, \ldots, a_\alpha,$$
>
> de la formule a_x, sont toutes de formes différentes relativement à un diviseur donné, nous dirons alors que la formule a_x peut fournit $\alpha+1$ valeurs de formes différentes [Cauchy, 1813, p. 40].

Cauchy considère ensuite le nombre de valeurs de formes différentes pris par certaines formules comme $k \pm a_x$, Aa_x, $k \pm Aa_x$, …, où k et A sont des nombres entiers, et où A n'est pas divisible par p. Le théorème XIV porte sur les résidus quadratiques :

> *Soit, pris pour diviseur, un nombre premier $p > 2$ et considérons la formule x^2 comme représentant le carré d'un nombre entier pris à volonté. Je dis que la formule x^2 pourra fournir $\frac{p+1}{2}$ valeurs de formes différentes* [Cauchy, 1813, p. 54].

Ce même résultat est énoncé en termes de résidus par Gauss dans les *Disquisitiones Arithmeticae*, mais également par Legendre dans [Legendre, 1798] et par Euler dans [Euler, 1760b]. Néanmoins, Cauchy ne fait aucune référence à ces travaux.

Il démontre ensuite le théorème énoncé initialement, puis en déduit des résultats sur les nombres polygones. Cauchy présentera d'ailleurs, le 13 novembre 1815, à l'Académie une démonstration complète du théorème de Fermat sur ces nombres[33] ; cependant, celle-ci ne se base plus sur les résidus ou les nombres de même forme.

Ceux-ci n'apparaissent donc ici que ponctuellement, dans le but de « simplifier les énoncés de [ses] théorèmes ». L'absence de toute référence suggère une élaboration indépendante, mais Cauchy ne développe pas de théorie de ses nombres, analogue à la théorie des résidus d'Euler ou à celle des congruences de Gauss. Il s'agit pour Cauchy de discuter

33. Voir notamment [Cauchy, 1818].

le nombre de valeurs de certaines expressions, une problématique qu'on retrouve dans ses travaux contemporains sur les substitutions[34].

(c) Les congruences binômes de Poinsot (1820)

Le deuxième mémoire inséré dans le *Journal de l'École Polytechnique* est de Louis Poinsot, et son contenu correspond aux recherches annoncées dans son *Extrait de quelques recherches nouvelles* de 1818. Ce *Mémoire sur l'application de l'algèbre à la théorie des nombres*, composé d'environ soixante-dix pages, est présenté en 1818 à l'Académie puis publié en 1820 dans le *Journal*. Il est également intégré dans le volume des années 1819-1820 des *Mémoires* de l'Académie, qui paraît en 1824. Ce travail a pour thème un résultat énoncé par Poinsot en ces termes :

> Considérons donc l'équation binôme indéterminée, $x^n - 1 = Mp$, où Mp désigne un multiple quelconque du nombre premier p, et n un exposant quelconque premier, que je supposerai d'abord diviseur de $p - 1$, afin que l'équation $x^n - 1 = Mp$ ait n racines ou solutions en nombres entiers inférieurs à p. Je dis que si l'on prend, à la place de cette équation indéterminée, l'équation binôme déterminée $x^n - 1 = 0$, et qu'on la résolve, l'expression algébrique de ses n racines, qui, excepté l'unité, sont toutes imaginaires, sera la représentation analytique des n nombres entiers qui résolvent l'équation $x^n - 1 = Mp$; c'est-à-dire qu'en ajoutant aux nombres qui sont sous les divers radicaux de cette formule imaginaire, des multiples convenables de p, on fera disparaître les imaginaires et les irrationnelles, on rendra toutes les opérations indiquées parfaitement exécutables, et l'on parviendra précisément aux n nombres entiers qui satisfont à la proposée $x^n - 1 = Mp$ [Poinsot, 1820, p. 349].

Comme dans son article précédent, Poinsot n'utilise pas la notation ≡ ou l'appellation *congruence* de Gauss, mais emploie la notation de Legendre Mp pour désigner un multiple de p. Du point de vue de la méthode, son étude est par contre centrée sur la résolution des congruences binômes et sur les propriétés de leurs racines, en analogie avec la méthode exposée par Gauss dans la section VII sur la résolution des équations binômes. Cela l'amène à considérer des racines imaginaires de congruences, dans le cas où n n'est pas un diviseur de $p - 1$. Poinsot insiste particulièrement sur la façon dont on peut exprimer les racines des équations et congruences binômes à partir d'une racine primitive et donne à nouveau des considérations sur l'ordre. Nous étudierons ce texte de manière approfondie dans la troisième partie.

(d) Une démonstration du petit théorème de Fermat par Binet (1831)

Jacques Philippe Marie Binet[35] est étudiant à l'École Polytechnique de 1804 à 1806. Il commence à y enseigner en 1807 et devient inspecteur des études en 1816. En 1823, il

34. Voir [Dahan Dalmedico, 1979] et [Dahan Dalmedico, 1980] à ce sujet.
35. Les indications biographiques données ici sont issues de [Shallit, 1994] et [Belhoste, 1985].

obtient la chaire d'astronomie au Collège de France. Proche du régime de Charles X, il subit comme son ami Cauchy les revers de la Révolution de Juillet et est démis de ses fonctions à l'École Polytechnique. Il est néanmoins élu à l'Académie des Sciences en 1843, avec l'appui de Cauchy.

Le mémoire de Binet publié en 1831 dans le *Journal de l'École Polytechique* est intitulé *Mémoire sur la résolution des équations indéterminées du premier degré en nombres entiers* et est présenté à l'Académie des Sciences le 15 octobre 1827. Ce texte ne traite pas à proprement parler des congruences mais Binet y expose une démonstration du petit théorème de Fermat, puis applique ce théorème pour résoudre les équations indéterminées du premier degré.

Il considère un nombre premier p et un entier a non divisible par p. Il note ensuite α_k les restes des nombres ka après division par p, où k est compris entre 1 et $p-1$. Il utilise à cette occasion la notation de Legendre pour noter par exemple : $2a = \alpha_2 + Mp$. Les restes obtenus sont tous différents et représentent donc dans un certain ordre tous les nombres compris entre 1 et $p-1$. Il obtient ainsi l'égalité :

$$1.2.3\ldots(p-1)a^{p-1} = \alpha_1\alpha_2\ldots\alpha_{p-1} + Mp$$

soit, puisque $\alpha_1\alpha_2\ldots\alpha_{p-1} = 1.2.3\ldots(p-1)$:

$$1.2.3\ldots(p-1)(a^{p-1}-1) = Mp.$$

Comme p est un nombre premier, $1.2\ldots(p-1)$ n'est pas divisible par p. Binet en déduit donc que $a^{p-1} = 1 + Mp$, d'où le petit théorème de Fermat.

Il applique ensuite ce théorème à la résolution de l'équation indéterminée $ax - by = 1$, tout en remarquant que la méthode ainsi obtenue est moins pratique que celle fondée sur l'utilisation des fractions continues :

> Nous ne nous occupons aucunement en tout ceci des réductions particulières, dont le calcul de ces formules serait susceptible dans leurs applications numériques, en se servant des théorèmes connus sur les résidus de puissances. Notre objet n'est pas de substituer le calcul arithmétique, en général très-pénible, que ces expressions supposent, à celui des fractions continues, mais seulement d'indiquer un type algébrique de solution générale tiré du théorème de *Fermat*. Nous aurions pu déduire du théorème de *Wilson* des expressions analogues aux précédentes ; mais elles seraient un peu plus compliquées [Binet, 1831, p. 296].

Ici, Binet n'utilise donc que des raisonnements élémentaires sur les restes. La citation précédente fait néanmoins ressortir deux points intéressants. D'une part, Binet relie et met en avant les théorèmes de Fermat et Wilson comme deux bases (alternatives) possibles pour ce genre de recherches ; ces théorèmes, démontrés au XVIII^{e} siècle, sont l'objet de beaucoup d'études et de commentaires tout au long de la première moitié du XIX^{e} siècle.

D'autre part, il insiste sur l'intérêt de cette approche qui ne vise pas à obtenir des valeurs numériques, mais bien une formule générale de résolution de ces équations indéterminées du premier degré ; les résidus servent donc ici à un problème de nature explicitement algébrique (comme c'était le cas dans les *Disquisitiones arithmeticae* de Gauss).

3 - Le *Bulletin de Férussac* (1823-1831)

(a) Aperçu

Nous avons relevé dans le *Bulletin de Férussac* un total de 23 entrées mentionnant les résidus et les congruences [36]. Nous comptabilisons les annonces d'ouvrages appartenant à notre corpus, même si leur contenu n'est pas détaillé : en effet, l'objectif ici est de déterminer si les sources de notre corpus sont bien recensées dans le *Bulletin* d'une manière ou d'une autre et de comprendre ainsi jusqu'à quel point est représentative l'image des recherches sur les résidus et les congruences que reflète ce périodique français. Les différents articles du périodique sont de nature diverse : les présentations à l'Académie sont généralement données en une phrase (comme dans les *Procès verbaux* des séances), et certaines parutions d'ouvrages se résument parfois à la référence de la publication : c'est par exemple le cas pour la cinquième édition du *Complément des éléments d'algèbre* de Lacroix. On retrouve également des extraits de textes déjà publiés : par exemple, une partie du rapport fait par Ampère et Cauchy sur un des mémoires *Théorie des nombres* de Libri est reproduite dans le troisième tome du *Bulletin*.

La majorité des entrées sont des comptes rendus d'ouvrages ou d'articles parus dans les *Mémoires* de l'Académie ou dans le *Journal de Crelle* ; ils sont vraisemblablement tous écrits par Cournot. Enfin, on compte cinq textes inédits : une note de Libri, deux mémoires de Cauchy, un de Galois et un de Lebesgue.

(b) Des comptes rendus de mémoires et d'ouvrages

Le premier compte rendu analyse le contenu de [Poinsot, 1820], suite à son insertion dans les *Mémoires* de l'Académie en 1824. Selon Cournot, « parmi les géomètres de l'école actuelle, aucun n'a porté dans la philosophie des sciences mathématiques des aperçus plus nouveaux et plus piquans que M. Poinsot » [37]. Dans sa présentation, Cournot met en relief certains points qu'il juge fondamentaux dans les idées de Poinsot : le fait que Poinsot démontre que les racines de l'équation $x^n - 1 = 0$ sont la « représentation symbolique » [38] des racines de l'équation $x^n - 1 = Mp$, qu'il insiste sur l'*ordre* dans lequel sont rangées les

36. Voir Annexe, page 486.

37. *Bulletin de Férussac*, 1825, t. 3, p. 144.

38. Ici, Cournot emploie cette expression pour désigner le processus décrit par Poinsot consistant à utiliser l'expression des racines complexes de l'équation $x^n = 1$ en ajoutant des multiples bien choisis de p à certains nombres de cette expression afin d'obtenir les racines entières de l'équation $x^n - 1 = Mp$ lorsque c'est possible.

racines de l'équation lorsqu'on les exprime à l'aide d'une racine primitive et qu'il illustre ses propos en imaginant que les racines de l'équation binôme ainsi données sont rangées autour de la circonférence d'un cercle. Ces idées de Poinsot se retrouvent donc diffusées dans trois périodiques différents entre 1820 et 1825.

En 1828, Cournot donne un aperçu du mémoire sur le dernier théorème de Fermat publié en 1827 par Legendre dans les *Mémoires* de l'Académie. Il récapitule le contenu de chaque partie, en indiquant que Dirichlet s'est également occupé du cas particulier du cinquième degré et que Sophie Germain est l'auteur de certaines preuves présentées par Legendre. Les résidus et les congruences ne sont pas explicitement mentionnés.

Un résumé de la troisième édition de la *Théorie des nombres* de Legendre est inséré dans le quatorzième volume du *Bulletin* en 1830. Par rapport aux éditions précédentes, Cournot indique des modifications importantes à partir de la quatrième partie ; dans la cinquième partie, on « trouve de nouveaux développements très étendus sur les méthodes proposées par Gauss, pour les équations à deux termes »[39]. Cournot ajoute également que deux démonstrations de la loi de réciprocité y sont également présentées. Les mots "résidus" et "congruences" ne sont jamais utilisés dans ce compte rendu.

En 1826, par l'intermédiaire de S. (qui correspond à Saigey), Cauchy avertit de la publication périodique de ses *Exercices de Mathématiques* dont il est l'unique auteur :

> Cet ouvrage, dit l'auteur, se composera d'une suite d'articles sur les différentes parties des sciences mathématiques. Il paraîtra par livraisons qui se succéderont à des époques peu éloignées l'une de l'autre. Dans ces articles on se propose de passer en revue les diverses branches de l'analyse, d'éclaircir les difficultés qu'elles présentent, et d'offrir de nouvelles méthodes à l'aide desquelles on puisse traiter plus facilement des questions déjà résolues, ou résoudre celles qui ne l'étaient pas encore. Les principales applications de ces méthodes seront relatives à la physique, à la mécanique et à la théorie des nombres[40].

Les différentes livraisons de ces *Exercices* sont commentées dans les tomes suivants du *Bulletin*. Peu d'articles contenus dans cette nouvelle série sont en rapport avec la théorie des résidus et des congruences, et ceux-ci ne sont pas résumés. Il est néanmoins intéressant de voir que la théorie des nombres fait partie des trois applications envisagées par Cauchy pour ses méthodes d'analyse dans la présentation de son périodique.

Enfin, Cournot publie également des analyses de travaux de savants avant que ceux-ci ne soient insérés dans les *Mémoires* de l'Académie. Ainsi, il résume un travail de Dirichlet

39. *Bulletin de Férussac*, 1830, t. 14, p. 90-91.
40. *Bulletin de Férussac*, 1826, t. 6, p. 21.

présenté à l'Académie le 11 juillet 1825, et ayant obtenu un rapport favorable de la part des commissaires Legendre et Lacroix qui en souhaitent une publication dans le recueil des *Savants étrangers*. Cournot observe d'ailleurs :

> La lenteur avec laquelle cette collection [le recueil des *Savants étrangers*] se publie a déterminé l'auteur du mémoire à le livrer lui-même à l'impression [41].

Il est effectivement indiqué dans le titre de cette entrée que le mémoire de Dirichlet a été publié en 1826 par l'éditeur Huzard sous la forme d'un in-quarto de vingt pages. Ce travail est également inséré dans le troisième tome du *Journal de Crelle* en 1828 et est annoncé à cette occasion une deuxième fois par Cournot sans commentaire supplémentaire.

Ici, Cournot nous donne une idée du raisonnement de Dirichlet en deux pages. Le lecteur y découvre que le travail de Dirichlet est basé sur une méthode de descente infinie déjà utilisée par Fermat et Euler pour démontrer que certaines équations indéterminées du troisième ou quatrième degré sont impossibles à résoudre. Cette méthode permet de démontrer l'impossibilité d'une classe infinie d'équations indéterminées du cinquième degré, ce qui n'est pas le cas dans les travaux de ses prédécesseurs. Cournot indique ensuite immédiatement que son analyse ne pourra être détaillée ; il ne présente donc que les principaux théorèmes démontrés par Dirichlet. Dans ce résumé, les « restes » ne sont mentionnés qu'une seule fois. Cependant, lorsque l'on examine le texte publié dans le *Journal de Crelle*, Dirichlet utilise régulièrement la notation ≡, « signe employé par M. Gauss » [Dirichlet, 1828b, p. 356], et applique couramment le (petit) théorème de Fermat, sans référence particulière :

> Comme 5 est un nombre premier, on aura
>
> $$x^5 \equiv x,\ y^5 \equiv y,\ z^5 \equiv z, \pmod 5$$
>
> [Dirichlet, 1828b, p. 366].

La différence entre le texte de Dirichlet et le compte rendu par Cournot est donc de notre point de vue très significative. Dirichlet utilise les congruences comme un outil bien assimilé, s'en sert pour exprimer le théorème de Fermat implicitement, théorème étant supposé bien connu. Le commentaire, au contraire, met en valeur surtout l'applicabilité à une famille d'équations.

(c) Des comptes rendus sur les articles publiés dans le *Journal de Crelle*

À partir de 1826, en fait, chaque livraison du *Journal de Crelle* est commentée dans le *Bulletin*. Cinq articles en liaison avec les résidus et les congruences et publiés dans le périodique allemand y sont résumés par Cournot. Les auteurs concernés sont Dirichlet, Jacobi et Moritz Abraham Stern. Seuls les comptes rendus des articles de Dirichlet et

41. *Bulletin de Férussac*, 1826, t. 6, p. 89.

Jacobi permettent d'avoir une idée du contenu du texte original.

Le texte de Jacobi, publié en 1827 dans la *Journal de Crelle* est intitulé *De residuis cubicis commentatio numerosa* (traduit par *Des résidus cubiques*) de Jacobi. Cournot rappelle que les savants attendent de lire les travaux de Gauss à ce sujet, promis depuis 1801 et la publication des *Disquisitiones Arithmeticae*. Jacobi donne trois théorèmes sur les relations des caractères cubiques de deux nombres premiers p et q selon leur forme, sans les démontrer. Cournot indique que ces théorèmes s'insèrent dans une « théorie neuve et piquante, celle des racines imaginaires des congruences et de leurs racines primitives » et ajoute :

> Depuis long-temps nous avions pensé (et les derniers mémoires de M. Poinsot l'indiquaient assez clairement) que la considération de cette sorte de racines était nécessaire pour compléter la théorie des nombres et étendre ses rapports avec l'analyse algébrique [42].

Dans le cas d'un mémoire de Dirichlet portant sur la démonstration des théorèmes de Fermat et de Wilson, Cournot reçoit une première version du travail avant publication et en donne un aperçu dans le *Bulletin*, puis s'y réfère à nouveau dans le onzième tome du *Bulletin* en 1829, lors de la parution du texte dans le *Journal de Crelle*. Dès 1827, Cournot, qui qualifie cette preuve du théorème de Wilson de « très-ingénieuse » [43], utilise cette fois la notation des congruences adoptée par Gauss (et Dirichlet), contrairement à ce qu'il avait fait pour le texte précédent de Dirichlet. Notons que la démonstration proposée par Dirichlet est similaire à celle donnée par Binet dans [Binet, 1831].

Cournot résume également un troisième mémoire de Dirichlet publié dans le *Journal de Crelle* : *Recherches sur les diviseurs premiers d'une classe de formules du 4^e degré*, qui contient des résultats sur les résidus biquadratiques. Cournot remarque que Gauss, dans son mémoire [Gauss, 1828] présenté en 1825 à Göttingen, avait promis certaines démonstrations, que Dirichlet commence par donner avant d'étudier les propriétés des diviseurs premiers des formes $\alpha x^4 + \beta x^2 + \gamma$. Cournot reproduit enfin les énoncés de quatre des résultats donnés par Dirichlet sur les résidus biquadratiques : « De là, au moyen d'une analyse fort délicate, M. Dirichlet établit deux théorèmes généraux qui font le principal objet du mémoire, et dont la démonstration est reprise encore sous une face nouvelle, dans une addition qui lui fait suite. Mais le seul énoncé de ces théorèmes présente déjà assez de complication, pour ne pouvoir être convenablement saisi, indépendamment des développements et des calculs de l'auteur » [44].

Victor-Amédée Lebesgue se réfère dans [Lebesgue, 1839] à ce compte rendu en indiquant : « Je ne connaissais pas le mémoire de M. Dirichlet quand j'ai trouvé la démons-

42. *Bulletin de Férussac*, 1827, t. 8, page 302.
43. *Bulletin de Férussac*, 1827, t. 7, p. 354 - 355.
44. *Bulletin de Férussac*, 1828, t. 9, p. 357

tration du théorème général (I) donné plus haut mais j'avais lu ce qu'on en dit dans le *Bulletin des Sciences Mathématiques* de M. Férussac » [Lebesgue, 1839, p. 59].

(d) Des mémoires inédits

Dans cinq des entrées comptabilisées dans notre corpus, des savants publient un texte original (de taille variable) afin de pallier l'absence ou le retard de publication de leurs travaux dans les *Mémoires* de l'Académie.

Cauchy : deux *Mémoires sur la théorie des nombres*

Ainsi, Cauchy insère en 1829 et 1831 deux *Mémoires sur la théorie des nombres*[45], dont les thèmes sont repris dans son grand *Mémoire sur la théorie des nombres* publié en 1840. Dans toutes ses publications de théorie des nombres après 1829, Cauchy utilise la notation ≡ de Gauss, mais il nomme *équivalences* les congruences. Il attribue logiquement la notion et le symbole ≡ à Gauss, mais, de façon plus étonnante, se réfère à Poinsot sans justifier ce choix lorsqu'il donne la définition de la racine primitive d'une équation ou d'une congruence. Les racines primitives ont pourtant été introduites par Euler dans [Euler, 1774] et leur importance a été particulièrement mise en avant dans [Gauss, 1801].

Le premier texte de Cauchy publié dans le *Bulletin de Férussac* contient notamment une trame de démonstration de la loi de réciprocité quadratique[46], qui est en fait un cas particulier des formules qu'il démontre. Il annonce effectivement un objectif général dans l'introduction de son mémoire :

> Dans la science des nombres, l'une des propriétés les plus importantes et les plus fécondes en conséquences dignes de remarque, est le théorème connu sous le nom de *loi de réciprocité* entre deux nombres premiers. On sait en particulier que cette proposition sert de base à la théorie des résidus quadratiques. Or, des recherches relatives à la résolution des équations binômes, après m'avoir fourni une démonstration nouvelle de la loi de réciprocité dont il s'agit, m'ont conduit à reconnaître qu'il existe une infinité de lois du même genre, mais d'un ordre plus élevé, et j'ai vu découler de ces lois des théories nouvelles, savoir : la théorie des résidus cubiques et généralement des résidus fournis par des puissances d'un degré quelconque. D'ailleurs l'analyse par laquelle je suis parvenu à découvrir ces mêmes lois, m'a offert le moyen de résoudre algébriquement une foule d'équations indéterminées et d'établir des théorèmes dignes de l'attention des géomètres [Cauchy, 1829a, p. 88].

Cauchy donne donc une place primordiale à la loi de réciprocité et annonce des résultats sur les résidus d'ordre quelconque. Il définit d'ailleurs un symbole de Legendre généralisé

45. Nous revenons sur ces deux textes dans notre quatrième partie.
46. Cette démonstration est reprise plus en détail dans la quatrième note du mémoire de 1840.

aux résidus de tous ordres : si n est un nombre premier, k un nombre entier et ρ une racine n^{e} de l'unité, alors $\left[\frac{k}{p}\right]$ est

une expression équivalente à

$$0 \text{ ou } 1 \text{ ou } \rho \text{ ou } \rho^2 \text{ ou } \rho^3 \text{ ou } \ldots \text{ ou } \rho^{n-1}$$

suivant que l'on aura

$$k^{\varpi} \equiv 0 \text{ ou } 1 \text{ ou } \rho \text{ ou } \rho^2 \text{ ou } \rho^3 \text{ ou } \ldots \text{ ou } \rho^{n-1} \pmod{p}.$$

[Cauchy, 1829a, p. 104].

Comme nous le verrons dans la quatrième partie, il en déduit une formule générale sur $\left[\frac{k}{p}\right]$.

Dans ce texte, Cauchy utilise principalement les sommes de la forme $\theta+\rho\theta^t+\rho^2\theta^{t^2}+\ldots+\rho^{p-2}\theta^{t^{p-1}}$, où p est un nombre premier, n un diviseur de $p-1$, ρ est une racine n^{e} de l'unité, θ une racine p^{e} de l'unité et t une racine primitive de p, et en étudie les propriétés. À la fin de son mémoire, il remarque que Jacobi a obtenu des résultats semblables : nous avons déjà fait référence dans notre introduction générale à ces résultats célèbres de Jacobi. S'ils sont analogues chez les deux mathématiciens, leurs développements ultérieurs auront des objectifs différents pour chacun. Nous reviendrons sur ce cas dans la quatrième partie.

Un dernier article publié par le même auteur, en 1831, se réduit à l'annonce d'un résultat sur les formes quadratiques de la forme $p^{\mu} = 4x^2 + ny^2$, où n est un diviseur de $p-1$, une manière de prendre date très vite sur des résultats de théorie des nombres.

Libri : une méthode de détermination des racines primitives

Libri profite également du *Bulletin* pour diffuser rapidement les résultats de ses recherches. En 1829, il insère un court texte d'une page sur une méthode pour la recherche des racines primitives d'un nombre premier [47]. Avant d'appliquer brièvement sa méthode sur un exemple, Libri explique pourquoi il tient à publier ce texte dans le *Bulletin de Férussac* :

> M. Cauchy a annoncé à l'Académie des Sciences de Paris dans sa séance du 9 novembre 1829, qu'il a découvert le moyen de déterminer les racines primitives des nombres, mais qu'il ne fera connaître sa méthode que plus tard. Depuis quelques mois j'ai trouvé deux solutions de ce problème qui diffèrent beaucoup entr'elles. J'avais l'intention de les publier dans le second volume de

47. Grâce à une indication à la fin de ce court texte, on sait qu'une déclaration similaire, mais en italien, a été publiée par Libri et datée du 26 novembre 1829 dans le périodique *Antologia. Giornale di Scienze, Lettere e Arti*, n° 108 (Décembre 1829), volume 36. Libri adresse également une note sur une *formule qui donne en nombres, directement et d'une manière générale, les racines primitives d'un nombre premier quelconque*, qui est lue à l'Académie pendant la séance du 12 juillet 1830

> mes *Mémoires de Mathématiques et de Physique* [*de Florence*] ; mais l'annonce de M. Cauchy me force à dire sur-le-champ quelques mots de mes recherches, afin de ne pas être prévenu par lui [48].

Libri donne donc un très bref aperçu de sa méthode pour déterminer les racines primitives du nombre 7 et indique que celle-ci permet également la résolution des congruences de tous les degrés. Comme pour Cauchy, ce sont les notations et le vocabulaire de Gauss qui sont utilisés.

Deux autres mathématiciens plus éloignés des milieux académiques publient également leurs recherches en lien avec les résidus et les congruences dans le *Bulletin* : il s'agit de Victor-Amédée Lebesgue et Évariste Galois [49].

Lebesgue : des résultats sur les résidus

Lebesgue publie en 1831 une *Note sur les résidus des puissances*, insérée à la fin d'un article intitulé *Note sur les fractions continues périodiques*. Lebesgue y est présenté simplement comme « bachelier ès sciences ». Ce court article est la seconde publication de Lebesgue sur la théorie des nombres [50]. La première partie de cet article contient des résultats sur les équations de la forme $ax^2 - 2bx + c = 0$, où a et b sont des nombres entiers positifs, et où c est un nombre entier. Ce passage ne contient aucune référence aux résidus. Par contre, Lebesgue indique quatre résultats « trouvés par induction » en rapport avec la théorie des résidus, dans une sous-partie nommée *Note sur les résidus des puissances*. Ces quatre résultats, qu'il « propose à démontrer aux géomètres qui s'occupent de cette partie » [51], concernent les résidus cubiques d'un nombre premier p de la forme $3n+1$, relativement aux nombres M et N définis par l'égalité $4p = M^2 + 27N^2$. Lebesgue ajoute qu'il n'a pas réussi à obtenir des résultats analogues pour les résidus biquadratiques et profite de cet article pour annoncer également la publication prochaine d'un mémoire contenant les démonstrations d'autres résultats de théorie des nombres annoncés par Jacobi et Dirichlet.

Galois : étude des racines imaginaires de congruences

Galois, enfin, publie deux textes dans le treizième tome du *Bulletin*, le premier consacré à la théorie algébrique des équations, le deuxième intitulé *Sur la théorie des nombres* [52].

48. *Bulletin de Férussac*, 1830, t. 13, p. 272 - 273.
49. Les travaux arithmétiques de Lebesgue sont néanmoins évoqués lors des séances de l'Académie.
50. Lebesgue a publié un mémoire de théorie des nombres dans le *Bulletin du Nord* de Moscou, que nous commentons à la fin de cette section. Nous donnerons quelques indications biographiques sur Lebesgue p.93.
51. *Bulletin de Férussac*,1831, t. 15, p. 158.
52. Une note - probablement écrite par un des rédacteurs - est ajoutée : « Ce mémoire fait partie

Ces articles seront reproduits en 1846 dans le onzième tome du *Journal de Liouville*, lors de l'édition posthume par Liouville des œuvres de Galois, et ce sont les seuls textes de Galois en rapport avec la théorie algébrique des équations publiés de son vivant. Galois commence par annoncer l'objectif de son mémoire, en se référant aux travaux de Gauss :

> Quand on convient de regarder comme nulles toutes les quantités qui, dans les calculs algébriques, se trouvent multipliées par un nombre premier donné p, et qu'on cherche dans cette convention les solutions d'une équation algébrique $Fx = 0$, ce que M. Gauss désigne par la notation $Fx \equiv 0$, on n'a coutume de considérer que les solutions entières de ces sortes de questions. Ayant été conduit par des recherches particulières à considérer les solutions incommensurables, je suis parvenu à quelques résultats que je crois nouveaux [Galois, 1830, p. 428].

Ainsi, ce mémoire porte sur l'étude de <u>toutes</u> les racines des congruences de degré supérieur à 2 : comme Poinsot, Galois prend en compte les racines imaginaires des congruences. Il se restreint au cas où l'équation est irréductible modulo p et de degré ν. Il indique alors une analogie possible entre les nombres complexes et les racines imaginaires de la congruence ainsi considérée :

> Dans ce cas, la congruence n'admettra donc aucune racine entière, ni même aucune racine incommensurable de degré inférieur. Il faut donc regarder les racines de cette congruence comme des espèces de symboles imaginaires, puisqu'elles ne satisfont pas aux questions de nombres entiers, symboles dont l'emploi dans le calcul sera souvent aussi utile que celui de l'imaginaire $\sqrt{-1}$ dans l'analyse ordinaire.
>
> C'est la classification de ces imaginaires et leur réduction au plus petit nombre possible, qui va nous occuper [Galois, 1830, p. 428].

Contrairement à la note publiée précédemment par Galois dans ce même tome, ce texte est un mémoire à part entière. Les démonstrations sont certes succinctes, voire incomplètes, mais Galois y expose ses principales idées et indique les méthodes employées [53]. On voit ici s'esquisser une étude qui se rapproche de la théorie actuelle des corps finis. Galois prend pour point de départ les notations de Gauss, puis continue en remplaçant le symbole $\equiv$ par le symbole $=$, sans toujours préciser quel module il considère.

Galois veut donc étudier les propriétés de l'ensemble de ces symboles imaginaires. Il considère une racine i du polynôme Fx et l'expression

$$a + a_1 i + a_2 i^2 + \ldots + a_{\nu-1} i^{\nu-1} \qquad (A)$$

des recherches de M. Galois sur la théorie des permutations et des équations algébriques » (*Bulletin de Férussac*, 1830, t. 13, p. 428). Nous renvoyons à [Ehrhardt, 2007] pour des commentaires sur cet article et sur sa reprise par Serret dans son *Cours d'algèbre supérieure.*

53. Comme nous l'avons indiqué précédemment, ce mémoire de Galois est repris en détail par Serret dans la vingt-cinquième leçon de la deuxième édition de son *Cours d'algèbre supérieure.*

où a, a_1, …, $a_{\nu-1}$ sont des nombres entiers. L'expression (A) peut prendre p^ν valeurs. En effet, comme on raisonne modulo p, les nombres a, a_1, …, $a_{\nu-1}$ sont compris entre 0 et $p-1$. En termes actuels, Galois considère ici que Fx est le polynôme minimal du nombre algébrique i, et l'ensemble des valeurs de l'expression (A) constitue le corps des racines de F, considéré comme polynôme sur $\mathbb{F}_p$.

Galois annonce qu'il veut démontrer que cet ensemble d'expressions a les « mêmes propriétés que les nombres naturels dans la *théorie des résidus des puissances* » [Galois, 1830, p. 428]. Après avoir esquissé sa méthode, inspirée notamment par les travaux de Gauss, pour déterminer les racines de ces congruences, il explique enfin comment la considération de l'ensemble des racines imaginaires des congruences lui servira dans la théorie des substitutions, et plus généralement dans la théorie algébrique des équations. Comme Gauss réindexait les racines de l'unité, solutions des équations cyclotomiques, à l'aide des racines primitives, donc utilisait les résidus et leurs propriétés pour décrire les substitutions entre racines plus efficacement, Galois utilise ses symboles imaginaires pour représenter les substitutions entre les racines d'équations algébriques.

4 - Le *Journal de Crelle* (1831-1835)

(a) Contenu

Pendant cette période, pendant laquelle, rappelons-le, le *Bulletin de Férussac* ne paraît plus, deux auteurs français (ou presque : Libri le deviendra en 1833) publient en français dans le *Journal de Crelle* : Libri et Germain. Nous commentons leurs publications respectives ci-dessous.

Mais, avant cela, évoquons brièvement les autres auteurs. Tout d'abord, tous utilisent systématiquement le symbole ≡ de Gauss, sauf Crelle lui-même qui, dans ses explications sur sa *Table des racines primitives*, emploie la notation Np pour désigner un multiple de p.

Jacobi publie un texte en lien avec les travaux de Legendre sur les formes quadratiques $x^2 + ny^2$.

Friedrich Julius Richelot 1808-1875) étudie la solution de l'équation $x^{257} = 1$ à partir de la méthode exposée par Gauss dans la section VII des *Disquisitiones Arithmeticae*, et propose une méthode de construction des racines.

Moritz Stern publie deux textes en 1832 et 1834, dans lesquels il se réfère notamment aux congruences binômes de degrés 3 et 4. Dans [Stern, 1834], il détermine le caractère quadratique de certains nombres en fonction de la forme du diviseur. Par exemple, il détermine le caractère quadratique de −3 ainsi :

Parce que l'équation $x^3 - 1 = 0$ a les trois racines

$$1, \frac{-1+\sqrt{-3}}{2}, \frac{-1-\sqrt{-3}}{2},$$

il faut que la congruence

$$x^3 - 1 \equiv 0 \pmod{p}$$

ait les trois racines

$$-1, \frac{-1+\sqrt{(mp-3)}}{2}, \frac{-1-\sqrt{(mp-3)}}{2}.$$

Mais cette congruence a trois racines réelles ou elle en a seulement une, selon que le nombre premier p est de la forme $3n+1$ ou de la forme $3n+2$. Ainsi dans le premier cas il faut qu'on ait

$$\sqrt{(mp-3)} = z$$

z désignant un nombre entier, ou bien

$$z^2 \equiv -3 \pmod{p}.$$

Dans le second cas on ne peut jamais trouver un tel nombre, c'est-à-dire : *le nombre* -3 *est un résidu ou un non-résidu quadratique du nombre premier* p *selon que ce nombre est de la forme* $3n+1$ *ou de la forme* $3n+2$ [Stern, 1834, p. 290].

Stern s'appuie donc sur une analogie entre les équations et les congruences correspondantes modulo p en ajoutant des multiples de p sous les radicaux, à la façon de Libri (auquel il se réfère plus tôt dans son article) et Poinsot. Il mène le même type de raisonnement à partir de la congruence $x^4 - 1 \equiv 0 \pmod{p}$ pour déterminer le caractère quadratique de -1. Il ne considère alors à aucun moment des racines imaginaires de congruences et ne fait aucun commentaire à ce sujet.

Enfin, Dirichlet propose en 1832 une *Démonstration d'une propriété analogue à la loi de réciprocité qui existe entre deux nombres premiers quelconques*. Dans cet article, il démontre effectivement la loi de réciprocité quadratique pour des nombres entiers complexes de la forme $a + b\sqrt{-1}$, où les nombres a et b sont entiers :

> Désignant par $\alpha + \beta\sqrt{-1}$ et $A + B\sqrt{-1}$ (β et B étant pairs et pouvant se réduire à zéro) deux nombres premiers complexes [54], le premier sera ou ne sera pas résidu quadratique du second, selon que le second est ou n'est pas résidu quadratique du premier [Dirichlet, 1832, p. 389].

Dirichlet aboutit à cet énoncé à la fin de son mémoire. Les nombres entiers complexes considérés ici ont précédemment été introduits par Gauss dans [Gauss, 1828] et

54. Gauss définit les nombres premiers entiers complexes de manière analogue aux nombres premiers naturels : un nombre premier complexe est un nombre dont les diviseurs sont les unités, et le produit de ce nombre par les unités.

[Gauss, 1832]. Dans son étude, Dirichlet transpose lui aussi à ces nombres entiers complexes les définitions des notions utilisées habituellement pour les entiers ordinaires dans le cadre de la théorie des résidus quadratiques (nombre premier, congruence, résidu quadratique). En introduction, il commente d'ailleurs l'analogie existant entre les nombres entiers réels et ces nouveaux nombres entiers :

> Dans un mémoire qui vient d'être publié dans le recueil de la société royale de Gottingue, Mr. Gauss a étendu le domaine de l'analyse indéterminée aux expressions de la forme $t + u\sqrt{-1}$, t et u désignant des nombres entiers positifs ou négatifs. Ce grand géomètre a reconnu que les expressions de cette espèce se rapprochent entièrement par leurs propriétés des nombres entiers réels qu'elles comprennent d'ailleurs comme cas particulier. L'analogie qui existe à cet égard est telle, que les énoncés des théorèmes connus relatifs aux entiers réels peuvent être transportés pour la plupart presque littéralement dans la théorie des nombres ainsi généralisée. Il n'en est pas de même des démonstrations qui paraissent présenter de nouvelles difficultés si l'on excepte les théorèmes très simples qui dérivent immédiatement des notions fondamentales [Dirichlet, 1832, p. 370] .

Cela semble être le premier texte en français contenant une étude de ce qu'on appelle aujourd'hui les entiers de Gauss. Comme nous le verrons dans le section suivante, la théorie des nombres entiers complexes fait partie de nombreux articles du *Journal de Crelle* après 1835 ; certains sont d'ailleurs traduits puis insérés dans un autre périodique français : le *Journal de Liouville*.

(b) Sophie Germain et le dernier théorème de Fermat

D'après son ami Libri, Sophie Germain [55] a dû se former seule et en cachette aux mathématiques, jusqu'à un niveau universitaire, car s'intéresser aux mathématiques était alors socialement incompréhensible et inadmissible pour une jeune femme. Elle s'est fait passer pour un vrai étudiant de l'École Polytechnique, nommé Leblanc, pour communiquer quelques recherches à l'illustre Lagrange. C'est également sous ce nom qu'elle débute en 1804 sa correspondance avec Gauss [56], qui apprend sa véritable identité en 1807. Elle a également échangé des lettres avec Legendre, Libri et Poinsot. De son vivant, Sophie Germain a été surtout reconnue pour ses travaux en physique mathématique [57] mais, comme elle le remarque dans sa correspondance, son premier amour mathématique reste la théorie des nombres [58].

55. Plusieurs travaux lui ont été consacrés : [Libri, 1832b], [Stupuy, 1879], [Hill, 1995]. Ses travaux inédits sur le théorème de Fermat sont étudiés dans [Del Centina, 2005], [Del Centina, 2008] et [Laubenbacher et Pengelley, 2010], où est aussi publiée une partie de sa correspondance et de ses manuscrits.

56. Voir [Laubenbacher et Pengelley, 2010, p. 18 - 24] pour un aperçu de la correspondance entre Gauss et Germain.

57. Voir en particulier [Bucciarelli, 1980].

58. Dans une lettre à Gauss datée du 12 mai 1819, Sophie Germain remarque :

Si on se limite aux publications, on trouve deux témoins de l'activité arithmétique de Sophie Germain en théorie des nombres : dans [Legendre, 1827], l'auteur attribue la démonstration d'un résultat à Sophie Germain. D'autre part, la mathématicienne aborde l'équation $\frac{4(x^p-1)}{x-1} = y^2 \pm pz^2$, dans un court article publié en 1831 dans le *Journal de Crelle*. L'objectif de Sophie Germain est de déterminer l'expression en x de y et z dans les équations $\frac{4(x^p-1)}{x-1} = y^2 \pm pz^2$ et $\frac{4(x^{p^2}-1)}{x-1} = y^2 \pm pz^2$. Pour cela, elle s'appuie sur un résultat de Legendre [59] :

> Mr. Le Gendre a remarqué (Théorie des Nombres, 1830, T. 2. No. 512.) que dans l'équation $\frac{4(x^p-1)}{x-1} = y^2 \pm pz^2$, due à M. Gauss, les coefficiens des diverses puissances de x dont se compose la valeur de y sont congrus mod p aux coefficiens des mêmes puissances, dans le développement de $2(x-1)^{\frac{p-1}{2}}$ [Germain, 1831, p. 201].

Germain en déduit alors des expressions explicites des valeurs de y et de z. Cette courte note nous apprend que Sophie Germain est familière avec certaines notations et le vocabulaire introduits par Gauss (elle utilise en effet l'expression "congru (mod p)") mais elle ne nous indique pas comment la mathématicienne utilise les résidus et les congruences. Pourtant, plusieurs sources indiquent sa connaissance approfondie des *Disquisitiones Arithmeticae* de Gauss. Dans [Goldstein et Schappacher, 2007a, p. 20], les auteurs observent qu'elle utilise les congruences dans ses recherches manuscrites sur le dernier théorème de Fermat et qu'elle donne une nouvelle démonstration du caractère quadratique de 2. D'autre part, on trouve dans sa correspondance avec Gauss des observations allant également dans ce sens. Dans une lettre datée du 3 septembre 1805, destinée à Wilhelm Olbers, Gauss observe :

> À la suite de plusieurs circonstances - en partie à cause de plusieurs lettres de Le Blanc à Paris qui étudie mes *Disquisitiones Arithmeticae* avec une vraie passion, s'est complètement familiarisé avec elles, et m'a communiqué à leur propos quelques jolies remarques ; en partie à cause de la présence d'un ami qui est aussi en train d'étudier cet ouvrage et me demande souvent conseil - et en partie aussi à cause d'une sorte de fatigue, ou au moins de lassitude vis à vis des mornes calculs mécaniques, je me suis laissé entraîner à [les] abandonner pour le moment et à reprendre mes chères recherches arithmétiques.

Ces indications nous amènent à donner un rapide aperçu des méthodes générales qu'elle

---

> Quoique j'ai travaillé pendant quelques tem[p]s à la théorie des surfaces vibrantes [...] je n'ai jamais cessé de penser à la théorie des nombres. Je vous donnerai une idée de ma préoccupation pour ce genre de recherches en vous avouant que même sans aucune espérance de succès je la préfère à un travail qui me donnerait nécessairement un résultat et qui pourtant m'intéresse... quand j'y pense.

Cette lettre est reproduite dans [Del Centina, 2008]. Nous avons également reproduit les corrections apportées par l'auteur entre crochets.

59. Legendre formule ce résultat sans les congruences (il considère un nombre premier n de la forme $2m+1$) : « Omettant dans cette équation les multiples de n, on aura $(x-1)Y^2 = 4(x-1)^n$ d'où l'on tire $Y^2 = 4(x-1)^{2m}$ et $Y = 2(x-1)^m$ » [Legendre, 1830, t. 2, art. 512].

développe en lien avec le dernier théorème de Fermat, qui sont notamment étudiées dans [Del Centina, 2008] et [Laubenbacher et Pengelley, 2010][60].

Dans une lettre à Gauss du 12 mai 1819, Sophie Germain le félicite pour son idée de représenter les congruences par le symbole ≡ et lui indique également qu'elle est persuadée depuis longtemps qu'il existe une connexion entre le dernier théorème de Fermat et la théorie des résidus. Elle donne l'idée générale de sa méthode[61] :

> Voici ce que j'ai trouvé :
>
> L'ordre dans lequel les résidus (puissances égales à l'exposant) se trouvent placés dans la série des nombres naturels détermine les diviseurs nécessaires qui appartiennent aux nombres entre lesquels on établit non seulement l'équation de Fermat mais encore beaucoup d'autres équations analogues à celle-là.

Elle affirme en effet que si l'équation $x^p + y^p = z^p$ admet une solution entière (x, y, z), alors tout nombre premier de la forme $\theta = 2Np + 1$, où N est un nombre entier, tel qu'il n'existe pas deux résidus non nuls p^{e} consécutifs modulo θ, divise nécessairement un des nombres x, y ou z. En effet, dans le cas contraire, on a la congruence $1 \equiv r^{sp} + r^{tp}$, ce qui implique l'existence de deux résidus p^{e} non nuls consécutifs[62]. L'objectif de Sophie Germain est donc de démontrer qu'il existe une infinité de nombres θ.

Plus loin dans la même lettre, Sophie Germain précise que c'est notamment le mémoire de Poinsot sur les congruences binômes [Poinsot, 1820] qui l'a aidée à percevoir « la métaphysique de [sa] méthode ». Elle le joint d'ailleurs à sa lettre pour que Gauss puisse en prendre connaissance. En effet, dans une lettre à Poinsot[63], datée du 2 juillet 1819, Sophie Germain le félicite d'une part pour l'utilisation des racines imaginaires dans la théorie des congruences et d'autre part pour ses réflexions sur les différents ordres que l'on obtient par la considération des racines des congruences binômes.

Les auteurs de [Laubenbacher et Pengelley, 2010] indiquent que, dans le manuscrit[64] intitulé *Remarque sur l'impossibilité de satisfaire en nombres entiers à l'équation* $x^p + y^p = z^p$, Sophie Germain commence par déterminer des conséquences générales de

60. Nous renvoyons d'ailleurs à ces deux textes pour des analyses approfondies et complémentaires des activités de Sophie Germain en lien avec la théorie des nombres.

61. On retrouve notamment une transcription de ce passage dans [Del Centina, 2008].

62. En effet, si θ ne divise aucun des nombres x, y, z, alors on peut par exemple diviser la congruence $x^p + y^p \equiv z^p \pmod{\theta}$ par x^p. Comme θ est premier, x admet un inverse et y/x, z/x sont donc congrus à deux nombres non nuls, qui peuvent être exprimés à l'aide de puissances d'une racine primitive r : r^s et r^t. On obtient ainsi : $(r^s)^p - (r^t)^p \equiv 1 \pmod{\theta}$.

63. Voir [Del Centina, 2005].

64. Il existe deux copies de ce manuscrit à la Bibliothèque Moreniana de Florence et à la Bibliothèque Nationale de Paris. C'est principalement à partir de ce texte que le travail de Germain sur le dernier théorème de Fermat est étudié dans [Del Centina, 2008] et [Laubenbacher et Pengelley, 2010]. En se basant sur le contenu de la correspondance de Sophie Germain, les auteurs de [Del Centina, 2008] supposent que ce mémoire a été écrit entre 1819 et 1820. Il semble que ce manuscrit a même été écrit bien plus tôt : les auteurs de [Laubenbacher et Pengelley, 2010] remarquent en effet que dans sa lettre de 1819, Sophie Germain se réfère à un résultat contenu dans ce manuscrit, et indique qu'il est « [extrait] d'une note déjà ancienne ».

l'existence de deux résidus p^{e} consécutifs modulo θ, pour établir ce qu'ils notent la "condition N-C" pour plusieurs valeurs de N et de p (avec $\theta = 2Np + 1$) : « Condition N-C (Non-Consecutivity). There do not exist two nonzero consecutive p^{th} power residues, modulo θ » [Laubenbacher et Pengelley, 2010, p. 25] . Ils observent d'ailleurs qu'à cette occasion, Sophie Germain est familière avec ce que l'on appelle aujourd'hui la structure cyclique des racines de l'unité :

> She employs throughout the notion and notation of congruences introduced by Gauss, and utilizes to great effect a keen understanding that the $2Np$ multiplicative units mod θ are cyclic, generated by a primitive $2Np$-th root of unity, enabling her to engage in detailed analyses of the relative placement of the nonzero p-th powers (i.e., the $2N$-th roots of 1) amongst the residues. She is acutely aware (expressed by us in modern terms) that subgroups of the group of units are also cyclic, and of their orders and interrelationships, and uses this in a detailed way [Laubenbacher et Pengelley, 2010, p. 27-28].

Comme nous le verrons dans la partie 3, Louis Poinsot insiste tout particulièrement sur les relations existant entre les racines de l'unité dans ses travaux, en représentant la structure de leur ensemble comme des objets placés équitablement autour d'un cercle.

Ainsi, même si le grand programme élaboré par Sophie Germain n'est finalement pas valide[65], ses recherches autour du dernier théorème de Fermat témoignent d'une connaissance approfondie des résidus de puissances de nombres premiers et de tentatives pour en explorer de nouvelles propriétés.

(c) Guglielmo Libri : les congruences comme application analytique

Issue d'une famille appartenant à la vieille noblesse toscane, Libri[66] apprend jeune l'anglais, le français et un peu l'allemand. Il intègre l'Université de Pise en 1816. En 1820, il obtient son doctorat et publie son mémoire de théorie des nombres *Memoria sopra la teoria die numeri*, pour lequel il est félicité par Babbage, Cauchy et Gauss. En 1823, Libri devient professeur de physique mathématique à l'Université de Pise. De 1824 à 1825, il effectue son premier voyage à Paris, dont le but originel est d'aider à la libération de son père de prison. Il est présenté à l'Académie des Sciences par Alexander von Humboldt, et rencontre de nombreux savants, comme Laplace et Fourier par exemple, ainsi que des hommes politiques. Son séjour à Paris a donc été l'occasion pour Libri d'établir un réseau de contacts très important, qui lui sert pendant les années suivantes. Il reste alors en Toscane jusqu'en 1830 mais en est exilé de 1831 à 1832, après avoir été impliqué dans une conspiration politique. Il fuit alors en France, devenant citoyen français et entrant le 18 mars de la même année à l'Académie des Sciences[67], en remplacement de Legendre. Élu

65. Voir [Laubenbacher et Pengelley, 2010] à ce sujet.
66. Ces quelques indications biographiques sont issues de [Maccioni Ruju et Mostert, 1995].
67. Libri est déjà membre correspondant de l'Académie des Sciences depuis le 31 décembre 1832.

au Collège de France contre Cauchy et Liouville, il se fit de nombreux ennemis au sein même de l'Académie. De 1838 à 1841, son principal travail fut une imposante histoire des mathématiques italiennes, très érudite, et il fut nommé Inspecteur des bibliothèques de France, en partie avec le soutien de son ami Guizot. Il semble s'être livré alors à un pillage important des collections, et avec le changement de régime en 1848, il est accusé de vol de livres et de manuscrits et fuit à Londres.

Nous avons inclus Libri dans notre groupe de savants de la scène française car c'est dans ce milieu qu'il travaille sur la théorie des nombres et il publie en français. Nous verrons plus loin que la nature même de son travail est aussi cohérente avec celle d'autres acteurs de cette scène. Libri présente d'ailleurs deux mémoires intitulés *Théorie des nombres* à l'Académie des Sciences de Paris[68] le 12 janvier 1824 et le 13 juin 1825. Ampère et Cauchy lisent les rapports correspondants le 9 août 1824 et le 13 mars 1826. Dans les deux cas, il est convenu que le mémoire de Libri sera inséré dans les *Mémoires* des savants étrangers ; un *Mémoire sur la théorie des nombres* y est effectivement publié, en 1838. D'après les rapports fournis par Cauchy et Ampère, il est vraisemblable qu'une partie des travaux présentée par Libri à l'Académie soit reproduite dans [Libri, 1832a] ; Libri conclut d'ailleurs ce dernier mémoire en indiquant que les résultats qui y sont développés ont été présentés en 1823 et 1825 à l'Académie des Sciences de Paris.

Le *Mémoire sur la théorie des nombres* dont nous allons donner un aperçu ici a été quant à lui publié en trois parties dans le neuvième tome du *Journal de Crelle* en 1832 ; ce même texte est également inséré avec d'autres mémoires du même auteur dans un ouvrage de Libri, publié en 1829 : [Libri, 1829]. La préface de ce livre donne des indications importantes sur la position de Libri par rapport à la théorie des nombres :

> Dès mes premiers pas dans l'étude des mathématiques, m'étant spécialement occupé de la théorie des nombres, je pensai que les obstacles que l'on rencontrait en traitant les problèmes numériques venaient, pour la plupart, du manque de méthode, et de l'état d'isolement dans lequel se trouvait cette branche de l'algèbre ; je dirigeai par conséquent mes efforts vers l'unique but de découvrir un principe général qui renfermât toute la théorie des nombres[...]
>
> En réunissant peu à peu tous ces matériaux, je m'aperçus que l'analyse indéterminée n'était qu'une branche de la théorie générale des fonctions entières ; théorie qui est du plus haut intérêt dans les mathématiques. En effet, elle renferme l'analyse indéterminée, le développement des fonctions, l'intégration des équations aux différences (et par conséquent l'intégration des équations différentielles), la résolution des équations numériques, la théorie des fonctions discontinues, le calcul des probabilités, et enfin une théorie nouvelle et fort délicate sur la comparaison des différens ordres d'irrationalité ; théorie qui sert à résoudre un grand nombre de questions importantes [Libri, 1829, p. v-vi].

68. L'Académie des Sciences reçoit également un *Memoria sopra la teoria dei numeri* le 22 janvier 1821, et un rapport en est fait par Cauchy le 19 janvier 1821.

Dans cette citation, on retrouve deux caractéristiques de l'activité arithmétique de Libri.

D'une part, son approche est analytique dans le sens où il veut ramener la théorie des nombres à un *principe général* et en déduire les différentes propositions particulières. Il fait également une remarque dans ce sens dans son mémoire : « L'analyse succincte que nous venons de donner de notre mémoire suffit pour montrer la possibilité de déduire d'un seul principe général toute la théorie des nombres » [Libri, 1832a, p. 58]. Remarquons par ailleurs que Libri énonce régulièrement des principes généraux et leurs conséquences sans démonstration complète, voire sans démonstration du tout. Il indique à ce sujet dans sa préface de [Libri, 1829] : « Ce volume ne renferme que des préliminaires, et je me suis attaché surtout à traiter les problèmes dont la résolution pourra m'être nécessaire dans la suite. J'ai négligé les détails, parce que je n'écrivais point un livre élémentaire, et j'ai tâché plutôt de faire saisir l'esprit de mes méthodes que d'en développer toutes les parties » [Libri, 1829, p. viii]. Sa dernière phrase sur les ordres d'irrationalité est également très intéressante puisqu'elle rappelle des questions soulevées notamment par Galois, puis par Hermite et Jordan sur la classification des irrationnelles [69]. Nous n'avons malheureusement pas retrouvé d'autres mentions à ces *ordres d'irrationalité* dans les travaux de Libri.

D'autre part, pour Libri, la théorie des nombres (qui semble être synonyme d'analyse indéterminée ici), est une branche de l'algèbre, qui doit être rattachée à d'autres parties des mathématiques pour sortir de son isolement. Le diagnostic est courant au début du XIX^{e} siècle, l'accueil favorable fait en France aux *Disquisitiones arithmeticae* de Gauss étant souvent lié explicitement à l'usage que Gauss fait de l'arithmétique dans la résolution des équations algébriques. En identifiant l'analyse indéterminée à la théorie des fonctions entières, Libri poursuit des objectifs perçus comme proches à cette époque de redéfinition de l'analyse. Il annonce d'ailleurs dans son mémoire qu'il montrera ultérieurement comment la théorie des nombres peut être appliquée à d'autres branches de l'analyse :

> En liant la théorie des nombres à d'autres parties de l'analyse, il était certain que, comme celles-ci contribueraient à son perfectionnement, elles en recevraient des secours ; et c'est ce que nous montrerons dans la suite de ces recherches à l'égard des intégrales définies et fonctions circulaires, dont plusieurs propriétés remarquables et inconnues jusqu'à présent, découlent de l'analyse indéterminée [Libri, 1832a, p. 58].

Ces deux caractéristiques se déclinent ensuite à plusieurs niveaux. Par exemple, Libri explicite le statut qu'il donne aux congruences à plusieurs reprises : ce sont pour lui des cas particuliers d'équations indéterminées. Il annonce ainsi dans l'introduction de son mémoire :

> Cependant pour qu'on ne puisse pas croire que notre théorie n'est pas susceptible d'être appliquée aux problèmes particuliers, et pour montrer de quelle manière nos formules peuvent se simplifier dans le plus grand nombre des cas, nous considérons

69. Cf. [Brechenmacher, 2011].

spécialement dans ce mémoire les équations qui sont du premier degré par rapport à une des inconnues, et que M. Gauss a appelées congruences[Libri, 1832a, p. 56].

Ou encore, son diagnostic sur les raisons de l'isolement de la théorie des nombres par rapport aux autres branches de l'analyse :

> De sorte que la théorie des nombres presqu'immobile au milieu des progrès des autres parties de l'analyse, qu'elle avait vu naître et s'élever successivement, s'en trouvait séparée et ne partageait pas leur perfectionnement commun. Cet isolement, qui forme la difficulté principale de la théorie des nombres, dépend de la méthode que l'on a suivie jusqu'ici pour mettre en équation les problèmes d'analyse indéterminée ; car en exprimant seulement les relations qui doivent exister entre les valeurs des inconnues, on a toujours négligé de représenter par des signes algébriques les conditions auxquelles ces inconnues doivent satisfaire, afin qu'elles soient des nombres entiers ou rationnels [Libri, 1832a, p. 54].

Libri insiste ici sur la nécessité d'exprimer algébriquement la nature particulière des racines des équations indéterminées. Il ne s'agit donc pas d'appliquer l'arithmétique à l'algèbre, comme chez Gauss, ou de trouver des relations entre questions arithmétiques et quantités algébriques, comme dans la formule des classes de Dirichlet, mais de traduire des conditions proprement arithmétiques (en l'occurrence l'intégralité) de manière algébrico-analytique. La tension entre arithmétique et algèbre que cette question révèle est apparente dès le XVII^{e} siècle, comme cela est analysé dans [Goldstein, 1995] :

> Une partie du message de Fermat sur les entiers, pourtant, a été entendu, si l'on en juge par les efforts déployés par ses successeurs pour attraper les solutions entières dans les questions d'analyse diophantienne, les remarques au détour des lettres. Mais il ne s'agit pas tant de mettre au point des méthodes démonstratives particulières ou de repenser celles offertes par le modèle euclidien : il s'agit de donner des solutions générales, ce qui signifie alors algébriques, sous une forme permettant de déduire les solutions entières par des restrictions sur les valeurs possibles des indéterminées ou l'élimination des dénominateurs [Goldstein, 1995, p. 172].

La conception de Libri est différente : il propose d'exprimer directement le fait d'être entier à l'aide des fonctions circulaires, tout en évitant par ailleurs le recours à des outils comme les racines primitives :

> La formule qui sert de base à notre théorie, et qui établit un rapport si singulier entre les solutions des congruences et les fonctions circulaires, fournit le moyen de résoudre directement les équations à deux termes. M. Gauss qui a découvert le premier cette résolution par une méthode particulière, et Lagrange qui l'a ramenée ensuite à sa théorie générale des équations, ont supposé la connaissance des racines primitives. La théorie que nous exposons dans ce mémoire est indépendante de cette recherche, et d'ailleurs elle est beaucoup plus simple que les méthodes trouvées par ces deux grands géomètres, qui exigent de très-longs calculs pour être appliquées [Libri, 1832a, p. 57].

Libri va ainsi exhiber des équations supplémentaires permettant d'exprimer le fait que les racines des équations diophantiennes cherchées doivent être entières. Par exemple, il considère une équation $\varphi(x, y, z, \ldots) = 0$, qu'il note $\varphi = 0$. Pour traduire le fait que les nombres x, y, z ..., doivent être entiers, il propose de prendre en compte aussi les équations $\sin x\pi = 0$, $\sin y\pi = 0$, $\sin z\pi = 0$, ... Ou encore, cherchant des racines entières telle que la première inconnue x soit inférieure à a par exemple, il remarque que x doit vérifier l'équation $x(x-1)(x-2)\ldots(x-(a-1)) = 0$. Après quelques formules générales déduites de ces considérations, Libri applique son principe au cas particulier des congruences : « Mais nous nous réservons de donner cette théorie générale dans une autre occasion, et nous nous bornerons pour le moment à considérer les équations dans lesquelles l'une des inconnues est élevée seulement au premier degré, et que M. Gauss a nommé congruences » [Libri, 1832a, p. 64].

Il considère donc la congruence $x^m + A_1x^{m-1} + A_2x^{m-2} + \ldots + A_{m-1}x + A_m \equiv 0 \pmod{p}$, et en raisonnant comme pour des équations, obtient les égalités liant les coefficients et les racines de cette congruence. Il en déduit le petit théorème de Fermat, ainsi que le théorème de Wilson. Il rappelle également le résultat énoncé par Poinsot dans [Poinsot, 1820] selon lequel les racines de la congruence $x^n - 1 \equiv 0 \pmod{np+1}$ « se déduisent des racines de l'équation $x^n - 1 = 0$, en ajoutant des multiples de $np + 1$ sous les radicaux compris dans l'expression de ces racines » [Libri, 1832a, p. 67] et donne une version généralisée de cette proposition. Remarquons toutefois que, contrairement à Poinsot, Libri ne fait ici aucune remarque sur l'éventuelle existence de racines imaginaires de congruence.

À partir de ses raisonnements sur les fonctions circulaires, Libri traduit plusieurs résultats de théorie des nombres en termes de sommes de fonctions. Ainsi, la somme des diviseurs de n, compris entre 1 et m est égale à :

$$\sum_{x=1}^{x=m+1}\sum_{y=0}^{y=x}\cos\frac{2ny\pi}{x} = \sum_{x=1}^{x=m+1}\frac{\sin 2\left(n-\frac{n}{2x}\right)\pi + \sin\frac{n\pi}{x}}{2\sin\frac{n\pi}{x}}.$$

Un résultat fondamental que Libri obtient est une formule générale, notée (24), permettant de connaître le nombre N de solutions de la congruence $\varphi(x, y, z, \ldots) \equiv 0 \pmod{m}$:

$$N = \frac{1}{m}\sum_{x=0}^{x=m}\sum_{y=0}^{y=m}\sum_{z=0}^{z=m}\ldots\left(1 + \cos\frac{2\varphi\pi}{m} + \cos\frac{4\varphi\pi}{m} + \ldots + \cos\frac{2u\varphi\pi}{m}\ldots + \cos\frac{2(m-1)\varphi\pi}{m}\right).$$

Il applique cette formule dans le cas des congruences du premier degré à une inconnue : $ax + b \equiv 0 \pmod{c}$. On a dans ce cas :

$$N = \frac{1}{c}\sum_{x=0}^{x=c}\left(1 + \cos 2(ax+b)\frac{\pi}{c}\ldots + \cos 2u(ax+b)\frac{\pi}{c}\ldots + \cos 2(c-1)(ax+b)\frac{\pi}{c}\right).$$

Il en déduit que :

- cette congruence a toujours une « solution entière et plus petite que c » [Libri, 1832a, p. 170] lorsque a et c sont premiers entre eux ;
- la congruence n'admet aucune solution entière lorsque le PGCD g de a et c est différent de l'unité et ne divise pas b ;
- la congruence admet g solution entières et inférieures à c si $\frac{b}{g}$ est un nombre entier.

Libri aborde ensuite le cas des congruences quadratiques. Il rappelle quelques propriétés des résidus quadratiques et en déduit des égalités en lien avec les sommes quadratiques de Gauss. Il indique d'ailleurs que les sommes quadratiques de Gauss sont « la base de tout ce que l'on sait sur les congruences du second degré » [Libri, 1832a, p. 177].

À partir de la formule (24) et des résultats précédents, Libri donne une formule donnant le nombre de solutions de la congruence $x^2 + ay^2 + b \equiv 0 \pmod{n}$, obtient des valeurs de nN et conclut que la congruence en question a toujours $n \pm 1$ solutions, le signe dépendant du caractère quadratique de a et b.

Dans la dernière partie de son mémoire, Libri traite plus généralement de la congruence $x^a + u^a + 1 \equiv 0 \pmod{n}$. Il note N_2, le nombre de solutions entières positives et inférieures à n de cette congruence à deux inconnues, et trouve :

$$nN_2 = \sum_{y=0}^{y=n} \sum_{x=0}^{x=n} \sum_{u=0}^{u=n} \left(\cos 2y(x^a + u^a + 1)\frac{\pi}{n} + \sqrt{-1} \sin 2y(x^a + u^a + 1)\frac{\pi}{n} \right).$$

Il en déduit des résultats sur l'équation binôme et sur les congruences cubiques et quadratiques. Nous nous arrêtons sur ces deux derniers cas.

Libri commence par considérer l'équation cubique $x^3 \equiv 1 \pmod{n}$, où n est de forme $6p+1$, rappelle que cette congruence admet toujours trois solutions entières et en déduit des relations sur les sommes cubiques de Gauss. Puis il détermine le nombre N_2 de solutions de la congruence $x^3 + y^3 + 1 \equiv 0 \pmod{n}$ et rappelle que lorsque n est de la forme $6n + 1$, alors il existe un unique couple d'entiers (a, b) tels que $4n = a^2 + 27b^2$. Il montre que $N_2 = n \pm a - 2$, et remarque ainsi que le nombre N_2 augmente avec n. De plus, le fait que le nombre a intervienne dans l'égalité précédente implique un résultat important sur les congruences cubiques :

> Ainsi, lorsqu'il s'agit des congruences du troisième degré, il ne suffit plus, pour trouver le nombre de leurs solutions, de connaître la forme linéaire des nombres premiers qui servent de module, mais il faut connaître aussi l'un des nombres de la forme quadratique à laquelle ces modules peuvent se réduire... [Libri, 1832a, p. 271].

Après avoir obtenu des résultats analogues pour les congruences quadratiques, Libri conclut de manière plus générale :

> On pourrait démontrer qu'étant donnée la congruence à deux inconnues
>
> $$x^n + y^n + 1 \equiv 0 \pmod{p},$$

dans laquelle p est un nombre premier quelconque, on pourra toujours assigner une limite p telle, que passé cette limite le nombre des solutions de cette congruence ira toujours en augmentant. Ce théorème n'est pas sans importance pour parvenir à la démonstration de l'impossibilité de résoudre l'équation

$$u^n + v^n = z^n,$$

en nombres entiers. Car il prouve qu'on tenterait en vain de démontrer cette impossibilité, en voulant établir que si cette équation était résoluble, l'une des inconnues serait divisible par un nombre infini de nombres premiers. Nous faisons cette observation, parce que nous avons motif de croire que plusieurs analystes ont tenté ce genre de démonstration... [Libri, 1832a, p. 275].

Cette évocation des méthodes utilisées pour démontrer le dernier théorème de Fermat semble se référer au programme de Sophie Germain, comme nous l'avons vu précédemment [70]. Elle témoigne une fois encore que l'objet au centre de l'intérêt commun est l'équation algébrique (ou plus encore des familles d'équations).

Ces commentaires suggèrent qu'il n'y a pas de discipline propre liée aux congruences pour Libri : les congruences sont un cas particulier d'équations indéterminées, qui sont les objets de l'analyse indéterminée, qui est elle-même une branche de l'analyse algébrique. On ne retrouve par exemple aucune réflexion sur la structure des congruences (stabilité par addition, multiplication, ...) et Libri rejette explicitement des outils arithmétiques fondamentaux, comme les racines primitives : son objectif est de réussir à obtenir toutes les propriétés de la théorie des nombres à partir de la considération de fonctions de l'analyse. Nous n'étudierons pas de manière plus approfondie les travaux de Libri en théorie des nombres. Rappelons néanmoins qu'il obtient plusieurs résultats intéressants, en particulier des formules donnant le nombre de racines d'une congruence ou le nombre de diviseurs d'un nombre donné.

5 - Les *Exercices de Mathématiques* de Cauchy

(a) *Sur diverses propositions relatives à l'algèbre et à la théorie des nombres*, ou des propriétés analogues des équations et des congruences

Ce Mémoire, publié en 1829 dans les *Exercices de mathématiques*, contient 17 théorèmes ainsi que des corollaires. Cauchy le présente comme un travail préliminaire, dont il utilisera les résultats pour la résolution d'équations indéterminées.

Dans l'introduction, Cauchy remarque : « il existe des relations dignes de remarque entre les quantités désignées dans la théorie des nombres sous le nom de *racines primitives*

70. Voir notamment [Laubenbacher et Pengelley, 2010, p. 31-32].

et d'autres quantités que renferment les produits de certaines expressions algébriques » [Cauchy, 1829b, page 259].

Les congruences apparaissent dans ce texte, mais Cauchy les nomme *équivalences*, même si, comme dans le *Bulletin de Férussac*, il utilise pour les indiquer la notation de Gauss. Il se réfère à leur propos aux travaux d'Euler, Lagrange, Gauss, Legendre, Poinsot et Libri.

Les quatre premiers théorèmes portent sur le nombre de racines d'une congruence d'un degré donné : modulo un nombre premier p, une congruence de degré m admet au plus m racines distinctes, et la congruence binôme $x^n \equiv 1 \pmod{p}$ admet exactement n racines quand n divise $p-1$. Cauchy en déduit une démonstration du théorème de Wilson. Les théorèmes suivants mettent particulièrement en relief les analogies entre les équations et les congruences (bien que, encore une fois, Cauchy ne prenne pas en compte les racines imaginaires de congruences, comme pouvait le faire Poinsot). Par exemple, voici le théorème VI :

Théorème VI. - *Soit n un nombre entier quelconque. L'équation*

$$x^n = 1 \tag{2}$$

admettra autant de racines primitives qu'il y a de nombres entiers premiers à n, mais inférieurs à n ; et si l'on suppose

$$n = a^\alpha b^\beta c^\gamma \ldots, \tag{34}$$

a, b, $c\ldots$ étant les facteurs premiers de n, chacune des racines primitives de l'équation (2) sera le produit de plusieurs facteurs u, v, w, $\ldots$, qui serviront de racines primitives aux équations

$$u^{a^\alpha} = 1, \quad v^{b^\beta} = 1, \quad w^{c^\gamma} = 1, \ldots \tag{35}$$

Dans une scholie, Cauchy explique comment obtenir toutes les racines primitives à partir d'une seule. Le théorème VII est l'analogue du théorème VI pour les congruences :

Théorème VII. - *Soit p un nombre premier quelconque et n un nombre entier diviseur de $p-1$. L'équivalence*

$$x^n \equiv 1 \pmod{p} \tag{3}$$

admettra autant de racines primitives qu'il y a de nombres entiers premiers à n, mais inférieurs à n ; et si l'on suppose

$$n = a^{\alpha} b^{\beta} c^{\gamma} \ldots, \tag{34}$$

a, b, c... étant les facteurs premiers de n, chacune des racines primitives de l'équivalence (3) sera le produit de plusieurs facteurs u, v, w, ..., qui serviront de racines primitives aux équations

$$u^{a^{\alpha}} \equiv 1, \quad v^{b^{\beta}} \equiv 1, \quad w^{c^{\gamma}} \equiv 1, \ldots \pmod{p}. \tag{35}$$

Cauchy se contente alors de renvoyer le lecteur à la démonstration du théorème précédent : « pour établir le théorème VII, il suffit de remplacer, dans la démonstration que nous avons donnée du théorème VI, le signe = par le signe ≡, en prenant le nombre p pour module » [Cauchy, 1829b, p. 272].

La suite du mémoire étudie les sommes de racines primitives de certaines congruences, ainsi que des équations algébriques (et les congruences correspondantes) liées aux fonctions symétriques.

(b) *Sur la résolution des équivalences dont les modules se réduisent à des nombres premiers*

Ce mémoire fait également partie du quatrième volume des *Exercices de mathématiques* et se partage en trois paragraphes : le premier contient des *Considérations générales* sur les équivalences, le second est consacré aux équations binômes tandis que le troisième traite de la *résolution des équivalences du troisième et du quatrième degré*. Les théorèmes démontrés dans l'article précédent sont effectivement utilisés dans plusieurs démonstrations.

Cauchy considère dans un premier temps l'équivalence $a_0 x^m + a_1 x^{m-1} + a_2 x^{m-2} + \ldots + a_{m-1} x + a_m \equiv 0 \pmod{p}$, où p est un nombre premier, m un nombre entier, inférieur à p, les a_i sont des quantités entières ou rationnelles dont les dénominateurs ne sont pas divisibles par p. (Dans le dernier cas, on peut toujours se ramener à une équivalence dont les coefficients seront des nombres entiers). Il pose :

$$f(x) = a_0 x^m + a_1 x^{m-1} + a_2 x^{m-2} + \ldots + a_{m-1} x + a_m.$$

Si r est une racine de l'équivalence, alors on a :

$$f(x) = f(r) + (x-r) f'(r) + (x-r)^2 \frac{f''(r)}{1.2} + \ldots + (x-r)^m \frac{f^{(m)}(r)}{1.2.3.m}$$

(c'est l'application de la formule de Taylor-Lagrange à la fonction f).

Dans le deuxième paragraphe, Cauchy travaille sur le nombre de racines d'une congruence binôme ou d'une congruence du second degré et donne plusieurs exemples concrets de résolution de telles congruences, à l'aide de tables d'indices. Il précise qu'une méthode similaire a déjà été présentée par Gauss en 1801, ainsi que par Libri.

Dans le dernier paragraphe, Cauchy explique dans un premier temps que son étude peut se restreindre à la résolution des congruences du troisième degré admettant trois racines distinctes, et à celle des congruences du quatrième degré admettant quatre racines distinctes. En effet, d'après les résultats obtenus dans la première partie de ce mémoire, une congruence du n^{e} degré n'admettant pas n racines distinctes peut être réduite à une congruence d'un degré inférieur ou n'admet aucune racine. Il expose ensuite une méthode pour résoudre chacun des cas, et l'illustre avec des exemples. Là encore, il utilise des méthodes similaires à celles employées pour résoudre les équations du troisième et du quatrième degrés.

6 - Retour sur le *Bulletin de Férussac* : un premier bilan

Lorsque l'on compare la liste des entrées sur les résidus et les congruences trouvées dans le *Bulletin de Férussac* avec notre corpus pour la période[71] 1824-1830, et si on met de côté les articles du *Journal de Crelle* correspondant à des solutions de problèmes posés dans ce même périodique, voici les seuls textes dont le *Bulletin* ne rend pas compte :

- une note de deux pages sur le théorème de Wilson de Verhulst, publiée en 1827 dans la *Correspondance mathématique et physique* de Quételet ;
- la première partie du travail sur les résidus biquadratiques de Gauss, présentée en 1825 à l'Académie de Göttingen puis publiée en 1828 dans les mémoires de cette académie ;
- un mémoire de Dirichlet publié en 1828 et intitulé *De formis linearibus, in quibus continentur divisores primi quarumdam formularum graduum superiorum commentatio*, où l'auteur utilise notamment les résidus quadratiques ;
- un mémoire sur les résidus de Lebesgue publié en 1829 dans le *Bulletin du Nord* de Moscou ;
- les deux mémoires de Cauchy sur les équivalences insérés dans les 45^{e} et 46^{e} livraisons des *Exercices de mathématiques*[72] publiées en mars et mai 1830.

Le *Bulletin de Férussac* permet donc d'avoir une vision assez complète des travaux intégrant des résidus et des congruences sur sa période de publication. En ce qui concerne la scène française, les articles non commentés dans le *Bulletin de Férussac* sont ceux publiés dans des sources difficiles d'accès : le *Bulletin* ne pallie à ce problème que dans la mesure où il ouvre par ailleurs ses pages à leurs auteurs écartés d'autres publications

71. Nous arrêtons cette comparaison en 1830, l'année 1831 étant la dernière année d'activité du *Bulletin*.
72. La dernière livraison de ce périodique analysée dans le *Bulletin* est la 44^{e}.

académiques (comme dans le cas de Lebesgue). Cela confirme bien l'analyse que Taton donne des objectifs de la première section du *Bulletin* :

> Le but du *Bulletin des Sciences mathématiques...* était de mentionner ou d'analyser, suivant leur importance, les diverses productions mathématiques : manuels, études diverses, articles publiés dans les recueils académiques et dans les journaux scientifiques. D'une façon générale, ce but semble atteint. Presque tous les livres de mathématiques français et de nombreux livres étrangers sont mentionnés de façon assez précise, sauf pour certains de ces derniers dont le Bulletin cite le titre, non dans sa langue originale, mais en traduction française [Taton, 1947, p. 109].
>
> L'intérêt essentiel du *Bulletin des Sciences mathématiques* réside surtout dans l'image fidèle qu'il donne des différentes tendances qui se font jour dans les recherches mathématiques de son époque [Taton, 1947, p. 115].

Le *Bulletin* permet au moins à Galois et Lebesgue de faire connaître l'existence de leurs travaux sans dépendre de l'avis favorable des académiciens et des lenteurs de publication, il fait circuler en France les idées de certains savants allemands, comme Jacobi ou Dirichlet, dont on trouve l'écho des premiers raisonnements sur les résidus cubiques et biquadratiques. Ces deux mathématiciens sont particulièrement mis en avant par Cournot, qui est au moins très proche de Dirichlet [73].

Du point de vue de notre étude, le seul texte que l'analyse conjointe des publications liées à l'Académie, du *Bulletin de Férussac*, des *Exercices* de Cauchy et du *Journal de Crelle* ne permet pas de détecter, est le mémoire de Lebesgue de 1829 (nous le commentons ci-dessous).

7 - Les premières recherches de Victor-Amédée Lebesgue en théorie des nombres : le mémoire de 1829

Le *Bulletin du Nord* est un mensuel éphémère « de science et de littérature », publié à Moscou par Georges Lecointe de Laveau, secrétaire de la société impériale des naturalistes ; il était destiné à témoigner de la vie intellectuelle dans la capitale russe. Le mémoire de Lebesgue, étalé sur plusieurs fascicules, y côtoie des récits de voyages et des contes.

73. En effet, dans ses *Souvenirs*, Cournot donne des détails sur les cours auxquels il a assisté à la Sorbonne.

> Dans des cours de mathématiques supérieures, tels que ceux qui devaient principalement m'occuper, en vue de la licence, on se compte facilement, même à la Sorbonne. J'avais là pour camarade et pour ami un Allemand de la Prusse rhénane, M. Dirichlet, plus jeune que moi de trois ans, devenu par la suite membre de l'Académie de Berlin et l'un des huit associés étrangers de l'Académie des Sciences de Paris [...] Son génie pénétrant et inventif avait déjà trouvé sa voie ; et, tout en suivant les cours pour y apprendre les généralités que tous les gens du métier sont tenus de savoir, il s'enfonçait dans les plus épineuses recherches de son sujet de prédilection, la Théorie des Nombres... [Cournot, 1913, p. 77].

Il contient des résultats sur les congruences à une inconnue et en particulier sur les congruences binômes. L'auteur s'y montre complètement familier des *Disquisitiones Arithmeticae* et utilise systématiquement le vocabulaire (congruence et module) et le symbole ≡ introduits par Gauss. Voici comment il introduit son travail :

> La théorie des congruences à une inconnue est encore peu avancée, et cela doit être puisque celle des équations déterminées avec lesquelles les congruences ont des rapports intimes ne l'est pas beaucoup plus. Il n'est donc pas étonnant qu'on n'ait point de solution générale et directe, même de la congruence du second degré, pour laquelle on est forcé d'employer l'ingénieuse méthode d'exclusion due à M. Gauss. Pour les degrés plus élevés on est, en général, réduit à des essais très longs. Il est donc indispensable d'éviter de les entreprendre quand la congruence est impossible, et pour cela il est nécessaire de connaître les conditions de possibilité des congruences. C'est principalement la recherche de ces conditions qui fait l'objet de cet extrait qui se compose de quatre paragraphes [Lebesgue, 1829, p. 23].

Lebesgue remarque donc les « rapports intimes » entre la théorie des équations et celle des congruences, qu'il met à nouveau en avant quelques lignes plus loin, en citant Poinsot :

> Le §1 montre comment la résolution d'une congruence pour un module composé, se tire de la résolution de la même congruence pour des modules premiers, diviseurs du module composé. On y trouve la théorie des racines multiples de la congruence dont le module est premier, théorie qui n'a point encore été donnée, du moins que je sache, et qui est nécessaire pour la résolution des congruences dont le module est composé. Cette théorie présente une analogie parfaite avec la théorie des racines égales des équations déterminées, ce qu'on devait naturellement inférer d'un mémoire de Poinsot sur l'application de l'algèbre à la théorie des nombres [Lebesgue, 1829, p. 23-24].

Il se réfère également à Gauss, Dirichlet et Jacobi pour leurs recherches sur les résidus cubiques et biquadratiques. Comme mentionné précédemment, les articles de ces deniers auteurs sur ce thème sont insérés dans le *Journal de Crelle* en 1827 et 1828. Lebesgue cite d'ailleurs le compte rendu fait par Cournot dans le *Bulletin de Férrussac* sur [Jacobi, 1827] [74] ; comme indiqué précédemment [75], il se réfère également au commentaire de Cournot sur [Dirichlet, 1828c]. Cela montre encore le rôle des comptes rendus que

74. Dans son introduction, Lebesgue annonce qu'il va obtenir la congruence ayant pour solutions les racines primitives et observe :

> J'ignore si ce résultat est connu, seulement j'ai vu par le Bulletin des sciences (t. 8 N^{o} 268) que le Dr. Jacobi « a donné l'annonce d'une théorie neuve et piquante, celle des racines imaginaires des congruences et de leurs racines primitives » [Lebesgue, 1829, p. 26].

75. Voir page 56.

Cournot insère dans le périodique, du point de vue de la circulation en France de certains articles contenus dans le *Journal de Crelle*.

Dans les deux premiers paragraphes de son mémoire, Lebesgue travaille autour du nombre de racines des congruences de degré quelconque à une inconnue pour un module premier, puis pour un module composé. Enfin, Lebesgue tente de généraliser le théorème de Lagrange, que Cauchy a démontré dans [Cauchy, 1813] : pour un nombre premier p et deux nombres entiers b et c, on peut toujours trouver[76] des entiers x et y tels que $x^n - by^n - c$ est divisible par p. Il propose une méthode qui « paraît pouvoir s'étendre à tous les cas, seulement elle exige des calculs forts longs » [Lebesgue, 1829, p. 259]. Il l'applique au cas où $n = 3$. Les deux paragraphes suivants sont consacrés aux congruences binômes ; Lebesgue commence par indiquer des propriétés générales de ces congruences, puis s'intéresse particulièrement aux équations binômes des degrés 1, 2 et 3 dans le dernier paragraphe.

Arrêtons-nous sur deux points de ce dernier paragraphe. Gauss, dans les *Disquisitiones Arithmeticae* a formulé la loi de réciprocité quadratique en termes de résidus quadratiques[77], tandis que Lebesgue la traduit en termes de congruences :

> Le théorème de M. Legendre revient au suivant que M. Gauss appelle fondamental :
>
> Si la congruence $x^2 \equiv a \pmod{p}$ est possible ou impossible, a et p étant deux nombres premiers impairs, la congruence $x^2 \equiv \pm p \pmod{a}$ sera aussi possible ou impossible en prenant le signe + quand p forme $4m + 1$ et le signe -1 quand p a la forme $4m + 3$ [Lebesgue, 1829].

Dans le paragraphe (39), Lebesgue revient sur ces congruences impossibles, en donnant cette fois la forme de leurs racines imaginaires :

> Si n est un non-résidu quadratique ou si la congruence $x^2 \equiv n \pmod{p}$ est impossible, p nombre premier, toute autre congruence impossible $x^2 \equiv a \pmod{p}$, aura pour racine une expression de la forme $\pm y\sqrt{n}$, y ayant une valeur entière et réelle [Lebesgue, 1829, p. 30].
>
> [...] Au moyen de cette remarque la résolution de toute congruence du 2e degré peut se ramener à celle d'un certain nombre de congruences $x^2 \equiv -1$, $x^2 \equiv a$, $x^2 \equiv b$, $x^2 \equiv c$, etc. a, b, c etc. étant des nombres premiers plus petits que $\frac{p-1}{2}$ [Lebesgue, 1829, p. 31].

Comme Poinsot (et bientôt Galois), Lebesgue considère donc des racines imaginaires de congruences binômes et donne des méthodes explicites pour les déterminer dans certains cas. Par exemple, dans le cas du module 37, il calcule les racines des nombres premiers

76. Le théorème de Lagrange correspond au cas particulier du second degré. Ce théorème est également traité en termes de congruences dans [Bouniakowsky, 1831] : l'auteur considère le cas du second degré, où le module est composé.

77. « Tout nombre qui, pris positivement, est résidu ou non-résidu de p, a, pour résidu ou non-résidu, $+p$ ou $-p$, selon que p sera de la forme $4n + 1$ ou $4n + 3$ » [Gauss, 1801, art. 130].

inférieurs à 18 modulo 37 : $\sqrt{-1} \equiv 6$, $\sqrt{2} \equiv \sqrt{2}$, $\sqrt{3} = 15$, ..., $\sqrt{17} = 8\sqrt{2}$. Il en déduit la solution de $x^2 \equiv 19 \pmod{37}$: comme $19 \equiv -18 \pmod{37}$, $x \equiv \sqrt{-18} \equiv \sqrt{-1} \times \sqrt{2} \times 3 \equiv 6 \times \sqrt{2} \times 3 \equiv 18\sqrt{2} \pmod{37}$.

Il conclut son mémoire avec quelques remarques sur les résidus cubiques et annonce qu'il reviendra sur ce thème dans un prochain travail.

Dans ce texte de Lebesgue, nous retrouvons des caractéristiques communes avec les travaux d'autres savants : comme Poinsot et Cauchy, Lebesgue insiste sur l'analogie existant entre les équations et les congruences ; comme Poinsot et Galois, il travaille avec les racines imaginaires des congruences. Comme Libri, il obtient des résultats sur le nombre de racines entières des congruences, mais sans utiliser d'outils étrangers à l'arithmétique, comme les fonctions trigonométriques. Il reviendra d'ailleurs sur ces thèmes à son retour en France, cette fois dans le *Journal de Liouville* à partir de 1837.

III Résidus et congruences dans les journaux : 1835-1850

1 - Une période riche en nouveaux développements arithmétiques

Nous allons maintenant examiner la période 1835-1850, qui voit la création en France de nouveaux périodiques, afin de prendre en compte d'éventuelles transformations liées aux modes de diffusion. Cette période s'accompagne de développements fondamentaux en théorie des nombres, qui sont pour la plupart développés dans le *Journal de Crelle*. Avant d'analyser les périodiques français, nous donnons un rapide aperçu des différentes thématiques abordées dans le *Journal de Crelle*. Contrairement à ce que l'on a observé dans la section précédente, aucun français ne publie d'article lié aux résidus et congruences dans ce journal entre 1835 et 1850.

Si l'on met de côté le traité de théorie des nombres élémentaires écrit par l'éditeur Crelle lui-même contenant peu de raisonnements sur les restes, on comptabilise quarante-six textes pour sept cent soixante-dix pages et dix auteurs. Parmi ces dix auteurs, les travaux de la moitié d'entre eux ont un volume bien supérieur à cent pages [78]. Ceci confirme bien l'effet essentiel du journal pour le développement de certains thèmes mathématiques en Allemagne, notamment pour la théorie des nombres en général et pour les résidus en particulier [79].

Nous nous contenterons ici de rappeler en quelques lignes les thèmes principaux abordés, notamment à titre comparatif avec le *Journal de Liouville*.

Tout d'abord, remarquons qu'à part Crelle qui continue d'employer des notations de

78. Voir en annexe, page 490 pour un tableau récapitulatif des auteurs et du nombre d'articles publiés par chacun.

79. Cette importance est déjà bien perçue au XIX^{e} siècle, voir par exemple [Klein, 1926-1927, ch. 3].

la forme Mp, tous les autres auteurs utilisent le signe ≡ de Gauss : nous allons voir que la situation est différente dans les périodiques français à la même période.

Ensuite, plusieurs articles sont consacrés à des résultats élémentaires sur les résidus, déjà prouvés dans les ouvrages d'Euler et Lagrange, voire de Gauss. Le principal auteur concerné est Peter Friedrich Arndt, qui revient entre autres sur le théorème de Wilson. Dirichlet [80] commente également en 1837 l'équation de Pell-Fermat $t^2 - pu^2 = 1$, résolue entièrement par Lagrange dans [Lagrange, 1773b] à partir des fractions continues. Son objectif est ici de donner une nouvelle méthode qu'il commente dans son introduction :

> Il est remarquable que la résolution de l'équation précédente puisse aussi se rattacher à la théorie des équations binômes de Mr. *Gauss*. Il résulte non seulement de cette théorie que l'équation $t^2 - pu^2 = 1$ est toujours résoluble, mais on peut même en déduire des formules générales qui expriment les inconnues t et u en fonctions circulaires.
>
> Quoique cette manière de traiter l'équation dont il s'agit soit applicable à tous les cas, je me bornerai dans cette note à développer celui où p est un nombre premier, ce cas suffisant pour faire connaître l'esprit de la méthode. Il est sans doute inutile d'ajouter que le mode de solution que nous allons indiquer, est beaucoup moins propre au calcul numérique que celui qui dérive de l'emploi des fractions continues et que cette nouvelle manière de résoudre l'équation $t^2+pu^2 = 1$, ne doit être envisagée que sous le rapport théorique et comme un rapprochement entre deux branches de la science des nombres [Dirichlet, 1837, p. 286-287].

La volonté d'associer algèbre, arithmétique et analyse est un fil directeur dans plusieurs textes de cet auteur [81], comme nous l'avons signalé auparavant.

Les principaux thèmes travaillés dans les articles considérés ici sont les congruences et les congruences supérieures en général (avec Schönemann [82]), la théorie des formes quadratiques à coefficients entiers réels et complexes, en particulier à partir de résultats liés aux résidus quadratiques et à la loi de réciprocité associée, la cyclotomie. Par exemple, Jacobi, dans [Jacobi, 1837] [83], développe les outils et méthodes utilisées implicitement

80. Nous renvoyons à [Goldstein et al., 2007] pour des commentaires sur les recherches arithmétiques de Dirichlet sur cette période.

81. De même, il remarque en 1838 dans un article sur les formes quadratiques :

> Ces nouvelles recherches [sur les séries] m'ont fait reconnaître que la considération des séries de cette espèce constitue une méthode très féconde d'analyse indéterminée, et qui s'applique à des questions très variées. En attendant que je puisse achever un travail étendu sur cette matière, je vais indiquer rapidement quelques applications nouvelles de ce genre d'analyse. La méthode que j'emploie, me paraît surtout mériter quelque attention par la liaison qu'elle établit entre l'Analyse infinitésimale et l'Arithmétique transcendante, et j'espère que sous ce rapport elle pourra même intéresser les géomètres qui ne s'occupent pas spécialement des questions relatives aux propriétés des nombres [Dirichlet, 1838, p. 259-260].

82. Voir [Frei, 2007].

83. Ce mémoire est inséré en 1837 dans les comptes rendus de l'Académie de Berlin, puis reproduit en

dans [Jacobi, 1827] et obtient des résultats sur les lois de réciprocité et sur les formes quadratiques abordées par Cauchy en 1829 et 1831. Comme indiqué dans notre introduction générale, on retrouve d'ailleurs des similarités frappantes entre les procédés employés par les deux mathématiciens [84]. De nombreux textes explorent la théorie des résidus et les lois de réciprocité : de nouvelles démonstrations de la loi de réciprocité quadratique sont présentées, et des preuves des lois de réciprocité cubique et biquadratique sont également données. Eisenstein publie ainsi huit textes sur ce thème en 1844.

Ces différents sujets ont un point commun : ils mènent souvent à la considération de nombres entiers complexes et aux questions qui en découlent. Les principaux auteurs approchant ces questions sont : Dirichlet avec ses travaux sur les progressions arithmétiques et les formes quadratiques notamment ; Jacobi, qui publie très peu mais indique certaines pistes de recherches sur les résidus d'ordre supérieur dans [Jacobi, 1839a] par exemple ; Eisenstein et ses recherches sur les lois de réciprocité [85] ; enfin, Kummer [86] qui introduit en 1847 les nombres idéaux afin de pallier l'absence de décomposition unique en facteurs premiers pour certains ensembles d'entiers cyclotomiques.

Arrêtons-nous maintenant sur les publications de la scène française en rapport avec les résidus et les congruences, dont les thématiques, comme nous allons le voir, ont très peu de points communs avec les sujets listés ci-dessus.

2 - L'Académie des Sciences

Il est en fait remarquable que les publications, anciennes ou nouvelles, de l'Académie, témoignent d'une grande continuité avec le début du siècle.

(a) Les *Mémoires*

Un *Mémoire sur la théorie des nombres* de Cauchy, partagé en deux parties, est publié en 1840. Il constitue de loin la contribution la plus volumineuse du mathématicien avec plus de 400 pages : la première partie est en fait un mémoire du même nom présenté en 1830 à l'Académie (donc dans notre première période), la deuxième partie, nouvelle, est composée de quatorze notes complétant le mémoire principal. Cauchy y retrouve notamment les résultats présentés dans le *Bulletin de Férussac* en 1829 (dans [Cauchy, 1829a]), et détaille en particulier dans la Note IV la preuve de la loi de réciprocité quadratique amorcée en 1829, mais c'est le seul passage où il démontre des résultats sur la théorie

1846 dans le *Journal de Crelle*, et enfin traduit et intégré dans les *Nouvelles Annales de Mathématiques* en 1856.

84. Nous revenons en détail sur ce point dans notre quatrième partie.

85. Voir [Lemmermeyer, 2000, ch. 8] notamment.

86. Se reporter notamment à [Edwards, 1975-1977], [Edwards, 1977], [Edwards, 1980] et [Lemmermeyer, 2009].

des résidus de puissances. Son objectif n'est pas la loi de réciprocité. Cauchy utilise les congruences et les racines primitives pour travailler sur les formes quadratiques de la forme $p^\mu = x^2 + ny^2$ et $4p^\mu = x^2 + ny^2$, où n est un diviseur de $p-1$, dans le plus grand nombre de cas possibles, en fonction des formes des nombres p et n. Les congruences et les racines primitives sont ici encore employées comme des outils : les racines primitives permettent à Cauchy, à la manière de la section VII des *Disquisitiones* de Gauss, de mettre en évidence des propriétés intéressantes de certaines expressions algébriques, les congruences servent à étudier les équations algébriques correspondantes. À côté de ces outils arithmétiques, Cauchy applique également dans ses démonstrations des outils analytiques comme du calcul intégral et différentiel et des développements de séries. Il réutilise, ou démontre à nouveau, des théorèmes sur les sommes de Gauss par exemple, en se référant aux travaux de Gauss, Dirichlet et Jacobi. Nous étudierons ce mémoire de manière approfondie dans la quatrième partie.

L'unique texte publié dans les *Mémoires des savants étrangers*, et contenant des raisonnements sur les résidus et les congruences est un des *Mémoire sur la théorie des nombres* présenté par Libri à l'Académie des Sciences entre 1824 et 1825. Approches, raisonnements et résultats sont similaires à ceux publiés dans le *Journal de Crelle* en 1832 [87].

(b) Les *Comptes Rendus* des séances de l'Académie

Comme nous l'avons indiqué précédemment, à partir de 1835, les savants ont la possibilité de publier des notes dans ce nouvel hebdomadaire académique. Nous avons relevé les différentes notes dont les titres mentionnent explicitement résidus ou congruences, ou les relient à un thème déjà repéré comme pertinent à notre sujet. Six auteurs apparaissent, la plupart déjà actifs pendant la première période : Lebesgue avec trois notes publiées en 1836, 1837 et 1844, Dirichlet avec une note publiée en 1840, Binet avec deux notes publiées en 1841 et 1849, Poinsot avec une note publiée en 1841, Liouville avec une note publiée en 1847 et enfin Cauchy avec vingt-deux notes au total (trois en 1839, sept en 1840, une en 1841 et onze en 1847).

L'entrée liée à Poinsot n'est que l'introduction de son mémoire [Poinsot, 1845] publié dans le *Journal de Liouville* : nous le commenterons rapidement dans la section sur le *Journal de Liouville* ci-après et en analyserons de manière plus approfondie certains extraits dans la troisième partie de notre travail.

Lebesgue et les résidus

En 1836, Lebesgue, alors enseignant et n'ayant pas encore obtenu son doctorat, présente deux mémoires à l'Académie, dont les rapports sont confiés à Poisson et Libri : un

87. Nous renvoyons donc à l'analyse faite à partir de la page 66.

Mémoire sur les résidus (séance du 5 septembre 1836, dont le rapport [88] est inséré dans les *Comptes Rendus* de la séance du 10 octobre 1836) et un *Mémoire sur les lois de réciprocité relatives à la théorie des résidus quadratiques cubiques et biquadratiques* (séance du 19 septembre 1836). D'après le rapport sur le premier mémoire, Lebesgue démontre des résultats sur le nombre de solutions d'une congruence, en déduit notamment une démonstration de la loi de réciprocité quadratique et des résultats sur les résidus cubiques et biquadratiques. Les rapporteurs proposent d'ailleurs d'insérer les travaux présentés à l'Académie par Lebesgue dans les *Mémoires* des savants étrangers ; ils n'y seront néanmoins jamais publiés.

Deux courtes notes de Lebesgue sur l'équation $x^p = 1$ paraissent également dans les *Comptes Rendus* des séances de l'Académie des Sciences, en 1837 et 1844. Dans les deux cas, il travaille sur les équations intermédiaires obtenues lors de la résolution de l'équation binôme $x^p = 1$ par la méthode exposée par Gauss dans la section VII des *Disquisitiones Arithmeticae*. Notons que Lebesgue reprend systématiquement la notation $\equiv$ introduite par Gauss pour désigner les congruences. Dans la première note, il donne deux règles pour former les équations intermédiaires de degré m, lorsque $p = mh + 1$:

la première règle explique comment former la série des résidus m^{e}, ainsi que les séries de non-résidus ;

la seconde discute les permutations que l'on peut effectuer entre les résidus m^{e}, ainsi que le nombre de solutions de la congruence $1 + x_1^m + x_2^m + \ldots + x_k^m \equiv 0 \pmod{p}$.

Lebesgue applique également ces principes à l'étude de l'équation $Y^2 - piZ^2 = 4\dfrac{x^p - 1}{x - 1}$, avec $p = 2h + 1 = 4q + i$ où [89] $i = \pm 1$. Il aborde les mêmes thèmes dans la deuxième note publiée en 1844. Comme nous le verrons plus loin, Lebesgue développe ces notes dans ses articles publiés dans le *Journal de Liouville*.

Un article de Liouville sur la loi de réciprocité

Liouville publie en 1847 une note (qui sera elle aussi développée dans le *Journal de mathématiques pures et appliquées* proposant une nouvelle preuve de la loi de réciprocité quadratique. Elle s'appuie sur l'égalité, que l' « on démontre sans peine » [Liouville, 1847, p. 578] :

$$\prod_{\alpha=1}^{\frac{p-1}{2}} \frac{\rho^{\alpha q} - \rho^{-\alpha q}}{\rho^{\alpha} - \rho^{-\alpha}} = \left(\frac{p}{q}\right).$$

et le schéma de preuve exposé ici par Liouville ne contient pas de raisonnement explicite sur les résidus [90].

88. Nous discutons les observations de ce rapport dans notre étude des publications de Lebesgue dans le *Journal de Liouville* : voir à partir de la page 93.

89. Nous reproduisons ici les notations choisies par Lebesgue ; la lettre i n'a ici aucun lien avec $\sqrt{-1}$.

90. Cette preuve est reprise dans [Edwards, 1977, p. 238-239]. Edwards la qualifie d'analytique.

Binet

Binet publie en fait quatre notes de théorie des nombres dans les *Comptes Rendus* entre 1841 et 1849. Il y utilise le mot « résidu » comme synonyme de reste de division. Lors des séances du 9 août 1841 et du 4 novembre 1844, il travaille sur la recherche du plus grand diviseur commun de deux nombres ou de deux polynômes et analyse le nombre d'étapes de l'algorithme permettant de calculer ce plus grand diviseur [91]. Il considère donc des divisions euclidiennes et appelle les restes obtenus des résidus. Il n'emploie néanmoins aucune méthode ni aucune propriété de la théorie usuelle des résidus (comme le petit théorème de Fermat, propriétés opératoires, ...). D'autre part, si la note publiée le 9 août 1841 est intitulée *Note sur une nouvelle méthode pour trouver le plus grand commun diviseur des nombres entiers, ou des polynômes algébriques, et sur l'application de cette méthode aux congruences du premier degré*, Binet n'utilise à aucun moment le terme « congruence » dans son texte, le titre se réfère à l'équation indéterminée $ax - Ay = 1$ (comme pour Libri). Ces notes ne font donc pas partie de notre corpus.

La note du 26 juillet 1841 a pour thème les *nombres associés d'Euler*, qui sont nos actuels nombres inverses dans le corps $\mathbb{F}_p^*$. Binet commence par rappeler que le théorème de Wilson ou le petit théorème de Fermat permettent de déterminer le nombre associé d'un nombre donné relativement à un diviseur premier p, mais « l'usage arithmétique de ces propositions fondamentales de la science des nombres devient impraticable dès que p devient un peu grand, vu la longueur des calculs » [Binet, 1841b, p. 210]. Il propose donc d'exposer une méthode « numériquement applicable » [Binet, 1841b, p. 210], basée sur des divisions euclidiennes. Enfin, dans le texte [Binet, 1849], l'auteur travaille sur l'équation $x^2 + y^2 = z^2$ en utilisant le petit théorème de Fermat, qu'il exprime comme égalité $a^p - a = pM$.

Finalement, les seules propriétés des résidus que Binet utilise dans ses travaux de théorie des nombres sont les théorèmes de Fermat et de Wilson. Il emploie la notation Mp de Legendre et utilise les mots “résidu” et “congruence” comme synonymes de “reste de division” et “équation indéterminée”.

Les vingt-deux notes de Cauchy

Cet ensemble de travaux de Cauchy peut être partagé en plusieurs parties ; tout d'abord, les dix notes publiées entre 1839 et 1840 abordent exactement les mêmes thèmes que le grand *Mémoire sur la théorie des nombres* publié en 1840 et résumé précédemment.

Quant à la note de 1841 *sur diverses formules relatives à l'Algèbre et à la théorie des*

91. À ce sujet, voir [Shallit, 1994]. Encore une fois, Binet publie sur ce thème un article plus conséquent dans le sixième tome du *Journal de Liouville* en 1841.

nombres, elle ne contient des raisonnements généraux sur les congruences du premier degré que dans le deuxième paragraphe, intitulé *Sur la résolution des équations indéterminées du premier degré en nombres entiers*[92]. L'objectif est de proposer une méthode de résolution des équations indéterminées en nombres entiers de la forme $ax + by = k$, qui peuvent se ramener à $mx \pm ny = \pm l$, où m et n sont premiers entre eux.

Selon Cauchy, cette dernière équation se traduit, en termes de congruence[93], en $mx \equiv \pm l \pmod{n}$, soit $x \equiv \pm\frac{l}{m} \pmod{n}$. Or, comme[94] $\frac{l}{m} \equiv l \times \frac{1}{m} \pmod{n}$, le problème se réduit à résoudre la congruence $x \equiv \frac{1}{m} \pmod{n}$.

Si n est un nombre premier, le petit théorème de Fermat donne $m^{n-1} \equiv 1 \pmod{n}$, et il suffit de poser $x \equiv m^{n-2} \pmod{n}$.

Cauchy remarque que Libri et Binet[95] obtiennent également ce résultat quand n est premier, puis ajoute que, lorsque n n'est pas premier, il suffit d'appliquer de la même façon le théorème d'Euler : $m^N \equiv 1 \pmod{n}$ où N représente le nombre d'entiers inférieurs et premiers à n. Finalement, l'équation initiale est résolue en posant $x \equiv m^{N-1}l \pmod{n}$: c'est l'objet du théorème I. Cauchy précise en note que Poinsot lui a affirmé avoir communiqué à Legendre une note où il propose une méthode de résolution semblable.

Cauchy consacre ensuite plusieurs paragraphes pour déterminer le nombre N d'entiers inférieurs et premiers à n. Puis il revient sur le problème initial et remarque que l'on peut prendre, à la place de N, n'importe quel entier i tel que $m^i \equiv 1 \pmod{n}$. Il souhaite donc déterminer la plus petite valeur possible pour i : « D'ailleurs cette valeur particulière de i jouit de propriétés remarquables qui peuvent servir à la faire reconnaître et calculer » [Cauchy, 1841, p. 122].

La suite du mémoire est donc consacrée à ce nombre i. Il rappelle que les termes de la progression (m^k) est périodique de période 1, m, m^2, …, m^{i-1}. Il rappelle la notion d'indice de Gauss : « L'exposant de la puissance à laquelle il faut élever la base m, pour obtenir un nombre équivalent suivant le module n à un reste donné, est ce qu'on nomme l'*indice* de ce nombre ou de ce reste » [Cauchy, 1841, p. 123][96]. Puis il définit la notion d'*indicateur* : c'est le plus petit des indices lorsque le reste considéré est l'unité, et introduit la notion d'*indicateur maximum*, noté I, qui est le PGCD des indicateurs des différentes bases m possibles pour le module n. Ainsi, I ne dépend que du module n. La suite du travail de Cauchy consiste à établir des méthodes pour déterminer l'indicateur maximum en fonction de la forme du module (nombre premier, puissance d'un nombre premier, …). Cela lui permet de construire une table[97] d'indicateurs maximum pour des

92. Ce paragraphe est reproduit dans la livraison de septembre 1841 des *Exercices de mathématiques et de physique mathématique*.

93. Cauchy continue d'utiliser l'expression *équivalence*.

94. Cauchy ne le précise pas mais c'est possible car m et n sont premiers entre eux.

95. Ces deux savants n'utilisent pas les congruences dans les travaux correspondants.

96. Voir [Gauss, 1801, art. 57] pour la définition de l'indice d'un nombre donnée par Gauss.

97. Cette table n'est reproduite que pour les modules inférieurs à 100 dans les *Comptes Rendus* de l'Académie. On retrouve la version complète dans les *Exercices d'analyse et de mathématique physique*.

modules inférieurs à 1000, et remarque qu'ainsi, sa méthode de résolution peut être appliquée sans connaître la décomposition en facteurs premiers du module[98] contrairement aux méthodes données par Binet et Libri. La notion d'indicateur maximum introduite ici par Cauchy lui sert également dans ses notes publiées en 1847 en relation avec le dernier théorème de Fermat.

Enfin, deux thèmes principaux sont abordés dans les notes publiées pendant l'année 1847. Dans dix d'entre elles, Cauchy utilise la théorie des résidus et des congruences dans le cadre de ses recherches sur le grand théorème de Fermat. Il étudie notamment les *polynômes radicaux*, qu'il introduit dans le mémoire [Cauchy, 1847b], intitulé *Mémoire sur les racines des équations algébriques à coefficients entiers, et sur les polynômes radicaux* et présenté à l'Académie le 15 mars 1847 :

> Soit ρ une racine primitive de l'équation binôme
>
> $$(1) \qquad x^n - 1 = 0,$$
>
> n étant un nombre entier quelconque. Une fonction entière $\varphi(\rho)$ de cette racine pourra toujours être réduite à la forme
>
> $$(2) \qquad \varphi(\rho) = a_0 + a_1\rho + a_2\rho^2 + \ldots + a_{n-1}\rho^{n-1},$$
>
> et représentera ce qu'on nomme quelquefois un nombre complexe. Mais ici le mot nombre paraît détourné de sa signification naturelle. Afin d'éviter cet inconvénient, je donnerai simplement à la fonction $\varphi(\rho)$ déterminée par la formule (2), le nom de *polynôme complexe*, ou mieux encore, de *polynôme radical*, pour rappeler l'origine d'un tel polynôme dont les divers termes sont proportionnels aux diverses puissances d'une même expression radicale, savoir d'une racine $n^{\text{ième}}$ de l'unité [Cauchy, 1847b, p. 410].

Ces textes font partie d'un ensemble de travaux sur ces nombres complexes, que l'on nomme aujourd'hui entiers cyclotomiques. Dans ses recherches, Cauchy utilise les congruences, dont en particulier les racines primitives, les sommes de Gauss, la notion d'indicateur maximum, et plus généralement des résultats développés dans ses travaux sur les formes quadratiques entre 1829 et 1840.

Dans la deuxième série de notes, Cauchy construit une « nouvelle théorie des imaginaires » dans laquelle les congruences occupent une place centrale : il y considère des polynômes dont la variable est i modulo le polynôme $x^2 + 1$. En termes actuels, Cauchy construit les nombres complexes comme éléments de $\mathbb{R}[X]/(X^2 + 1)$.

98. Il ne le précise pas mais la construction de la table se base sur la décomposition en facteurs premiers du module…

3 - Les *Exercices d'analyse et de physique mathématique* de Cauchy

Cauchy fait à nouveau publier un périodique dont il est l'unique auteur dès 1839. Une fois encore, il s'agit de développer ce qui ne peut paraître dans les bornes restreintes des publications de l'Académie, même augmentées des comptes rendus. Cauchy insère dans ce périodique personnel la deuxième partie de [Cauchy, 1841] avec une table des indicateurs maximaux pour tous les modules inférieurs à 1000.

Le deuxième mémoire est publié en 1845, sous le nom *Note sur quelques propositions relatives à la théorie des nombres*. Le principal théorème que Cauchy y démontre va ensuite lui servir dans ses travaux sur la théorie des permutations publiés ultérieurement dans son journal [99]. Il démontre que, pour un nombre entier i, dont la décomposition en facteurs premiers entre eux est $abc\ldots$, et un entier l inférieur à i, alors on peut toujours trouver des nombres entiers x, y, z, ... respectivement inférieurs à a, b, c, ..., tels que la congruence $i\left(\frac{x}{a}+\frac{y}{b}+\frac{z}{c}+\ldots\right)\equiv l \pmod{i}$ soit vérifiée.

Le troisième et dernier mémoire en rapport avec les résidus et les congruences contenu dans les *Exercices* est publié en 1847 sous le nom de *Mémoire sur la théorie des équivalences algébriques substituée à la théorie des imaginaires*. Il revient cette fois sur les résultats obtenus dans les mémoires sur sa théorie des imaginaires publiés dans les *Comptes Rendus* de l'Académie en 1847.

4 - Le *Journal de Liouville* (1836 - 1850)

(a) Les résidus et les congruences dans le *Journal de Liouville* : aperçu général

Nous avons répertorié dix-neuf articles en lien avec la théorie des résidus et des congruences [100] publiés dans le *Journal de Liouville* entre 1836 et 1850. Nous avons écarté deux textes contenant la notation ≡, utilisée en tant qu'écriture seulement, et un mémoire où les résidus sont mentionnés uniquement dans le paragraphe d'introduction :

- Liouville, dans [Liouville, 1843], introduit son mémoire en rappelant que travailler avec les nombres complexes de la forme $p+q\sqrt{-1}$, où p et q sont des nombres entiers réels, a permis à Gauss de développer une théorie des résidus biquadratiques de manière analogue à celle des résidus quadratiques.
- Lamé, dans [Lamé, 1847a], travaille sur l'équation générale du dernier théorème de Fermat et utilise une fois la notation ≡ pour désigner la congruence binôme $1-x^{n-1}\equiv 0 \pmod{n}$.
- Charles Hermite, dans [Hermite, 1849], utilise la notation ≡ pour exprimer que deux différences sont divisibles par un entier k : $x\equiv x', y\equiv y' \pmod{k}$.

99. Voir [Cauchy, 1846].
100. Voir annexe, page 489.

Remarquons toutefois que ces occurrences témoignent d'une familiarité grandissante avec les congruences. Parmi les dix-neuf textes retenus, huit sont déjà publiés ailleurs. L'article *Sur la théorie des nombres* de Galois est déjà paru en 1830 dans le *Bulletin de Férussac*, et est reproduit ici dans le cadre de l'édition par Liouville des travaux de Galois. Les deux articles de Cauchy et celui de Liouville sont insérés dans les *Comptes Rendus* des séances de l'Académie respectivement en 1840 et 1847 : nous renvoyons aux sections correspondantes pour un commentaire sur ces trois textes. Les quatre autres textes sont des articles de Jacobi, Dirichlet et Kummer publiés précédemment dans le *Journal de Crelle*, dans les mémoires de l'Académie de Berlin ou de façon indépendante en Allemagne.

Restent ensuite douze textes originaux. Huit de ces articles sont de Lebesgue. Les trois autres articles sont de Poinsot, Lamé et Serret. Dans les textes de Serret et Lamé, les résidus et les congruences ne sont utilisés que comme outils.

Dans [Lamé, 1847a], Lamé considère l'équation $A^5 + B^5 + C^5 = 0$ dans le cadre de ses recherches sur le dernier théorème de Fermat [101]. Il utilise des raisonnements sur les résidus à deux reprises dans [Lamé, 1847a, p. 156 et p. 163] pour déterminer la forme d'un nombre. Par exemple, il remarque qu'une expression de la forme $M = (a^2 - 5b)^2 - 5c^2$, lorsque a est premier à 5 est congrue à $a^4 \equiv 1 \pmod 5$ (d'après le petit théorème de Fermat), donc M est de la forme $5k + 1$.

Serret, dans [Serret, 1848], expose des résultats découverts alors qu'il cherchait une « démonstration élémentaire » du théorème des deux carrés : tout nombre premier p de la forme $4k + 1$ est somme de deux carrés. Il obtient des propriétés liant le fait que -1 est résidu quadratique modulo p, soit $q^2 \equiv -1 \pmod p$, au développement en fraction continue de $\frac{p}{q}$. La notation $\equiv$ et l'expression "résidu quadratique" apparaissent dans l'énoncé des théorèmes, puis Serret utilise ensuite le « quotient de $q^2 + 1$ par p » [Serret, 1848, p. 12] pour exposer sa démonstration. Il n'applique pas de propriétés propres à la théorie des résidus et des congruences dans son texte.

Nous allons maintenant donner un aperçu plus détaillé des textes où la théorie des résidus et des congruences joue un rôle plus important. Nous commençons par expliciter les thèmes des mémoires publiés une première fois en Allemagne, afin de savoir à quelles recherches allemandes les lecteurs du *Journal de Liouville* ont eu accès, puis nous consacrerons une section à chacun des auteurs restants.

(b) Quatre textes précédemment publiés en Allemagne

Le premier article, par Dirichlet, est lu en 1837 à l'Académie de Berlin, imprimé en allemand en 1839 dans les mémoires de l'Académie de Berlin, puis traduit par Terquem

101. Nous renvoyons à [Goldstein, 2009] pour une analyse des recherches de Lamé en théorie des nombres.

et inséré dans le quatrième tome du *Journal de Liouville* la même année. Il y démontre la proposition suivante : « Toute progression arithmétique dont le premier terme et la raison sont des entiers sans diviseur commun, contient une infinité de nombres premiers » [Dirichlet, 1839b, p. 393]. Comme l'auteur le rappelle dans son introduction, Legendre avait admis ce résultat dans sa *Théorie des nombres* en vue de la démonstration de la loi de réciprocité quadratique[102]. Il commence par prouver le théorème dans le cas où la raison de la progression est un nombre premier impair, puis dans le cas général, en s'appuyant sur les propriétés des racines primitives.

Un deuxième article de Dirichlet, d'abord présenté en 1841 à l'Académie de Berlin, est traduit par Faye et paraît dans le neuvième tome du *Journal de Liouville* en 1844. Dirichlet reprend ses recherches sur les entiers naturels et les transpose aux entiers de Gauss :

> Ce Mémoire n'est qu'une partie d'un travail considérable dans lequel je me propose d'étendre aux nombres complexes la plupart des solutions que j'ai déjà trouvées pour des questions relatives à la théorie des nombres entiers réels[...].
>
> Je m'occuperai exclusivement, dans ce présent Mémoire, de démontrer le théorème dont voici l'énoncé : « L'expression $kt + l$, dans laquelle t désigne un nombre entier complexe indéterminé, et où k, l représentent de semblables nombres donnés sans facteurs communs, contient toujours une infinité de nombres premiers ». Cette démonstration ressort, comme celle de la loi analogue pour les nombres réels, du théorème fondamental sur certaines propriétés de la forme quadratique des nombres complexes ; aussi me bornerai-je, pour éviter les répétitions inutiles, à renvoyer le lecteur aux recherches déjà mentionnées[103] [Dirichlet, 1843].

Dirichlet commence par transposer des définitions et propriétés utilisées dans la théorie des congruences et des résidus relatifs aux entiers réels aux entiers de Gauss. Par exemple, puisque on ne peut pas parler d'un nombre complexe inférieur à un autre, Dirichlet définit :

> On peut toujours former, relativement à un module complexe donné m, une série de nombres qui possède cette double propriété : qu'il se trouve toujours parmi ses termes un nombre congru à un nombre quelconque pour le module m, mais qu'il ne s'en trouve qu'un seul. Le nombre de termes ainsi incongrus entre eux est $N(m)$ [Dirichlet, 1843, p. 246-247].

À partir de cette définition, Dirichlet détermine le nombre de termes $\psi(m)$ de ce système premiers à m, puis en déduit le théorème d'Euler-Fermat : $l^{\varphi(m)} \equiv 1 \pmod{m}$. Il définit ensuite ce qu'est une racine primitive, puis la notion associée d'indice. Il démontre l'existence d'une racine primitive dans le cas où le module est une puissance d'un nombre premier impair $a + bi$, puis donne également des propriétés pour des modules d'autres

102. Voir à ce sujet [Lemmermeyer, 2000, p. 7-8]. Cet article de Dirichlet, et son utilisation des séries, est également commenté dans [Goldstein et Schappacher, 2007a, p. 30-31].
103. Dirichlet renvoie à [Dirichlet, 1842].

formes. Il propose enfin une démonstration du théorème énoncé initialement.

Les deux articles sont célèbres, en ce qu'ils introduisent des objets analytiques (séries infinies et intégrales) pour établir des propriétés de l'arithmétique élémentaire sur la répartition de nombres premiers. Dirichlet indique d'ailleurs à propos de sa démonstration : « Elle n'est pas purement *arithmétique*, puisqu'elle est fondée en partie sur la considération de grandeurs continues » [Dirichlet, 1839b, p. 394]. Cet aspect est abondamment commenté à l'époque, et approuvé dans la mesure où il contribue à faire sortir l'arithmétique de son isolement et à la relier à d'autres branches de l'analyse, un thème déjà souligné plus haut.

Le troisième article est un texte de Jacobi publié en 1839 en allemand dans le *Journal de Crelle*[104], puis traduit en français par Faye et inséré dans le huitième tome du *Journal de Liouville* en 1843. Il concerne aussi les nombres complexes : Jacobi commence par y rappeler les rôles respectifs des nombres de la forme $a + b\sqrt{-1}$ et $\frac{a+b\sqrt{-3}}{2}$ dans les théories des résidus biquadratiques et cubiques, puis expose des idées sur la décomposition de certaines formes de nombres en produits de nombres complexes composés de racines cinquième, huitième, ou douzième de l'unité. Même si la note est très succincte, Jacobi détaille l'exemple des résidus huitièmes : il décompose les nombres de la forme $a + b\sqrt{-1}$ en produit de deux facteurs de la forme $y' + y''\sqrt{-1} \pm \sqrt[4]{-1}(z' + z''\sqrt{-1})$, où y', y'', z', z'' sont des nombres entiers réels, puis en déduit que tout nombre premier de la forme $8n+1$ (donc aussi $a^2 + b^2$) se décompose en quatre facteurs $\varphi\alpha$, $\varphi\alpha^3$, $\varphi\alpha^5$, $\varphi\alpha^7$, où $\alpha = \sqrt[4]{-1}$ est une racine huitième de l'unité et $\varphi\alpha = y' + y''\alpha^2 + z'\alpha + z''\alpha^3$. Ce sont ces facteurs que Jacobi souhaite considérer comme de nouveaux nombres complexes premiers, étendant donc le sens d'entiers complexes premiers jusque là attaché aux seuls entiers de Gauss premiers. Jacobi conclut qu'en combinant de différentes façons ces quatre facteurs complexes premiers, on obtient les trois formes quadratiques pour le nombre premier : $a^2 + b^2$, $c^2 - 2d^2$, $e^2 + 2f^2$.

Les auteurs de [Goldstein et Schappacher, 2007a] soulignent l'importance de cet article de Jacobi pour les recherches mathématiques ultérieures : celles de Kummer sur les nombres idéaux, celles de Eisenstein et Kronecker sur la multiplication complexe[105], mais aussi celles d'Hermite sur les minima de formes[106], pour lesquelles Hermite se réfère à l'article publié en français :

> The impulse for all the far-reaching and diverging developments we are about to sketch in this section was given by a programmatic 5-page note written by Jacobi, [Jacobi 1839]. Not much is proved there ; results obtained are alluded to, as was still allowed in those days, and the paper is really about how to look at things, more

104. Nous discutons également ce texte dans la partie 4, afin de particulièrement comparer les thématiques abordées par Jacobi et Cauchy.
105. Voir en particulier [Schappacher, 1997], [Schappacher, 1998] et [Houzel, 2007].
106. Voir notamment [Goldstein, 2007].

specifically at "complex prime numbers" [Goldstein et Schappacher, 2007a, p. 39-40].

Le quatrième article reproduit dans le *Journal de Liouville* est le texte de Kummer publié initialement de manière confidentielle à Breslau en 1844 : il est inséré en latin non traduit dans le douzième tome du *Journal de Liouville* en 1847. Comme nous le développons dans la quatrième partie, l'année 1847 voit naître de nombreux textes autour du dernier théorème de Fermat en France, dont les auteurs sont notamment Cauchy et Lamé. La question d'une décomposition unique en facteurs premiers de nombres entiers complexes est soulevée à cette occasion. C'est à cette question que ce premier mémoire de Kummer répond, puisqu'il y montre que l'unicité n'est pas conservée en général. Dans le même volume du *Journal de Liouville*, l'éditeur inclut également un *Extrait d'une lettre de M. Kummer à M. Liouville*, dans lequel Kummer annonce l'envoi de son texte accompagnée de la thèse de Kronecker en expliquant :

> Dans ces Mémoires, que je vous prie d'accepter en signe de ma profonde estime, vous trouverez des développements sur quelques points de la théorie des nombres complexes composés de racines de l'unité, c'est-à-dire de l'équation $r^n = 1$, qui ont été récemment le sujet de quelques discussions au sein de votre Académie, à l'occasion de l'essai d'une Démonstration du théorème de Fermat, proposée par M. Lamé. Quant à la proposition élémentaire pour ces nombres complexes, qu'*un nombre complexe composé ne peut être décomposé en facteurs premiers que d'une seule manière*, que vous regrettez très-justement dans cette démonstration défectueuse en outre en quelques autres points, je puis vous assurer qu'*elle n'a pas lieu généralement* tant qu'il s'agit de nombres complexes de la forme $\alpha_0 + \alpha_1 r + \alpha_2 r^2 + \ldots + \alpha_{n-1} r^{n-1}$, mais qu'on peut la sauver en introduisant un nouveau genre de nombres complexes que j'ai appelé *nombre complexe idéal*.

Dans son mémoire, Kummer cite en particulier les travaux de Jacobi à plusieurs reprises. Comme annoncé dans sa lettre, il considère les nombres entiers complexes de la forme $\alpha_0 + \alpha_1 r + \alpha_2 r^2 + \ldots + \alpha_{n-1} r^{n-1}$, où $r^n = 1$ et base la construction de ses nombres idéaux sur la correspondance entre une équation et une congruence, où il remplace r par une racine de la congruence $x^n \equiv 1 \pmod{p}$ [107].

Finalement, le *Journal de Liouville* apporte sur la scène française des articles importants, dont l'impact n'est pas négligeable. Néanmoins, d'après le résumé donné en début de section sur les recherches publiées dans le *Journal de Crelle*, nous voyons que la lecture seule du *Journal de Liouville* est insuffisante pour se tenir au fait des travaux insérés dans le périodique allemand.

107. Pour l'étude de ces travaux de Kummer et la polémique entre Liouville, Lamé, Cauchy qui sert de contexte à la publication de Kummer dans le journal de Liouville, voir [Edwards, 1980] et [Lemmermeyer, 2009].

(c) Louis Poinsot : une synthèse élémentaire sur la théorie des nombres

L'article de Poinsot publié en 1845 dans le *Journal de Liouville* est intitulé *Réflexions sur les principes fondamentaux de la théorie des nombres*. Dans l'introduction [108], Poinsot commence par regretter le peu de place laissée à la théorie des nombres dans les ouvrages :

> Mais depuis longtemps il semble que les auteurs aient regardé la théorie des nombres comme une spéculation singulière, qui ne se lie à rien ni dans l'Analyse ni dans la Géométrie, et qui n'offre ainsi à l'esprit que des vérités plus curieuses qu'utiles. À peine en trouve-t-on quelques traces dans les Traités ordinaires d'Arithmétique et d'Algèbre. Et cependant, pour peu qu'on y veuille réfléchir, il est aisé de voir que cette arithmétique transcendante est comme le principe et la source de l'algèbre proprement dite [Poinsot, 1845, p. 2].

Poinsot illustre ces propos presque inévitablement à l'aide de la section VII des *Disquisitiones Arithmeticae* de Gauss, où « la théorie des nombres a fait faire à la fois à l'algèbre et à la géométrie [un pas inattendu et bien remarquable] » [Poinsot, 1845, p. 2].

Il évoque la division classique des mathématiques en deux domaines, mais la reformule : au lieu d'opposer l'étude des grandeurs (la géométrie) à celle des nombres (l'arithmétique), comme dans la tradition grecque, il contraste l'étude de la mesure à l'étude de l'ordre, pour y situer ensuite l'algèbre, la théorie des nombres et la géométrie.

> Les mathématiques ne sont pas seulement la science des rapports, je veux dire que l'esprit n'y a pas uniquement en vue la proportion ou la mesure ; il peut encore considérer le nombre en lui-même, l'ordre ou la situation des choses, sans aucune idée de leurs rapports, ni des distances plus ou moins grandes qui les séparent [Poinsot, 1845, p. 3].

Cette classification des matières mathématiques l'amène à conclure :

> De toutes ces réflexions, et d'une foule d'autres que je pourrais y ajouter, je conclus donc que les principes de l'algèbre et de la théorie des nombres devraient être unis ensemble dans nos ouvrages élémentaires, comme ils sont inséparables par la nature même de ces deux sciences. Ainsi, j'espère qu'on me pardonnera, et même qu'on me saura quelque gré de revenir sur ces principes fondamentaux, d'essayer de les rendre plus clairs, et plus sensibles, et de faciliter ainsi aux jeunes géomètres une étude très-ardue, et en apparence très stérile, mais en effet très-féconde, et peut-être, comme je l'ai dit, la seule d'où l'analyse mathématique puisse attendre aujourd'hui de véritables découvertes [Poinsot, 1845, p. 11].

Le mémoire de Poinsot est composé de quatre chapitres, qui traitent de résultats sur les congruences, et en particulier les congruences binômes. Poinsot n'utilise à aucun

108. Comme nous l'avons indiqué précédemment, cette introduction est également publiée dans les *Comptes Rendus* de la séance du 10 mai 1841 de l'Académie des Sciences.

moment ce terme : il travaille avec des équations indéterminées, et utilise la notation de Legendre : $x^n - 1 = Mp$ écrit-il par exemple. Comme annoncé dans son introduction, il propose effectivement des démonstrations de théorèmes usuels de la théorie des nombres : le petit théorème de Fermat, le théorème de Wilson, le théorème de Lagrange sur le nombre maximum de solutions pour une congruence de degré donné et de module premier, etc. Ces preuves sont fondées sur des principes propres à Poinsot, notamment « tirées de la considération de l'ordre » (qui apparaissent déjà dans ses précédentes publications).

Nous étudierons en détail ce mémoire dans la partie consacrée à Poinsot.

(d) Un auteur dominant dans le *Journal de Liouville* : Victor-Amédée Lebesgue et ses travaux autour des résidus et des congruences

Victor - Amédée Lebesgue [109] est, après Cauchy, le mathématicien français ayant publié le plus grand nombre d'articles en lien avec les résidus et les congruences sur la période considérée, et cela principalement dans le *Journal de Liouville* [110]. Enseignant tout d'abord dans plusieurs collèges de province, il devient précepteur à Londres pendant un an, puis en Russie jusqu'en 1830. L'année 1836 est importante pour Lebesgue qui, suite aux encouragements de Poisson, publie un premier article dans le *Journal de Crelle* sur des systèmes d'équations linéaires, puis un texte intitulé *Théorème sur les quantités incommensurables* dans le premier tome du *Journal de Liouville*. Comme nous l'avons vu précédemment, Lebesgue présente également deux mémoires sur les résidus à l'Académie en 1836. Poisson et Liouville l'encouragent d'ailleurs à publier ses travaux présentés à l'Académie dans le *Journal de Liouville* et le *Journal de Crelle*. Il devient docteur ès sciences en 1837, puis obtient en 1838 son premier poste universitaire de titulaire à l'université de Bordeaux à l'âge de 47 ans. Il joue un rôle important dans le *Journal de Liouville*, aussi bien en tant qu'auteur (il fait partie des six auteurs dominants dans les premières années 1836-1840 du journal) qu'en tant que traducteur. Il devient également un des principaux auteurs des *Nouvelles Annales de Mathématiques*, en publiant quarante-trois articles, dont onze d'arithmétique à partir de 1850. Il participe également à un projet de publication d'« une théorie des nombres plus complète que celle de Legendre » [111], qui n'aboutira pas ; seule une *Introduction à la théorie des nombres* sera publiée en 1864.

Des informations sur ses travaux en mathématiques, et plus particulièrement en théorie des nombres sont données dans *Notice sur les principaux travaux de V. - A. Lebesgue rédigée par lui-même* [Abria et Houël, 1876], qu'il a écrit en 1860 en pensant présenter sa candidature à la place de membre de l'Académie des Sciences, en remplacement de Poinsot (Lebesgue avait déjà été élu membre correspondant en 1847). Il indique d'ailleurs :

109. Notre présentation s'inspire de la *Notice sur la vie et les travaux de Victor-Amédée Lebesgue* publiée en 1876 [Abria et Houël, 1876] et des nombreuses informations contenues dans [Verdier, 2009].
110. Parmi les treize textes publiés par Lebesgue en lien avec les résidus et les congruences entre 1801 et 1850, huit le sont dans le *Journal de Liouville*, ce qui représente 237 pages sur 307.
111. Extrait d'une lettre à Hoüel datée du 20 novembre 1861 : [Verdier, 2009, p. 120-121].

[...] si j'ose me mettre sur les rangs pour succéder à M. Poinsot, sans avoir, cela va sans dire, la prétention de pouvoir le remplacer, c'est parce que cet ingénieux géomètre prisait fort la théorie des nombres, théorie qui n'est généralement pas en faveur [Abria et Houël, 1876, p. 578].

Nous résumons ici les textes de Lebesgue publiés dans le *Journal de Liouville*.

Recherches sur les nombres (1837-1839) : nombre de solutions de congruences et applications à l'étude des résidus

Son travail le plus conséquent sur les résidus et les congruences est publié en trois parties sous le nom de *Recherches sur les nombres* entre 1837 et 1839. Ces trois mémoires sont composés en tout de cinq paragraphes : Lebesgue détermine dans un premier temps le nombre de solutions de congruences de la forme $ax^m+by^m+\ldots+ku^m \equiv l \pmod{p=hm+1}$, où p est un nombre premier, et applique les résultats obtenus à l'équation $x^p = 1$, aux résidus quadratiques, cubiques et biquadratiques.

Dans [Lebesgue, 1837b][112], Lebesgue reprend la question abordée par Libri sur le nombre de racines de la congruence $ax^m + by^m + \ldots + ku^m \equiv l \pmod{p = hm + 1}$:

> Quoique M. Libri ait déjà donné une formule très remarquable qui détermine le nombre de solutions d'une congruence quelconque, j'ai cru devoir cependant reprendre la question en suivant une autre marche, afin de ne pas supposer la résolution de l'équation $x^p = 1$, voulant au contraire la déduire des formules de ce paragraphe [Lebesgue, 1837b, p. 253].

Comme nous l'avons indiqué précédemment, Libri, dans [Libri, 1832a], avait développé une méthode permettant d'obtenir ce nombre de solutions sans utiliser la notion de racine primitive d'un nombre premier, mais à l'aide des fonctions trigonométriques. Ici, Lebesgue adopte une démarche inverse : il privilégie des outils arithmétiques - les racines primitives et les résidus - et non les fonctions circulaires. Or, Lebesgue a présenté en 1836 à l'Académie des sciences des recherches qui semblent proches de ce qui est publié ici. Libri et Poisson sont chargés de rédiger un rapport sur ce travail ; Libri, qui en est le rapporteur, indique :

> Cependant des travaux plus récents ont permis de ramener la théorie des congruences et celle des résidus à la théorie des équations binômes et des fonctions circulaires. C'est en s'appuyant sur ce rapprochement, et sur une formule générale déjà connue, que M. Lebesgue est parvenu à des résultats intéressants. Il a d'abord démontré d'une manière simple et générale un théorème qui fait la base de la théorie des résidus quadratiques. Ce théorème, que M. Legendre avait énoncé le premier, et auquel il avait donné le nom de loi de réciprocité, a été démontré déjà de plusieurs manières ; mais la démonstration de M. Lebesgue n'en a pas moins d'intérêt, car elle est la seule

112. Ces travaux de Lebesgue sont notamment cités dans [Weil, 1949].

qui découle immédiatement de la théorie générale des congruences par une méthode tout analytique, et sans l'emploi de ces artifices, qui ont empêché si long-temps la théorie des nombres de se lier à l'analyse algébrique [Libri et Poisson, 1836, p. 440].

Toujours selon le rapport, les résultats développés par Libri dans [Libri, 1832a] sont ici repris par Lebesgue : or ce dernier n'utilise point les formules de Libri dans ses articles publiés dans le *Journal de Liouville*, ni d'ailleurs dans son premier mémoire de 1829. On peut donc se demander si la présentation de Libri est biaisée pour donner l'impression d'un rapprochement entre ses travaux et ceux de Lebesgue du point de vue de la méthode, ou s'il existe des différences substantielles entre les travaux présentés par Lebesgue à l'Académie et ceux publiés ensuite entre 1837 et 1839. Lebesgue indique, au sujet de sa démonstration de la loi de réciprocité quadratique : « J'ai déjà donné cette démonstration dans une note sur les résidus présentée à l'Académie des Sciences. Avec cette seule différence, qu'au lieu de calculer directement les N_q, je les ai déduites d'une formule de M. Libri » [Lebesgue, 1838, p. 134]. Il est donc possible que Lebesgue, dans ses travaux de 1836, se soit d'abord appuyé sur les résultats de Libri, ou ait utilisé des méthodes similaires, puis qu'il ait ensuite obtenu les démonstrations arithmétiques qu'il présente ici.

Lebesgue commence par donner une condition, donnée sous la forme d'une congruence, qui doit être vérifiée par le nombre de solutions d'une congruence algébrique et entière de la forme $f(x_1, x_2, \ldots, x_k) \equiv 0 \pmod{p}$. En notant ce nombre de solutions S_k, où k désigne le nombre d'inconnues de la congruence, il énonce :

> Théorème. *Soit S_k le nombre de solutions de la congruence $f(x_1, x_2, \ldots, x_k) \equiv 0 \pmod{p}$, si l'on fait $f(x_1, x_2, \ldots, x_k) = X_k$ et que l'on suppose $X_k^{p-1} = \sum A x_1^a x_2^b \ldots x_k^g$, on aura, en représentant par $\sum A_{e(p-1)}$ la somme des coefficients des termes du développement de X_k^{p-1}, où les inconnues entrent toutes (c'est-à-dire en nombre k) avec des exposants multiples de $p-1$ et plus grands que zéro,*
>
> $$S_k \equiv (-1)^{k+1} \sum A_{e(p-1)} \pmod{p} \tag{1}$$
>
> [Lebesgue, 1837b, p. 254].

Lebesgue démontre ce résultat en considérant les arrangements que l'on peut faire entre les différents x_i et le fait que la somme $\sum_{i=0}^{p-1} i^a$ est congrue modulo p à $p-1 \equiv -1$ si a est multiple de p et à zéro dans le cas contraire. Il conclut en observant que (1) donne directement le nombre de solutions cherché dans les cas $k = 1, 2$ seulement.

Il applique ensuite ce théorème général à plusieurs cas particuliers de congruences :

- $x^m \equiv a \pmod{p = hm + 1}$;
- $a_1 x_1^m + a_2 x_2^m \equiv a_3 \pmod{p = hm + 1}$;

- $a_1x_1^m + a_2x_2^m + \ldots + a_kx_k^m \equiv a_{k+1} \pmod{p = hm+1}$;
- $a_1x_1^2 + a_2x_2^2 + \ldots + a_kx_k^2 \equiv a_{k+1} \pmod{p = 2h+1}$;
- $a_1x_1^3 + a_2x_2^3 \equiv a_3 \pmod{p = 3h+1}$;
- $a_1x_1^4 + a_2x_2^4 \equiv a_3 \pmod{p = 4h+1}$;
- $A_0 + A_1x_1^m + A_2x_2^m + \ldots + A_kx_k^m \equiv a_{k+1} \pmod{p = hm+1}$.

Ses résultats sont fondés sur des propriétés des résidus m$^{\text{e}}$, qu'il explique sur trois pages ([Lebesgue, 1837b, p. 257-259]). Il commence par rappeler la définition des résidus et non-résidus m^{e} :

> *Les résidus de m^e puissance pour le module $p = mh+1$ sont les racines de la congruence $x^{\frac{p-1}{m}} \equiv 1 \pmod{p}$. Ils sont en nombre $\frac{p-1}{m}$, et si l'un d'eux est représenté par a, la formule ay^m les contient tous.*
>
> Les nombres qui ne sont pas résidus de $m^{\text{ième}}$ puissance pour le module p, sont nommés non-résidus ; ils sont en nombre $p-1-\frac{p-1}{m} = (m-1).\frac{p-1}{m}$: ils se subdivisent en $m-1$ classes de $\frac{p-1}{m}$ nombres chacune. Voici le principe de cette classification importante ; il est bon de la rappeler ici, à cause de l'usage continuel que nous en ferons [Lebesgue, 1837b, p. 257].

Il classe ensuite les résidus et non-résidus m^{e} en utilisant une racine primitive ρ du nombre premier p et en appliquant la méthode de Gauss pour former les périodes dans la section VII ; par exemple, puisque le nombre premier p est de la forme $mh+1$, les résidus m^{e} sont les nombres 1, ρ^m, ρ^{2m}, …, $\rho^{(h-1)m}$ et les non-résidus de k^{e} classe sont les nombres ρ^k, ρ^{m+k}, ρ^{2m+k}, …, $\rho(h-1)m+k$. Il en déduit ensuite des propriétés sur le produit des résidus et non-résidus en fonction de leur classe.

Sans entrer dans le détail des démonstrations, illustrons son approche par le calcul du nombre de solutions de la congruence $y_1^2 + y_2^2 + \ldots + y_k^2 \equiv a \pmod{p = 2h+1}$, sur lequel est basé sa démonstration de la loi de réciprocité quadratique de Legendre. Libri introduit de nouvelles notations dans le cas de cette congruence : « nous représenterons le nombre de solutions par N_k^0, N_k, N_k' selon que l'on aura $a \equiv 0 \pmod{p}$, ou que a sera résidu quadratique, ou enfin non-résidu quadratique » [Lebesgue, 1837b, p. 267]. Puis il démontre le théorème suivant :

> Théorème. *On a pour k nombre impair,*

$$(18) \qquad \begin{cases} N_k^0 = p^{k-1}, \\ N_k = p^{k-1} + (-1)^{\frac{p-1}{2}\cdot\frac{k-1}{2}}.p^{\frac{k-1}{2}}, \\ N_k' = p^{k-1} - (-1)^{\frac{p-1}{2}\cdot\frac{k-1}{2}}.p^{\frac{k-1}{2}}, \end{cases}$$

> *et pour k pair, on a*

$$(19) \qquad \begin{cases} N_k^0 = p^{k-1} + (-1)^{\frac{p-1}{2}\cdot\frac{k}{2}}.(p-1)p^{\frac{k}{2}-1}, \\ N_k = N_k' = p^{k-1} - (-1)^{\frac{p-1}{2}\cdot\frac{k}{2}}.p^{\frac{k}{2}-1} \end{cases}$$

[Lebesgue, 1837b, p. 270]

Lebesgue conclut cette première partie en redémontrant des résultats en partie déjà obtenus par Libri dans [Libri, 1832a], mais en fondant ses preuves uniquement sur des arguments combinatoires (substitutions) et arithmétiques (racines primitives et résidus de puissances). Les théorèmes de ce texte sont réutilisés dans les mémoires suivants : nous allons nous arrêter sur certaines de ces applications.

Dans le deuxième paragraphe, Lebesgue utilise les résultats de [Lebesgue, 1837b] pour la résolution de l'équation $x^p = 1$, et en particulier pour déterminer directement les équations intermédiaires obtenues dans la méthode proposée dans la section VII des *Disquisitiones Arithmeticae* de Gauss.

Le troisième paragraphe est intitulé *Des résidus de puissances en général et des résidus quadratiques en particulier*. Lebesgue énonce puis prouve tout d'abord un théorème liant l'appartenance d'un nombre q à la classe de résidus m^{e} ou à une des classes de non-résidus au nombre de solutions d'une congruence donnée (ρ est ici une racine primitive du nombre premier p) :

> Théorème. Le nombre de solutions n_q de la congruence $x_1^m + x_2^m + \ldots + x_q^m \equiv \rho^a \pmod p$, où q est premier a nécessairement l'une des formes suivantes :
>
> 1°. $m^q(qQ+1)$, si q est de la classe a^{ieme}, et
>
> 2°. $m^q(qQ)$, si q n'est pas de la classe a^{ieme}
>
> [Lebesgue, 1838, p. 132].

Lebesgue donne ensuite une nouvelle démonstration de la loi de réciprocité quadratique, basée sur les résultats précédents. Notons que Lebesgue, même s'il rappelle la signification du symbole $\left(\frac{p}{q}\right)$, énonce la loi de réciprocité quadratique ainsi : « Soient p et q deux nombres premiers impairs et $q^{\frac{p-1}{2}} \equiv i \pmod p$ (i étant +1 ou −1) on aura $p^{\frac{q-1}{2}} \equiv i(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \pmod q$ » [Lebesgue, 1838, p. 134].

Il distingue deux cas :

- Si q est résidu quadratique de p, alors $q^{\frac{p-1}{2}} \equiv 1 \pmod p$, et $N_q \equiv 2 \pmod q$. Donc, d'après (18) : $p^{q-1} + (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.p^{\frac{q-1}{2}} \equiv 2 \pmod q$. Donc, en divisant par $p^{\frac{q-1}{2}}$, on obtient bien : $p^{\frac{q-1}{2}} \equiv (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \equiv i(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \pmod q$.
- Si q est non-résidu quadratique de p, alors $q^{\frac{p-1}{2}} \equiv -1 \pmod p$, et $N_q \equiv 0 \pmod q$, ou $p^{q-1} + (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.p^{\frac{q-1}{2}} \equiv 0 \pmod q$. Donc, en divisant par $p^{\frac{q-1}{2}}$, on obtient bien : $p^{\frac{q-1}{2}} \equiv -(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \equiv i(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \pmod q$.

Il complète ces théorèmes par les démonstrations des caractères quadratiques de 2 et 3.

Dans la dernière section de ce paragraphe, Lebesgue reproduit des résultats présentés par Gauss dans [Gauss, 1818] :

> Pour cette application [déterminer si un nombre a est résidu ou non-résidu quadratique d'un nombre premier p], rien n'est plus commode qu'un algorithme ou procédé de calcul, que M. Gauss a joint postérieurement à sa troisième démonstration. Cet algorithme ne se trouvant point dans la troisième édition de la théorie des nombres de Legendre, bien que la troisième démonstration de M. Gauss y soit rapportée, nous pensons être utile et agréable aux amateurs de la théorie des nombres, en donnant dans l'article suivant la troisième démonstration de M. Gauss, avec l'algorithme qu'il a exposé dans *Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et ampliationes novae*. C'est, selon nous, ce qu'on peut donner de plus direct pour la démonstration et de plus simple pour l'application. Nous avons d'ailleurs simplifié la partie de la démonstration rapportée par Legendre [Lebesgue, 1838, p. 137].

Ce mémoire de Gauss est publié dans les mémoires de Göttingen en latin et n'a pas été traduit depuis ; il est donc intéressant de voir que Lebesgue résume ces recherches de théorie des nombres de Gauss en français, et dans un périodique certainement plus accessible, le *Journal de Liouville*. Le rôle de Lebesgue est donc ici à mi-chemin de celui de traducteur et de celui d'auteur. Constatons qu'il n'attache pas d'importance à la transmission des seuls résultats généraux, mais également des algorithmes de calcul et des méthodes praticables.

Dans [Lebesgue, 1839], Lebesgue démontre cette fois des propriétés des résidus cubiques et biquadratiques. Dans les deux cas, il cite Gauss [113] et Cauchy [114]. Pour les résidus cubiques, il fonde son travail sur la courte note publiée en 1827 par Jacobi dans le *Journal de Crelle* : Lebesgue propose des démonstrations des résultats alors annoncés sans preuve par Jacobi. Dans sa partie sur les résidus biquadratiques, Lebesgue cite un article de Dirichlet, [Dirichlet, 1828c], tout en remarquant qu'il n'en connaît que le compte rendu écrit par Cournot dans le *Bulletin de Férussac*.

Nous allons donner ici un aperçu de la partie sur les résidus cubiques pour avoir une idée des méthodes employées par Lebesgue. Des résultats similaires pour les résidus biquadratiques figurent dans le dernier paragraphe de ses *Recherches sur les nombres*.

Lebesgue commence par exposer quelques considérations sur les racines imaginaires des congruences du second degré et des congruences binômes en observant que « la considération des racines imaginaires des congruences étant utile dans la théorie des résidus des puissances, [il se réfère à [Jacobi, 1827]], nous exposerons dans un premier article quelques propositions concernant ces racines imaginaires, qu'il importe d'introduire dans la théorie des nombres »[Lebesgue, 1839, p. 10]. Notons qu'ici, Lebesgue ne cite que

113. Il se réfère à [Gauss, 1801] pour un résultat en lien avec les résidus cubiques et aux mémoires sur les résidus biquadratiques - [Gauss, 1828] et [Gauss, 1832] - dans sa partie sur les résidus biquadratiques.
114. Il se réfère à [Cauchy, 1829a], en observant qu'il ne sait pas si Cauchy a développé davantages ses résultats.

Jacobi sur le thème des racines imaginaires des congruences. Or, comme nous l'avons précédemment remarqué, deux mathématiciens français considèrent des racines imaginaires de congruences dans leurs travaux : Poinsot, dans [Poinsot, 1820], et Galois dans [Galois, 1830]. Lebesgue connaît le texte de Poinsot, puisqu'il le cite dans ses écrits antérieurs. Galois, en revanche, n'est cité dans aucun des textes de Lebesgue considérés ici, or son article est pourtant publié en 1830 dans le *Bulletin de Férussac*. Or, Lebesgue lisait ce périodique, puisqu'il s'y réfère régulièrement.

La forme des racines imaginaires des congruences est d'abord commentée en ces termes :

> On peut conclure de là que si n est un non-résidu quadratique de p, et que la congruence $x^2 + ax + b \equiv 0 \pmod{p}$ soit impossible, on peut lui trouver deux racines imaginaires de la forme $f \pm g\sqrt{n}$, f et g étant des entiers.
>
> Il n'en est pas cependant des racines imaginaires des congruences comme des racines imaginaires des équations. Si l'on suppose, par exemple, a non-résidu cubique du nombre premier $p = 3h+1$, la congruence $x^3 \equiv a \pmod{p}$ sera impossible, l'expression $\sqrt[3]{a} \pmod{p}$ sera imaginaire, mais elle ne saurait se réduire à la forme $y + z\sqrt{n}$, où y et z sont des entiers et n un non-résidu quadratique de p [Lebesgue, 1839, p. 10].

Lebesgue annonce ensuite qu'il va étudier des congruences binômes dont toutes les racines peuvent s'exprimer sous la forme $f + g\sqrt{n}$: les congruences $x^{p+1} \equiv a \pmod{p = mq+1}$. Il expose notamment le cas particulier où $m = 3$, et rappelle comment déterminer si la racine de la congruence $x^{p+1} \equiv 1 \pmod{p = 3q+1}$, qui est de la forme $f + g\sqrt{-3}$, est résidu cubique, ou non-résidu cubique de première classe ou de deuxième classe.

À l'aide des résultats précédents sur le nombre de solutions de congruences, il détermine les caractères cubiques de 2, 3, 5 et 7 pour les nombres premiers de la forme $p = 3h + 1$ et déduit les théorèmes généraux donnés par Jacobi dans [Jacobi, 1827] :

> Théorème. Si p et q sont deux nombres premiers de la forme $6K + 1$, q sera résidu quadratique de p, si, en supposant $\beta^2 + 3 \equiv 0 \pmod{q}$ et $4p = L^2 + 27M^2$, l'on a $4p(L+3M\beta)$ (ou $p.\dfrac{L+3M\beta}{2}$ en divisant par le cube 8), ou encore $\dfrac{L+3M\beta}{L-3M\beta} \pmod{q}$, résidu cubique de q. Autrement q sera non-résidu cubique de p [Lebesgue, 1839, p. 27].

> Théorème. Si p est un nombre premier de la forme $6n + 1$, et q un nombre premier de la forme $6n - 1$, q sera résidu cubique du nombre premier p toutes les fois que $\dfrac{L+3M\sqrt{-3}}{L-3M\sqrt{-3}} \pmod{q}$, sera résidu cubique de q ; autrement q sera non-résidu cubique de p [Lebesgue, 1839, p. 31].

Dans ses *Recherches sur les nombres*, Lebesgue déduit tous les résultats sur la théorie des résidus de théorèmes sur le nombre de solutions de certaines congruences. Libri com-

mente d'ailleurs : « M. Lebesgue a eu le mérite de le déduire d'une proposition unique par une méthode uniforme et générale[...] »[Libri et Poisson, 1836, p. 440], comme lui-même l'a fait dans [Libri, 1832a]. La différence fondamentale entre les recherches de Lebesgue et de Libri consiste en ce que Lebesgue obtient ses propositions sur le nombre de solutions de congruences à partir de considérations combinatoires et arithmétiques seulement, tandis que Libri inclut la théorie des nombres dans celle des fonctions entières, et fait appel à des fonctions analytiques.

Résidus quadratiques, symbole de Legendre et applications

Les textes de Lebesgue publiés ensuite dans le *Journal de Liouville* abordent les sommes de Gauss et les symboles de Legendre et de Jacobi, et n'ont pas pour objectif une étude des résidus en tant que tels. Nous en donnons néanmoins un aperçu pour comprendre comment les résidus interviennent dans ces travaux.

Dans [Lebesgue, 1840b], Lebesgue utilise à deux reprises le fait que les nombres compris entre 1 et $p-1$, où p est un nombre premier, peuvent être partagés en deux groupes de même effectif, les résidus quadratiques et les non-résidus quadratiques, pour déterminer le signe des sommes quadratiques $\sum_{i=0}^{p-1} \sin i^2 \frac{2h\pi}{p}$ et $\sum_{i=0}^{p-1} \cos i^2 \frac{2h\pi}{p}$, où h est premier à p. Il rappelle que ce résultat a déjà été démontré par Gauss par exemple mais que sa méthode est plus simple et qu'elle se base sur l'algorithme de Gauss qui permet de déterminer si un nombre est résidu ou non-résidu quadratique. Lebesgue conclut cette note par deux problèmes ouverts, dont un concernant les sommes cubiques et biquadratiques de Gauss, en se référant aux travaux de Libri :

> M. Libri dit dans son Mémoire sur les intégrales définies aux différences finies, que la somme $\sum_{x=0}^{x=n} \cos \frac{2x^3\pi}{n}$ peut s'obtenir en fonction de a, le nombre a étant donné par l'équation indéterminée $4n = a^2 + 27b^2$; il suit en effet de la théorie de M. Gauss que
>
> $$\sum_{x=0}^{x=n-1} \left(\cos \frac{2x^3\pi}{p} + \sin \frac{2x^3\pi}{p} \sqrt{-1} \right)$$
>
> est racine de l'équation
>
> $$z^3 - 3pz - na = 0,$$
>
> en supposant a de la forme $3a' + 1$, ce qui détermine son signe. Mais il se présente ici une ambiguité du genre de celle qui a lieu pour les sommes $\sum \sin \frac{2x^2\pi}{n}$, $\sum \cos \frac{2x^2\pi}{n}$. On doit fixer le choix de la valeur de z : tant que cela ne sera point fait, la somme $\sum \cos \frac{2x^3\pi}{n}$ ne sera pas déterminée ; quand à la somme $\sum \sin \frac{2x^3\pi}{n}$, elle sera toujours nulle. On demande une règle pour fixer le choix de la valeur de z égale à $\sum \cos \frac{2x^3\pi}{n}$? On a $n = 3q + 1$.
>
> On peut proposer une semblable question pour les sommes $\sum \cos \frac{2x^4\pi}{n}$, $\sum \sin \frac{2x^4\pi}{n}$, dans l'hypothèse de $n = 4q + 1$[Lebesgue, 1840b, p. 70-71].

L'article [Lebesgue, 1842] porte sur les résidus et les non-résidus quadratiques, et sur des sommes et produits trigonométriques. Lebesgue introduit d'abord une longue suite de notations destinées à simplifier les formules en jeu. Il note les résidus quadratiques du nombre premier p : a', a'', …, $a^{(\frac{p-1}{2})}$, et généralement a, les non-résidus quadratiques b', b'', …, $b^{(\frac{p-1}{2})}$, et généralement b. La somme des résidus quadratiques de p est $\sum a$, et celle des non-résidus quadratiques, $\sum b$. Lebesgue désigne ensuite[115] par $R\frac{1}{2}$ et $R\frac{2}{2}$, le nombre de résidus quadratiques de p respectivement compris entre 0 et $\frac{p}{2}$ et entre $\frac{p}{2}$ et p ; les sommes correspondantes sont notées $\sum a\frac{1}{2}$ et $\sum a\frac{2}{2}$. Des notations similaires sont introduites pour le nombre de non-résidus quadratiques compris entre 0 et $\frac{p}{2}$, $N\frac{1}{2}$, et entre $\frac{p}{2}$ et p, $N\frac{2}{2}$ (les sommes correspondantes étant notées $\sum b\frac{1}{2}$ et $\sum b\frac{2}{2}$). Les notations a et b sont utilisées dans l'expression des sommes quadratiques de Gauss, et d'autres sommes et produits trigonométriques. Par exemple, $\sum \sin a\omega = \sin a'\omega + \sin a''\omega + \ldots + \sin a^{(\frac{p-1}{2})}\omega$ et $\prod \sin a\omega = \sin a'\omega . \sin a''\omega \ldots \sin a^{(\frac{p-1}{2})}\omega$. L'objectif de ce mémoire est de calculer les sommes $\sum \sin a\omega$, $\sum \cos a\omega$, $\sum \tan a\omega$, $\sum \text{cotan } a\omega$, $\sum \text{séc } a\omega$, $\sum \text{coséc } a\omega$, les mêmes sommes avec les non-résidus b, pour $\omega = \frac{2\pi}{p}$ et les produits correspondants pour $\omega = \frac{\pi}{p}$ et $\omega = \frac{2\pi}{p}$, en fonction de la forme du nombre premier p. On retrouve donc ici des recherches mêlant résidus quadratiques et fonctions circulaires.

Les résultats obtenus par Lebesgue dépendent notamment de $R\frac{1}{4}$ et $N\frac{1}{4}$. Il donne donc des méthodes pratiques pour obtenir les valeurs de ces expressions : lorsque p est inférieur à 1000, il renvoie au *Canon Arithmeticus* de Jacobi[116], et dans le cas où p est supérieur à 1000, il se réfère aux travaux de Dirichlet[117], où les formules recherchées sont liées avec le nombre h de formes quadratiques distinctes de déterminant $-p$: $h = 2(R\frac{1}{4} - N\frac{1}{4})$ en indiquant qu'il est plus rapide de calculer la quantité de formes quadratiques que le nombre de résidus. Néanmoins, il ajoute que cette deuxième méthode devient également impraticable lorsque le nombre p est très grand.

Le dernier problème traité par Lebesgue dans ce mémoire ne fait plus intervenir de fonctions trigonométriques : « Le produit $1.2.3 \ldots \frac{p-1}{2}$, où l'on suppose p premier de la forme $4q - 1$, est-il résidu ou non-résidu quadratique de p ? » [Lebesgue, 1842, p. 156]. À l'aide du théorème de Wilson, cette question revient à déterminer la parité de $N\frac{1}{2}$: Lebesgue renvoie encore aux méthodes de Jacobi et Dirichlet selon la grandeur de p. Il remarque également que dans ce cas, Cauchy a également donné une formule permettant de calculer directement la différence $R\frac{1}{2} - N\frac{1}{2}$ et donc $N\frac{1}{2}$ (puisque $R\frac{1}{2} + N\frac{1}{2} = \frac{p-1}{2}$). Néanmoins, Lebesgue remarque que cette méthode n'est pas vraiment utilisable en pratique : « Mais comme on ne connaît que les premiers des nombres dits de Bernoulli, la solu-

115. Lebesgue emploie des notations similaires pour les nombres et les sommes de résidus et non-résidus quadratiques compris entre 0 et $\frac{p}{4}$, …. Ainsi, $R\frac{1}{4}$ désigne par exemple le nombre de résidus quadratiques de p compris entre 0 et $\frac{p}{4}$.

116. Voir [Jacobi, 1839a] : Jacobi y présente notamment une table des indices pour les nombres premiers inférieurs à p.

117. Voir [Dirichlet, 1840].

tion précédente n'est bonne qu'en théorie » [Lebesgue, 1842, p. 157]. Lebesgue donne alors sa propre méthode, valable dans les cas où le nombre p n'est pas trop grand, et qui se réduit à calculer $\sum a$. Il observe enfin que Libri a également donné des résultats sur ce thème mais là encore : « ces formules ne paraissent pas facilement réductibles en nombres, ce qui est nécessaire pour voir une solution pratique » [Lebesgue, 1842, p. 159].

Dans [Lebesgue, 1847a], Lebesgue commente les démonstrations de la loi de réciprocité quadratique données par Cauchy [118], Jacobi [119], celle que lui-même donne dans [Lebesgue, 1838], celle de Liouville [120] et surtout celle publiée en allemand par Eisenstein en 1844 dans le *Journal de Crelle* [121], en lien avec les preuves données précédemment par Gauss. Il conclut en exposant une version simplifiée de son calcul du nombre de solutions des congruences quadratiques $x_1^2 + x_2^2 + \ldots + x_q^2 \equiv a \pmod{p}$ et de sa démonstration de la loi de réciprocité quadratique.

Dans [Lebesgue, 1847b] et [Lebesgue, 1850b], Lebesgue s'intéresse aux symboles de Legendre et de Jacobi $\left(\frac{a}{b}\right)$. Dans le premier paragraphe, il rappelle la définition de $\left(\frac{a}{b}\right)$ de Legendre puis de Jacobi, puis donne quelques propriétés fondamentales pour les deux symboles : les valeurs de $\left(\frac{p}{q}\right)^{2k}$ et $\left(\frac{p}{q}\right)^{2k+1}$, les propriétés de multiplication par rapport à a et à b dans $\left(\frac{a}{b}\right)$, les caractères quadratiques de -1, 2, et la loi de réciprocité quadratique. Il énonce ensuite dans un second paragraphe les « équations fondamentales » [Lebesgue, 1847b, p. 498] données dans le paragraphe, en utilisant à nouveau le vocabulaire de classes : les nombres k tels que $\left(\frac{k}{p}\right) = 1$ sont de la première classe. Par exemple, le caractère quadratique de 2 s'énonce : « Le nombre 2 est de première classe relativement aux nombres de forme $8k \pm 1$, et de seconde classe relativement aux nombres de forme $8k \pm 3$ » [Lebesgue, 1847b, p. 499]. Lebesgue rappelle ensuite comment passer de certaines des équations fondamentales pour des diviseurs premiers aux équations correspondantes dans le cas de diviseurs composés. Il donne certaines étapes de la troisième démonstration de la loi de réciprocité quadratique donnée par Gauss, qui est fondée sur des arguments arithmétiques et se réfère également au traitement géométrique d'une des étapes de cette preuve proposé par Eisenstein dans [Eisenstein, 1844c]. Le troisième paragraphe du mémoire de Lebesgue contient plusieurs algorithmes de calcul de $\left(\frac{a}{b}\right)$, dont celui donné par Eisenstein. Dans les paragraphes suivants, Lebesgue donne plusieurs applications des énoncés précédents : il expose en particulier une méthode pour déterminer le signe des sommes $\sum_{i=0}^{p-1} \sin i^2 \frac{2h\pi}{p}$ et $\sum_{i=0}^{p-1} \cos i^2 \frac{2h\pi}{p}$, puis en déduit le calcul de certaines sommes alternées des racines primitives d'équations binômes.

118. [Cauchy, 1829a] et [Cauchy, 1840a].
119. Cette preuve est développée et présentée par Legendre dans [Legendre, 1830].
120. [Liouville, 1847].
121. [Eisenstein, 1844d].

Ainsi, dans ses textes, Lebesgue aborde à plusieurs reprises les mêmes thèmes : propriétés des résidus quadratiques, loi de réciprocité quadratique, sommes de Gauss et autres sommes trigonométriques. Il obtient des formules pour calculer ces sommes de fonctions circulaires à partir de propriétés sur les résidus quadratiques, et en particulier en les partageant en plusieurs groupes. Pour cela, il retrouve des résultats déjà présentés par Jacobi, Dirichlet et Cauchy notamment. Il insiste à plusieurs reprises sur le degré de praticabilité des méthodes, en fonction de la taille des nombres considérés, et indique par exemple que certaines ne sont valides que théoriquement. Il aborde à nouveau plusieurs fois la question des algorithmes de calcul pour les symboles de Legendre et Jacobi $\left(\frac{a}{b}\right)$. Il indique notamment l'algorithme présenté par Eisenstein dans le *Journal de Crelle*[122]. Dans son article sur la loi de réciprocité quadratique, il commente plusieurs démonstrations de ce théorème, dont celles données par Gauss et Eisenstein. Or, cette démonstration de Gauss et tous les articles d'Eisenstein cités par Lebesgue sont publiés en latin et en allemand : comme nous l'avons déjà remarqué pour ses textes publiés entre 1837 et 1839, Lebesgue participe ainsi à la circulation de textes en France qui ne peuvent pas être lus par tous les savants.

Enfin, observons qu'ici Lebesgue applique des résultats arithmétiques sur les résidus quadratiques au calcul de formules trigonométriques notamment. Il expose d'ailleurs dans un autre texte, également publié en 1840 dans le *Journal de Liouville*, des réflexions sur la nature des démonstrations de résultats de théorie des nombres. Dans cette note, il discute une formule de Cauchy présentée à l'Académie et insérée dans le même volume du périodique :

> Dans le *Compte Rendu des séances de l'Académie des Sciences*, 6 avril 1840, M. Cauchy a montré que les théorèmes les plus élevés de la théorie des résidus quadratiques peuvent être déduits de la formule
>
> $$a^{\frac{1}{2}}(\frac{1}{2} + e^{-a^2} + e^{-4a^2} + e^{-9a^2} + \ldots) = b^{\frac{1}{2}}(\frac{1}{2} + e^{-b^2} + e^{-4b^2} + e^{-9b^2} + \ldots),$$
>
> où $ab = \pi$ [Lebesgue, 1840a, p. 186].

Lebesgue conclut cet article ainsi :

> Au reste, beaucoup de propriétés des nombres sont des conséquences plus ou moins immédiates de certaines identités. Les unes sont empruntées à l'algèbre élémentaire ; leur nombre pourrait être augmenté. D'autres sont empruntées à une algèbre plus élevée : telles sont les formules singulières de M. Gauss et autres semblables. D'autres dépendent de l'analyse infinitésimale, ou de certaines intégrales définies, telles que les fonctions elliptiques et les intégrales eulériennes de seconde espèce. Ces dernières applications deviendront sans doute de plus en plus nombreuses et reculeront les bornes de l'arithmétique transcendante ; mais peut-être

122. Voir [Eisenstein, 1844a].

conviendra-t-il, cependant, de chercher des démonstrations purement arithmétiques des théorèmes obtenus par cette voie [Lebesgue, 1840a, p. 188].

Lebesgue et les congruences

Finalement, dans les trois premiers textes analysés ici, Lebesgue reprend les thèmes travaillés par Libri quelques années plus tôt : il détermine le nombre de solutions de certaines congruences et en déduit des résultats sur les résidus quadratiques, cubiques, biquadratiques. Néanmoins, contrairement à Libri, Lebesgue appuie ses raisonnements sur des principes arithmétiques, et donne ainsi de l'autonomie à sa théorie des résidus. D'autre part, nous avons également vu qu'il considère les racines imaginaires de congruences binômes et développe des résultats similaires à ceux que Jacobi indique dans [Jacobi, 1827]. Par contre, Lebesgue ne fait allusion à aucun moment aux mémoires de Poinsot et de Galois en lien avec ces racines imaginaires. Contrairement à ces deux autres mathématiciens français qui étudient les congruences en rapport avec les équations, Lebesgue étudie certaines racines imaginaires en vue de résultats sur la théorie des résidus cubiques et biquadratiques : c'est également ce que l'on retrouve dans les travaux de Gauss, Dirichlet et Jacobi. Il se réfère également, à plusieurs reprises, à ces trois savants allemands, ainsi qu'à Eisenstein, pour les méthodes pratiques qu'ils ont développées dans leurs écrits. Enfin, il reviendra à nouveau sur les travaux de ces mathématiciens après 1850 : par exemple, dans [Lebesgue, 1854], Lebesgue entreprend de démontrer les propriétés de nos actuelles sommes de Gauss et de Jacobi, qui sont énoncées sans démonstration par Jacobi dans les premières pages de [Jacobi, 1837] [123].

On a d'ailleurs observé à plusieurs reprises que Lebesgue commente, voire récapitule, des travaux de ces trois mathématiciens, et plus tard d'Eisenstein ; ces travaux sont publiés en latin ou allemand, dans des sources parfois difficiles d'accès (comme les mémoires de Göttingen par exemple). Il semble donc non seulement connaître les travaux de ces savants allemands, mais participe également à leur circulation en France, à travers le *Journal de Liouville*.

Lebesgue apparaît donc, en tant qu'arithméticien, quelque peu dissident. Paradoxalement, sa connaissance des travaux allemands ne semble pas avoir contribué à la reconnaissance de son travail, ni même à son impact à moyen terme (puisqu'il a été largement oublié). Il serait certainement essentiel d'étudier ses différentes publications de théorie des nombres dans le contexte des travaux de Jacobi, Dirichlet, Eisenstein, Schönemann, Kummer, mais nous ne les approfondirons pas ici.

123. Ce mémoire de Jacobi est d'ailleurs traduit et inséré dans les *Nouvelles Annales de Mathématiques* en 1856.

5 - Les *Nouvelles Annales de Mathématiques* (1842-1850)

À partir de 1842 sont publiées les *Nouvelles Annales de Mathématiques*, co-éditées par Terquem et Gérono. Comme nous l'avons indiqué précédemment, les textes composant ce journal sont *a priori* destinés à l'enseignement, comme pour les *Annales de Gergonne* au début du siècle. Il est donc intéressant de trouver treize textes en rapport avec la théorie des résidus et des congruences dans les neuf premiers tomes de ce périodique[124] : nous en détaillons le contenu pour souligner l'intérêt manifesté par certains auteurs pour les résidus et les congruences d'un point de vue élémentaire. Ces textes sont écrits par six auteurs différents, dont deux publient plusieurs textes : Terquem (cinq textes) et Eugène Prouhet (quatre textes) (à la mort de Terquem en 1862, c'est Prouhet qui lui succède à la co-direction des *Nouvelles annales*). Remarquons que Lebesgue utilise aussi les *Nouvelles annales* pour annoncer son projet de publication d'un traité de théorie des nombres, qui ne verra pas le jour :

> Ces *Exercices* contiendront dans un ordre et avec des démonstrations simplifiées, les recherches contenues dans la *Théorie des Nombres* de Legendre, et les *Disquisitiones Arithmeticae*, de Gauss. Les travaux de M. Cauchy, notamment ceux qui ont rapport à l'équation binôme, et de nombreux Mémoires de MM. Jacobi, Dirichlet, Eisenstein, Kummer, etc., entreront en substance dans ces *Exercices*... [Lebesgue, 1849, p. 87].

(a) La *Théorie élémentaire des nombres* de Terquem

Sur les cinq articles de Terquem, quatre sont fortement inspirés de mémoires publiés par des mathématiciens allemands - Gauss, Jacobi, Dirichlet et Kronecker - entre 1801 et 1845 dans le *Journal de Crelle*.

Par cette diffusion retardée, Terquem semble souhaiter mettre en avant la théorie des résidus et des congruences. Ainsi, dans [Midy, 1845, p. 147], il se réfère à la méthode de résolution des équations indéterminées du premier degré présentée par l'auteur en indiquant en note : « Cette méthode est précisément celle des congruences de M. Gauss. C'est pour la propager que nous avons inséré cet article (III, 343) ». L'article (III, 343) est en fait une page de sa *Théorie élémentaire des nombres*[125].

Toutefois, même si Terquem et les autres auteurs d'articles sur les résidus et les congruences des *Nouvelles annales* se réfèrent très souvent à l'ouvrage de Gauss, on ne trouve le symbole $\equiv$ que dans un seul des treize textes : une courte note de Lebesgue, publiée en 1850, où il discute de l'appellation *équivalence* utilisée par Cauchy à la place de congruence. Dans tous les autres articles, c'est la notation $\dot{p}$ qui est utilisée, pour désigner un multiple de p. Il semble que Terquem soit à l'origine de ce choix, dans le cinquième de

124. Ces différents écrits sont listés en annexe, à partir de la page 493.
125. Voir [Terquem, 1844].

ses articles et le plus personnel, sa *Théorie élémentaire des nombres*, paru en 1844 ; il y indique d'ailleurs, dans la partie *Division, diviseurs, résidus* :

> *Notation.* Nous proposons de désigner le multiple quelconque d'un nombre par un point placé sur ce nombre ; ainsi, $\dot{5}$, $\dot{p}$ désignent des multiples quelconques de 5 ou de p, et l'équation $a = \dot{p}$ signifie que a est un multiple de p.
>
> *Observation.* Le point est déjà employé pour désigner une multiplication quand il est placé à côté du nombre [Terquem, 1845, p. 214].

À la fin de son mémoire, il justifie encore son choix :

> *Remarque.* Euclide, au livre X, prop. 80, dit qu'une ligne est *congrue* à une autre, lorsqu'elle satisfait à certaine condition de commensurabilité. M. Gauss a transporté cette locution en arithmétique et en a fait la base d'une doctrine qui fait époque dans la théorie des nombres ; l'illustre géomètre écrit ainsi les congruences $a \equiv b \pmod{p}$; les notations étant purement conventionnelles, lorsqu'elles n'ont pas encore acquis la sanction des siècles, on peut et on doit les changer, s'il y a avantage. Legendre a adopté cette forme $a - b = M(p)$, où M est la lettre initiale du mot multiplicateur ; quelquefois encore, il emploie cette forme $\frac{a-b}{p} = e$, e étant la lettre initiale du mot entier. Nous avons pensé que le point, étant déjà admis pour une multiplication, pourrait par analogie encore servir dans les congruences. On fait ce signe facilement et promptement ; ce qui est un avantage pour le calculateur et aussi sous le rapport typographique [Terquem, 1845, p. 343] .

La première partie de la théorie de Terquem contient des définitions générales, comme celles d'*unité* ou de *compter*, et des propriétés de la multiplication. La deuxième partie, sur les diviseurs, rassemble des résultats sur les *résidus*, *résidu* ayant le sens général de reste de division euclidienne. Terquem y donne des propriétés générales, comme « le résidu d'un produit est égal au produit des résidus des facteurs » [Terquem, 1844, p. 216]. Dans la troisième et dernière partie, Terquem discute notamment l'algorithme d'Euclide permettant de déterminer le plus grand diviseur commun de deux nombres ; c'est aussi dans cette partie qu'il rappelle la définition de deux nombres *congrus* selon Gauss ; le dernier paragraphe, *Théorie des résidus dans les progressions arithmétiques ; congruences du 1er degré* montre en particulier que « n nombres entiers consécutifs étant divisés chacun par n, donnent les résidus 0, 1, 2, 3, …, $n-1$, dans un ordre quelconque » [Terquem, 1844, p. 344].

(b) Les comptes rendus de Terquem

Dans ses quatre autres articles, Terquem expose le contenu d'articles ou de sections de mémoires d'auteurs allemands.

En 1843, il s'agit de la démonstration du théorème de Wilson proposée par Gauss dans les *Disquisitiones Arithmeticae* (section III, art. 76), qui s'appuie sur les *nombres associés* d'Euler : deux nombres dont le produit est $\dot{p} + 1$.

En 1845, Terquem reproduit l'article de Dirichlet, publié dans le *Journal de Crelle* en 1828, qui contient des démonstrations des théorèmes de Fermat et Wilson [126]. Il rappelle une définition généralisée des nombres associés, donnée par Dirichlet : soit p un nombre premier, a, m et n des nombres entiers inférieurs à p. Alors m et n sont *associés* lorsque $mn = a + \dot{p}$ (Terquem faisant observer que « ces symboles ne sont pas ceux de l'auteur » [Terquem, 1845, p. 380]). Ni Terquem, ni Dirichlet en 1828, ne donnent un nom spécifique au nombre a.

En 1848, Terquem reprend une démonstration d'un théorème d'*arithmologie* [127] de Steiner donnée par Jacobi en 1835. Il applique le théorème de Fermat pour prouver que

> p est un nombre premier ; a_1, a_2, …, a_n sont n nombres premiers à p et dont les résidus après division par p sont *différents* ; la somme des combinaisons avec répétition de la classe $p - r$ de ces n éléments est divisible par p lorsque $r > 1$ et $< n - 1$ [Terquem, 1848, p. 268].

Enfin, Terquem expose une démonstration, qu'il qualifie de plus simple, de l'irréductibilité de l'équation $1 + x + x^2 + \ldots + x^{p-1}$ lorsque p est un nombre premier proposée par Kronecker, alors étudiant, en 1845 dans le *Journal de Crelle*. Il note f une fonction à coefficients entiers $f(x) = a + a_1 x + a_2 x^2 + \ldots a_{p-1} x^{p-1}$, et α une racine imaginaire de $x^p = 1$: la preuve est fondée sur la congruence $B - A^{p-1} = \dot{p}$, où $A = f(1)$, $B = f(\alpha) f(\alpha^2) \ldots f(\alpha^{p-1})$.

(c) Eugène Prouhet et la théorie des résidus

Eugène Prouhet, professeur au collège royal de Auch, est un des principaux auteurs des *Nouvelles Annales* avant 1855 [128]. Il publie dans le périodique quatre textes où interviennent les résidus et les congruences.

Dans le premier article publié en 1845, *Note sur le nombre qui indique combien il y a d'entiers inférieurs et premiers à un nombre donné*, Prouhet détermine le nombre d'entiers inférieurs et premiers à un nombre donné N. Il nomme cette quantité l'indicateur de N et le note $i(N)$. Concernant les résidus et les congruences, il n'utilise ici que la notation de Terquem. Il donne néanmoins un premier lemme qui lui sert également dans son article suivant : « si a et b sont deux nombres premiers entre eux ; α un nombre inférieur et premier à a ; β un nombre inférieur et premier à b ; il n'existe qu'un seul nombre $z < ab$, qui soit à la fois $\dot{a} + \alpha$ et $\dot{b} + \beta$. Il conclut également que l'indicateur permet de déduire de nombreux théorèmes, dont : « Deux nombres a et p étant premiers entre eux, on a toujours $a^{i(p)} - 1 = \dot{p}$ » [Prouhet, 1845a, p. 81]. Ainsi, il formule le théorème d'Euler-Fermat à l'aide de la notation de Terquem.

126. Nous avons abordé ce mémoire, [Dirichlet, 1828a], dans notre analyse du contenu du *Bulletin de Férussac*.

127. Cette terminologie est utilisée fréquemment par les auteurs des *Nouvelles Annales* au lieu de « théorie des nombres ».

128. Norbert Verdier le cite à ce titre aux côtés de Catalan, Faure, Gerono, Lebesgue et Terquem dans [Verdier, 2009, p. 278].

Il publie un deuxième texte dans lequel il revient sur la notion de nombres associés, et indique qu'il nomme un nombre *a associé double* s'il est associé avec lui-même : $a^2 = \dot{p} + 1$. L'objectif de son texte est de déterminer combien il y a d'associés doubles pour un nombre p donné. Par exemple, pour un nombre composé de deux facteurs premiers entre eux A et B, il utilise le lemme énoncé dans l'article précédemment : il existe un et un seul nombre x qui est de la forme $\dot{A} + 1$ et $\dot{B} - 1$, soit $x^2 = 1 + \dot{AB}$. De même on peut prendre x de la forme $\dot{A} - 1$ et $\dot{B} + 1$: Prouhet montre que cela donne un associé double différent. Il en déduit que, pour chaque décomposition en deux facteurs premiers entre eux du nombre p, on a un nouveau couple d'associés doubles, puis obtient finalement le nombre d'associés doubles, noté ν, en fonction de la forme de P, et une version généralisée du théorème de Wilson. L'éditeur Terquem remarque en note que des démonstrations de ces résultats ont également été données par Gauss en 1801, puis par Poinsot en 1845.

En 1846, paraît un texte de Prouhet sur les résidus de puissances. Il considère un nombre premier P et rappelle que si a^n est la première puissance dont le résidu est 1, alors : « tous les résidus précédents seront différents entre eux ; au delà, ils se reproduiront dans le même ordre » [Prouhet, 1846, p. 176]. Il indique également que le nombre n est un diviseur de l'indicateur de P (sans remarquer que c'est une conséquence du théorème d'Euler-Fermat, énoncé dans son article précédent). Il nomme *période de a* les résidus de a, a^2, a^3, …, a^n et *système de périodes* les périodes de tous les nombres inférieurs et premiers à P. Il utilise ce vocabulaire pour rappeler la définition d'une racine primitive : relativement au diviseur P une *racine primitive par rapport à n* est un nombre dont la période est de n termes, et une *racine primitive* est un nombre dont la période est de $i(P)$ termes. Il remarque que sa définition est bien en accord avec celles d'Euler, pour le cas particulier où P est un nombre premier, et de Poinsot [129]. Il justifie ensuite son étude :

> Cela posé, l'objet de ce mémoire est l'étude détaillée et complète autant que possible des différents systèmes de périodes. Les théorèmes que nous démontrerons ne sont pas nouveaux ; à quelques développements près, ils se trouvent dans l'ouvrage de Legendre, mais séparés et déduits de théories différentes. Nous avons cru utile de les réunir et de les déduire les uns des autres d'une manière uniforme. Ce travail aura en outre l'avantage de faciliter aux jeunes lecteurs de ce journal, l'accès de la théorie des nombres, partie difficile et encore peu cultivée des mathématiques, et sur laquelle paraît aujourd'hui reposer l'avenir de la science [Prouhet, 1846, p. 178].

Prouhet partage la suite de son texte en deux parties : l'étude générale des périodes, puis le cas où le nombre P est premier. Il montre par exemple qu'en général, si la période de a comporte n termes, alors les nombres a^m et a^{n-m} sont associés, puis en déduit le produit des résidus d'une période : si la période a un nombre impair de termes, le produit des résidus est $\dot{P} + 1$; dans le cas contraire, le produit est $\dot{P} - 1$. Il en déduit le théorème de Wilson dans son deuxième paragraphe.

129. Il se réfère à [Poinsot, 1845].

Il conclut son article sous la forme d'un exercice, consistant à déterminer les preuves de deux théorèmes d'Euler :

- si dans une période, γ et γs sont des résidus premiers avec P, alors s est également un résidu ;
- si α est un résidu et a est un non-résidu, alors le produit $a\alpha$ est un non-résidu.

Dans le dernier texte, publié en 1850, Prouhet traite de l'irréductibilité de l'équation cyclotomique $1 + x + \ldots + x^{p-1} = 0$. Pour démontrer ce résultat, il s'appuie notamment sur le théorème énoncé ainsi : « une congruence de degré n ne peut avoir plus de n racines, lorsque le module est premier » [Prouhet, 1850, p. 348].

(d) Applications des résidus et congruences

Voyons maintenant les articles des autres auteurs.

Catalan, dans [Catalan, 1842], revient sur la théorie des fractions décimales périodiques en utilisant des résultats sur les restes :

> La note suivante ne contient rien de neuf : si je me décide à la publier, c'est parce que la manière dont on présente ordinairement la théorie des fractions périodiques n'est, si je ne me trompe, ni très-logique, ni très-rigoureuse. En outre, cette théorie s'appuie assez naturellement sur le théorème de Fermat et sur d'autres propriétés intéressantes... [Catalan, 1842, p. 457].

Parmi ces propriétés, on retrouve notamment : si n et a sont premiers entre eux, alors les restes de a, $2a$, $3a$, ..., $(n-1)a$ après division par n sont tous distincts. Catalan rappelle également le théorème de Fermat, et sa version généralisée, en termes de divisibilité. Par exemple : « Si D est un nombre premier par rapport à N, et si k indique le nombre des entiers inférieurs et premiers à D, on a $\frac{N^k-1}{D}$ = entier » [Catalan, 1842, p. 464]. Cette formulation "à la Legendre" semble bien éloignée des résidus et des congruences, mais plus loin, Catalan remarque que « 10 est une *racine primitive* de 7, c'est-à-dire que les 6 premières puissances de 10 divisées successivement par 7, donnent pour restes les 6 nombres qui précèdent 7. Le théorème de Fermat donne $10^6 = \dot{7} + 1$ » [Catalan, 1842, p. 469]. Il exprime de même le théorème de Wilson à l'aide du symbole de Terquem. Ici, on voit que, petit à petit, Catalan intègre des notations associées aux congruences dans son exposé d'arithmétique élémentaire.

De même, Midy, dans son article sur la résolution de l'équation indéterminée du premier degré $ax \pm by = \pm c$, annonce qu'il va utiliser une méthode plus simple :

> Aussi diverses méthodes de résolution sont-elles développées avec soin et une certaine étendue, dans les ouvrages estimés d'algèbre qui sont actuellement entre les mains des élèves. La suivante, fondée sur la théorie des restes, donnera toujours, nous le croyons du moins, une solution plus facile et plus prompte [Midy, 1845, p. 147].

C'est ce commentaire de Midy [130] qui donne d'ailleurs lieu à la remarque de Terquem citée plus haut concernant son souhait de propager la théorie des congruences de Gauss. Dans ce mémoire, Midy considère ainsi les résidus issus de progressions arithmétiques.

Drot, dans [Drot, 1845], veut déterminer à quelle puissance il faut élever un nombre N pour que le dernier, les deux derniers, puis les trois derniers chiffres se reproduisent. Dans la méthode proposée, il applique le petit théorème de Fermat, et expose des raisonnements sur les restes pour finalement conclure :

> Je terminerai en observant qu'on pourrait simplifier davantage ces sortes de recherches, en ayant recours aux différents principes démontrés dans les *Disquisitiones Arithmeticae* de Gauss... [Drot, 1845, p. 644].

(e) Conclusion

La théorie des résidus et des congruences, d'un point de vue élémentaire, tient donc une place non négligeable dans les *Nouvelles Annales*. Aux yeux de Terquem au moins, les résultats autour de ces objets semblent être dignes de l'enseignement [131] ; rappelons que dans le premier tiers du siècle, on ne trouve pas de textes sur les résidus ou les congruences dans le prédécesseur des *Nouvelles Annales* : les *Annales de Gergonne*. Les auteurs des textes considérés ici donnent des exposés accessibles en lien avec les résidus et les congruences, utilisant des résultats démontrés par Euler, ou encore des propriétés élémentaires contenues dans les *Disquisitiones Arithmeticae*. Par contre, les symboles $\equiv$ de Gauss ou Mp de Legendre ne sont pas intégrés : tous les auteurs cités ici emploient le signe $\dot{p}$ pour désigner un multiple quelconque de p.

Enfin, notons que des travaux en rapport avec la théorie des résidus et des congruences continuent d'être insérés dans les *Nouvelles Annales* après 1850. On peut par exemple citer un article non élémentaire de Jacobi sur la cyclotomie, publié en 1837 dans les *Mémoires* de l'Académie de Berlin. Jacobi y expose notamment des résultats fondamentaux sur les sommes de Gauss et de Jacobi, et sur la cyclotomie plus généralement. Ce mémoire est traduit puis inséré dans les *Nouvelles Annales* en 1856.

130. Le seul renseignement que nous avons sur cet auteur est qu'il était professeur au collège de Nantes en 1835.

131. Cette position favorable ne semble pas être partagée par tous : en effet, en 1843, Réalis publie un article intitulé *De la résolution algébrique de l'équation $x^p - 1 = 0$, quand l'exposant p est un nombre premier*, où l'auteur rapporte de façon élémentaire la méthode de résolution algébrique de l'équation binôme $x^p = 1$ exposée par Gauss dans la section VII des *Disquisitiones Arithmeticae*. Il décrit comment décomposer graduellement l'équation cyclotomique $\frac{x^p-1}{x-1}$ en termes de divisibilité, sans utiliser explicitement des congruences ou des racines primitives.

CHAPITRE 4

Des sources communes pour des perspectives différentes

I Résidus et congruences dans les journaux en France de 1801 à 1850

Nous sommes maintenant en mesure de préciser où et comment interviennent dans les périodiques disponibles sur la scène française les travaux arithmétiques liés aux résidus et les congruences. Remarquons tout de suite que ces conclusions ne valent pas pour l'ensemble des travaux arithmétiques : les *Annales de Gergonne* ou le *Bulletin de la Société Philomathique* n'apparaissent pas ici, puisqu'on n'y retrouve pas de texte sur notre thème. Ces périodiques mathématiques du début du siècle contiennent néanmoins des articles de recherche sur l'arithmétique [1].

Avant 1825, en dehors des livres, les seules publications pertinentes, d'ailleurs très rares, sont de nature académique : comme nous l'avons dit, le *Journal de l'École Polytechnique* apparaît alors fortement lié à l'Académie des sciences, avec les mêmes auteurs. L'article [Poinsot, 1820] est le seul mémoire où les congruences ont une place de choix, et son auteur est le principal auteur de cette période en France.

1 - Le milieu des années 1820 : le *Bulletin de Férussac*

Ce n'est qu'à partir de 1825 que l'on retrouve des entrées en lien avec notre thème dans un autre type périodique en France : le journal en question est le *Bulletin de Férussac*. Cette période voit par ailleurs une floraison d'articles dans le *Journal de Crelle*, en particulier ceux de Jacobi et Dirichlet.

Le rôle du *Bulletin de Férussac* est ici double. D'une part, il fait fonction de répertoire des différentes productions publiées pendant sa période d'existence : nous avons montré que les travaux présentés à l'Académie ou insérés dans les *Mémoires* de l'Académie sont souvent signalés, voire commentés. Des publications indépendantes, non périodiques, comme les ouvrages de Lacroix et de Legendre, sont également indiquées. Enfin, le contenu de plusieurs périodiques y est résumé, c'est-à-dire pour notre thème, le *Journal de Crelle*. Les comptes rendus des articles de ce périodique allemand sont pratiquement tous confiés à Cournot, qui joue donc un rôle significatif dans la diffusion des résultats et des méthodes pour notre sujet. Lebesgue s'y réfère par exemple à au moins deux reprises dans

1. Voir par exemple la démonstration du théorème de Fermat sur les nombres polygones donnée par Cauchy insérée dans une note en 1815 dans le *Bulletin de la Société Philomathique* ou encore l'article de Gergonne sur les nombres polygones publié en 1814 dans ses *Annales*.

ses travaux, dans lesquels il reprend notamment des résultats développés auparavant par Poinsot, Jacobi, Dirichlet.

Cournot intègre effectivement des commentaires étayés sur plusieurs articles arithmétiques du *Journal de Crelle* et sur d'autres mémoires, en insistant particulièrement sur certaines idées qu'il juge importantes. Il fait également le lien entre différents travaux : ainsi, dans son compte rendu de [Jacobi, 1827], il rappelle que Gauss a l'intention de publier lui aussi des travaux sur le sujet abordé par Jacobi, et que Poinsot a mis lui-même en avant les idées qui y sont développées. De plus, Cournot, proche de Dirichlet notamment, donne la primeur de certains résultats ou démonstrations non encore publiés aux lecteurs du *Bulletin*. Ces commentaires introduisent certains décalages par rapport aux textes originaux : nous avons vu, par exemple, que dans son compte rendu de [Dirichlet, 1828b], Cournot met en avant les résultats sur les équations, en omettant d'utiliser les congruences, pourtant largement présentes dans le texte original. Compte tenu de l'importance du *Bulletin de Férussac* et celle, en particulier, des commentaires de Cournot comme source d'informations pour les savants de la scène française, ces décalages de formulation ne sont pas anodins ; le *Bulletin* donne une forme spécifique à la réception des congruences.

Le deuxième rôle du *Bulletin de Férussac* est celui de permettre l'insertion de plusieurs mémoires inédits. Ainsi, Cauchy et Libri, ayant pourtant leurs entrées à l'Académie des Sciences, choisissent néanmoins d'insérer dans le périodique certains de leurs travaux, sous forme de note succincte ou d'article d'une dizaine de pages, probablement pour pallier les lenteurs de l'institution. Les recherches de Cauchy sur les formes quadratiques, présentées à l'Académie et diffusées par le *Bulletin de Férussac* ne seront publiées que dix ans plus tard dans les *Mémoires*. D'autres profitent du *Bulletin de Férussac* comme un des seuls moyens à leur disposition pour rendre leurs travaux publics : pour notre thème, c'est le cas de Lebesgue, ou du mémoire de théorie des nombres de Galois sur les racines imaginaires de congruences.

Dans ce périodique, tous les aspects des travaux sur les résidus et les congruences sont abordés. Dans les différentes entrées du *Bulletin*, nous retrouvons effectivement quelques commentaires sur des travaux élémentaires, comme, par exemple, la note de Hörner sur le théorème de Fermat parue en 1826, des traités généraux et des comptes rendus (voire des mémoires complets) sur des travaux de recherche de Cauchy, Galois, Lebesgue, Jacobi, Dirichlet, ... Ainsi, sans ce périodique, nous n'aurions retrouvé aucune trace sur la scène française d'études sur les résidus d'ordre supérieur et les lois de réciprocité associées. Jusqu'au début des années 1830, ce périodique constitue donc la source, une ressource globale, rendant compte en temps court des différents travaux sur les résidus et les congruences.

2 - Début des années 1830 : le grand vide pour les périodiques français

L'édition du *Bulletin de Férussac* cesse en 1831 ; cet arrêt prive ainsi les savants français d'un moyen de communication efficace et facilement accessible par rapport aux publications institutionnelles. Sur cette période, les seuls articles écrits par des auteurs de la scène française et contenant des raisonnements significatifs sur les résidus et les congruences sont au nombre de deux et sont insérés dans le *Journal de Crelle* ; les auteurs en question sont Libri et Germain [2]. Le périodique allemand prend ainsi provisoirement le relais des éventuels moyens de communication français, et son rôle dans la diffusion du thème est majeur.

3 - À partir de 1835 : de nouveaux espaces éditoriaux et une redistribution des publications

Entre 1835 et 1850, trois nouveaux périodiques publiés en France deviennent pertinents pour notre enquête : cette fois, chacun a ses propres spécificités, du point de vue des auteurs et des contenus, mais aussi de leurs liens les uns avec les autres. Ainsi, les *Comptes Rendus* des séances de l'Académie contiennent les travaux de recherche ayant reçu l'approbation académique. Dans ce périodique institutionnel, Cauchy est le principal pourvoyeur de travaux sur notre thème, avec plus de vingt notes. Les notes sont généralement développées dans des mémoires intégrés à d'autres périodiques : les *Mémoires* de l'Académie, le *Journal de Liouville* ou encore les *Exercices d'analyse et de physique mathématique* dans le cas de Cauchy.

Le *Journal de Liouville*, créé en 1836, est relié à l'Académie dans la mesure où des textes de Cauchy, Liouville et Poinsot insérés dans le *Journal de Liouville* ont, dans un premier temps, été présentés à l'Académie. Mais il est aussi relié au *Journal de Crelle* ou aux publications de l'Académie de Berlin, dont il reproduit certains articles, la plupart traduits en français. Il offre enfin une place à d'autres auteurs, un en particulier, puisque huit des dix articles originaux sont de Lebesgue. De ce point de vue, à cette époque, le *Journal de Liouville* constitue un remplacement (partiel, nous le verrons dans un instant) du *Bulletin de Férussac*, ce qui n'est pas le cas des *Comptes Rendus* de l'Académie des sciences. [3] Là encore, l'éditeur Liouville joue un rôle dans la circulation de ces travaux, notamment en entretenant une correspondance avec Jacobi et Kummer. Cette continuité entre les deux publications est illustrée de manière frappante par la réédition de l'article

2. Norbert Verdier souligne d'ailleurs la persistance de Crelle à vouloir intégrer des articles d'auteurs étrangers dans son journal ; le rédacteur allemand insiste particulièrement auprès de Hachette et Abel pour trouver des auteurs français. Norbert Verdier indique également que Sophie Germain entre en contact avec Crelle vraisemblablement par l'intermédiaire de Libri : voir [Verdier, 2009, ch. 2].

3. Comme l'a montré Hélène Gispert, ceux-ci semblent occuper un rôle de plaque tournante, au moins pour la scène française, dans la deuxième moitié du siècle, voir [Gispert, 1991].

de Galois de 1830 en 1846, lors de l'édition par Liouville des œuvres de Galois.

Le troisième journal, les *Nouvelles Annales de Mathématiques*, se distingue radicalement des deux autres par ses objectifs et la nature de son contenu : les articles le composant sont en grande majorité destinés à l'enseignement et les textes liés aux résidus et aux congruences, dont les principaux auteurs sont Terquem et Prouhet, témoignent à la fois du souhait d'intégrer ces sujets à la formation de base (au moins celle des enseignants) et du fait qu'une partie au moins de cette théorie y est considérée à un niveau élémentaire. Il est remarquable de totaliser plus de dix textes sur ce thème, alors que la théorie des nombres ne figure pas aux programmes des concours dont la préparation est officiellement le principal but du journal. Certains de ces textes ont explicitement un objectif pédagogique : nous pouvons par exemple penser à l'article [Prouhet, 1850], dans lequel l'auteur propose au lecteur, en guise d'exercice, de déterminer des résultats sur les propriétés opératoires des résidus et non-résidus de puissances énoncés par Euler au XVIII^{e} siècle. Presque tous les textes repérés se distinguent par la présence d'une nouvelle notation visant à remplacer le symbole $\equiv$ de Gauss, et vraisemblablement proposée par Terquem. Ainsi, les auteurs concernés abordent les notions fondamentales de la théorie des résidus, ou reprennent des articles de savants comme Gauss, Dirichlet ou Jacobi, en remplaçant le signe $\equiv$ par leur propre notation. Avec ces quelques textes des *Nouvelles Annales*, nous assistons par conséquent à un développement d'une théorie élémentaire des résidus et des congruences qui semble se vouloir autonome et destiné à l'enseignement. Par rapport aux *Annales de Gergonne*, publiées au début du siècle et annonçant des objectifs similaires, la place des résidus et des congruences dans la communauté enseignante semble donc avoir évolué.

Le seul auteur commun entre les *Nouvelles Annales* et les deux autres journaux est également le seul à conserver la notation de Gauss dans la note qu'il insère dans les *Nouvelles Annales* : Lebesgue publie ainsi un court texte élémentaire dans ce journal [4], insère quelques notes aux *Comptes Rendus* de l'Académie des Sciences et domine de manière écrasante les productions de théorie des nombres dans le *Journal de Liouville*. Cette diversité de possibilités éditoriales permet donc à des savants dont la position n'est pas centrale de faire connaître leurs travaux ; elle témoigne aussi de la manière dont un auteur comprend le paysage éditorial qui lui est alors offert.

Un sujet qui reste tout au long de la période très marginal, comme les congruences, permet donc malgré tout de repérer certains changements du paysage éditorial en France entre 1800 et 1850. Au *Bulletin de Férussac*, dont la diversité couvre presque tous les domaines liés aux résidus et aux congruences, succède après 1835 une répartition éditoriale entre les articles élémentaires, publiés dans les *Nouvelles Annales*, et les travaux

4. De nombreux articles de Lebesgue continuent à paraître dans les *Nouvelles Annales* à partir de 1850.

de recherche édités dans les *Comptes Rendus* de l'Académie et le *Journal de Liouville*. La tentative de développer une notation indépendante montre d'ailleurs que les auteurs des *Nouvelles Annales* ne voient pas leurs articles comme une simple vulgarisation, mais comme la base d'une possible discipline d'enseignement retravaillée dans cet objectif. Nous avons de plus souligné les différences dans les thématiques abordées dans les deux derniers journaux. Enfin, alors les auteurs des *Nouvelles Annales* sont le plus généralement liés à l'enseignement, l'auteur dominant des *Comptes Rendus* est au centre de l'institution, alors que celui du *Journal de Liouville* a une position bien plus marginale. Cette position, par rapport à la prolixité de l'auteur, montre bien qu'une spécialisation sur l'arithmétique, en particulier sur les congruences, ne sert pas à elle seule à assurer facilement une carrière académique en France [5].

Soulignons au passage que le rôle bien connu de certains hommes dans la circulation des idées mathématiques à cette époque se retrouve à l'échelle bien plus petite des résultats sur les résidus et les congruences : en effet, les commentaires de Cournot donnent un aperçu général de certaines recherches publiées à l'étranger, Crelle encourage la collaboration de certains auteurs français à son journal, Liouville agit, comme l'a souligné de manière plus générale Norbert Verdier, pour « faire de son *Journal* un lieu d'échanges et de sociabilité »[Verdier, 2009, p. 178].

Par rapport au *Bulletin de Férussac* dans les années 1820, ni *Journal de Liouville* ni les *Nouvelles Annales* ne contiennent de comptes rendus détaillés sur le *Journal de Crelle* par exemple. Néanmoins, d'après les références données par les auteurs français publiant dans les années 1840, les travaux publiés dans le périodique allemand par Jacobi, Dirichlet, Eisenstein, Kummer, semblent au moins en partie connus. Plus généralement, l'examen de ces références croisées permet de mettre en lumière plusieurs choses [6] :

Tout au long de la période, nos auteurs citent Euler, Lagrange, Legendre et Gauss. Ces références sont présentes de manière générale, mais dans les années 40, Lagrange est moins cité par les auteurs du *Journal de Crelle*. Par ailleurs, on constate que les auteurs de notre corpus pour la deuxième période se citent souvent entre eux, et citent aussi les auteurs de la première période, comme Poinsot et Libri. Poinsot, en revanche disparaît des références du *Journal de Crelle*. Celles-ci d'ailleurs tendent à se refermer sur elles-mêmes : en 1844, Eisenstein cite Gauss, Jacobi et Dirichlet presque exclusivement (deux fois Legendre, une fois Abel), alors que c'est beaucoup moins le cas pour les auteurs de notre corpus. Cauchy par exemple fait référence à presque tous les autres auteurs. On peut se demander si c'est un effet de la nature du *Journal de Liouville* qui donne un aperçu assez complet de nombreux auteurs, ou si cela tient aux recherches engagées en tant que telles. Le contenu du *Journal de Crelle* semble être connu au moins partiellement

5. Il serait intéressant d'explorer cette question en référence avec les cas contraires rapportés pour la Prusse dans [Pieper, 2007].

6. Nous ne développons pas cette approche ici, mais renvoyons aux exemples de [Goldstein, 1999], [Gauthier, 2007], [Brechenmacher, 2010].

par Cauchy : nous verrons dans notre quatrième partie que Cauchy se réfère en 1847 à un texte de Kummer, publié en allemand dans le *Journal de Crelle* seulement. Quoi qu'il en soit, nous comprenons mieux comment a pu se développer, à partir de la seule lecture des textes du *Journal de Crelle* une historiographie quelque peu tronquée du sujet - il est à noter d'ailleurs que certains auteurs de ce journal, comme Arndt, n'en sont pas moins oubliés.

II Résidus et congruences en France de 1801 à 1850 : un discours commun, des réponses variées

Ces différences dans les modes de publication et les références sont-elles le signe de différences dans les pratiques mathématiques elles-mêmes ? Dans l'analyse développée dans le chapitre précédent, nous avons mis en évidence certaines spécificités des savants français au cours de la première moitié du XIX^{e} siècle. Dès l'introduction générale et dans l'étude des monographies liées aux résidus et aux congruences dans notre deuxième chapitre, nous avons confirmé que la réception en France des *Disquisitiones Arithmeticae* de Gauss au début du siècle est liée principalement à la section VII, c'est-à-dire au traitement de l'inscription des polygones réguliers dans le cercle, que Gauss interprète comme l'étude de l'équation vérifiée par les racines de l'unité ; c'est à cette étude qu'il applique sa théorie des congruences, en utilisant tout particulièrement les racines primitives, développée dans les premières sections. Ce lien entre théorie algébrique des équations et théorie des nombres en général, congruences en particulier transparaît implicitement ou explicitement dans la plupart des travaux des auteurs rencontrés dans notre corpus.

La plupart de ces auteurs observent aussi régulièrement, en le déplorant, ce qu'ils décrivent comme l'isolement de la théorie des nombres. À partir de ce constat, ils proposent différentes approches visant le plus souvent à rattacher les congruences à d'autres domaines mathématiques. Leurs écrits sont parsemés de commentaires sur la nature des démonstrations des résultats arithmétiques, sur la nature et la praticabilité des méthodes proposées. Ce sont les modalités des travaux *de recherche* sur les résidus que nous examinons dans cette section, cette fois, du point de vue des auteurs eux-mêmes.

Remarquons tout d'abord leur petit nombre, une douzaine sur l'ensemble de la période. Mis à part Legendre, né au milieu du dix-huitième siècle, on y trouve d'exacts contemporains de Gauss (Sophie Germain et Louis Poinsot sont respectivement nés en 1776 et 1777), puis la génération née autour de la Révolution (comme Cauchy né en 1789 ou Lebesgue né en 1791) ; viennent ensuite Libri, Jacobi, Dirichlet (nés entre 1803 et 1805), enfin un groupe né autour de 1810 (Galois, Liouville, Kummer, Schönemann).

1 - Jusqu'en 1825 : Louis Poinsot

Selon l'historiographie usuelle, un quart de siècle s'écoule après la publication des *Disquisitiones Arithmeticae* de Gauss sans véritable développement de ses idées, sauf par lui-même[7]. Les recherches récentes de Andrea Del Centina, Reinhard Laubenbacher et David Pengelley sur les manuscrits de Sophie Germain, dont nous avons parlé auparavant, ont déjà montré comment le programme de recherche de cette mathématicienne sur le dernier théorème de Fermat s'appuie sur les congruences et les résidus : ses recherches arithmétiques ont donc pour objet la résolution d'un célèbre problème d'analyse indéterminée, qu'elle étudie à partir de sa connaissance approfondie des *Disquisitiones Arithmeticae*.

Dans notre corpus, Poinsot est le seul auteur qui publie des mémoires de recherche en lien direct avec les congruences (même s'il n'adopte pas la notation introduite par Gauss, mais utilise la notation Mp de Legendre). Les extraits cités dans le chapitre précédent nous donne plusieurs informations sur sa pratique arithmétique. Dans son article publié en 1818, il résume ses recherches de géométrie, algèbre et théorie des nombres en indiquant que ces trois domaines sont basés sur une notion commune : l'ordre. Ses recherches de théorie des nombres sont centrées sur la résolution des équations binômes : il met en avant une analogie existant entre les racines des équations binômes et celles des congruences binômes afin d'obtenir une expression de ces dernières. Il commente à cette occasion l'introduction des racines imaginaires de congruences, qui sera développée en 1820. La section VII y est interprétée comme mêlant géométrie, algèbre et arithmétique, trois domaines dont l'interaction est mise en relief par Poinsot. Le lien qu'il propose entre algèbre et arithmétique est un transfert par analogie des questions et outils de l'algèbre des équations aux congruences.

2 - 1825-1835 : des directions variées

D'ordinaire, cette période est considérée comme celle marquant la renaissance d'un intérêt pour les résidus, surtout avec les travaux de Jacobi et Dirichlet sur les lois de réciprocité supérieures, lesquels contribuent (notamment avec les cours de Jacobi) à faire des résidus l'objet central d'une discipline enseignée à l'université. Or, si nous ne trouvons pas cette tendance chez les auteurs de notre corpus, nous constatons néanmoins un développement du sujet, toujours fortement ancré à la théorie des équations.

Legendre, dont les trois éditions du traité de théorie des nombres paraissent entre 1798 et 1830, publie également deux articles arithmétiques. Dans tous ses travaux, les résidus

7. D'après notre relevé, Gauss propose en particulier entre 1808 et 1818 quatre nouvelles preuves de la loi de réciprocité quadratique : nous revenons rapidement sur les mémoires en question dans notre deuxième partie.

ont une place très secondaire et sont utilisés pour compléter certaines démonstrations. Il n'emploie jamais le symbole ≡ proposé par Gauss, et utilise sa propre notation Mp pour désigner certaines équations indéterminées. Comme il l'indique lui-même dans la préface de sa *Théorie des Nombres*[8], la théorie des nombres est chez lui confondue avec l'analyse indéterminée, ce qui explique en partie l'absence des congruences et le peu de raisonnements utilisant les résidus dans ses publications. La même analyse s'applique aux travaux d'un nouveau venu, Binet (né en 1786), qui reprend d'ailleurs la notation Mp de Legendre et propose une démonstration du petit théorème de Fermat pour obtenir une nouvelle méthode algébrique de résolution des équations indéterminées du premier degré.

Cauchy produit deux types de travaux en lien avec notre thème entre 1829 et 1831. D'une part, il insère dans ses *Exercices* deux mémoires dans lesquels il étudie les propriétés des congruences en lien avec la théorie des équations : il transpose explicitement des résultats et des démonstrations connus de la théorie des équations à celle des congruences. D'autre part, il publie dans le *Bulletin de Férussac* un mémoire dans lequel il met en avant l'importance des lois de réciprocité ; il développe des résultats sur des expressions étudiées par Gauss dans la section VII des *Disquisitiones*, les sommes de Gauss, pour obtenir des formules intégrant une version généralisée du symbole de Legendre et des résultats sur les formes quadratiques de la forme $4p^{\mu} = x^2 + ny^2$ où p est premier et n un diviseur de $p-1$, formes dont certains cas particuliers sont déjà abordés par Gauss dans la section VII. Cette précision est fondamentale car Cauchy ne se réfère à aucun moment à la théorie des formes quadratiques développée par Gauss dans la section V. Son deuxième mémoire intégré dans le *Bulletin de Férussac* ne contient qu'un seul résultat consistant en un théorème général sur les formes quadratiques considérées précédemment. Dans les différentes publications de Cauchy, nous retrouvons donc la mise en avant d'analogies entre les équations et les congruences, l'étude de formes quadratiques comme équations indéterminées.

Libri présente ses travaux de théorie des nombres en 1825 devant l'Académie des Sciences de Paris ; des mémoires de théorie des nombres contenant des thèmes très semblables sont publiés dans le *Journal de Crelle* et dans les *Mémoires des Savants étrangers* en 1832 et 1838 respectivement. Dans ses travaux, Libri adopte une position forte vis-à-vis des congruences : ce sont pour lui des cas particuliers de la théorie des équations indéterminées, théorie qui est complètement intégrée à l'analyse. Nous avons évoqué dans notre introduction générale le courant de recherche nommé *analyse algébrique arithmétique* par les auteurs de [Goldstein et Schappacher, 2007a] ; il nous semble que Libri appartient de ce courant étant donné qu'il affirme la nécessité de traduire des conditions arithmétiques en termes algébriques analytiques et montre la volonté de fonder la théorie des équations indéterminées, qui comprend celle des congruences, sur les fonctions circulaires. Il utilise d'ailleurs ces dernières pour exprimer la condition d'intégralité des

8. Nous la commentons dans notre deuxième partie : voir page 191.

racines des congruences, déterminer le nombre de solutions entières de congruences de forme donnée ; il transpose également des propriétés des équations, comme les relations coefficients-racines, à celle des congruences.

Galois, quant à lui, étudie aussi les racines imaginaires de congruences en vue d'une application à la théorie algébrique des équations : à la manière de Gauss dans sa section VII, les congruences lui permettent de décrire plus commodément les relations entre permutations des racines d'équations algébriques. Ses travaux font également partie de l'*analyse algébrique arithmétique*, puisqu'il applique par exemple ses résultats aux fonctions modulaires [9].

Avant 1835, Lebesgue produit un mémoire dans le *Bulletin du Nord* (1829) et une courte note sur les résidus cubiques dans le *Bulletin de Férussac* (1831). Dans son premier texte, Lebesgue souligne l'analogie existant entre les équations et les congruences, en se référant à Poinsot. Il consacre une partie de son travail à déterminer le nombre de racines de certaines congruences, et indique une méthode de démonstration pour une version généralisée d'un théorème prouvé par Lagrange. Enfin, il propose également des premiers résultats sur les racines imaginaires des congruences quadratiques, et conclut par quelques observations sur les résidus cubiques. Là encore, nous retrouvons chez ce mathématicien l'importance donnée aux analogies existant entre la théorie des équations et des congruences.

Si des auteurs comme Germain, Cauchy (dans ses commentaires sur les lois de réciprocité de[Cauchy, 1829a]) et Lebesgue s'inscrivent plus directement dans les thématiques développées par Gauss, puis reprises par Jacobi et Dirichlet à la même époque, nous constatons toutefois, en examinant l'ensemble de leur travail, une problématique presque toujours sous l'influence de la théorie des équations algébriques ou indéterminées. Il s'agit parfois d'une immersion de l'arithmétique dans un autre domaine du point de vue de ses propres objets (par exemple l'interprétation d'une congruence comme une famille d'équations), parfois de l'usage des congruences dans la théorie des équations sur le modèle de Gauss. Les parallèles établis entre congruences et équations (parallèles soulignés par Gauss en 1801) orientent la recherche vers l'obtention, pour les congruences, de résultats analogues à ceux déjà connus pour les équations : nombre de racines (à un moment où les travaux de Sturm ont attiré l'attention vers cette question pour les équations algébriques), résolution explicite des congruences, considération des racines imaginaires des congruences.

9. Voir là-dessus [Goldstein et Schappacher, 2007a, p. 33-35].

3 - 1835-1850 : Continuité des pratiques ?

Après 1835, nous trouvons en France une forte continuité avec la période précédente (alors que se développe ailleurs, surtout en Allemagne, l'étude des lois de réciprocité, et que de jeunes chercheurs commencent à publier tôt dans leur carrière sur ces thèmes).

Binet emploie toujours les résidus et les congruences comme synonymes de restes et équations indéterminées. Poinsot expose une synthèse sur les congruences binômes. Il persiste à souligner l'importance de la notion d'ordre dans la théorie des nombres, l'algèbre et la géométrie, tout en restant dans la continuité de ce que nous avons observé précédemment. Même si nous avons délibérément laissé de côté le réseau d'auteurs des *Nouvelles Annales de Mathématiques* en choisissant de centrer notre étude sur les journaux de recherche, il nous faut souligner que Binet et Poinsot exposent ici des résultats élémentaires ; la volonté pédagogique dépasse donc le cadre du journal officiellement destiné aux enseignants (rappelons que l'Académie se voyait aussi investie de la mission de discuter les textes, méthodes, ou machines, destinés à un usage public plus vaste).

Cauchy, après une période d'interruption dûe de son exil, est un des auteurs les plus prolifiques à partir de 1839 : ses travaux arithmétiques sont essentiellement concentrés sur les années 1839-1840 et 1847. Si en 1829, Cauchy soulignait l'importance des lois de réciprocité à la fin d'un mémoire, suggérant un alignement sur les problématiques du *Journal de Crelle*, la seule référence à celles-ci dans ses travaux ultérieurs est la preuve qu'il propose de la loi de réciprocité quadratique dans une note de [Cauchy, 1840a]. Ses textes publiés entre 1839 et 1840 sont alors essentiellement consacrés à la mise en place d'une méthode générale sur les formes quadratiques de la forme $4p^{\mu} = x^2 + ny^2$, où p est un nombre premier et n un diviseur de $p-1$. Les recherches arithmétiques du savant sont donc alors entièrement centrées sur les équations indéterminées, à l'exception de quelques articles sur les expressions appelées sommes de Gauss et de Jacobi, qui sont de toutes façons à la base de ses méthodes sur les formes quadratiques. Cauchy s'éloigne donc du courant de recherche de prédilection des Jacobi, Dirichlet, Kummer, ... (et Lebesgue), lequel consiste à étudier les objets directement liés aux congruences et résidus, c'est-à-dire les résidus d'ordre supérieur, les lois de réciprocité associées (et finalement les entiers algébriques, qui s'introduisent alors en lien étroit avec les lois de réciprocité). En revanche, comme nous l'avons déjà souligné, les similarités avec des résultats de Jacobi sont remarquables, malgré leurs divergences de perspectives. Cauchy applique ensuite certains résultats obtenus sur les formes quadratiques dans ses recherches liées au dernier théorème de Fermat en 1847. Toujours en 1847, il construit une nouvelle théorie des nombres imaginaires, fondée sur la considération de congruences entre polynômes, donc sur des bases purement algébriques.

La principale exception est Lebesgue, qui publie un très grand nombre de textes de 1836

à 1850. Si son mémoire le plus conséquent, intitulé *Recherches sur les nombres* et édité entre 1837 et 1839, reprend certains des thèmes abordés dans les années 1820 (Lebesgue y consacre toute une partie à déterminer le nombre de racines entières de congruences de formes données, à l'aide d'arguments purement arithmétiques ou combinatoires), il dédie ensuite une grande majorité de son texte aux résidus quadratiques, cubiques, biquadratiques et aux lois de réciprocité associées, et commente à plusieurs reprises la forme des nombres complexes rencontrés à cette occasion. Il se réfère plus d'une fois aux travaux de Dirichlet, Jacobi, Gauss, Eisenstein, reproduit d'ailleurs des méthodes publiées par ces deux derniers et met ainsi à disposition des lecteurs du *Journal de Liouville* des matériaux difficilement accessibles pour certains savants. Avec ses travaux mettant particulièrement en avant les résidus d'ordre supérieur et les lois de réciprocité, Lebesgue fait donc figure d'exception en France ; sa position excentrée institutionnellement se double donc d'une position excentrée thématiquement.

Remarquons donc que c'est toujours la génération née avant la fin du dix-huitième siècle qui est ici concernée. C'est seulement à la fin de la période en question nous voyons intervenir de nouveaux venus, Liouville (contemporain de Kummer) [10], et surtout Serret. Ce dernier aura une importance décisive compte tenu de la place des résidus et des congruences dans son *Cours d'algèbre supérieure*, et ce dès les premières éditions ; remarquons toutefois qu'il s'agit bien pour lui à la fois de lier les congruences à la théorie des équations, lesquelles forment le focus de ce cours et d'englober la théorie des congruences dans l'algèbre, dans la suite de travaux vus précédemment. Charles Hermite (né trois ans après Serret), qui n'apparaît qu'à la limite de notre corpus, utilisera des congruences dans ses travaux sur les formes quadratiques et sur les équations à partir de la fin des années 1840 [11].

Ces orientations particulières appellent plusieurs questions, que nous allons étudier par la suite.

En amont d'abord : tous les auteurs ont plusieurs sources communes (en plus des références différenciées selon le cas) que nous allons les examiner en détail dans la partie suivante, afin de repérer quelles pratiques de travail, quels résultats (et sous quelle forme) ont pu en être hérités. Un point particulièrement intriguant est la place de Lagrange dans les références de notre corpus, car nous pouvons nous demander jusqu'à quel point cet auteur a formaté les spécificités du travail avec les résidus que nous avons remarquées dans le corpus français.

En profondeur ensuite. Du bilan que nous venons de faire, nous retenons tout particulièrement les travaux de deux auteurs : Poinsot et Cauchy. Ceux-ci occupent un rôle

10. Celui-ci insèrera par la suite dans son *Journal* plus de cent mémoires sur des formes quadratiques particulières entre 1858 et 1863 : voir par exemple [Verdier, 2009, ch. 15].

11. Voir notamment [Archibald, 2002], [Goldstein, 2007] et [Goldstein, 2011].

important par la quantité de leurs publications, et aussi par les références qui sont faites à leurs recherches par les autres auteurs de notre corpus (alors que Lebesgue, par exemple, est très peu mentionné). Par ailleurs, ils appartiennent à des générations antérieures à celles qui instaurent des cours sur les résidus et les congruences dans les années 1830 et 1840 et peuvent donc nous renseigner sur un état des lieux antérieur, encore mal connu. Nous allons donc examiner en détail leurs travaux dans les deux dernières parties. Observons que le choix d'étudier particulièrement les travaux de Poinsot et de Cauchy répond également à l'extrait cité dans notre introduction générale du début du *Report on the Theory of Numbers*, publié entre 1859 et 1865 de Henry J. S. Smith que nous rappelons ici :

> The arithmetical memoirs of Gauss himself, subsequent to the publication of the ' Disquisitiones Arithmeticae ' ; those of Cauchy, Jacobi, Lejeune Dirichlet, Eisenstein, Poinsot, and, among still living mathematicians, of MM. Kummer, Kronecker, and Hermite, have served to simplify as well as to extend the science.[Smith, 1859-1865, p. 38]

Les travaux arithmétiques de Poinsot et de Cauchy restaient dans cette liste de savants les moins étudiés à ce jour. Outre leurs modalités propres, nous nous intéresserons aussi à la manière dont ils ont été ou non intégrés dans le développement global de la théorie des nombres.

PARTIE II

Sources communes : les résidus et les congruences chez Euler, Lagrange, Legendre, Gauss.

CHAPITRE 5

Les travaux d'Euler et de Lagrange autour du théorème des quatre carrés - vers une théorie des résidus ?

I Introduction

Dans ce chapitre, nous étudions quelques travaux d'Euler et Lagrange en théorie des nombres [1]. Aucun autre mathématicien n'a atteint à cette époque la position dominante occupée par Euler dans toutes les branches des mathématiques. Ses travaux en théorie des nombres lui assurent à eux seuls une place éminente dans l'histoire de cette science, et n'occupent pourtant que quatre volumes sur les soixante-dix qui rassemblent son œuvre complète. Selon [Burckhardt, 1983], la production mathématique d'Euler compte 760 mémoires publiés avant 1783, et des centaines publiés après sa mort, trois mille pages de carnets de notes, dont mille pages dévolues à la théorie des nombres. Parmi les mémoires [2], soixante textes de théorie des nombres sont présentés devant l'Académie de Berlin ou celle de Saint-Pétersbourg avant la mort d'Euler et publiés avant 1785, et trente-cinq autres sont publiés après 1785. Les recherches d'Euler en théorie des nombres débutent particulièrement dans la correspondance qu'il entretient avec Christian Goldbach [3]. Goldbach indique à Euler certains résultats contenus dans les écrits de Fermat, en particulier sur la conjecture de Fermat affirmant que tous les nombres de la forme $2^{2^n}+1$ sont premiers [4], dans une lettre du 1er décembre 1729 . Le 22 mai 1730, il envoie de nouveau une lettre à Euler en notant que les restes des carrés des termes d'une progression arithmétique après division par un nombre premier forment une séquence périodique, résultat qu'Euler redémontre plus tard dans le cadre de sa théorie des résidus. Euler répond à Goldbach le 4 juin 1730 : il éprouve de l'intérêt pour la théorie des nombres, et notamment pour le « théorème non inélégant » qui affirme que tout nombre peut s'écrire sous la forme de quatre

1. Euler (1707 - 1783) travaille au sein de l'Académie de Saint-Petersbourg de 1727 et 1741, puis de 1766 jusqu'à sa mort, après un séjour à l'Académie de Berlin. Lagrange (1736 - 1813), de son côté, remplace Euler à l'Académie de Berlin de 1766 à 1787, après un début de carrière à l'École d'artillerie et à l'Académie de Turin, puis prend un poste à l'Académie de Paris. Il commence à enseigner à l'École Polytechnique en 1795. Une correspondance entre les deux hommes débute en 1755, à l'occasion d'une lettre de Lagrange à Euler sur ses travaux en calcul de variations. Il existe de nombreux textes sur la vie et les travaux scientifiques d'Euler et Lagrange : pour Euler, on peut notamment voir [Bradley et Sandifer, 2007], [Burckhardt, 1983] et [Calinger, 1996] ; on trouvera des éléments de biographie de Lagrange dans [Julia, 1942 - 1950].

2. Ces données sont issues du site *The Euler Archive*, qui donne notamment un aperçu complet des travaux d'Euler publiés. Les indications que nous donnons sur les dates de présentation et de publications des différents textes d'Euler sont prises sur ce site.

3. Ces informations sont issues de [Suzuki, 2007].

4. Euler démontre que le cinquième nombre de Fermat, $2^{32}+1$ est composé, et donc que la conjecture est fausse dans [Euler, 1738], présenté en 1732 à l'Académie de Berlin, puis publié en 1738.

carrés. Les recherches d'Euler sont fondées en grande partie sur des conjectures contenues dans les travaux de Fermat, et il développe des travaux en lien avec les nombres parfaits, amicaux, les formes quadratiques, les résidus de puissances, quadratiques, cubiques, la loi de réciprocité quadratique et le dernier théorème de Fermat. Il publie en particulier de nombreux articles sur les nombres de la forme $x^2 + ny^2$.

Parmi ses publications, beaucoup sont des textes assez courts, ne contenant que des résultats particuliers, souvent non accompagnés de démonstration. Les méthodes de recherche et de démonstration d'Euler sont très diverses : il met en avant l'utilité des observations et conjectures dans [Euler, 1761a] , utilise des outils arithmétiques, mais aussi les séries et le calcul infinitésimal dans ses recherches, et utilise de manière récurrente plusieurs méthodes de démonstration (induction, descente infinie, manipulations algébriques, ...). Euler ne voit pas la théorie des nombres comme un ensemble de résultats épars. En effet, dans une lettre à Goldbach de 1742, Euler essaie de fusionner un ensemble de résultats particuliers pour obtenir des résultats généraux et remarque [5] :

> By the way, the prime divisors of all series of numbers which are given by the formula $\alpha xx \pm \beta yy$ show a very orderly pattern which, although I have no demonstration of it as yet, seems to be completely correct.
>
> [...] But I am convinced that I have not exhausted this material, rather, that there are countless wonderful properties of numbers to be discovered here, by means of which the theory of divisors could be brought to much greater perfection... [Edwards, 1983, p. 285-286].

Un de ses mémoires [6], présenté en 1748 à l'Académie de Saint-Pétersbourg, puis publié en 1751, contient par exemple 59 théorèmes, sans démonstration, sur les diviseurs de nombres de la forme $x^2 + ny^2$.

Euler est également l'auteur d'un traité de théorie des nombres inachevé, dont le thème principal est la théorie des résidus : le *Tractatus de numerorum doctrina capita sedecim, quae supersunt*, publié en 1849.

Contrairement à Euler, Lagrange publie des écrits de théorie des nombres sur une période très courte : entre 1766 et 1777. On compte en tout une dizaine de mémoires, en moyenne bien plus longs que ceux d'Euler, contenant des démonstrations sur l'équation de Pell, et plus généralement sur les équations indéterminées du second degré, sur le théorème des quatre carrés et le théorème de Wilson, et sur les formes quadratiques (il donne notamment une méthode pour déterminer la forme des diviseurs des formes $ax^2 + bxy + cy^2$). Contrairement à Euler, Lagrange n'utilise (presque) pas les résidus dans ses travaux. Néanmoins, ses recherches en théorie des nombres répondent très souvent à

5. Cette lettre est écrite en allemand et latin : nous utilisons ici la traduction donnée par Edwards dans [Edwards, 1983].

6. Voir [Euler, 1751]. Edwards commente cette publication dans [Edwards, 1983], en donnant notamment une méthode permettant de vérifier expérimentalement les théorèmes indiqués par Euler pour un nombre important d'exemples.

celles d'Euler.

Dans cette partie, notre but n'est pas de faire une étude exhaustive des travaux d'Euler et de Lagrange en lien avec la théorie des résidus, mais de comprendre de quelles pratiques touchant aux résidus héritent les mathématiciens du début du XIX^{e} siècle rencontrés dans la partie précédente. C'est pourquoi nous avons décidé de nous concentrer sur les écrits en lien avec le théorème des quatre carrés [7], qui fait partie des recherches plus générales d'Euler sur les sommes de carrés et qui semble avoir été un des premiers théorèmes auxquels il s'est intéressé en théorie des nombres. De plus, l'analyse de ces textes permet de mettre en avant l'évolution d'Euler sur les résidus : les raisonnements basés sur des critères de divisibilité sont progressivement remplacés par l'emploi des résidus dans les démonstrations. Par ailleurs, on y voit très nettement la compétition ouverte à laquelle Euler et Lagrange se livrent, les influences croisées comme leurs spécificités. Ceci permet donc de mesurer les différentes pratiques.

Ce thème nous a conduit à sélectionner un certain nombre d'articles [8]. Pour Lagrange, nous résumons dans un premier temps les méthodes développées dans le mémoire *Sur la solution des problèmes indéterminés du second degré*, dont l'objet est la résolution des équations indéterminées du second degré à deux inconnues, puis nous étudions l'article où Lagrange présente une première preuve complète du théorème des quatre carrés. Le premier texte permet de dévoiler les méthodes propres de Lagrange, de tester leur efficacité et de comprendre l'origine des techniques utilisées dans sa démonstration du théorème des quatre carrés. Nous traitons parallèlement les textes d'Euler en lien avec le petit théorème de Fermat, et les théorèmes des deux carrés et des quatre carrés : là aussi, ces écrits nous permettent de retracer l'évolution des méthodes et raisonnements d'Euler. Nous avons enfin choisi d'étudier aussi les articles sur le théorème de Wilson, car ils montrent comment les pratiques des deux hommes se sont alors un peu rapprochées. Nous concluons ce chapitre par un aperçu du développement autonome de la théorie des résidus que l'on retrouve dans des mémoires d'Euler présentés à partir de 1755. Cette étude est également l'occasion d'apprécier les différentes méthodes - algébriques, analytiques et arithmétiques - utilisées par Euler et Lagrange dans les textes de théorie des nombres considérés ici.

Dans ce chapitre, nous ne développons pas toutes les preuves des résultats d'Euler et de Lagrange mais détaillons les extraits de mémoires dans la mesure où ils permettent d'illustrer l'évolution d'Euler par rapport aux résidus et les différences entre les épistémologies d'Euler et Lagrange [9].

7. Certains passages des recherches d'Euler en lien avec le théorème des quatre carrés sont également commentés dans [Pieper, 1993].

8. Les textes que nous étudions ici sont également en partie commentés, en particulier du point de vue des méthodes de descente infinie employés par les deux mathématiciens, dans [Bussotti, 2006]. Notre objectif est ici différent puisque nous axons notre analyse sur la place des résidus dans les raisonnements d'Euler et Lagrange.

9. Nous renvoyons le lecteur à [Boucard, 2006] notamment pour une étude approfondie des démonstrations présentées par les deux mathématiciens.

II Euler et les sommes de carrés : 1736-1751

Comme nous l'avons indiqué précédemment, la correspondance entre Euler et Goldbach est une source intéressante pour connaître l'évolution des recherches d'Euler en théorie des nombres. Grâce à l'étude de celle-ci [10], nous savons qu'Euler est capable de démontrer dès 1742 que les nombres de la forme a^2+b^2, où a et b sont premiers entre eux, n'admettent pas de diviseurs de la forme $4n-1$. Sa démonstration se base d'ailleurs sur le petit théorème de Fermat [11], dont nous analyserons les différentes preuves proposées par Euler. À partir des lettres envoyées à Goldbach, on voit qu'une partie des recherches d'Euler est consacrée aux sommes de deux carrés. À partir de 1747, on retrouve de plus en plus de références aux sommes de trois ou quatre carrés. En 1748, Euler prouve une identité fondamentale pour la suite : le produit de deux sommes de quatre carrés de nombres entiers est une somme de quatre carrés de nombres entiers.

Dans une lettre du 12 avril 1749, Euler annonce au sujet du théorème des deux carrés : « Nunmehr habe ich endlich einen bündigen Beweis gefunden [...] » [12]. Dans cette même lettre, il donne également une preuve similaire à celle trouvée pour le théorème des deux carrés, basée sur l'identité obtenue en 1748, du fait que tout nombre est au moins somme de quatre carrés rationnels : c'est une version faible du théorème des quatre carrés.

Dans cette section, nous allons étudier tout particulièrement les publications d'Euler correspondant aux résultats énoncés et démontrés dans cette lettre. Dans un premier temps, nous nous intéressons au mémoire *Theoremata circa Divisores Numerorum* [13], publié en 1750, où l'on trouve une preuve du petit théorème de Fermat et d'autres résultats qu'Euler réutilisera par la suite. Puis nous analysons les deux mémoires contenant la démonstration du théorème des deux carrés présentés par Euler à l'Académie de Berlin entre 1749 et 1750, et publiés en 1758 et 1760. Enfin, nous considérons le mémoire où il donne la preuve de la version faible du théorème des quatre carrés.

1 - Un premier mémoire sur le petit théorème de Fermat et sur les sommes de deux carrés

Le mémoire *Theoremata circa Divisores Numerorum* a été présenté à l'Académie de Saint-Pétersbourg le 2 septembre 1748, et aurait déjà été lu à l'Académie de Berlin le 23 mars 1747. Il a ensuite été publié dans le premier volume des Nouveaux Commentaires

10. Nous utilisons ici les données de [Weil, 1984, p. 177-179] concernant les recherches d'Euler sur les sommes de carrés.

11. Nous désignons par "petit théorème de Fermat" le résultat suivant : $a^{p-1} \equiv 1 \pmod{p}$ pour p nombre premier et pour a premier à p, pour le distinguer du "théorème d'Euler - Fermat", énoncé par Euler : $a^{\varphi p} \equiv 1 \pmod{p}$ où a nombre premier à p et où φp désigne la quantité de nombres inférieurs à p et premiers à p.

12. « J'ai maintenant enfin trouvé une preuve concluante ... »

13. On peut traduire ce titre par : *Théorèmes autour des diviseurs des nombres.*

de l'Académie des Sciences de Saint-Pétersbourg en 1750 (pp.20-48).

Nous rappelons dans cette section les énoncés de certains théorèmes et quelques étapes de démonstration pour que le texte se suffise à lui-même.

(a) Deux démonstrations du petit théorème de Fermat à partir du binôme de Newton

Dans un premier temps, Euler démontre le petit théorème de Fermat : si p est un nombre premier et si a est un nombre quelconque non divisible par p, alors le nombre $a^{p-1} - 1$ est divisible par p. Il en a donné une première preuve en 1736.

Une première démonstration dans un mémoire de 1736

Dans le mémoire de 1736, intitulé *Theorematum quorundam ad numeros primos spectantium demonstratio*[14], il se propose de démontrer que pour tout p premier, et tout a non divisible par p, la formule $a^{p-1}-1$ est toujours divisible par p. Il commence par donner deux justifications pour le cas particulier de $a = 2$, car cela permet de mieux comprendre le passage au cas général[15].

Pour montrer que pour tout p premier impair, $2^{p-1} - 1$ est toujours divisible par p, il commence par utiliser le binôme de Newton pour obtenir la formule :

$$(1+1)^{p-1} = 1 + \frac{p-1}{1} + \frac{p-1}{1}.\frac{p-2}{2} + \frac{p-1}{1}.\frac{p-2}{2}.\frac{p-3}{3} + \frac{p-1}{1}.\frac{p-2}{2}.\frac{p-3}{3}.\frac{p-4}{4}\ldots,$$

dont il groupe les termes deux à deux. Dans la deuxième démonstration, qui sert ensuite de trame à celle du théorème général, il remarque que montrer que $2^{p-1} - 1$ est divisible par p revient à montrer que $2^p - 2$ est divisible par p, tant que p est un nombre premier impair et utilise une nouvelle fois le binôme de Newton :

$$2^p = (1+1)^p = 1 + \frac{p}{1} + \frac{p}{1}.\frac{p-1}{2} + \ldots + \frac{p}{1}.\frac{p-1}{2} + 1,$$

et, comme tous les termes sont divisibles par p, à part le premier et le dernier, il en déduit que $2^p - 1 - 1 = 2^p - 2$ est divisible par p, d'où la conclusion.

Il réitère son raisonnement pour le cas particulier où $a = 3$, puis passe à la preuve du théorème général par récurrence, en montrant que si $a^p - a$ est divisible par p, alors $(a+1)^p - (a+1)$ est divisible par p. Pour cela, il utilise le binôme de Newton :

14. On peut traduire par *Une démonstration de certains théorèmes à propos des nombres premiers.* D'après les registres, ce mémoire a été présenté à l'Académie de Pétersbourg le 2 août 1736. Il a été publié pour la première fois dans le dixième tome des *Commentarii academiae scientiarum Petropolitanae*, en 1741 : voir [Euler, 1741b].

15. Dans ses mémoires, Euler commence régulièrement par justifier des cas particuliers avant d'exposer la démonstration du cas général, afin de bien faire comprendre l'esprit de sa méthode de démonstration.

$$(1+a)^p = 1 + \frac{p}{1}.a + \frac{p}{1}.\frac{p-1}{2}.a^2 + \ldots + \frac{p}{1}.a^{p-1} + a^p.$$

Comme précédemment, tous les termes de la formule sont divisibles par p, sauf le premier et le dernier. On en déduit donc que $(1+a)^p - 1 - a^p$ est divisible par p. Or, $(1+a)^p - 1 - a^p = (1+a)^p - a - 1 + a - a^p$, et comme par hypothèse, $a^p - a$ est divisible par p, on a bien le résultat.

Par itération, il en déduit que si $a^p - a$ est divisible par p, alors $(a+b)^p - a - b$ est divisible par p pour tout entier naturel b. Or, avec $a = 2$, on sait que $2^p - 2$ est divisible par p, donc $(b+2)^p - b - 2$ est bien divisible par p, d'où $(b+2)^{p-1} - 1$ est divisible par p tant que $b+2$ n'est pas divisible par p, d'où le théorème.

Il ne le remarque pas, mais il a en fait montré que $a^p - a$ est divisible par p pour tout nombre premier p et tout entier naturel a, et il en déduit que $a^{p-1} - 1$ est alors divisible par p lorsque p ne divise pas a.

Finalement, on voit que dans cette démonstration, les outils utilisés sont le binôme de Newton et ses propriétés, ainsi que des théorèmes fondamentaux d'arithmétique, notamment le fait que, pour tout nombre premier p, si p divise le produit de deux nombres ab, et si p est premier avec a, alors p divise b.

La démonstration du petit théorème de Fermat dans le mémoire *Theoremata circa divisores Numerorum* (1750)

Dans le mémoire de 1750, Euler reprend une partie des raisonnements précédents pour démontrer à nouveau le petit théorème de Fermat. Comme nous l'avons observé dans notre première partie, on retrouve des démonstrations de ce théorème, devenu un outil fondamental dans les recherches en lien avec les résidus et les congruences, dans de nombreux mémoires sur la période 1801 - 1850. Euler donne à lui seul quatre preuves de ce théorème entre 1736 et 1763 ; Lagrange en propose également plusieurs.

Euler commence ici par montrer que, si p est un nombre premier, alors tout nombre de la forme $(a+b)^p - a^p - b^p$ est divisible par p. Il utilise la même méthode que dans les démonstrations précédentes, en remarquant que les combinaisons $\binom{p}{k}$, où k est compris entre 1 et $p-1$, sont divisibles par p. Puis il en déduit le cas particulier qu'il avait exposé au début de sa démonstration précédente. Il montre ensuite que si $a^p - a$ et $b^p - b$ sont divisibles par le nombre premier p, alors $(a+b)^p - a - b$ est également divisible par p. Cela se déduit du premier théorème, puisque $(a+b)^p - a - b = (a+b)^p - a^p - b^p + a^p - a + b^p - b$. De là, il pose $b = 1$ et, comme $1^p - 1$ est divisible par p, alors $(a+1)^p - a - 1$ est également divisible par p, si $a^p - a$ est divisible par p. Et, par itération, il peut alors en conclure que $c^p - c$ est divisible par p pour tout entier naturel c et en déduire le petit théorème de Fermat.

À partir de ce théorème, il déduit des résultats sur les diviseurs premiers des nombres de la forme $a^{2n} + b^{2n}$. Certaines de ces propriétés sont en lien avec le théorème des deux carrés. De plus, on observe dans la suite de ce texte un glissement progressif de raisonnements basés sur des critères de divisibilité vers la considération de restes de divisions euclidiennes, restes qui deviendront dans ses travaux ultérieurs les résidus.

(b) Les conséquences du théorème d'Euler-Fermat sur les diviseurs des nombres de la forme $a^m \pm b^m$

Euler commence par énoncer un théorème découlant directement du théorème d'Euler-Fermat :

Théorème 4

Si deux nombres a et b ne sont pas divisibles par p, alors tous les nombres de la forme $a^{p-1} - b^{p-1}$ sont divisibles par p.

Il suffit en effet de remarquer que : $a^{p-1} - b^{p-1} = (a^{p-1} - 1) - (b^{p-1} - 1)$.

Il suppose alors que p est un nombre premier impair et pose $p = 2m + 1$. Il en déduit ainsi à partir du petit théorème de Fermat que $a^{2m} - b^{2m}$ est divisible par p, tant que a et b ne sont pas divisibles par p. Il liste ensuite des corollaires permettant d'aboutir à la distinction entre les nombres premiers de la forme $4n - 1$ et ceux de la forme $4n + 1$. Il déduit d'abord du théorème que $a^{2m} + b^{2m}$ n'est pas divisible par $p = 2m + 1$. Puis, comme $a^{2m} - b^{2m} = (a^m - b^m)(a^m + b^m)$, l'un des nombres $a^m + b^m$ ou $a^m - b^m$ est divisible par p. De plus, ces deux nombres ne peuvent être divisibles simultanément par p car a et b ne sont pas divisible par p, p est un nombre premier impair, et $a^m - b^m + a^m + b^m = 2a^m$. Il affirme alors que si m est pair (soit $m = 2n$), et que $a^m - b^m$(soit $a^{2n} - b^{2n}$) est divisible par $2m + 1$, alors soit $a^n + b^n$, soit $a^n - b^n$ est divisible par $p = 4n + 1$.

Le théorème suivant a pour objet les diviseurs des sommes de deux carrés :

Théorème 5

Les sommes de deux carrés $aa + bb$ ne peuvent être divisées par aucun nombre premier de la forme $4n - 1$, sauf si les deux nombres a et b sont divisibles par $4n - 1$.

Sa démonstration se base sur un corollaire du théorème 4, en remarquant que $a^{4n-2} + b^{4n-2}$ n'est pas divisible par p, et admet $a^2 + b^2$ comme facteur. Il en déduit alors que les sommes de deux carrés ne peuvent pas admettre de facteur premier de la forme $4n - 1$, et que les seuls diviseurs sont alors nécessairement de la forme $4n + 1$. Ce résultat est à nouveau démontré dans un mémoire plus tardif à partir d'une méthode différente. En effet, ici, pour ses démonstrations, il n'utilise que des théorèmes fondamentaux de l'arithmétique, ainsi que des identités algébriques, dont les principales sont :

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \dots ab^{n-2} + b^{n-1}),$$
$$a^{2n+1} + b^{2n+1} = (a+b)(a^{2n} - a^{2n-1}b + a^{2n-2}b^2 - \dots - ab^{2n-1} + b^{2n}).$$

À partir des théorèmes 4 et 5, il montre également que les diviseurs impairs des expressions du type $a^4 + b^4$ sont de la forme $8n + 1$, que ceux des expressions $a^8 + b^8$ sont de la forme $16n + 1$, et qu'en général, les diviseurs de $a^{2^m} + b^{2^m}$ sont de la forme $2^{m+1}n + 1$. Il déduit ce dernier résultat par itération à partir des cas particuliers. Ce théorème lui permet, au paragraphe 33 de son texte, de montrer que la conjecture de Fermat selon laquelle tous les nombres de la forme $2^{2^m} + 1$ sont premiers, est fausse. En effet, pour $m = 5$, son théorème permet d'affirmer que les diviseurs éventuels de $2^{32} + 1$ sont de la forme $64n + 1$, ce qui réduit considérablement les calculs : le nombre obtenu pour $n = 10$, 641, divise le nombre en question. Euler met ainsi en avant l'utilité des résultats exposés ici et l'efficacité des méthodes qui en découlent.

Il énonce ensuite des résultats qui donnent les diviseurs possibles des nombres de la forme $a^m - b^m$. Il commence par rappeler que $a - b$ divise toujours $a^m - b^m$, et de façon plus générale, que $a^p - b^p$ divise $a^m - b^m$ si p divise m. Il réutilise cette propriété dans ses démonstrations notamment. Le théorème 9 contient un nouveau critère de divisibilité : si $a^m - b^m$ est divisible par $2n + 1$, et si p est le PGCD de m et $2n$, alors $a^p - b^p$ est divisible par $2n + 1$. C'est dans la démonstration de ce théorème qu'Euler commence à utiliser les restes de divisions euclidiennes. Il y utilise le reste q de la division euclidienne $2n = \alpha m + q$ dans des manipulations algébriques, ainsi que le petit théorème de Fermat.

Ce sont ensuite les théorèmes 11 à 13, et les corollaires qui en découlent, qui contiennent des résultats sur les résidus quadratiques, cubiques, et d'ordre n qui deviendront les premiers résultats des théories correspondantes.

Le théorème 11 établit une propriété des résidus de la division des carrés par $2m + 1$:

Théorème 11

Soit $a = f^2 \pm (2m + 1)\alpha$ *et* $2m + 1$ *un nombre premier, alors l'expression* $a^m - 1$ *est divisible par* $2m + 1$.

En termes modernes, si p est un nombre premier, et si r est un résidu quadratique de p, alors $r^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Ici, sa démonstration repose sur le fait que $f^{2m} - 1 = (f^2)^m - 1$ est divisible par $2m+1$ d'après le théorème de Fermat, puis il applique le théorème précédent. Il n'utilise donc pas de raisonnements sur les résidus. Par contre, Euler utilise les termes "restes" et "résidus" dans certains des corollaires qui suivent :

Corollaire 4

C'est pourquoi, pour rechercher les valeurs de a pour lesquelles $a^m - 1$ est divisible par le nombre premier $2m + 1$, on doit rechercher les restes qui résultent de la division de

chaque nombre carré par $2m+1$. En effet, si r est le reste de cette forme, alors $(2m+1)p+r$ est une valeur appropriée pour a.

Corollaire 5

De plus, tous ces restes r sont inférieurs à $2m+1$, et d'autre part, tous les nombres inférieurs à $2m+1$ ne sont pas des valeurs pour r (car le nombre de valeurs pour r ne peut pas être plus grand que m). Ainsi, il y a toujours m nombres qui ne peuvent être pris pour r.

Corollaire 6

En fait, les valeurs de r sont tout d'abord les carrés inférieurs à $2m+1$, mais aussi les résidus qui résultent de la division des carrés plus grands par $2m+1$, et de plus, aucune valeur parmi celles prises pour r ne peut être supérieure au nombre m.

Il indique donc comment obtenir les valeurs de a à partir de la recherche de ce qui sera par la suite appelé les résidus quadratiques et donne la méthode pour les obtenir. Il indique également le nombre de résidus quadratiques pour les nombres premiers de la forme $2m+1$. Il illustre ensuite le théorème 11 par trois exemples pour les nombres premiers 5, 7, 11. Par exemple, pour $2m+1=7$, il recherche les valeurs de a telles que a^3-1 soit divisible par 7. Il trouve que, puisque les trois résidus qui résultent de la division des carrés par 7 sont 1, 2, et 4, les valeurs de a sont $7n+3$, $7n+5$, $7n+6$. Puis il ajoute que si a est de l'une des formes $7n+3$, $7n+5$, ou $7n+6$, alors a^3-1 n'est pas divisible par 7, mais a^3+1 est divisible par 7. Il ne donne pas d'explication pour la dernière affirmation sur les diviseurs de a^3+1, mais, dans le cas où m est impair, et si l'on considère un résidu négatif (en effet, si r est résidu, alors $r-(2m-1)$ est également un résidu), que l'on note $-r$ (où r est positif), alors on obtient que $(-r)^m-1$ est divisible par $2m+1$, soit $-r^m-1$ divisible par $2m+1$, ou encore r^m+1 divisible par $2m+1$. Dans le cas où $2m+1=7$, soit $m=3$, les résidus sont 1, 2, et 4, et leurs équivalents négatifs sont -6, -5 et -3, donc les formes $7n+6$, $7n+5$, et $7n+3$ sont des valeurs de a, telles que a^3+1 soit divisible par 7. En revanche, pour $2m+1=5$, soit $m=2$, on ne pourra pas réitérer le même raisonnement, puisque, comme m est pair, on obtient $(-r)^m-1=r^m-1$.

Le théorème 12 est similaire pour les résidus cubiques : si $a=f^3\pm(3m+1)\alpha$, alors a^m-1 est divisible par $3m+1$. Euler démontre cela de la même manière que précédemment en remarquant que $f^{3m}-1=(f^3)^m-1$ est divisible par $3m+1$. Il donne une propriété supplémentaire, à savoir que si r est un résidu pour le diviseur $3m+1$ (ici, le terme de résidu désigne un nombre qui résulte de la division d'un cube par $3m+1$), alors $3m+1-r$ est également résidu. Il remarque également que le nombre de résidus dans ce cas est toujours égal à m.

Il généralise finalement ces résultats aux résidus de puissances n^{e} dans le théorème 13 : si a est de la forme $f^n \pm (mn+1)\alpha$, où $mn+1$ est premier, alors $a^m - 1$ est divisible par $mn+1$. Il utilise une fois de plus le théorème de Fermat et l'égalité $f^{mn} = (f^n)^m$. Il en déduit alors que si $a^m - 1$ n'est pas divisible par $mn+1$, alors a ne peut pas être mis sous la forme $f^n \pm (mn+1)\alpha$. Il remarque alors que la réciproque doit être vraie, c'est-à-dire que si $a^m - 1$ est divisible par $mn+1$, alors il existe une puissance f^n qui laisse a comme reste après division par $mn+1$.

Il conclut ce mémoire par trois théorèmes sur les diviseurs d'expressions de la forme $af^n - bg^n$.

Dans ce mémoire, Euler donne une deuxième preuve du théorème d'Euler-Fermat, et montre qu'une des conjectures de Fermat est fausse. Il commence également à considérer des restes de divisions euclidiennes dans ses preuves et donne des résultats sur les restes de carrés, cubes et puissances n^{e}. Même si presque toutes ses démonstrations utilisent des critères de divisibilité, Euler commence à obtenir des propriétés sur ce qu'il nomme des restes ou des résidus.

2 - Une démonstration du théorème des deux carrés en deux étapes

La première démonstration du théorème des deux carrés présentée par Euler entre 1749 et 1750 n'utilise pas de raisonnement sur les résidus. Nous la résumons néanmoins dans cette section car elle contient les méthodes qu'il utilise très souvent - la méthode de descente infinie et certaines manipulations algébriques - et son architecture est semblable à celle de ses autres travaux sur les sommes de carrés. Nous donnons donc ici un aperçu des deux mémoires en question (sans toutefois nous arrêter sur les nombreux corollaires les composant) qui contiennent généralement des exemples ou des applications des théorèmes principaux.

(a) Une démonstration du théorème des deux carrés inachevée

Le mémoire que nous allons étudier ici s'intitule *De numeris qui sunt aggregata duorum quadratorum*[16] et a été publié pour la première fois en 1758. Comme son titre l'indique, ce mémoire renferme des résultats importants sur les nombres représentés par une somme de deux carrés, dont les propositions suivantes :

– le produit de deux sommes de deux carrés est encore une somme de deux carrés ;

16. On peut traduire ce titre par *Sur les nombres qui sont somme de deux carrés*. Ce mémoire a été lu le 20 mars 1749 à l'Académie de Berlin, son contenu est en partie exposé dans une lettre d'Euler à Goldbach datée du 6 mai 1747. Il a été publié la première fois dans le tome IV des *Novi Commentarii academiae scientiarum Petropolitanae* en 1758.

– les diviseurs des sommes de deux carrés premiers entre eux sont nécessairement somme de deux carrés ;
– le théorème des deux carrés (dont la démonstration est achevée dans un autre texte) : tous les nombres premiers de la forme $4n + 1$ sont sommes de deux carrés ;
– un critère de primalité : si un nombre de la forme $4n+1$ est décomposable de manière unique comme somme de deux carrés premiers entre eux, alors il est premier ;
– si un nombre peut se décomposer de deux manières différentes comme somme de deux carrés, alors il n'est pas premier.

Euler commence par étudier des cas particuliers. Par exemple, il donne les premiers carrés, de 0^2 à 14^2, pour en déduire tous les nombres qui sont somme de deux carrés entre 0 et 200, et ceux qui ne le sont pas. Il fait également des observations sur la forme que peut prendre une somme de deux carrés, selon que les nombres sont pairs ou impairs. Il rappelle qu'aucun nombre de la forme $4n - 1$ ne peut être somme de deux carrés puis continue en donnant trois résultats qu'il va ensuite généraliser :

– Si le nombre p est somme de deux carrés, alors les nombres $4p$, $9p$, $16p$, et plus généralement nnp, sont également somme de deux carrés.
– Si le nombre p est somme de deux carrés, alors les nombres $2p$, et généralement $2nnp$, sont aussi somme de deux carrés. (En effet, $2aa + 2bb = (a + b)^2 + (a - b)^2$.)
– Si le nombre pair $2p$ est somme de deux carrés, alors sa moitié p est aussi somme de deux carrés (car $aa + bb = 2\left(\frac{a+b}{2}\right)^2 + 2\left(\frac{a-b}{2}\right)^2$.).

La démonstration proposée ici pour le théorème des deux carrés est composée de trois étapes. À l'aide de manipulations algébriques, Euler commence par prouver des identités sur les sommes de deux carrés : le produit de deux sommes de deux carrés est une somme de deux carrés, le quotient de deux sommes de deux carrés est une somme de deux carrés. Il utilise ensuite la méthode de descente infinie pour prouver que si un nombre divise une somme de deux carrés premiers entre eux, alors ce nombre est aussi somme de deux carrés. Puis, avec le petit théorème de Fermat et la méthode des différences finies, il montre que tout nombre premier de la forme $4n + 1$ divise une somme de deux carrés premiers entre eux, et conclut à l'aide du résultat obtenu dans la deuxième étape.

Il commence tout d'abord par généraliser ses résultats sur les produits de sommes de deux carrés :

Théorème

Si p et q sont deux nombres, qui sont chacun somme de deux carrés, alors le produit pq est aussi somme de deux carrés.

En effet, si on a $p = aa + bb$ et $q = cc + dd$, alors $pq = (ac + bd)^2 + (ad - bc)^2$.

Proposition 1

Si le produit pq est somme de deux carrés, et si le facteur p est un nombre premier somme de deux carrés, alors l'autre facteur q sera également somme de deux carrés.

Démonstration

Soit $pq = aa + bb$ et $p = cc + dd$. Comme p est un nombre premier, c et d sont premiers entre eux. Comme q est entier et tel que

$$q = \frac{aa + bb}{cc + dd},$$

le numérateur $aa + bb$ est divisible par le dénominateur $cc + dd$. Donc, de même, les nombres $cc(aa + bb)$ et $aa(cc + dd)$ sont divisibles par $cc + dd$ et donc leur différence $bbcc - aadd$ est nécessairement divisible par $cc + dd$.

Comme $cc + dd$ est un nombre premier et comme $bbcc - aadd = (bc + ad)(bc - ad)$, l'un des deux facteurs $bc \pm ad$ est divisible par p.

Ainsi, soit : $bc \pm ad = mcc + mdd$, où les nombres a et b peuvent s'écrire $b = mc + x$ et $a = \pm md + y$ avec x et y entiers. Si on remplace les valeurs de a et b dans l'égalité $bc \pm ad = mcc + mdd$, on obtient : $mcc + cx + mdd \pm dy = mcc + mdd$, soit : $cx \pm dy = 0$.
Donc $\frac{x}{y} = \mp\frac{d}{c}$ et comme d et c sont des nombres premiers entre eux, il est nécessaire que $x = nd$ et $y = \mp nc$ d'où on a : $a = \pm md \mp nc$ et $b = mc + nd$, où les nombres a et b doivent être tels que le nombre $pq = aa + bb$ soit divisible par le nombre premier $p = cc + dd$.

On remplace les valeurs de a et b dans le produit pq :

$$pq = mmdd - 2mncd + nncc + mmcc + 2mncd + nndd$$

donc

$$pq = (mm + nn)(cc + dd).$$

On en déduit donc que $q = mm + nn$.

■

Ici, on voit qu'il commence par établir des égalités, donne des expressions de a et b en fonction de c et d en utilisant la division euclidienne, puis réinsère ces valeurs dans les égalités précédentes. C'est une méthode qui sera très utilisée par Euler et Lagrange dans ce type de recherches.

Proposition 2

Si le produit pq est une somme de deux carrés, et si le facteur q n'est pas somme de deux carrés, alors l'autre facteur p, si c'est un nombre premier, n'est pas somme de deux carrés, et s'il n'est pas premier, il admet au moins un facteur premier qui n'est pas somme de deux carrés.

Démonstration

Il raisonne par l'absurde et distingue deux cas. Premièrement, si p est premier et somme de deux carrés, q serait également somme de deux carrés (d'après la proposition 1), donc p ne peut pas être somme de deux carrés. Deuxièmement, si p est un nombre composé, et si tous ses facteurs premiers sont somme de deux carrés, alors l'autre facteur q serait de la même nature. Donc les facteurs premiers de p ne peuvent pas être tous somme de deux carrés.

■

Proposition 3

Si une somme de deux carrés premiers entre eux $aa + bb$ est divisible par un nombre p, on peut toujours trouver une autre somme de deux carrés $cc + dd$ divisible par p et inférieure à la moitié de pp.

C'est un résultat fondamental pour la suite, puisqu'il va permettre à Euler de mettre en œuvre la méthode de descente infinie.

Démonstration

Soit une somme de deux carrés premiers entre eux $aa + bb$ divisible par un nombre p et telle que a et b sont aussi grands que l'on veut. Comme[17] ni a ni b ne sont divisibles par p, les nombres a et b peuvent s'exprimer comme suit :

$$a = mp \pm c \text{ et } b = np \pm d$$

où les nombres m et n peuvent être choisis de façon à ce que c et d soient inférieurs à $\frac{1}{2}p$. Comme dans sa démonstration précédente, il réinsère alors les nouvelles expressions de a et b : $aa + bb = mmpp \pm 2mcp + cc + nnpp \pm 2ndp + dd$. Cette formule est divisible par p par hypothèse et comme la partie $mmpp \pm 2mcp + nnpp \pm 2ndp$ est divisible par p, il est nécessaire que $cc + dd$, qui est somme de deux carrés, soit divisible par p.

Comme les racines c et d ne dépassent pas $\frac{1}{2}p$, la somme $cc + dd$ ne dépasse pas $\frac{1}{2}pp$.

■

Ce genre de raisonnement, à savoir obtenir une formule du type $xp+y$ pour en déduire que y est divisible par p, sera également beaucoup utilisé, par Euler et surtout par Lagrange. On remarque ici encore l'utilisation d'une variante de la division euclidienne. En effet, au lieu de poser de manière traditionnelle $a = mp+c$, où $0 \leq c < p$, on choisit de poser $a = mp \pm c$, où la valeur absolue de c est alors inférieure à $\frac{p}{2}$. Cela est fondamental pour nombre de démonstrations qui suivent dans ce mémoire, et dans des travaux ultérieurs. En particulier, ces méthodes ont une place fondamentale dans les travaux d'Euler sur les

17. Comme la somme de leur carré est divisible par p qui est premier, si par exemple a était divisible par p, alors bb serait divisible par p, et donc b serait aussi divisible par p, ce qui est impossible puisque a et b sont premiers entre eux. Mais Euler ne donne aucune précision à ce sujet.

résidus exposés dans [Euler, 1760b].

Il montre ensuite que les diviseurs des sommes de deux carrés premiers entre eux sont également somme de deux carrés :

Proposition 4

Une somme de deux carrés premiers entre eux ne peut pas être divisée par un nombre qui n'est pas somme de deux carrés.

Démonstration

Il raisonne à nouveau par l'absurde : il suppose que la somme de deux carrés premiers entre eux $aa + bb$ est divisible par p, qui n'est pas somme de deux carrés.

D'après la proposition 3, il dit que l'on peut trouver une somme de deux carrés premiers entre eux[18] $cc + dd$ inférieure à $\frac{1}{2}pp$ qui est divisible par p.

Alors $cc + dd = pq$ et, d'après la proposition 2, comme p n'est pas somme de deux carrés, soit le nombre q n'est pas une somme de deux carrés, soit q admet au moins un facteur r qui n'est pas somme de deux carrés. Comme $pq < \frac{1}{2}pp$, alors $q < \frac{1}{2}p$ et de même $r < \frac{1}{2}p$.

Donc, comme $cc + dd$ est divisible par $r < \frac{1}{2}p$, la proposition précédente affirme que l'on peut trouver une somme de deux carrés $ee + ff$ divisible par r et plus petite que $\frac{1}{2}rr$, c'est-à-dire plus petite que $\frac{1}{8}pp$. Le nombre r n'étant pas somme de deux carrés, on peut continuer de la même manière que précédemment à trouver des sommes de deux carrés de plus en plus petites, qui seront divisibles par des nombres qui ne sont pas somme de deux carrés. En conséquence, comme les sommes de deux carrés premiers entre eux sont au minimum nulles, et qu'elles sont toujours divisibles par un nombre qui n'est pas somme de deux carrés, on aboutit nécessairement à une somme de deux carrés qui est soit un nombre premier, soit l'unité, et qui n'est donc pas divisible par un nombre qui n'est pas somme de deux carrés.

■

Euler utilise donc ici la méthode de descente infinie afin de compléter un raisonnement par l'absurde, pour finalement aboutir au théorème de Fermat sur les sommes de deux carrés :

18. Or, sa proposition 3 donne effectivement une somme de deux carrés $cc + dd$ mais il ne montre pas qu'ils sont nécessairement premiers entre eux. Néanmoins, on peut toujours se ramener à une telle somme où les carrés sont premiers entre eux. En effet, dans la démonstration précédente, on a posé $a = mp \pm c$ et $b = np \pm d$. Or, si c et d admettent pour facteur commun le nombre premier s, alors ss divise $cc + dd = pr$ (puisque p divise cette somme). Si s divise p, alors s divise a et b, ce qui est en contradiction avec l'hypothèse. D'autre part, si s divise r, alors on peut poser : $c = sc'$, $d = sd'$, et $r = ssr'$. Ainsi, en substituant ces valeurs dans l'égalité $cc + dd = pr$, et en divisant par ss, on obtient : $c'c' + d'd' = pr'$, où c' et d' restent bien inférieurs à $\frac{1}{2}p$. On peut ainsi éliminer tous les facteurs communs premiers de c et d.

Proposition 5

Tout nombre premier de la forme $4n+1$ *est somme de deux carrés.*

Démonstration

Il utilise pour cette preuve les résultats vus précédemment, sauf un qu'il ne démontrera que dans un mémoire ultérieur [19]. C'est pourquoi il qualifie sa démonstration de *Tentamen demonstrationis*.

Il rappelle que $a^{4n} - b^{4n}$ est toujours divisible par $4n+1$ (d'après le petit théorème de Fermat) quand celui-ci est premier et ne divise ni a ni b. Donc $4n+1$ divise nécessairement $a^{2n} - b^{2n}$ ou $a^{2n} + b^{2n}$.

Ensuite, même s'il ne le démontre qu'après dans [Euler, 1760a], il affirme qu'il existe des nombres a et b tels que $a^{2n} - b^{2n}$ ne soit pas divisible par $4n+1$.

Il pose finalement $p = a^n$, $q = b^n$ et on a bien une somme de deux carrés divisible par $4n+1$. De plus, même si pp et qq admettent un plus grand diviseur commun mm différent de l'unité, celui-ci est premier avec $4n+1$ (sinon, $4n+1$ diviserait p et q, et donc $p^2 - q^2 = a^{2n} - b^{2n}$ ce qui est contraire à ce qui précède), et c'est donc la nouvelle somme de deux carrés premiers entre eux qui est divisible par $4n+1$. Il conclut alors avec la proposition 4.

■

Le mémoire contient ensuite d'autres propositions sur les sommes de deux carrés et sur les nombres premiers de la forme $4n+1$.

Dans ce mémoire, nous avons donc une première démonstration, certes incomplète, du théorème des deux carrés dont l'architecture est la même que celle des démonstrations des résultats sur les sommes de carrés qui suivront, à savoir : dans un premier temps, montrer qu'une forme donnée est stable par multiplication, puis montrer que pour tout nombre premier, il existe une expression de la forme en question divisible par ce nombre premier, enfin que cette expression a des propriétés particulières qui permettent d'achever la démonstration. Ici, pour démontrer le théorème des deux carrés, Euler utilise des manipulations algébriques, des divisions euclidiennes, le petit théorème de Fermat, ainsi que la méthode de descente infinie.

(b) Complément de la démonstration du théorème des deux carrés

Il achève la démonstration du théorème des deux carrés dans le mémoire intitulé *Demonstratio theorematis Fermatiani omnem numerum primum formae* $4n+1$ *esse summam*

19. Le résultat en question se trouve dans [Euler, 1760a], nous le résumons ci-après.

duorum quadratorum[20], qui a été envoyé pour la première fois dans une lettre destinée à Goldbach datée du 12 avril 1749.

C'est dans ce mémoire qu'il montre qu'étant donné un nombre premier de la forme $4n+1$, il existe des nombres a et b tels que $a^{2n} - b^{2n}$ n'est pas divisible par $4n+1$. Pour cela, il considère la suite des nombres de 1 à $4n$ mis à la puissance $2n$:

$$1,\ 2^{2n},\ 3^{2n},\ldots,(4n)^{2n},$$

et il raisonne par l'absurde : il suppose que toutes les différences premières

$$2^{2n}-1, 3^{2n}-2^{2n}, 4^{2n}-3^{2n}, \ldots, (4n)^{2n}-(4n-1)^{2n}$$

sont divisibles par $4n+1$. Il en déduit que toutes les différences secondes sont également divisibles par $4n+1$, ainsi que les différences troisièmes, ..., et jusqu'à la différence d'ordre $2n$, qui est égale à $1.2.3.\ldots.2n$[21], qui ne peut être divisible par le nombre $4n+1$ qui est premier. Il en déduit donc qu'il y a au moins une des différences premières qui n'est pas

20. On peut traduire le titre de ce mémoire par : *Démonstration d'un théorème de Fermat : tout nombre premier de la forme $4n+1$ est somme de deux carrés.*. Il a été lu pour la première fois à l'Académie de Berlin le 15 octobre 1750, a été publié en 1760 : voir [Euler, 1760a].

21. Ces résultats viennent de la théorie des différences finies, déjà connue de Leibniz, qu'Euler expose notamment dans le volume 1 de son *Institutiones calculi differentialis cum eius usu in analysi finitorum ac doctrina serierum*, publié en 1755. On peut rapidement résumer la méthode que l'on retrouve chez Euler dans son ouvrage de 1755. Il considère une fonction f, un accroissement fixe ω, et travaille sur les suites x, $x+\omega$, $x+2\omega$, ..., et $f(x)$, $f(x+\omega)$, $f(x+2\omega)$, ... (que lui note y, y^I, y^{II}, ...).

Il définit alors la suite des différences premières :

$$\Delta f(x) = f(x+\omega) - f(x), \Delta f(x+\omega) = f(x+2\omega) - f(x+\omega), \Delta f(x+2\omega) = f(x+3\omega) - f(x+2\omega), \ldots,$$

notées $\Delta y = y^I - y, \ldots$. Puis il définit les différences secondes :

$$\begin{aligned} \Delta^2 f(x) &= \Delta f(x+\omega) - \Delta f(x), \\ \Delta^2 f(x+\omega) &= \Delta f(x+2\omega) - \Delta f(x+\omega), \\ \Delta^2 f(x+2\omega) &= \Delta f(x+3\omega) - \Delta f(x+2\omega), \ldots, \end{aligned}$$

et ainsi de suite. Il prend ensuite l'exemple de la fonction $f(x) = x$ et montre que les différences premières pour cette fonction sont constantes, et que les différences d'ordre supérieur sont nulles. Puis il essaie de trouver une formule qui donne les différences d'ordre quelconque de la fonction f en fonction de $f(x)$, $f(x+\omega)$, $f(x+2\omega)$, ..., et remarque que la différence d'un ordre donné d'une somme de fonctions est la somme des différences de cet ordre de chaque fonction. Il donne également la formule des différences de produits de fonctions. En fait, pour une fonction f, on a, en notations modernes :

$$\Delta^n f(x) = \sum_{j=0}^{n} (-1)^{n-j} \binom{n}{j} f(x+j\omega).$$

Il poursuit en donnant les exemples des fonctions x^2, x^3, et x^4. Son exemple IV est le calcul des différences finies pour la fonction $f(x) = x^n$. On a :

$\Delta f(x) = (x+\omega)^n - x^n$, qui est un polynôme de degré $n-1$, et ayant pour coefficient de plus haut degré $\omega n x^{n-1}$;

$\Delta^2 f(x)$ qui est un polynôme de degré $n-2$ de coefficient de plus haut degré $\omega^2 n(n-1)x^{n-2}$;

... ;

$\Delta^n f(x)$ qui est un polynôme constant égal à $\omega^n n(n-1)(n-2)\ldots 2.1$.

Les différences d'ordre supérieur à n sont nulles.

divisible par $4n+1$, d'où le résultat.

Cette méthode des différences finies est très importante dans les travaux de Lagrange, en particulier pour ses démonstrations du théorème des quatre carrés et du théorème de Wilson.

3 - Une approche des résidus par Euler et une démonstration d'un cas particulier du théorème des quatre carrés

Dans son mémoire *Demonstratio theorematis Fermatiani omnem numerum sive integrum sive fractum esse summam quatuor pauciorumve quadratorum*[22] , Euler traite d'une manière toute différente les sommes de carrés. Il consacre en effet une grande majorité de son mémoire aux résidus en exposant douze théorèmes sur les restes de carrés après division par un nombre p : il appelle ces restes les *residua*. Il applique ensuite les résultats obtenus à des propositions sur les sommes de carrés. Les théorèmes 19 et 20 s'appuient sur les propriétés précédentes et permettent d'obtenir une version faible du théorème des quatre carrés. Ce texte est le premier où Euler utilise systématiquement les résidus et est à la base de ses mémoires suivants. On y voit apparaître en particulier certaines propriétés opératoires des résidus. C'est pourquoi nous allons étudier en détail chacun des résultats de ce mémoire.

(a) Quelques propriétés des résidus quadratiques

Dans cette série de propriétés, Euler commence par considérer les restes de carrés après division par un nombre p quelconque, puis il suppose que le nombre p est premier impair. Enfin, il obtient des résultats selon la forme du nombre premier p ($4n+1$ ou $4n-1$). Ici, le mot "résidu" utilisé par Euler désigne ce que l'on appelle aujourd'hui un résidu quadratique.

Où le nombre p est quelconque

Dans le théorème 1 et les corollaires suivants, Euler indique quels sont les carrés dont les restes après division par un nombre quelconque p peuvent être ramenés à des nombres non nuls inférieurs à p : ce sont les nombres carrés dont la racine n'est pas un multiple de

22. On peut traduire ce titre par : *Démonstration d'un théorème de Fermat : tout nombre entier ou fractionnaire est somme de quatre ou d'un nombre moindre de quatre carrés.* Ce traité a été lu à l'Académie de Berlin le 17 juin 1751. Il a été publié pour la première fois en 1760 : voir[Euler, 1760b]. Les trois mémoires [Euler, 1758], [Euler, 1760a] et [Euler, 1760b] sont consécutifs dans les recherches arithmétique d'Euler.

p, c'est-à-dire les nombres qui ne sont pas de la forme k^2p^2. Il observe dans une scholie que l'étude de ces résidus permet d'obtenir des résultats remarquables et non élémentaires.

Théorème 2

Si la suite des entiers carrés continuée à l'infini est divisée en groupes de la manière suivante :

$$1, 4, \ldots, pp \mid (p+1)^2, \ldots, 4pp \mid (p+2)^2, \ldots, 9pp \mid (p+3)^2, \ldots, 16pp \mid \text{etc.}$$

alors si l'on divise par le nombre premier p les nombres situés à la même place dans les groupes, ils auront le même résidu.

Autrement dit, si on considère un nombre α compris entre 1 et p, tous les nombres $(kp+\alpha)^2$, où $k > 0$, auront le même résidu, c'est-à-dire le même reste après division par p. Il démontre ainsi que la suite des résidus des carrés est périodique.

Puis suivent cinq corollaires où il remarque que les nombres carrés plus petits que p sont leur propre résidu, et que si les carrés sont plus grands que p, on peut les ramener après divisions successives par p à des résidus plus petits que p. Ainsi, le résidu $np+\alpha$ est α pour tout nombre entier n. Il observe que les résidus seront parmi les termes $1, 4, 9, 16, \ldots, (p-1)^2$, et qu'il y en aura donc au plus $p-1$.

Théorème 3

Si tous les nombres de la série 1, 4, 9, 16 etc. sont divisés par un nombre quelconque p, tous les nombres plus petits que p ne sont pas résidus.

Pour démontrer ce résultat, il commence par faire une liste des carrés de tous les nombres compris entre 1 et $p-1$, et remarque que, comme $(p-1)^2 = p^2 - 2p + 1$, le résidu de $(p-1)^2$ est 1. Il généralise, en disant que si l'on considère le carré $(p-n)^2$, il aura le même résidu que le nombre n^2. Ainsi, comme les résidus sont égaux deux à deux, il y en a nécessairement moins que $p-1$. Il ajoute même dans le corollaire qui suit que le nombre de résidus distincts est au plus $\frac{p-1}{2}$ si p est impair, et $\frac{p}{2}$ si p est pair. Il consacre le corollaire 2 au cas particulier $p = 2$. Ensuite, il en déduit, dans le corollaire 3, le nombre minimal de termes compris entre 1 et $p-1$ qui ne sont pas résidus : $\frac{p-1}{2}$ si p est impair, et $\frac{p-2}{2}$ si p est pair. Il nomme ces termes les *non-résidus* (*non-residua*). Puis il finit par un tableau où il donne les résidus des carrés des nombres compris entre 1 et $p-1$ pour p entre 3 et 12, et dont les données confirment bien les résultats précédents. Voici un extrait de ce tableau :

Sit	$p = 3$	$p = 4$	$p = 5$	$p = 6$
	1,4	1, 4, 9	1, 4, 9, 16	1, 4, 9, 16, 25
residua	1, 1	1, 0, 1	1, 4, 4, 1	1, 4, 3, 4, 1
non-residua	2	2, 3	2, 3	2, 5

Théorème 4

Si l'on veut trouver les résidus qui résultent de la division d'un carré par un nombre p quelconque, il suffit de les rechercher pour les nombres carrés depuis 1 jusqu'à $\left(\frac{p-1}{2}\right)^2$ *si p est impair, ou* $\left(\frac{p}{2}\right)^2$ *si p est pair.*

Il introduit alors une notation pour représenter les nombres résidus : il les représentera par les lettres grecques 1, α, β, γ, etc. Il annonce qu'il veut étudier quelques propriétés de ces résidus. Les propriétés qu'il va démontrer ci-dessous sont les propriétés qu'il démontre également plus tard lorsqu'il travaille sur les résidus de puissances.

Théorème 5

Si le nombre r est dans la série des résidus 1, α, β, γ, δ, ϵ,*etc., alors toutes les puissances de ce nombre* r^2, r^3, r^4, *etc. qui donnent un reste sont dans cette série.*

Autrement dit : les puissances d'un résidu quadratique sont des résidus quadratiques. Il écarte le cas où la puissance de r ne donne pas de reste, c'est-à-dire le cas où elle est divisible par p. Pour démontrer ce résultat, il suppose que r est le résidu du carré aa. Il remarque alors que $a^4 = (mp + r)^2$ admet le même résidu que le nombre r^2. De même, le nombre $a^6 = (mp + r)^3$ donne le même résidu que le nombre r^3, et ainsi de suite. Or, les résidus des carrés proviennent des carrés plus petits 1, 4, 9, ..., $\left(\frac{p-1}{2}\right)^2$ ou $\left(\frac{p}{2}\right)^2$ selon la parité de p et sont dans la série 1, α, β, γ, δ, ϵ, etc. On peut donc en déduire que les puissances de r sont bien dans cette série.

Dans un des corollaires de ce théorème, il observe que comme la série des résidus comporte un nombre fini de termes, il y aura dans la série des puissances une infinité de termes qui donneront le même résidu. Puis il affirme que si les puissances r^m et r^n donnent le même résidu, la différence $r^m - r^n = r^n(r^{m-n} - 1)$ est divisible par p. Donc si r^n est premier avec p, par exemple dans le cas où r est premier à p, alors $r^{m-n} - 1$ est divisible par p, et le résidu de r^{m-n} est donc 1. De là, si on trouve un nombre λ tel que le reste de la division de r^λ par p est 1, alors la puissance $r^{\lambda+k}$ a pour résidu r^k. Ainsi, comme il y a au plus $\frac{p-1}{2}$ ou $\frac{p}{2}$ résidus distincts, il y a nécessairement un nombre λ plus petit que $\frac{p-1}{2}$ ou $\frac{p}{2}$ tel que le résidu de r^λ est 1.

Théorème 6

Si dans la série 1, α, β, γ, δ, ϵ,*etc. des résidus qui résultent de la division des nombres carrés par* p, *on prend les nombres* r *et* s, *le produit* rs *est dans la série des résidus.*

Il énonce ici que le produit de deux résidus quadratiques est encore un résidu quadratique. Il démontre ce résultat en posant $aa = mp + r$ et $bb = np + s$, puis calcule $aabb = mnpp + msp + nrp + rs$ qui laisse bien rs pour reste de la division par p. Dans le corollaire 1, il énonce que si r et s sont des résidus, alors tous les produits de puissances quelconques de r et s sont des résidus quadratiques. Il ajoute également que le produit de plusieurs résidus quadratiques est également un résidu quadratique. Il illustre ces résultats à partir de l'exemple $p = 19$.

Théorème 7

Si on prend deux nombres r *et* rs *dans la série des résidus de la division des carrés par* p, *et s'ils sont premiers avec* p, s *est aussi un résidu.*

Pour démontrer ce résultat, il suppose que r et rs sont des résidus, et pose donc $aa = mp + r$ et $bb = np + rs$. Donc la différence $bb - aas = np - mps$ est divisible par p. Comme r et rs sont premiers avec p, les carrés aa et bb le sont aussi. Si les carrés aa et bb ne sont pas premiers entre eux, il suffit de diviser l'égalité par le PGCD de a et de b au carré, qui est bien sûr premier avec p. Alors, $(mp \pm b)^2 - aas$ est divisible par p pour tout m, et on prend m tel que $mp \pm b = ac$[23]. Alors $aa(cc - s)$ est divisible par p. Or aa est premier à p, donc $cc - s$ est divisible par p, d'où s est le résidu de cc.

Il prend ensuite un contre-exemple pour montrer que r et s doivent être premiers avec p puis il énonce son résultat dans le cas où p est premier : si p est premier, r et rs des résidus quadratiques, alors s est résidu quadratique.

Où le nombre p est premier

À partir du théorème 8, Euler suppose que p est un nombre premier impair, et pose $p = 2q + 1$. Les résidus sont les restes des divisions des carrés 1, 4, 9,..., qq, et leur nombre est inférieur à q. On observe que, comme p est premier, 0 ne peut pas être un résidu. De plus, les non-résidus sont les nombres compris entre 1 et $p - 1$ qui ne sont pas résidus.

23. Euler ne le démontre pas ici mais l'éditeur Ferdinand Rudio note qu'il suffit que a et p soient premiers entre eux, ce que l'on a d'ailleurs vu. En fait, c'est l'actuel théorème de Bézout. On retrouve ce type de résultat dans un mémoire ultérieur d'Euler : *Theoremata arithmetica nova methodo demonstrata*, lu en 1759 à l'Académie de Saint-Pétersbourg, et publié pour la première fois en 1763, dans le tome VIII des *Novi Commentarii academiae scientiarum Petropolitanae*. Il y énonce que si les termes d'une progression arithmétique sont divisés par un nombre quelconque n, et si la raison d de la progression est premier avec n, alors on a dans les résidus de cette progression tous les nombres plus petits que n, soit les nombres de 1 à $n - 1$. Pour sa démonstration, il considère les restes de la division par n des termes a, $a + d$, ..., $a + (n - 1)d$ et montre par un raisonnement par l'absurde que ces restes sont tous distincts. En effet, si deux restes sont égaux, on a alors : $a + \nu d - (a + \mu d) = (\nu - \mu)d$ qui est divisible par n. Or, ceci est impossible car $0 < \nu - \mu < n$ est premier à n, et d est aussi premier à n par hypothèse.

Il rappelle enfin que le produit de plusieurs résidus est un résidu, et que, si r et rs sont résidus, alors leur quotient est aussi un résidu.

Théorème 8

Si le diviseur p est premier et égal à $2q+1$*, la série des résidus des carrés* 1, α, β, γ, δ, ϵ,*etc. contient q éléments distincts.*

On n'obtient tout d'abord aucun résidu nul, car un carré inférieur à qq ne peut être divisible par le nombre p qui est premier. On suppose alors que deux résidus résultant de la division de aa et bb par p sont égaux. Alors, $aa - bb$ est divisible par $p = 2q + 1$. Or, comme a et b sont inférieurs à q, $a + b$ est inférieur à $2q$, soit inférieur à p. Or, comme $aa - bb$ est divisible par p, soit $a + b$ soit $a - b$ est divisible par p, ce qui est impossible puisque ces deux nombres sont inférieurs à p. D'où le résultat.

Il en déduit donc qu'il y a exactement q résidus distincts issus de la division par p, et qu'il y a donc également q non-résidus. Il dresse alors la table des résidus et des non-résidus pour les nombres premiers de 3 à 29.

Théorème 9

Si la série des résidus de la division des carrés par un nombre premier $p = 2q+1$ *est* 1, α, β, γ, δ, ϵ, *etc., et la série des non-résidus a, b, c, d, e, etc., et que r est un non-résidu, alors* αr, βr, γr, δr,*etc. sont non-résidus.*

Ce théorème revient à dire que le produit d'un non-résidu quadratique avec un résidu quadratique est un non-résidu quadratique. Il le montre en utilisant le théorème 7 : en effet, si α est un résidu, et αr aussi, alors r est également un résidu, ce qui est en contradiction avec l'hypothèse sur r.

De là, il observe que comme tous les résidus 1, α, β, γ, δ, ϵ, etc., sont distincts et qu'ils sont au nombre de q, on obtient, à partir d'un seul non-résidu r, tous les non-résidus, qui sont alors donnés par r, αr, βr, γr, δr,etc [24].

Théorème 10

Les produits de deux nombres non-résidus seront des résidus, pourvu qu'ils résultent de la division des carrés par un nombre premier p.

En prenant les même notations que précédemment, il suppose que r est un non-résidu,

24. Il ne démontre pas ce résultat. On peut néanmoins le prouver en utilisant une démarche similaire à la démonstration du théorème 8 : si on a, pour $\alpha \neq \beta$, $\alpha r = \beta r$, alors $\alpha r - \beta r$ est divisible par p. Donc $\alpha - \beta$ ou r est divisible par p, ce qui est impossible car ces deux nombres sont plus petits que p, qui est premier.

et obtient donc la liste des non-résidus : r, αr, βr, γr, δr,etc. Le produit de deux de ces non-résidus sera donc de la forme $\alpha\beta r^2$, qui est le produit des deux résidus $\alpha\beta$ et r^2, le premier comme produit de deux résidus, et le deuxième en tant que carré. Le nombre $\alpha\beta r^2$ est donc un résidu lui-même, comme produit de deux résidus.

Dans un premier corollaire, il résume les résultats précédents : le produit de deux résidus ou de deux non-résidus est un résidu, tandis que le produit d'un résidu et d'un non-résidu est un non-résidu. Il en déduit un résultat sur les divisions : la division d'un résidu par un résidu donne un résidu ; celle d'un non-résidu par un non-résidu donne un résidu ; mais celle d'un résidu par un non-résidu, ou alors d'un non-résidu par un résidu, donne un non-résidu [25]. Puis il donne un résultat plus général sur le produit d'un nombre quelconque de non-résidus.

Il introduit ensuite une nouvelle notion, qui est fondamentale pour les résultats suivants, et pour la démonstration du théorème des quatre carrés :

Définition

Le complément d'un résidu est la différence entre ce résidu et le diviseur ; si le diviseur est p et le résidu r, alors le complément du résidu est $p - r$.

Il commence par énoncer quelques corollaires qui suivent immédiatement la définition, et qui permettent d'introduire les résidus négatifs. Tout d'abord, il remarque que, puisque les nombres de la forme $np + r$ ont tous les même résidu, où n est un entier quelconque, alors leur complément sera $p - np - r$, soit, avec $n = 1$, $-r$. Ensuite, dans l'expression du résidu $np + r$, si l'on prend $n = -1$, on obtient le résidu $r - p$, qui est négatif, et qui sera équivalent au résidu positif r. Ainsi, si le résidu r est supérieur à $\frac{p}{2}$, le résidu négatif équivalent sera inférieur à $\frac{p}{2}$. Il en déduit alors que, en tenant compte des expressions négatives, les résidus peuvent tous être exprimés par des nombres inférieurs à $\frac{p}{2}$. Il ne le précise toujours pas, mais il considère ici les valeurs absolues des résidus. Il applique également ces expressions négatives aux non-résidus, et donne un exemple pour $p = 23$. De là, il remarque qu'il est alors intéressant de savoir si le complément d'un résidu est un résidu.

Théorème 11

Si la série des résidus de la division des carrés par un nombre premier $p = 2q + 1$ est 1, α, β, γ, δ, ϵ, etc. et si le complément de l'un de ses termes est un résidu, alors il en

25. Ici, on remarque qu'il ne donne pas pour l'instant de précision sur ce qu'il qualifie de division. D'après ses démonstrations précédentes, il se place dans le cas d'une division où le quotient est *a priori* un nombre entier. En revanche, il ne démontre pas que tout nombre admet un inverse modulo p.

est de même pour tous les autres compléments.

En effet, si r et $-r$ (soit le complément de r) sont des résidus, alors $\frac{r}{-r} = -1$ est un résidu. Alors, les nombres -1, $-\alpha$, $-\beta$, $-\gamma$, $-\delta$, $-\epsilon$, etc., qui sont les compléments des résidus, sont également des résidus, comme produits de deux résidus.

Il observe alors que dans ce cas, le nombre de résidus est nécessairement pair. Ce nombre valant q, on en déduit que q doit être pair : ce résultat est donc valable pour les nombres premiers p de la forme $4n+1$. Pour le moment, il remarque que si q est impair, alors le complément d'un résidu ne peut être un résidu. Finalement, si p est de la forme $4n+3$, les compléments des résidus sont des non-résidus.

Il insiste alors sur le fait que l'on voit bien apparaître une séparation entre les nombres premiers impairs de la forme $4n+1$ et $4n-1$. Il rappelle que Fermat a dit que les nombres de la forme $4n+1$ sont somme de deux carrés, et que lui-même l'a déjà démontré. Il ajoute que l'on peut facilement montrer que les autres types de nombres, à savoir ceux qui sont de la forme $4n-1$, ne sont pas somme de deux carrés, et que l'on peut même prouver que la somme de deux carrés $aa+bb$ n'admet pas de facteur de la forme $p = 4n-1$, à moins que chacun des carrés aa et bb ne soit divisible par le nombre p. Son but est ici de démontrer que tous les nombres de la forme $4n-1$ sont en revanche des sommes de trois ou quatre carrés.

Théorème 12

Si la série des résidus de la division des carrés par un nombre premier $p = 4n-1$ est 1, α, β, γ, δ, ϵ, etc., le complément d'un résidu ne peut être un résidu.

Ici, les résidus résultent de la division de $1, 4, 9, 16, \ldots, (2n-1)^2$ (car ici, $q = 2n-1$), soit un nombre impair de termes. Donc, d'après ce que l'on a observé précédemment, le complément d'un résidu ne peut pas être un résidu car on aurait alors un nombre pair de résidus.

De là, il observe que le dernier résidu, qui est le reste de la division de $(2n-1)^2 = 4nn - 4n + 1 = (4n-1)n - 3n + 1$ par $4n-1$, est égal à $-3n+1$, c'est-à-dire à n (puisque $-3n+1 = -(4n-1)+n$). Il en déduit que le complément, $-n$ ou $3n-1$, est donc un non-résidu. Donc, comme $mp - n = m(4n-1) - n$, les nombres qui, divisés par $4n-1$, donnent $-n$ comme reste ne peuvent être des carrés (sinon, $-n$ serait un résidu). Il remarque aussi, que dans ce cas, les opposés des nombres carrés sont des non-résidus.

(b) Les résidus quadratiques appliqués aux sommes de carrés

Théorème 13

Si la somme de deux carrés est divisible par un nombre premier $4n-1$*, ces deux nombres sont divisibles par* $4n-1$*. Donc la somme de deux carrés premiers entre eux ne peut être divisible par le nombre premier* $4n-1$*.*

Soient a et b tels que $aa+bb$ soit divisible par $4n-1$, et tels que ni aa ni bb ne soient divisibles par $4n-1$. Soient r et s, les résidus respectifs de aa et bb par la division par $4n-1$. Or, comme par hypothèse, $aa+bb$, qui a pour résidu $r+s$, est divisible par $4n-1$, on a soit $s=4n-1-r$, soit $s=-r$, ce qui signifie que le complément de r est résidu, et c'est impossible d'après le théorème 12. On peut donc en déduire que les deux carrés aa et bb sont divisibles par p.

Il énonce alors deux corollaires. Il observe dans le premier que le fait qu'aucun nombre de la forme $aa+1$ n'est divisible par un nombre premier de la forme $4n-1$ implique que le résidu d'un nombre carré aa ne peut être égal à 1. Dans le deuxième, il déduit du théorème 13 qu'une somme de deux carrés $aa+bb$ ne peut être divisible par un nombre p qui admet un facteur de la forme $4n-1$, à moins que les deux carrés ne soient divisibles par le facteur en question.

Théorème 14

Que le nombre $4n-1$ *soit premier ou non, aucune somme de deux carrés premiers entre eux n'est divisible par* $4n-1$*.*

Le résultat a déjà été montré dans le cas où le nombre $4n-1$ est premier. S'il n'est pas premier, il est alors produit de nombres de la forme $4m-1$ ou $4m+1$. Mais les produits de nombres de la forme $4m+1$ donnent des nombres de la forme $4n+1$. Le nombre $4n-1$ admet donc au moins un facteur de la forme $4m-1$, et on utilise le corollaire précédent pour conclure.

Il remarque alors qu'aucune somme de deux carrés n'est donc égale à $4n-1$, puis ajoute que cela peut se montrer beaucoup plus facilement, en considérant la forme des nombres carrés. Il ajoute également que les nombres de la forme $m(4n-1)$ ne peuvent être une somme de deux carrés a^2+b^2 que si a et b sont premiers entre eux.

Théorème 15

Aucun nombre de la forme $4mn-m-n$ *ne peut être un carré.*

D'après ce qui précède, on ne peut pas avoir $(4m-1)(4n-1) = 1+aa$, c'est-à-dire qu'on ne peut avoir $16mn - 4m - 4n = aa$, d'où le résultat. Dans [Weil, 1984, p. 205], l'auteur justifie la présence de ce résultat : en travaillant sur le fait que les sommes de deux carrés n'admettent pas de diviseur de la forme $4n - 1$, Euler aurait prouvé que cette assertion est équivalente au fait que les nombres $4mn-m-1$ et $4mn-m-n$ ne peuvent être des carrés.

Théorème 16

Si la série des résidus de la division des carrés par un nombre quelconque p est 1, α, β, γ, δ, *etc., et que le complément d'un résidu est un résidu, on peut alors trouver deux carrés dont la somme soit divisible par p.*

Si aa a pour résidu r et bb a pour résidu $-r$, ou $p-r$, alors la somme de carrés[26] $aa+bb$ est divisible par p.

De là, il déduit que si p est un nombre premier et si le complément d'un des résidus est un résidu, alors les compléments des autres résidus sont des résidus, et si le résidu de aa est r, il est alors possible de trouver x inférieur à $\frac{p}{2}$ tel que $aa + xx$ soit divisible par p. De même, si la somme de deux carrés $aa + bb$ est divisible par p premier, et donc que les résidus de a et b sont complémentaires, alors le résidu d'un autre carré cc aura un complément qui sera résidu : il existe donc x tel que $cc + xx$ est divisible par p. Ces résultats ne s'appliquent que pour les nombres premiers de la forme $4n + 1$.

Il remarque alors qu'il reste à trouver une démonstration directe, c'est-à-dire avec les outils utilisés dans ce mémoire, et non des méthodes analytiques comme les différences finies, pour prouver que le théorème 16 est vrai pour tous les nombres premiers de la forme $4n + 1$. Il admet que lui n'a pas réussi, mais donne néanmoins les exemples de quelques nombres premiers, qui sont concluants. Il observe également que si à partir du nombre $4n+1$, on a la série des $2n$ résidus 1, α, β, γ, δ, etc., et que le complément d'aucun résidu n'est un résidu, alors -1, $-\alpha$, $-\beta$, $-\gamma$, $-\delta$, etc., représentent tous les non-résidus. Donc si, on peut trouver un non-résidu dont le complément est non-résidu, alors c'est en contradiction avec la série des non-résidus que l'on vient d'obtenir. On pourra alors en déduire qu'aucun résidu n'a de complément qui soit non résidu, et on aura alors la démonstration directe désirée.

Théorème 17

Si la série des résidus de la division des carrés par un nombre p quelconque est 1, α, β, γ, δ, *etc., et si le complément de la somme de deux de ces résidus est aussi un résidu, alors il est possible d'exhiber trois carrés dont la somme est divisible par p, et tels*

26. Ces carrés aa et bb existent nécessairement par définition d'un résidu.

qu'aucune des racines ne soit supérieure à $\frac{p}{2}$.

En effet, si r et s sont les résidus respectifs de deux carrés aa et bb, et que le complément de $r+s$, soit $-r-s$, est un résidu, alors il existe un carré $cc < \frac{pp}{4}$ qui a $-r-s$ comme reste de la division par p. Dans ce cas, la somme $aa+bb+cc$ est divisible par p.

Il remarque alors que, de la même façon, si on trouve un résidu qui est le complément de la somme de trois résidus, on peut alors exhiber une somme de quatre carrés qui est divisible par p.

De là, il énonce son théorème qui sera à la base de sa démonstration du théorème des quatre carrés fractionnaires.

Théorème 18

Pour tout nombre premier p, si toute somme de deux carrés premiers entre eux ne peut être divisible par p, on pourra toujours trouver une somme de trois carrés divisible par p.

Si dans la série des résidus, il y a -1, tous les compléments des résidus seront résidus, et il y aura plusieurs sommes de deux carrés divisibles par p.

Si -1 n'est pas dans la série des résidus, -1 est non-résidu et aucun complément de résidus n'est résidu. Dans ce cas, aucune somme de deux carrés n'est divisible par p, sauf si chaque carré est divisible par p. Montrons que l'on peut alors trouver une somme de trois carrés divisible par p. On remarque d'abord que si r est résidu, $-r$ est non résidu, et si r est non-résidu, $-r$ est résidu. On suppose qu'aucune somme de trois carrés n'est divisible par p. Puisque 1 est résidu, -2 est non-résidu (sinon le complément de la somme $1+(-2)$ est 1 et est donc un résidu). On obtiendrait ainsi une somme de trois carrés divisibles par p d'après le théorème 17, ce qui est contraire à l'hypothèse de départ . On en déduit donc que 2 est résidu puisque -2 est non-résidu. Ainsi, -3 est non-résidu, et 3 est donc résidu. En continuant, on trouve que tous les nombres 1,2,3 ...sont résidus, et qu'il n'y a donc pas de non-résidus, ce qui est impossible. On en déduit qu'il existe une somme de trois carrés divisible par p dont aucun des carrés n'est divisible par p.

Il remarque que, à partir de ce résultat, on peut voir que pour tout p, il existe une somme de quatre carrés divisible par p. De plus, si p ne divise pas de somme de deux carrés, mais qu'il en divise une de trois carrés aa, bb, cc, tels que chacun des carrés soit inférieur à $\frac{pp}{4}$, alors la somme sera inférieure à $\frac{3pp}{4}$, et le quotient de la somme par p sera inférieur à $\frac{3p}{4}$, c'est-à-dire strictement inférieur à p. C'est ce qui va permettre à Euler d'utiliser un raisonnement par l'absurde pour démontrer le théorème 20.

Théorème 19

Si la somme $aa+bb+cc+dd$ de quatre carrés est divisée par la somme de quatre carrés $pp+qq+rr+ss$, leur quotient est aussi la somme de quatre carrés de fractions.

Il suffit de multiplier le numérateur et le dénominateur de la fraction $\dfrac{aa+bb+cc+dd}{pp+qq+rr+ss}$ par la somme $pp+qq+rr+ss$. Au dénominateur, on obtient alors le carré d'un entier et au numérateur, on a le produit de deux sommes de quatre carrés. Or, le produit de deux sommes de quatre carrés est encore une somme de quatre carrés. Il suffit pour voir cela de poser :

$$\begin{aligned} x &= ap+bq+cr+ds,\\ y &= aq-bp\pm cs\mp dr,\\ z &= ar\mp bs-cp\pm dq,\\ v &= as\pm br\mp cq-dp. \end{aligned}$$

On obtient alors : $(aa+bb+cc+dd)(pp+qq+rr+ss)=xx+yy+zz+vv$. Finalement, le quotient obtenu est bien une somme de quatre carrés de nombres rationnels.

Après ce théorème, Euler démontre le théorème des quatre carrés, mais en admettant des sommes de nombres rationnels. Il remarque dans un premier temps que, comme le produit de deux sommes de quatre carrés est encore une somme de quatre carrés, il suffit de montrer le théorème pour les nombres premiers.

Théorème 20

Tous les nombres sont somme de quatre carrés (ou moins) si l'on accepte les carrés de fractions.

En effet, si on suppose que ce n'est pas le cas, on peut considérer le plus petit nombre premier p qui ne peut pas être exprimé comme une somme de quatre carrés rationnels.

Il existe alors une somme de trois carrés $aa+bb+cc$ divisible par p, ceci d'après le théorème 18, chacun des carrés étant inférieur à $\frac{pp}{4}$. Alors $aa+bb+cc<\frac{3pp}{4}$.

Le quotient $\dfrac{aa+bb+cc}{p}$ est donc inférieur à $\frac{3p}{4}$, et donc à p. On en déduit, d'après l'hypothèse sur p, que le quotient sera une somme de quatre carrés ou d'un nombre moindre de carrés, soit $xx+yy+zz+vv$. On aura donc $p=\dfrac{aa+bb+cc}{xx+yy+zz+vv}$. Le nombre p est donc lui-même une somme de quatre carrés d'après le théorème 19, ce qui contredit l'hypothèse. Finalement, tous les nombres premiers sont somme de quatre carrés, et, puisque le produit de sommes de quatre carrés donne une somme de quatre carrés, on peut en conclure que tous les nombres entiers sont somme de quatre carrés.

Il généralise le résultat aux fractions. En effet, si on considère la fraction $\frac{m}{n}$, on a $\frac{m}{n} = \frac{mn}{nn}$ et on peut en déduire le résultat.

4 - Vers une théorie des résidus quadratiques

À partir des mémoires d'Euler que l'on vient d'étudier, on peut lister plusieurs outils dont il se sert régulièrement. Les premiers outils sont bien sûr des théorèmes fondamentaux d'arithmétique, l'utilisation du binôme de Newton et des propriétés de ses coefficients, et les différences finies. Un outil clé de théorie des nombres est également le petit théorème de Fermat. Enfin, petit à petit, on voit apparaître des considérations sur les restes de divisions euclidiennes, jusqu'à l'élaboration de ses résultats sur les résidus quadratiques. Dans [Euler, 1760b], Euler indique explicitement qu'il souhaiterait d'ailleurs obtenir des démonstrations directes des résultats sur les sommes de deux carrés, c'est-à-dire basées sur des outils arithmétiques, comme les résidus par exemple, en évitant le recours à des résultats "étrangers" à la théorie des nombres. Comme nous l'avons observé dans la première partie, c'est une problématique que l'on retrouve tout au long du XIX^{e} siècle : bâtir la théorie des nombres sur ses propres objets.

Les démonstrations du théorème des deux carrés et de la version faible du théorème des quatre carrés sont construites selon le même squelette :

- On montre la stabilité par multiplication et division des formes concernées (sommes de deux carrés ou de quatre carrés) : cela permet de réduire les recherches au cas où le nombre p est premier et de conclure la dernière étape ;
- on prouve que, pour tout nombre premier p, il existe une telle forme (somme de deux ou quatre carrés) divisible par p ;
- On en déduit que p peut également être mis sous cette forme.

On retrouve cette architecture dans les démonstrations du théorème des quatre carrés proposées par Lagrange et Euler, même si les deux mathématiciens utilisent des outils très différents pour arriver à leur fin.

Afin d'obtenir une démonstration fondée sur des objets arithmétiques, Euler établit tout un ensemble de résultats importants sur les résidus quadratiques dans [Euler, 1760b], après avoir fait allusion aux résidus dans ses travaux précédents.

Si on lit ce mémoire à la lumière de la théorie des corps finis moderne, on peut remarquer qu'Euler se restreint très rapidement au cas où le nombre p est premier, en retraduisant éventuellement certains résultats démontrés dans un cas quelconque - par exemple dans un corollaire du théorème 7. De plus, dans le cas des nombres premiers, il exclut le nombre 0, qu'il n'intègre ni dans les résidus, ni dans les non-résidus : toujours à la lumière des corps finis, certains résultats alors obtenus par Euler peuvent être traduits comme des propriétés d'éléments du corps $\mathbb{F}_p$. Il distingue dans ce corps les résidus et les

non-résidus , parmi ses $p-1$ éléments. Puis il commence à déterminer certaines propriétés de ces résidus, en considérant tout d'abord les puissances successives d'un résidu, qui seront elles aussi des résidus. Ce qu'il montre alors (corollaire du théorème 5) est équivalent à montrer que si deux puissances d'un résidu ont le même résidu, alors elles sont égales dans $\mathbb{F}_p$. Ce qu'il en déduit peut se traduire par le fait [27] que l'ordre d'un résidu dans $\mathbb{F}_p$ est inférieur ou égal à $\frac{p-1}{2}$.

Ensuite, il énonce que si r et rs sont des résidus, alors s est un résidu. On peut rapprocher cela du fait que l'inverse d'un résidu dans $\mathbb{F}_p$ est encore un résidu. Mais Euler démontre seulement que le quotient d'un résidu quadratique par un autre résidu quadratique est encore un résidu quadratique dans le cas où le quotient est un nombre entier. Il détermine alors, par le théorème 8 et ses corollaires, les nombres de carrés et de non carrés dans le corps $\mathbb{F}_p$, qui sont tous les deux égaux à $\frac{p-1}{2}$. On voit ici qu'Euler commence à ramener une infinité de nombres à un seul résidu. C'est ce qui précède la considération de classes de nombres. Ensuite, après avoir rappelé les propriétés multiplicatives des résidus et des non-résidus, il introduit la notion de complément, et commence alors à considérer les restes négatifs de la division par p, qui seront alors tous inférieurs en valeur absolue à $\frac{p}{2}$. Ce travail sur les compléments est ensuite très utile pour obtenir les propriétés des sommes de carrés.

Il distingue les cas où le nombre p est de la forme $4n+1$ ou $4n-1$ et en déduit des conséquences sur les séries des résidus et des non-résidus. Dans un corollaire du théorème 13, il montre que, si un nombre premier est de la forme $4n-1$, alors -1 ne peut pas être résidu, c'est-à-dire que -1 n'est pas un carré dans $\mathbb{F}_p$. Donc, si -1 est résidu, le nombre premier est nécessairement de la forme $4n+1$. À la suite du théorème 16, Euler dit qu'il reste à montrer que, pour tout nombre premier de la forme $4n+1$, les compléments de tous les résidus issus de la division par $4n+1$, sont des résidus. Mais montrer que, si p est premier de la forme $4n+1$, alors le complément de tout résidu est résidu, revient à montrer que -1 est résidu. Or, dans certains ouvrages actuels, une base de la démonstration du théorème des deux carrés d'Euler est justement de montrer que -1 est un carré dans $\mathbb{F}_p$ si et seulement si p est congru à 1 modulo 4, soit si et seulement si p est de la forme $4n+1$. Il est donc intéressant de voir qu'Euler avait bien observé que la démonstration du théorème des deux carrés impliquait que pour tout nombre premier de la forme $4n+1$, les compléments des résidus étaient des résidus, et qu'il voulait démontrer ce résultat de manière directe, en se basant uniquement sur la théorie des résidus.

Ainsi, dans le mémoire [Euler, 1760b], Euler donne une première approche de la théorie des résidus quadratiques et prouve leurs propriétés fondamentales - stabilité par

27. Il montre en effet que si r est un résidu, il existe un nombre inférieur ou égal à $\frac{p-1}{2}$ tel que la division de r par p donne pour reste l'unité.

multiplication et division, nombre de résidus quadratiques, ...- pour obtenir des propriétés participant à la démonstration du théorème des quatre carrés. Pour l'instant, la théorie des résidus quadratiques semble être développée par Euler uniquement dans le but d'obtenir une preuve de l'assertion de Fermat. Il ont donc pour l'instant le statut d'outil de démonstration. Euler reprendra d'ailleurs ces différentes propriétés pour donner sa propre démonstration du théorème des quatre carrés. Néanmoins, il présente parallèlement à partir de 1755 des mémoires consacrés à la théorie des résidus, et aux conséquences obtenues sur les diviseurs de nombres de forme donnée.

III Lagrange et la résolution de problèmes indéterminés du second degré : 1766-1770

Dans cette section, nous résumons le mémoire *Sur les solutions des problèmes indéterminés du second degré*[Lagrange, 1769], dans lequel Lagrange propose une méthode complète de résolution d'équations indéterminées du second degré. Comme l'indique Lagrange, Euler a également proposé des recherches sur ce thème mais présente une méthode qui permet seulement de trouver une infinité de solutions au problème à partir d'une solution donnée. Lagrange, de son côté, démontre l'existence d'une solution particulière et donne une méthode pour en déduire toutes les solutions de l'équation donnée lorsqu'elle en admet. La lecture de ce mémoire permet de connaître les méthodes utilisées par Lagrange en théorie des nombres, et en particulier celles dont il fait usage plus tard dans sa démonstration du théorème des quatre carrés. Ici, nous ne détaillons pas les raisonnements de Lagrange qui ne sont pas en lien avec notre thème, nous indiquons seulement les idées principales [28].

L'objet de ce travail est de résoudre les équations indéterminées de la forme $A + Bt^2 = u^2$, où A et B sont des nombres entiers non carrés. Lagrange précise que ces équations sont fondamentales car toute équation indéterminée du second degré à deux inconnues peut s'y ramener :

> Les recherches que j'ai faites depuis quelque temps sur cette matière m'ont conduit à des méthodes directes, générales et nouvelles, pour résoudre les équations de la forme $A + Bt^2 = u^2$, et en général toutes les équations du second degré à deux inconnues, soit que les inconnues puissent être des nombres quelconques entiers ou fractionnaires, soit qu'elles doivent être des nombres entiers. Ce sont ces méthodes qui font l'objet de ce Mémoire ; je les crois d'autant plus dignes de l'attention des Mathématiciens qu'elles laissent encore un vaste champ à leurs recherches [Lagrange, 1769, p. 379].

28. Pour un exposé plus détaillé sur les méthodes de Lagrange, voir [Buraux-Bourgeois, 1993], [Boucard, 2006] et [Bussotti, 2006].

Il commence par prouver, à l'aide de manipulations algébriques, que toute équation indéterminée du second degré se ramène effectivement à une équation de la forme $A+Bt^2 = u^2$, puis il distingue les deux cas de résolution en nombres rationnels et en nombres entiers.

1 - Résolution de $A = u^2 - Bt^2$ en nombres rationnels

À partir de l'équation, Lagrange obtient, à partir de changements de variables, une équation équivalente $Ar^2 = p^2 - Bq^2$ à résoudre en nombres entiers. Il pose des conditions sur A et B et montre que p et q doivent être premiers entre eux. Il observe ensuite que A doit être le diviseur d'un nombre de la forme $\alpha^2 - B$, avec $\alpha < \frac{|A|}{2}$, pour que l'équation soit résoluble. Cela revient à dire, en termes modernes, que B doit être un résidu quadratique modulo A pour que l'équation soit résoluble. Pour cela, il utilise la stabilité par multiplication des formes du type $p^2 - Bq^2$, et le développement en fraction continue d'une fraction [29] . Finalement il obtient une série d'équations, qu'il nomme *équations secondaires* :

(a)
$$\begin{cases} AA_1 = \alpha^2 - B, \\ A_1A_2 = \alpha_1^2 - B, \\ A_2A_3 = \alpha_2^2 - B, \\ \text{.....}, \end{cases}$$

où les nombres A, A_1, ..., forment une suite strictement décroissante.

En réitérant son procédé, il obtient une série d'*équations principales*, dont la résolution d'une implique la résolution des précédentes :

$$\begin{cases} Ar^2 = p^2 - Bq^2, \\ Br_1^2 = p_1^2 - Cq_1^2, \\ Cr_2^2 = p_2^2 - Dq_2^2, \\ Dr_3^2 = p_3^2 - Eq_3^2, \\ \text{.....}, \end{cases}$$

où A, B, C, ... forment une suite décroissante. On obtient donc nécessairement un terme égal à l'unité pour le coefficient du membre de droite, et on se ramène donc toujours ainsi à la résolution d'une équation du type $Vz^2 = x^2 - y^2$, dont il donne ensuite une méthode de résolution.

Les différentes étapes de cette démonstration d'une quinzaine de pages s'appuient sur plusieurs outils : manipulations algébriques, fractions continues, considérations arithmétiques élémentaires. Cela permet à Lagrange d'appliquer la méthode de descente infinie

29. Voir en annexe, à partir de la page 495.

et de ramener ainsi son problème initial à la résolution d'une équation indéterminée dont la forme est plus simple. Il clôt ce paragraphe par plusieurs exemples d'application, puis reprend la résolution de l'équation $A = u^2 - Bt^2$, mais en nombres entiers cette fois-ci.

2 - Résolution de $A = u^2 - Bt^2$ en nombres entiers

Comme précédemment, il se ramène au cas le plus simple possible : une équation de la forme $A = p^2 - Bq^2$ où p et q sont premiers entre eux. Il pose alors des conditions sur les nombres A et B et montre que l'on peut considérer que A et B sont premiers entre eux. De là, il utilise la même méthode que pour la résolution de l'équation en nombres rationnels : pour que l'équation soit résoluble, il faut trouver deux nombres α et A_1 tels que $AA_1 = \alpha^2 - B$ et tel que A_1 soit de la forme $p_1^2 - Bq_1^2$. On obtient alors une nouvelle équation $A_1 = p_1^2 - Bq_1^2$, où $A_1 < A$.

L'équation initiale $A = p^2 - Bq^2$ est donc résoluble en nombres entiers si la nouvelle équation $A_1 = p_1^2 - Bq_1^2$ est aussi résoluble en nombres entiers, et si les expressions de p et q en fonction de p_1, q_1, α, B, et A, sont des entiers. Il remarque que si on trouve a valeurs de α, on obtient alors le même nombre a d'équations du type $A_1 = p_1^2 - Bq_1^2$ à résoudre.

Il montre comment trouver toutes les valeurs possibles et inférieures à $\frac{|A|}{2}$ pour α à partir d'une seule, et prouve que si A admet n facteurs premiers distincts, alors aucune valeur de α convient, ou il y a 2^{n-1} valeurs possibles de α.

En réitérant le procédé, il obtient une série d'équations secondaires :

$$\begin{cases} AA_1 = \alpha^2 - B, \quad \alpha < \dfrac{A}{2} \\ A_1A_2 = \alpha_1^2 - B, \quad \alpha_1 = \mu_1 A_1 \pm \alpha < \dfrac{A_1}{2} \\ A_2A_3 = \alpha_2^2 - B, \quad \alpha_2 = \mu_2 A_2 \pm \alpha_1 < \dfrac{A_2}{2} \\ \ldots\ldots\ldots\ldots\ldots\ldots, \end{cases}$$

(en considérant les α_i et les A_i comme positifs dans les inégalités). Il obtient ensuite une série d'équations principales, où les A_i forment une suite strictement décroissante :

$$\begin{cases} A = p^2 - Bq^2, \\ A_1 = p_1^2 - Bq_1^2, \\ A_2 = p_2^2 - Bq_2^2, \\ A_3 = p_3^2 - Bq_3^2, \\ \ldots\ldots\ldots\ldots\ldots\ldots \end{cases}$$

On peut alors retrouver les inconnues initiales p et q à l'aide des équations suivantes :

$$\begin{cases} \pm p = p_2 - \mu_1 p_1, \quad \pm q = q_2 - \mu_1 q_1, \\ \pm p_1 = p_3 - \mu_2 p_2, \quad \pm q_1 = q_3 - \mu_2 q_2, \\ \pm p_2 = p_4 - \mu_3 p_3, \quad \pm q_2 = q_4 - \mu_3 q_3, \\ \ldots\ldots\ldots\ldots\ldots, \end{cases}$$

où les signes de p, q, et α doivent être les mêmes, ainsi que ceux des p_i, q_i, et α_i.

On utilise également les formules :

$$\begin{cases} p_{n-1} = \dfrac{\alpha_{n-1} p_n \pm B q_n}{A_n}, \\ q_{n-1} = \dfrac{\alpha_{n-1} q_n \pm B p_n}{A_n}. \end{cases}$$

Ainsi, si on peut résoudre une équation $A_n = p_n^2 - Bq_n^2$, alors $A = p^2 - Bq^2$ est résoluble si et seulement si les nombres p_n, q_n, p_{n-1}, et q_{n-1} sont entiers.

Il distingue alors deux cas selon le signe de B et les méthodes correspondantes pour savoir quand l'équation est résoluble et pour trouver les nombres p_n, q_n, p_{n-1}, et q_{n-1}.

Cette méthode de résolution, exposée sur plus de cinquante pages, s'appuie sur les mêmes outils. Dans chacun des cas, il faut notamment déterminer un nombre α tel que $\alpha^2 - B$ soit divisible par A : autrement dit, il faut que B soit un résidu quadratique modulo A. Il consacre le quatrième paragraphe de ce mémoire à cette question.

3 - Condition pour que $\alpha^2 - B$ soit divisible par A

Nous ne résumons là encore qu'une seule partie de ce paragraphe, contenant des méthodes utilisées par Lagrange dans sa démonstration du théorème des quatre carrés.

Lagrange se ramène au cas où le nombre A est premier et démontre que $\alpha^2 - B$ est divisible par A si seulement si $B^{\frac{A-1}{2}} - 1$ est également divisible par A. En termes de résidus et de congruences, Lagrange montre donc que B est un résidu quadratique modulo A si et seulement si $B^{\frac{A-1}{2}} \equiv 1 \pmod{A}$.

Il prouve dans un premier temps que $\alpha^2 - B$ est divisible par A seulement si $B^{\frac{A-1}{2}} - 1$ l'est aussi.

Il pose alors $m = \frac{A-1}{2}$, $P = \alpha^{2(m-1)} + \alpha^{2(m-2)} B + \alpha^{2(m-3)} B^2 + \ldots + B^{m-1}$ et obtient :

$$(\alpha^2 - B)P = \alpha^{2m} - B^m = \alpha^{A-1} - B^m = \alpha^{A-1} - 1 - (B^m - 1).$$

De là, il remarque d'abord que si $\alpha^2 - B$ est divisible par A, comme B n'est pas divisible par A, alors α n'est pas divisible par A non plus. Il applique donc le petit théorème de Fermat : le nombre $\alpha^{A-1} - 1$ est toujours divisible par A. Il peut donc en déduire que

$B^{\frac{A-1}{2}} - 1$ l'est aussi.

Réciproquement, il montre que si A est un diviseur de $B^{\frac{A-1}{2}} - 1$, alors il existe un nombre α tel que A divise $\alpha^2 - B$.

Pour montrer ce résultat, il utilise à nouveau l'égalité précédente en remarquant que si $B^m - 1$ est divisible par A, alors $(\alpha^2 - B)P$ est également divisible par A. Comme A est un nombre premier, un des deux facteurs est divisible par A, et le problème se réduit à montrer l'existence d'une valeur de α telle que le nombre P ne soit pas divisible par A.

Or, si l'on remplace successivement α par les nombres $1, 2, 3, \ldots, A-2$ dans l'expression de P et que l'on nomme $P_1, P_2, P_3, \ldots, P_{A-2}$ les valeurs correspondantes de P, on a, par la théorie des différences :

$$P_1 - (A-3)P_2 + \frac{(A-3)(A-4)}{2}P_3 - \ldots + P_{A-2} = 1.2.3.4.\ldots(A-3).$$

On peut alors en déduire que, comme A est premier, le second membre de l'égalité n'est pas divisible par A, et donc qu'il existe au moins une des valeurs de α telle que la valeur correspondante P ne soit pas divisible par A. Avec cette valeur de α, le nombre $\alpha^2 - B$ est alors divisible par A.

Il remarque que ces résultats sont dus à Euler et donne pour référence les tomes I et VI des *Nouveaux Commentaires de Pétersbourg*. Le théorème démontré par Lagrange est effectivement ce qu'on appelle actuellement le critère d'Euler. Comme nous l'avons vu précédemment, le théorème 11 de [Euler, 1750] affirme bien : si $a = f^2 \pm (2m+1)$, où le nombre $2m+1$ est premier, alors $a^m - 1$ est divisible par $2m+1$. Les deux mathématiciens formulent donc leur théorème en termes de divisibilité. Néanmoins, Euler en déduit des corollaires où il raisonne sur des résidus. Dans le corollaire 4 par exemple, il indique que pour trouver tous les nombres a tels que $a^m - 1$ est divisible par le nombre premier $2m+1$, il suffit de considérer tous les résidus de carrés après division par $2m+1$. De même, il développe ensuite des exemples, où il détermine explicitement des restes de carrés.

4 - Quelques méthodes de Lagrange

Bien que ces rapides résumés ne permettent pas d'avoir une vision réelle de tous les calculs effectués par Lagrange pour démontrer la validité de sa méthode de résolution des équations du second degré, nous avons ici mis en avant les principaux outils, de natures différentes, que Lagrange utilise par la suite pour sa démonstration du théorème des quatre carrés : des manipulations algébriques sur des égalités, utilisation du petit théorème de Fermat, différences finies et méthode de descente infinie, ... mais pas de raisonnement sur ce qu'Euler nomme les résidus. Lagrange exprime tous les résultats concernés en termes de divisibilité. Remarquons enfin que Lagrange et Euler emploient tous deux la méthode de descente infinie, mais de façon différente : nous avons vu jusque là qu' Euler l'applique dans le cadre de raisonnement par l'absurde tandis que Lagrange l'utilise, par

exemple, pour obtenir une équation plus simple qu'il peut résoudre et qui lui permet d'en déduire la résolution de toutes les équations obtenues précédemment [30]. Nous allons voir dans la section suivante comment nos deux mathématiciens usent de leurs propres méthodes, et intègrent, ou au contraire évitent, les démarches de l'autre, pour obtenir une démonstration complète du théorème des quatre carrés.

IV Euler, Lagrange et le théorème des quatre carrés : 1770-1773

Dans cette section, nous étudions la démonstration donnée par Lagrange et les deux démonstrations d'Euler pour le théorème des quatre carrés. Les deux mathématiciens utilisent les travaux commentés précédemment afin d'obtenir chacun une démonstration complète. La preuve proposée par Lagrange est insérée dans les *Nouveaux Mémoires* de l'Académie de Berlin pour l'année 1770, publiés en 1772. Euler soumet alors sa proposition de démonstration une première fois le 21 septembre 1772 à l'Académie de Saint-Pétersbourg.

1 - La première démonstration du théorème des quatre carrés par Lagrange (1770)

(a) Euler, comme référence de Lagrange

Lagrange introduit son mémoire avec un historique du problème, en insistant en particulier sur l'importance des travaux d'Euler :

> À l'égard de M. Euler, si son travail sur ce sujet n'a pas eu tout le succès qu'on pourrait désirer, on lui a du moins l'obligation d'avoir ouvert la route qu'il faut suivre dans ces sortes de recherches. On peut voir dans le tome V des *Nouveaux Commentaires de Pétersbourg* le résultat des tentatives ingénieuses que ce grand Géomètre a faites pour parvenir à démontrer le Théorème de M. Bachet [Lagrange, 1772, p. 190].

Lagrange, même s'il suit la même trame de démonstration, propose presque systématiquement des démonstrations différentes de celles d'Euler pour les résultats intermédiaires, dont les énoncés sont aussi parfois plus généraux.

Il rappelle les propositions prouvées par Euler dans ses publications :

– le produit de deux nombres qui sont la somme de quatre carrés est une somme de quatre carrés ;

30. Sur l'utilisation de la méthode de descente infinie par ces deux mathématiciens, voir [Bussotti, 2006].

– pour tout nombre premier p, il existe deux ou trois carrés, premiers avec p, tels que leur somme soit divisible par p et tel que le quotient de cette somme par p soit plus petit que p.

Puis il conclut :

> De là, M. Euler conclut, avec raison, que le Théorème en question serait démontré pour tous les nombres premiers si l'on pouvait seulement démontrer cette autre proposition, savoir, que lorsque le produit de deux nombres est la somme de quatre ou d'un nombre moindre de carrés, et que l'un des nombres produisants est pareillement la somme de quatre ou d'un nombre moindre de carrés, l'autre produisant le sera de même [Lagrange, 1772, p. 190].

Selon Lagrange, un raisonnement par l'absurde suffit [31], mais il n'en dit pas plus et propose de démontrer plus généralement que « tout nombre premier qui est diviseur d'un nombre quelconque composé de quatre ou d'un nombre moindre de carrés, sans l'être de chacun des carrés en particulier, est nécessairement aussi composé de quatre ou d'un nombre moindre de carrés » [Lagrange, 1772, p. 191].

Sa démonstration est composée d'un lemme démontré par Euler, et de deux théorèmes suivis de corollaires.

(b) Préliminaires sur les sommes de deux carrés

Lemme

Les nombres qui sont la somme de deux carrés premiers entre eux n'admettent d'autres diviseurs que ceux qui sont pareillement la somme de deux carrés.

Il ne revient pas sur la démonstration de cette proposition qui a été démontrée, comme nous l'avons vu, par Euler dans [Euler, 1758].

Lagrange continue ensuite en énonçant deux corollaires, que l'on ne retrouve pas chez Euler, et qui sont fondamentaux pour la démonstration du théorème des quatre carrés exposée plus loin. Ces deux résultats sont proches de ceux obtenus par Euler, mais mettent en jeu des sommes de deux carrés qui ne sont pas nécessairement premiers entre eux.

Corollaire I. - *Si deux nombres égaux chacun à la somme de deux carrés, tels que* p^2+q^2 *et* r^2+s^2 *sont divisibles par un même nombre* ρ*, et que les quatre carrés* p^2*,* q^2*,* r^2*,* s^2 *n'aient aucun diviseur commun, je dis que les deux quotients* $\dfrac{p^2+q^2}{\rho}$ *et* $\dfrac{r^2+s^2}{\rho}$ *seront*

31. Si on suppose que tout nombre premier ne s'exprime pas comme la somme de quatre carrés entiers, on peut considérer le plus petit nombre premier p qui ne s'exprime pas comme somme de quatre carrés.

Alors, il existe a, b, c entiers, premiers et strictement inférieurs à $\dfrac{p}{2}$ tels que : $N = a^2+b^2+c^2 = np$ où $n < p$.

Or $n = \dfrac{N}{p} < p$ donc les facteurs premiers de n sont strictement plus petits que p et sont donc somme de quatre carrés. On en déduit donc que n est somme de quatre carrés, et donc que p aussi, si on arrive à démontrer le résultat manquant à Euler.

aussi chacun égaux à la somme de deux carrés.

Cette démonstration se base sur le lemme précédent bien sûr, et sur des considérations de divisibilité et de PGCD.

Dans un premier temps, il introduit m et n, les PGCD respectifs de p, q, et de r, s ; il pose ainsi : $p = mp'$, $q = mq'$, $r = nr'$, $s = ns'$ et il peut donc appliquer le lemme précédent sur les sommes $p'^2 + q'^2$ et $r'^2 + s'^2$. De plus, m et n sont nécessairement premiers entre eux puisque p, q, r et s n'admettent pas de diviseur commun. Comme ρ divise $m^2(p'^2 + q'^2)$ et $n^2(r'^2 + s'^2)$, il pose $\mu = PGCD(m^2, \rho)$ et obtient $\rho = \mu\rho'$. Le nombre ρ' est donc premier à $\frac{m^2}{\mu}$ et divise donc $p'^2 + q'^2$, d'où :

$$\frac{p^2 + q^2}{\rho} = \frac{m^2}{\mu}\left(\frac{p'^2 + q'^2}{\rho'}\right).$$

Grâce au lemme, ρ' et $\dfrac{p'^2 + q'^2}{\rho'}$ sont sommes de deux carrés. On peut donc poser $\dfrac{p'^2 + q'^2}{\rho'} = \alpha^2 + \beta^2$.

Il considère alors le plus grand facteur carré de μ, noté ν, et pose $\mu = \nu^2\mu'$. Donc m^2 n'est divisible par μ que si m est divisible par $\nu\mu'$, d'où $m = K\nu\mu'$. On a donc :

$$\frac{m^2}{\mu} = K^2\mu'.$$

La deuxième somme de deux carrés : $n^2(r'^2 + s'^2)$ est également divisible par ρ, et donc par μ. Comme μ divise m^2, μ, et μ', divisent $(r'^2 + s'^2)$. Or, r' et s' sont premiers entre eux, donc μ' est une somme de deux carrés d'après le lemme précédent, soit : $\mu' = \gamma^2 + \delta^2$ et :

$$\frac{m^2}{\mu} = K^2(\gamma^2 + \delta^2).$$

Finalement : $\dfrac{p^2 + q^2}{\rho} = K^2(\gamma^2 + \delta^2)(\alpha^2 + \beta^2) = K^2(\gamma\alpha + \delta\beta)^2 + K^2(\gamma\beta - \delta\alpha)^2$, d'où le résultat.

Il réitère le raisonnement pour montrer que $\dfrac{r^2 + s^2}{\rho}$ est aussi une somme de deux carrés.

Corollaire II. - *Si la somme de deux carrés est divisible par une autre somme de deux carrés, le quotient sera toujours égal à la somme de deux carrés.*

Il utilise le corollaire précédent en se ramenant au cas où les quatre carrés sont premiers entre eux. En effet, si les sommes de carrés considérées sont $a^2 + b^2$ et $c^2 + d^2$, on note

l le PGCD des nombres a, b, c, d et on a : $a = lp$, $b = lq$, $c = lr$, et $d = ls$. On obtient alors : $\dfrac{a^2+b^2}{c^2+d^2} = \dfrac{p^2+q^2}{r^2+s^2}$. Il pose donc $r^2 + s^2 = \rho$. Il ne le précise pas mais, pour utiliser le corollaire précédent, il faut deux sommes de deux carrés divisibles par ρ. Il suffit de considérer $p^2 + q^2$ et $r^2 + s^2$.

Ce résultat est proche de la proposition I du mémoire [Euler, 1758] d'Euler ; le diviseur n'est néanmoins pas supposé premier.

(c) Où l'on montre que si un nombre premier divise une somme de quatre carrés, il est lui-même somme de quatre carrés

Ici, on voit que Lagrange suit le même chemin qu'Euler : il démontre d'abord qu'un nombre divisible par une somme de quatre carrés est lui-même une somme de quatre carrés. Dans l'étape suivante de sa preuve, il montrera que tout nombre premier divise une somme de trois carrés.

Théorème I

Si la somme de quatre carrés est divisible par un nombre premier plus grand que la racine carrée de la même somme, ce nombre sera nécessairement égal à la somme de quatre carrés.

Nous détaillons ce passage car certains raisonnements ultérieurs développés par Euler dans son mémoire sur le théorème des quatre carrés s'en rapprochent.

Il démontre dans un premier temps que l'on peut supposer que les nombres composant la somme de quatre carrés, notés p, q, r et s, sont premiers entre eux[32] .

Il considère l'équation $Aa = p^2 + q^2 + r^2 + s^2$.

Si le nombre $p^2 + q^2$ n'est pas premier à a, soit ρ leur PGCD tel que : $a = b\rho$ et $p^2 + q^2 = t\rho$; b et t sont donc premiers entre eux.

On a alors :

$$Ab\rho = t\rho + r^2 + s^2.$$

Donc $r^2 + s^2$ est divisible par ρ et en nommant leur quotient u, on obtient :

$$Ab = t + u.$$

Or ρ divise p^2+q^2 et r^2+s^2. De plus, p, q, r et s sont premiers entre eux. On en déduit

32. Il pose $Aa = p^2 + q^2 + r^2 + s^2$ où A est un nombre premier tel que $A > \sqrt{p^2 + q^2 + r^2 + s^2}$ et donc $a < \sqrt{p^2 + q^2 + r^2 + s^2}$. Si p, q, r et s ont pour PGCD d, la somme des quatre carrés sera divisible par d^2 et Aa sera donc également divisible par d^2. Or $d^2 < Aa$ donc $d < \sqrt{Aa} < A$. Donc A et d seront premiers entre eux. On en déduit donc que si Aa est divisible par d^2, c'est a qui est divisible par d^2. On peut donc se ramener au cas où p, q, r et s sont premiers entre eux.

donc, d'après le corollaire I, que $t = \dfrac{p^2+q^2}{\rho}$ et $u = \dfrac{r^2+s^2}{\rho}$ sont des sommes de deux carrés : $t = m^2+n^2$ et $u = h^2+l^2$. Le produit est également une somme de deux carrés ; on peut donc poser $tu = x^2+y^2$.

En multipliant par t, on obtient $Abt = t^2+x^2+y^2$.

Comme b et t sont premiers entre eux, on peut trouver des nombres v et w tels que $vb \pm wt$ soit égal à un nombre donné v plus petit [33] que $\frac{b}{2}$: $x = \alpha t + \gamma b$ et $y = \beta t + \delta b$, où α, β, γ, δ sont des entiers relatifs et on peut supposer que α et β, pris positivement, sont inférieurs à $\dfrac{b}{2}$.

On a alors : $Abt = t^2(1+\alpha^2+\beta^2) + 2\alpha\gamma tb + 2\beta\delta tb + \gamma^2b^2 + \delta^2b^2$.

On en déduit donc que $t^2(1+\alpha^2+\beta^2)$ doit être divisible par b. Or b et t sont premiers entre eux donc b divise $(1+\alpha^2+\beta^2)$.

Il pose : $a'b = 1+\alpha^2+\beta^2 < \dfrac{b^2}{2}+1$ donc $a' < \dfrac{b}{2}+\dfrac{1}{b}$.

Donc : $At = a't^2 + 2\alpha\gamma t + 2\beta\delta t + (\gamma^2+\delta^2)b$.

On en déduit que $(\gamma^2+\delta^2)b$ est divisible par t et donc que $\gamma^2+\delta^2$ est divisible par t, puisque b et t sont premiers entre eux.

On multiplie maintenant l'équation par a' :

$$Aa't = (a't+\alpha\gamma+\beta\delta)^2 + \gamma^2(a'b-\alpha^2) + \delta^2(a'b-\beta^2) - 2\alpha\beta\gamma\delta.$$

Or $a'b = 1+\alpha^2+\beta^2$ donc :

$$Aa't = (a't+\alpha\gamma+\beta\delta)^2 + (\beta\gamma-\alpha\delta)^2 + \gamma^2 + \delta^2.$$

Or $\gamma^2+\delta^2$ est divisible par t donc $(a't+\alpha\gamma+\beta\delta)^2 + (\beta\gamma-\alpha\delta)^2$ est divisible par t. t est une somme de deux carrés donc, d'après le corollaire II : $\gamma^2+\delta^2 = t(p'^2+q'^2)$ et $(a't+\alpha\gamma+\beta\delta)^2 + (\beta\gamma-\alpha)^2 = t(r'^2+s'^2)$.

On en déduit : $Aa' = p'^2+q'^2+s'^2+r'^2$, où $a' < \dfrac{b}{2}+\dfrac{1}{b}$, soit $a' < a$.

De là, il utilise la méthode de descente infinie :

> Il s'ensuit de là que si Aa est la somme de quatre carrés, Aa' sera aussi la somme

33. Lagrange démontre ce résultat dans [Lagrange, 1770, p. 659] . Dans sa démonstration, il dit que l'on peut choisir les multiples tels que l'un soit plus petit que $\frac{bt}{2}$. Cela doit être une erreur car dans son théorème, le multiple est inférieur à $\frac{b}{2}$ et, dans la suite de la démonstration, il suppose que α et β sont inférieurs à $\frac{b}{2}$. Dans [Lagrange, 1770], il démontre ce théorème en considérant les restes des divisions euclidiennes de $x-\gamma b$ par t ... Remarquon que l'on retrouve ici le même genre de démonstration que celle du mémoire d'Euler dans lequel celui-ci prouve l'actuel théorème de Bézout.

de quatre carrés, a' étant plus petit que $\frac{b}{2} + \frac{1}{b}$ et $a = b\rho$; ainsi, si a est plus grand que 1, a' sera nécessairement plus petit que a ; et si a' est encore plus grand que 1, on prouvera de la même manière que Aa'' sera aussi la somme de quatre carrés, a'' étant plus petit que a' ; et ainsi de suite ; donc comme les nombres a, a', a'' sont des nombres entiers, dont aucun ne peut être égal à zéro (à cause que ces nombres sont des diviseurs des nombres $1 + \alpha^2 + \beta^2$, $1 + \alpha'^2 + \beta'^2$,... qui, comme on voit, ne peuvent jamais devenir nuls), et que ces nombres vont en diminuant, il est clair qu'on parviendra nécessairement à un de ces nombres qui sera égal à l'unité, et alors on aura A égal à la somme de quatre carrés entiers [Lagrange, 1772, p. 197].

Lagrange utilise, comme pour résoudre certains problèmes indéterminés, la méthode de descente infinie afin de démontrer l'existence d'un objet, à partir de l'égalité $Aa' = p'^2 + q'^2 + s'^2 + r'^2$, où $a' < a$. Afin d'obtenir celle-ci, il a notamment appliqué une variante de l'actuel théorème de Bézout, permettant d'obtenir des nombres de plus en plus petits. Euler, dans ses travaux sur les sommes de deux carrés, utilise également une variante de la division euclidienne en considérant les restes négatifs pour réduire la valeur absolue des restes.

Ainsi, Euler et Lagrange utilisent tous deux la méthode de descente infinie pour obtenir des résultats sur les sommes de carrés. Néanmoins, pour les mémoires analysés ici, Euler utilise cette méthode dans le cadre de raisonnements par l'absurde, tandis que, là encore, Lagrange l'applique pour démontrer l'existence d'une expression de la forme voulue. Comme nous le verrons plus loin, Euler reprend cette utilisation de la méthode de descente infinie pour achever sa démonstration du théorème des quatre carrés.

À partir du théorème précédent, Lagrange obtient un résultat plus général :

Corollaire. - *Si un nombre premier quelconque est un diviseur de la somme de quatre carrés qui n'aient point de commun diviseur, ce nombre sera aussi la somme de quatre carrés.*

Il observe d'abord que si A est le nombre premier donné et si la somme de quatre carrés $p^2 + q^2 + r^2 + s^2$ est divisible par A, si chacune des racines p, q, r et s est inférieure à $\frac{A}{2}$, alors $p^2 + q^2 + r^2 + s^2$ sera inférieur à A^2 et on conclut avec le théorème précédent.

De plus, on peut toujours réduire les nombres p, q, r et s « à être moindres que $\frac{A}{2}$ » car si $p > \frac{A}{2}$, et si $p^2 + q^2 + r^2 + s^2$ est divisible par A, alors $(p - mA)^2 + q^2 + r^2 + s^2$ est aussi divisible par A pour tout entier m et on peut toujours trouver un m tel que $|p - mA| < \frac{A}{2}$.

Enfin, il remarque qu'au plus deux des nombres p, q, r et s sont divisibles par A

(puisqu'ils sont premiers entre eux) et que $p^2+q^2+r^2+s^2$ ne peut être nul.

Lorsque Lagrange dit que $p^2+q^2+r^2+s^2$ est divisible par A implique que $(p-mA)^2+q^2+r^2+s^2$ est également divisible par A, l'utilisation du nombre $p-mA$ revient à effectuer la division euclidienne de p par A et à dire que p et $p-mA$ ont les mêmes restes après division par A. Ainsi, cela s'approche des raisonnements exposés par Euler dans ses mémoires sur le même thème. On remarque néanmoins que Lagrange n'emploie pas le même vocabulaire.

La démonstration du théorème des quatre carrés s'achève par une dernière étape : montrer que, pour tout nombre premier, il existe une somme de quatre carrés ou moins divisible par le nombre premier en question ; c'est l'objet du dernier théorème que Lagrange énonce dans son mémoire.

(d) Fin de la démonstration du théorème des quatre carrés avec les différences finies

Ce dernier théorème permet d'obtenir un premier corollaire qui ressemble au théorème 18 du mémoire [Euler, 1760b], mais aucune condition n'est imposée sur les carrés : ils peuvent être divisibles par le nombre premier en question.

Théorème II

Si A est un nombre premier et que B et C sont des nombres quelconques positifs ou négatifs non divisibles par A, je dis qu'on pourra toujours trouver deux nombres p et q tels que le nombre $p^2 - Bq^2 - C$ soit divisible par A.

Si on peut trouver q tel que Bq^2+C soit divisible par A, on peut prendre $p=0$ ou p divisible par A.

On suppose qu'il n'existe pas de q tel que Bq^2+C soit divisible par A. Lagrange reprend ici la méthode employée précédemment dans ses travaux sur les problèmes indéterminés du second degré. Il pose $Bq^2+C=b$ et :

$$P = p^{A-3} + bp^{A-5} + b^2p^{A-7} + \ldots + b^{\frac{A-3}{2}}.$$

On a :

$$(p^2 - Bq^2 - C)P = p^{A-1} + b^{\frac{A-1}{2}} = p^{A-1} - 1 - (b^{\frac{A-1}{2}} - 1).$$

Lagrange multiplie par $Q = b^{\frac{A-1}{2}} + 1$:

$$(p^2 - Bq^2 - C)PQ = Q(p^{A-1} - 1) - (b^{A-1} - 1).$$

Les nombres p et b ne sont pas divisibles par A donc, d'après le petit théorème de

Fermat : $p^{A-1} - 1$ et $b^{A-1} - 1$ sont divisibles par A. Dans ce cas, on peut donc en déduire que $(p^2 - Bq^2 - C)PQ$ est divisible par A.

On doit donc montrer que l'on peut toujours trouver p et q tels que p, P et Q ne sont pas divisibles par A.

Il montre d'abord que, pour tout q, on peut trouver $p < A$ (et p n'est donc pas divisible par A) tel que P ne soit pas divisible par A. Pour cela, il utilise la théorie des différences finies rencontrée dans un de ses précédents mémoires. Il nomme P', P'', P''', ..., $P^{(A-2)}$ les valeurs de P où l'on a respectivement remplacé p par 1, 2, 3, ..., $A - 2$ et obtient :

$$P' - (A-3)P'' + \frac{(A-3)(A-4)}{2}P''' - \ldots + P^{(A-2)} = (A-3)\ldots 3.2.1.$$

Il conclut alors que si tous les nombres P', P'',..., sont divisibles par A, le nombre $(A-3)\ldots 3.2.1$ doit également être divisible par A, ce qui est impossible puisque A est premier. Donc on peut trouver un nombre p tel que P ne soit pas divisible par A. De plus, le nombre p est inférieur à A : il est donc aussi non divisible par A.

Il reste enfin à montrer qu'on peut prendre q tel que $Q = (Bq^2 + C)^{\frac{A-1}{2}} + 1$ ne soit pas divisible par A. Il pose $m = \dfrac{A-1}{2}$ et on a :

$$Q = B^m q^{(A-1)} + mB^{m-1}q^{A-3}C + \frac{m(m-1)}{2}B^{m-2}q^{A-5}C^2 + \ldots mBq^2C^{m-1} + C^m + 1.$$

Si $C^m + 1$ n'est pas divisible par A, il suffit de prendre q divisible par A.

Si $C^m + 1$ est divisible par A, il faut que q ne le soit pas et que la quantité $B^m q^{A-3} + mB^{m-1}q^{A-5}C + \dfrac{m(m-1)}{2}B^{m-2}q^{A-7}C^2 + \ldots mBC^{m-1}$ ne le soit pas non plus. Il utilise alors une nouvelle fois la théorie des différences finies pour conclure.

Corollaire I. - Si l'on fait $B = -1$ et $C = -1$, on aura le nombre $p^2 + q^2 + 1$ qui sera divisible par A ; d'où il suit qu'*étant donné un nombre premier quelconque on peut toujours trouver un nombre égal à la somme de trois carrés entiers dont l'un soit même l'unité, lequel soit divisible par le nombre premier.*

Corollaire II. - *Tout nombre premier est nécessairement égal à la somme de quatre ou d'un moindre nombre de carrés entiers.* D'où il est aisé de conclure que *tout nombre entier est aussi égal à la somme de quatre ou d'un moindre nombre de carrés entiers.*

À la lecture de la démonstration proposée par Lagrange, on peut se demander quelle

est l'origine de ces suites d'identités algébriques et des expressions introduites, comme la formule de P par exemple. On a déjà un élément de réponse en lisant son mémoire [Lagrange, 1769] dans lequel il utilise également la théorie des différences finies en théorie des nombres. Il s'en sert alors pour montrer que si a est un diviseur de $b^{\frac{a-1}{2}}-1$, il existe un nombre α tel que a divise α^2-b, où a est un nombre premier. Ici, on est exactement dans le même cas, avec $b=Bq^2+C$ et b non divisible par A, ce qui permet de montrer que $b^{\frac{a-1}{2}}-1$ est divisible par A. Les deux démonstrations sont ensuite très semblables. De plus, Lagrange se réfère très régulièrement aux travaux d'Euler. Nous avons déjà remarqué que la démonstration de Lagrange suit le même canevas que certaines preuves données par Euler sur les sommes de carrés. Ce dernier utilise également la théorie des différences finies dans certains de ses travaux d'arithmétiques : par exemple, il applique cette méthode dans [Euler, 1761b], publié en 1761 pour montrer que si a^m-1 est divisible par le nombre premier $p=mn+1$, alors on peut toujours trouver des nombres x et y, tels que ax^n-y^n soit divisible par le nombre p. Il suffit de prendre $n=2$ pour obtenir : si $a^{\frac{p-1}{2}}$ est divisible par $p=2m+1$, alors on peut toujours trouver x et y tels que ax^2-y^2 soit divisible par p, ce qui est bien sûr très semblable au résultat démontré par Lagrange.

Ainsi, pour replacer au moins en partie ce mémoire dans son contexte de production, il est en particulier fructueux de l'insérer dans l'ensemble de textes publiés par Euler sur les sommes de carrés et par l'auteur lui-même : cela permet de commencer à visualiser d'où viennent les différents points clés de la preuve de Lagrange. Ici, Lagrange s'approprie donc certaines pratiques d'Euler tout en donnant de nouvelles preuves pour tous les résultats démontrés par ce dernier à partir de la théorie des résidus. Nous avons d'ailleurs remarqué à plusieurs reprises que Lagrange ne considère que très peu de restes de divisions dans les travaux étudiés ici.

2 - Une nouvelle démonstration du théorème : la réponse d'Euler à Lagrange

Dans son mémoire [Euler, 1780] publié en 1780 mais soumis à l'Académie dès 1772, Euler annonce avec joie qu'il a finalement réussi à produire une démonstration complète du théorème des quatre carrés, bien différente de celle de Lagrange et moins laborieuse[34]. Avant d'exposer son travail, Euler rappelle brièvement des étapes de la démonstration de Lagrange, et insiste sur son objectif : éclaircir les passages trop longs de la démonstration de Lagrange et donc en proposer une nouvelle, qui sera, selon lui, plus claire et concise.

(a) Amélioration de la démonstration pour le théorème des deux carrés

Il revient dans un premier temps sur les sommes de deux carrés pour proposer une nouvelle preuve du théorème des deux carrés.

34. Voir [Euler, 1780, p. 193].

Dans un premier lemme, il énonce que le produit de deux sommes de deux carrés est également une somme de deux carrés : en effet, si on a le produit $(aa+bb)(\alpha\alpha+\beta\beta)$, il suffit de poser $A=a\alpha+b\beta$ et $B=a\beta-b\alpha$ pour avoir : $(aa+bb)(\alpha\alpha+\beta\beta)=AA+BB$.

Euler donne ensuite un premier théorème, qui est en fait la proposition 4 de [Euler, 1758], qu'il démontre de manière plus directe.

Théorème 1

Si le nombre N divise une somme de deux carrés P^2+Q^2 premiers entre eux, alors ce nombre N est lui-même somme de deux carrés.

Il développe un raisonnement utilisé à plusieurs reprises qui lui permet ensuite d'appliquer la méthode de descente infinie : aussi grands que puissent être P et Q, on peut toujours former une autre somme de deux carrés $pp+qq$ telle que les racines p et q ne dépassent pas la moitié du nombre proposé N. En effet, si on pose $P=fN\pm p$ et $Q=gN\pm q$, on peut prendre p et q tels qu'ils ne dépassent pas $\frac{1}{2}N$. Alors on a

$$PP+QQ=NN(ff+gg)+2N(\pm fp\pm gq)+pp+qq,$$

et, puisque par hypothèse, la somme $PP+QQ$ est divisible par N, alors la somme $pp+qq$ est également divisible par N, tout en étant inférieure à $\frac{N}{2}$. Pour cela, Euler a utilisé des divisions euclidiennes en considérant des restes positifs ou négatifs dont la valeur absolue est inférieure à $\frac{N}{2}$.

I. On note n, le quotient de $pp+qq$ par N : $Nn=pp+qq$. D'après ce qui précède, n est inférieur à $\frac{N}{2}$.

II. On peut exprimer les nombres p et q en fonction du nombre n, toujours en utilisant des divisions euclidiennes dont les restes peuvent être positifs ou négatifs : $p=a+\alpha n$ et $q=b+\beta n$, où a et b sont inférieurs à $\frac{1}{2}n$. Ainsi :

$$Nn=aa+bb+2n(a\alpha+b\beta)+nn(\alpha\alpha+\beta\beta),$$

et, en posant $a\alpha+b\beta=A$:

$$Nn=aa+bb+2nA+nn(\alpha\alpha+\beta\beta).$$

III. Par conséquent, l'expression du premier membre $aa+bb$ est nécessairement divisible par n et on peut donc poser : $aa+bb=nn'$. Puisque $a<\frac{1}{2}n$ et $b<\frac{1}{2}n$, , $nn'<\frac{1}{2}nn$ d'où $n'<\frac{1}{2}n$.

Finalement, en divisant par n, on obtient : $N=n'+2A+n(\alpha\alpha+\beta\beta)$.

IV. On multiplie cette égalité par n'. Comme $nn'=aa+bb$ et d'après stabilité de la

multiplication des sommes de deux carrés, on a : $nn'(\alpha\alpha + \beta\beta) = (aa + bb)(\alpha\alpha + \beta\beta) = AA + BB$.

On a ainsi $Nn' = n'n' + 2n'A + AA + BB = (n' + A)^2 + B^2$.

V. Finalement, à partir du produit initial Nn, qui est somme de deux carrés, on obtient un nouveau produit Nn', également somme de deux carrés, et tel que $n' < \frac{1}{2}n$, ce qui est fondamental pour apliquer la méthode de descente infinie : on peut continuer à former des produits de plus en plus petits qui sont sommes de deux carrés, à savoir Nn'', Nn''', etc., avec $n'' < \frac{1}{2}n'$, $n''' < \frac{1}{2}n''$, etc. Il est donc nécessaire d'arriver au produit $N.1$. On en conclut que le nombre N est bien somme de deux carrés.

Contrairement à la démonstration exposée par Euler dans [Euler, 1758], celle-ci ne se base pas sur des outils tels les différences finies : seules des manipulations algébriques et des divisions euclidiennes entrent en jeu pour obtenir ce qui permet d'appliquer la méthode de descente infinie. Euler utilise d'ailleurs cette méthode comme Lagrange précédemment, et non pas dans le cadre d'un raisonnement par l'absurde. De plus, lorsqu'il arrive à l'égalité $Nn = aa+bb+2nA+nn(\alpha\alpha+\beta\beta)$, il utilise un raisonnement semblable à celui de Lagrange : il en déduit que $aa + bb$ est divisible par n, pose $aa + bb = nn'$, divise l'égalité par n puis la multiplie par n', ce qui lui permet d'amorcer la descente. Néanmoins, par rapport à Lagrange, Euler ne se sert pas uniquement du fait que le produit de deux sommes de deux carrés est une somme de deux carrés : il utilise également les expressions A et B introduites dans la preuve de ce lemme, ce qui simplifie beaucoup les calculs par rapport au type de démonstration de Lagrange.

(b) Une démonstration plus claire et plus concise du théorème des quatre carrés

Sa démonstration, comme il le précise lui-même, est la version étendue à la somme de quatre carrés de la démonstration du théorème précédent. Avant d'énoncer le théorème 4, Euler utilise le même schéma de démonstration pour obtenir des équivalents du théorème 1 pour les nombres de la forme $pp + 2qq$ et $pp + 3qq$. Il obtient ainsi une architecture de démonstration applicable à plusieurs problèmes sur les sommes de carrés.

Pour les sommes de quatre carrés, il énonce d'abord son résultat sur le produit de deux sommes de quatre carrés :

Lemme 4

Le produit de deux nombres, qui sont tous deux des sommes de quatre carrés, peut toujours être également exprimé comme somme de quatre carrés.

Si on considère le produit $(aa + bb + cc + dd)(\alpha\alpha + \beta\beta + \gamma\gamma + \delta\delta)$, il "suffit" de poser :

$$A = a\alpha + b\beta + c\gamma + d\delta,$$

$$B = a\beta - b\alpha - c\delta + d\gamma,$$
$$C = a\gamma + b\delta - c\alpha - d\beta,$$
$$D = a\delta - b\gamma + c\beta - d\alpha,$$

pour avoir :

$$A^2 + B^2 + C^2 + D^2 = (aa + bb + cc + dd)(\alpha\alpha + \beta\beta + \gamma\gamma + \delta\delta).$$

Il prouve ensuite le théorème qui lui manquait en 1751.

Théorème 4

Si N est un diviseur d'une forme $pp+qq+rr+ss$, tel que chaque carré n'est pas divisible par N, alors N est aussi une somme de quatre carrés.

On remarque que l'on peut diminuer suffisamment les racines p, q, r, s pour qu'elles soient plus petites que la moitié de N ; la démonstration se fait alors de la manière suivante.

I. On note n le résultant de cette division : $Nn = pp + qq + rr + ss$, où $p = a + n\alpha$, $q = b + n\beta$, $r = c + n\gamma$, $s = d + n\delta$, où a, b c, d, inférieurs à $\frac{1}{2}n$, peuvent être négatifs. Donc $aa + bb + cc + dd < nn$.

II. On peut substituer ces valeurs dans l'égalité précédente :

$$Nn = aa + bb + cc + dd + 2n(a\alpha + b\beta + c\gamma + d\delta) + nn(\alpha\alpha + \beta\beta + \gamma\gamma + \delta\delta),$$

et, en utilisant la formule obtenue pour A dans la preuve du Lemme 4, on a :

$$Nn = aa + bb + cc + dd + 2nA + nn(\alpha\alpha + \beta\beta + \gamma\gamma + \delta\delta).$$

On voit que le membre $aa+bb+cc+dd$ doit être divisible par n donc : $aa+bb+cc+dd = nn'$, où $n' < n$ (puisque $aa + bb + cc + dd < nn$).

On divise par n :

$$N = n' + 2A + n(\alpha\alpha + \beta\beta + \gamma\gamma + \delta\delta).$$

III. On multiplie maintenant par n', et comme $nn' = aa + bb + cc + dd$, nous avons, avec le lemme 4 : $Nn' = n'n' + 2n'A + A^2 + B^2 + C^2 + D^2$, qui se réduit à une somme de quatre carrés :

$$Nn' = (n' + A)^2 + B^2 + C^2 + D^2.$$

IV. Dans la mesure où $n' < n$, on peut comme précédemment former une suite décroissante Nn'', Nn''',etc., où n, n', n'', ..., est une suite décroissante de nombres entiers positifs,

et donc parvenir finalement à la forme $N.1$: N est également une somme de quatre carrés.

Euler fait suivre cette démonstration de deux corollaires sur des cas particuliers, avant de reprendre la démonstration du théorème des quatre carrés, laissée inachevée dans [Euler, 1760b].

(c) Reprise de la démonstration du théorème 18 de [Euler, 1760b]

D'après le théorème 18, démontré dans [Euler, 1760b] : pour tout nombre premier p, on peut trouver une somme de trois carrés divisible par p, telle que chaque carré ne soit pas divisible par p. Ainsi, la démonstration du théorème des quatre carrés est terminée. Néanmoins, Euler propose ici une démonstration, qui s'appuie toujours sur la théorie des résidus, d'une version légèrement différente du théorème 18.

Théorème 5

Pour tout nombre premier N, on peut trouver non seulement quatre carrés, mais encore trois carrés, d'une infinité de manière[35]*, tels que leur somme soit divisible par N sans qu'aucun d'eux ne le soit.*

Euler rappelle dans un premier temps ses précédents résultats sur les résidus, en introduisant des appellations nouvelles : les résidus sont maintenant les « formas primae classis » (formes de première classe), et les non-résidus, les formes de seconde classe. Les premiers sont notés a, b, c, ..., et les seconds, α, β, γ, ... Il rappelle les propriétés du produit de deux formes de première classe, d'une forme de première classe avec une forme de seconde classe, et de deux formes de seconde classe. Puis il commence sa démonstration proprement dite : il reprend le même raisonnement par l'absurde qu'en 1751 pour conclure que si N ne divise aucune somme de trois carrés, alors cela implique que, si f est une forme de première classe, alors tous les nombres -1, $-f-1$, $-f-2$, etc., sont des formes de deuxième classe, ce qui est impossible. Le théorème 18 est ainsi prouvé, et la démonstration du théorème des quatre carrée achevée.

Il termine ce mémoire avec l'énoncé d'un nouveau théorème :

Théorème 6

Pour tout nombre premier N, on peut trouver trois carrés xx, yy, zz, tels que $\lambda xx + \mu yy + \nu zz$ soit divisible par N, pourvu que λ, μ et ν soient premiers avec N.

Sa démonstration se base sur les raisonnements par l'absurde précédents et il arrive à la conclusion impossible que tous les nombres sont des non-résidus.

35. En effet, une fois que l'on a une somme de trois carrés $a^2+b^2+c^2$ divisible par N, toutes les sommes de trois carrés de la forme $(a+\alpha N)^2+(b+\beta N)^2+(c+\gamma N)^2$ sont encore divisibles par N.

Conclusion

Nous avons étudié dans cette section un ensemble de textes arithmétiques d'Euler et de Lagrange aboutissant à deux démonstrations du théorème des quatre carrés : tout nombre entier peut être mis sous la forme d'une somme de quatre carrés entiers. L'analyse de ces différents écrits permet d'obtenir des indications sur la pratique de l'arithmétique par ces deux mathématiciens.

Elle fait d'une part ressortir des influences réciproques entre Euler et Lagrange, et ce, à plusieurs niveaux : sur les méthodes de démonstrations et sur les outils utilisés. Comme nous l'avons déjà observé, les deux mathématiciens se basent sur la même trame de démonstration, constituée de trois étapes, pour prouver les résultats sur les sommes de carrés. C'est Euler qui l'utilise d'abord pour sa démonstration du théorème des deux carrés. Ensuite, on voit que la méthode de descente infinie est appliquée différemment : Euler l'intègre dans un premier temps dans le cadre de raisonnements par l'absurde, tandis que Lagrange, dans ses travaux sur les problèmes indéterminés du second degré, s'en sert pour prouver l'existence d'une solution d'une équation en construisant une suite d'équations dont les coefficients sont de plus en plus petits, et telles que la résolution d'une de ces équations implique la résolution de la suivante ou de la précédente. Il emploie à nouveau la méthode de descente infinie pour sa démonstration du théorème des quatre carrés pour obtenir une suite de produits de la forme Nn_i qui peuvent être mis sous la forme d'une somme de carrés, tels que les n_i forment une suite décroissante : là encore, cela permet de prouver l'existence du produit $N.1 = N$ et de conclure que le nombre N est également une somme de carrés. Dans [Euler, 1780], Euler reprend cette méthode pour prouver les théorèmes de la forme "Si N divise une somme de k carrés, tels qu'il ne divise aucun des carrés, alors il est lui-même somme de k carrés". Il donne ainsi un modèle unifié de preuve pour des résultats de la même forme.

On retrouve également des liaisons entre les différents outils utilisés. Lagrange utilise de longues séries d'identités algébriques qu'il lie à l'aide notamment de critères de divisibilité et de changements de variables. Euler reprend quelques-unes de ces techniques opératoires en intégrant ses propres séries de calculs. Les deux mathématiciens utilisent tous deux les différences finies, ainsi que le petit théorème de Fermat, dont Euler propose plusieurs démonstrations.

Néanmoins, on retrouve des pratiques propres à chacun des deux mathématiciens. Comme nous l'avons dit, Euler utilise les différences finies pour démontrer le théorème des deux carrés. En revanche, il ne les emploie pas dans son texte sur le théorème des quatre carrés. Lagrange se sert également de cet outil, sous une forme légèrement différente, dans la résolution de problèmes indéterminés du second degré et pour la preuve du

théorème des quatre carrés. De même, le petit théorème de Fermat a une place importante dans les recherches d'Euler, tout particulièrement dans ses résultats sur les résidus. Lagrange, de son côté s'en sert de manière ponctuelle, et majoritairement en termes de divisibilité. De manière plus générale, Lagrange ne considère que très peu de restes de divisions euclidiennes, tandis qu'Euler essaie d'en faire une des bases de ses preuves sur le théorème des quatre carrés : il obtient ainsi une démonstration purement arithmétique, sans utiliser les différences finies par exemple. C'est sans doute la grande divergence entre les travaux d'arithmétique des deux mathématiciens : Lagrange base ses raisonnements sur des manipulations algébriques, et sur des critères de divisibilité en reprenant les démonstrations d'Euler avec ses propres techniques, tandis qu'Euler développe petit à petit des méthodes et des démonstrations fondées sur les résidus : il utilise par exemple plusieurs raisonnements par l'absurde où la contradiction consiste en ce que tous les nombres sont des non-résidus.

V Euler, Lagrange et le théorème de Wilson : 1771-1773

Ce théorème, désigné ici sous le nom de théorème de Wilson, est notamment publié sans démonstration par Waring en 1770 dans ses *Meditationes Algebraicæ*, qui l'attribue à un de ces étudiants John Wilson. Comme nous l'avons vu dans la première partie, ce théorème constitue avec le petit théorème de Fermat, une source de démonstrations variées pour les travaux de théorie des nombres au XIX^{e} siècle. Avec les notations de Gauss, ce théorème peut être énoncé sous la forme : si p est un nombre premier, alors $(p-1)! \equiv -1 \pmod{p}$. Lagrange donne deux démonstrations de ce résultat dans [Lagrange, 1773a] et Euler en présente sa propre démonstration cette même année ; elle est publié en 1783 dans [Euler, 1783c].

1 - Les deux démonstrations du théorème de Wilson par Lagrange

Avant d'exposer ses deux preuves, Lagrange indique qu'il a découvert ce théorème dans l'ouvrage de Waring et énonce le théorème en termes de divisibilité, et en termes de restes :

> Si n est un nombre premier quelconque, le nombre
>
> $$1.2.3.4.5 \ldots (n-1) + 1$$
>
> sera toujours divisible par n ;[. . .]
>
> ou bien que si l'on divise ce même produit par n, on aura -1, ou, ce qui est la même chose, $n-1$ pour reste [Lagrange, 1773a, p. 54].

(a) Une première démonstration à partir d'identités polynomiales

Lemme

Étant donné le produit continuel

$$(x+1)(x+2)(x+3)(x+4)\dots(x+n-1),$$

on propose de le développer suivant les puissances de x.

Il pose :

$$(x+1)(x+2)(x+3)(x+4)\dots(x+n-1) = x^{n-1} + A'x^{n-2} + A''x^{n-3} + A'''x^{n-4} + \dots + A^{(n-1)}$$

et substitue dans cette égalité $x+1$ à x :

$$(x+2)(x+3)(x+4))\dots(x+n) = (x+1)^{n-1} + A'(x+1)^{n-2} + A''(x+1)^{n-3} + \dots + A^{(n-1)};$$

Donc, en multipliant la première égalité par $(x+n)$ et la seconde par $(x+1)$, on obtient :

$$(x+n)(x^{n-1} + A'x^{n-2} + A''x^{n-3} + A'''x^{n-4} + \dots + A^{n-1})$$
$$= (x+1)^n + A'(x+1)^{n-1} + A''(x+1)^{n-2} + \dots + A^{(n-1)}(x+1),$$

soit, en développant, à partir du binôme de Newton :

$$x^n + (n+A')x^{n-1} + (nA'+A'')x^{n-2} + (nA''+A''')x^{n-3} + \dots$$
$$= x^n + (n+A')x^{n-1} + \left[\frac{n(n-1)}{2} + (n-1)A' + A''\right]x^{n-2}$$
$$+ \left[\frac{n(n-1)(n-2)}{1.2.3} + \frac{(n-1)(n-2)}{2}A' + (n-2)A'' + A'''\right]x^{n-3} + \dots$$

De là, il tire des expressions pour les coefficients A', A'', A''', …, en identifiant les coefficients correspondant aux monômes de même degré des deux polynômes :

$$
\begin{aligned}
A' &= \frac{n(n-1)}{2},\\
2A'' &= \frac{n(n-1)(n-2)}{2.3} + \frac{(n-1)(n-2)}{2}A',\\
3A'' &= \frac{n(n-1)(n-2)(n-3)}{2.3.4} + \frac{(n-1)(n-2)(n-3)}{2.3}A' + \frac{(n-2)(n-3)}{2}A'',\\
&\ldots \quad \ldots \quad \ldots
\end{aligned}
$$

Puis il remarque dans un Corollaire que les coefficients A', A'', ... sont les sommes des entiers naturels de 1 à $(n-1)$, des produits de ces nombres multipliés deux à deux, trois à trois, etc. Ils sont donc tous nécessairement entiers, et $A^{n-1} = 1.2.3.\ldots.(n-1)$.

Théorème

Les mêmes choses étant posées que dans le Lemme précédent, je dis que, si n est un nombre premier, les nombres A', A'', A''', ... jusqu'à $A^{(n-2)}$ inclusivement, sont tous divisibles par n, et que le dernier nombre $A^{(n-1)}$ sera divisible par n, étant augmenté de l'unité.

Ce théorème implique le théorème de Wilson puisque dire que « dernier nombre $A^{(n-1)}$ [est] divisible par n, étant augmenté de l'unité », revient à prouver le théorème de Wilson.

Pour sa démonstration, il s'appuie sur le fait que les coefficients qui forment les expressions des nombres A', A'',..., $A^{(n-1)}$ sont en fait des coefficients du binôme de Newton élevés à une certaine puissance et qu'ils sont donc entiers.

De plus, les nombres A'', A''',..., $A^{(n-2)}$ sont la somme d'un coefficient du binôme de Newton élevé à la puissance n, qui est donc divisible par n car ce n'est pas un des coefficients extrêmes, et d'une expression en fonction des A^i précédents. Donc, puisque $A' = \frac{n(n-1)}{2}$, il est divisible par n, et par suite, les coefficients A'', A''',..., $A^{(n-2)}$ sont également divisibles par n.

D'autre part, pour déterminer le coefficient $A^{(n-1)}$, on a la formule :

$$nA^{(n-1)} = 1 + A' + A'' + A''' + \ldots + A^{(n-2)} + A^{(n-1)},$$

soit

$$A^{(n-1)} + 1 = nA^{(n-1)} - A' - A'' - \ldots - A^{(n-2)}.$$

On peut alors en déduire que $A^{(n-1)} + 1$ est divisible par n.

De là, il déduit immédiatement le corollaire :

Corollaire I

Donc le nombre $1.2.3.4\ldots(n-1)+1$ *sera toujours divisible par* n*, lorsque* n *sera un nombre premier, ce qui est le Théorème qu'il s'agissait de démontrer.*

Il observe alors que, plus généralement, on aura toujours :

$$(x+1)(x+2)(x+3)\ldots(x+n-1)-x^{n-1}+1$$

qui est divisible par n dès que n est un nombre premier.
De là, il fait deux remarques :

1. En posant $x=0$, on obtient le théorème de Wilson.
2. En prenant x non nul et non divisible par n, alors le produit

$$(x+1)(x+2)(x+3)\ldots(x+n-1)$$

est nécessairement divisible par n. De plus, $-x^{n-1}+1$, et de la même façon, $x^{n-1}-1$, sont divisibles par n. On retrouve là le petit théorème de Fermat. Lagrange ajoute que sa démonstration a « l'avantage de faire voir la liaison et la dépendance mutuelle des deux Théorèmes dont il s'agit » [Lagrange, 1773a, p. 430].

Lagrange donne ainsi une troisième démonstration du petit théorème de Fermat, basée sur le théorème de Wilson. Il en déduit également une méthode pour trouver une somme de deux carrés divisible par un nombre premier donné, qui permet d'obtenir une nouvelle preuve du théorème des deux carrés.

Pour cela, il observe qu'en considérant les restes après division par n, on peut remplacer les nombres $n-1$, $n-2$, $n-3$, ... par -1, -2, -3, ..., dans la formule $1.2.3.\ldots(n-1)$. On obtient ainsi toute une série de formules divisibles par n :

$$\begin{gathered}
1.2.3.\ldots(n-1)+1,\\
1.2.3.\ldots(n-2)-1,\\
1.2^2.3.\ldots(n-3)+1,\\
1.2^2.3^2.\ldots(n-4)-1,\\
\ldots\\
\left[1.2.3\ldots\left(\frac{n-1}{2}\right)\right]^2\pm 1.
\end{gathered}$$

Dans la dernière expression, on prend le signe + quand le nombre $\frac{n-1}{2}$ est pair, et le signe - quand $\frac{n-1}{2}$ est impair. De là suivent deux conclusions :

1. Si $\frac{n-1}{2}$ est pair, on peut poser $\frac{n-1}{2}=2m$. On a alors $n=4m+1$, et on obtient la somme de deux carrés $(1.2.3\ldots 2m)^2+1$ divisible par n ; le théorème des deux carrés suit.

2. Si $\frac{n-1}{2}$ est impair, on peut poser $\frac{n-1}{2} = 2m-1$, et donc $n = 4m-1$, et on obtient que $(1.2.3\ldots(2m-1))^2-1$ est divisible par n. Finalement, comme $(1.2.3\ldots(2m-1))^2-1 = [1.2.3.\ldots.(2m-1)+1][1.2.3.\ldots.(2m-1)-1]$, il faut que $[1.2.3.\ldots.(2m-1)\pm 1]$ soit divisible par n.

Il conclut son mémoire par plusieurs remarques. La première consiste à interpréter ce qu'il vient d'exposer comme un test de primalité. En effet, il observe que ce qu'il vient de montrer n'est valable que pour n premier, car dans le cas contraire, le produit $1.2.3\ldots(n-1)$ est nécessairement divisible par n et, de là, la formule $1.2.3\ldots(n-1)+1$ ne pourra pas être divisible par n. Il montre ainsi la réciproque du théorème de Wilson et conclut que cela donne une « méthode directe pour reconnaître si un nombre quelconque impair n est premier ou non » [Lagrange, 1773a, p. 432]. Il admet néanmoins que sa méthode devient très rapidement « extrêmement laborieuse et presque impraticable » [Lagrange, 1773a, p. 433] quand n croît, et qu'il faudrait réussir à la simplifier.

Sa deuxième remarque consiste en fait en une seconde démonstration du théorème de Wilson, à partir du théorème de Fermat.

(b) Une deuxième démonstration à partir du petit théorème de Fermat

Il commence par décrire cette autre méthode de démonstration comme beaucoup plus simple que la précédente. Cette méthode s'appuie en fait sur le petit théorème de Fermat et sur la méthode des différences finies. Il considère la différence $(n-1)^{\text{e}}$ des termes de la suite 1^{n-1}, 2^{n-1}, 3^{n-1}, …, n^{n-1} :

$$n^{n-1}-(n-1)(n-1)^{n-1}+\frac{(n-1)(n-2)}{2}(n-2)^{n-1}-\frac{(n-1)(n-2)(n-3)}{2.3}(n-3)^{n-1}+\ldots+1.$$

D'autre part, comme la série 1^{n-1}, 2^{n-1}, 3^{n-1}, …, n^{n-1} est en fait la fonction $f(x) = x^{n-1}$ évaluée en 1, 2, …, n, qui est de degré $n-1$, alors la différence $(n-1)^{\text{e}}$ est égale au produit $1.2.3.\ldots(n-1)$, d'où l'égalité :

$$1.2.3.\ldots(n-1) = n^{n-1}-(n-1)(n-1)^{n-1}+\frac{(n-1)(n-2)}{2}(n-2)^{n-1}-\frac{(n-1)(n-2)(n-3)}{2.3}(n-3)^{n-1}+\ldots+1.$$

De là, il examine le reste du second membre de cette dernière égalité après division par n. Il remarque que, d'après le petit théorème de Fermat, les termes x^{n-1}, pour $1 \le x \le n-1$, ont pour reste 1. De là, il suit :

$$-(n-1)+\frac{(n-1)(n-2)}{2}-\frac{(n-1)(n-2)(n-3)}{2.3}+\ldots,$$

soit, d'après le binôme de Newton :

$$(1-1)^{n-1}-1=-1,$$

d'où le théorème de Wilson.

Sa dernière remarque a pour objet deux théorèmes sur les nombres premiers :

1. Si trois nombres premiers sont en progression arithmétique, leur différence doit être divisible par 6, à moins que l'un de ces trois nombres ne soit égal à 3.
2. Si cinq nombres premiers sont en progression arithmétique, leur différence doit être divisible par 30, à moins que 5 ne soit l'un des termes de cette progression.

(c) En résumé ...

Lagrange nous présente dans ce texte deux démonstrations du théorème de Wilson : la première utilise surtout des méthodes d'algèbre polynômiale, et permet d'en déduire le petit théorème de Fermat. Lagrange insiste alors sur le lien existant entre ces deux résultats. Inversement, sa deuxième preuve est basée sur le petit théorème de Fermat, et Lagrange y considère également les différences finies et les restes de divisions euclidiennes. Cette démonstration est donc plus arithmétique qu'algébrique. De plus, il en déduit une nouvelle preuve du théorème des deux carrés, et des corollaires sur les nombres premiers. Cette deuxième partie se rapproche donc plus de ce qu'on appellerait un travail de théorie des nombres : Lagrange y obtient des résultats en lien avec les nombres entiers, et ses raisonnements sont principalement fondés sur des propriétés arithmétiques : petit théorème de Fermat et restes de divisions euclidiennes.

2 - La réponse d'Euler : les résidus pour une troisième preuve du théorème de Wilson

Le mémoire *Miscellanea analytica* d'Euler est présenté le 15 novembre 1773 à l'Académie de Saint-Pétersbourg, puis publié pour la première fois dans le premier tome des *Opuscula Analytica* en 1783. Le théorème de Wilson est le premier résultat présenté et démontré dans ce mémoire. D'après [Weil, 1984], Euler envoie sa preuve du théorème de Wilson après avoir reçu les deux démonstrations proposées par Lagrange.

Proposition d'une démonstration pour le théorème de Waring

Si n est un nombre premier, alors le produit $1.2.3\ldots(n-1)$ *donne toujours pour reste -1 après division par le nombre n.*

Lagrange, pour présenter ce résultat, en donne deux versions équivalentes : en terme de divisibilité, et en terme de restes de division euclidienne, en ajoutant que l'on peut

considérer le reste -1 ou $n-1$. Euler, de son côté, ne propose qu'une version basée sur la considération du reste -1.

Ici, Euler fonde sa preuve sur les propriétés des résidus de puissances, étudiées notamment dans [Euler, 1774] [36]. Soit un nombre premier n, et a un nombre premier à n. Alors les puissances a^0, a^1, a^2, ..., a^{n-1} donnent, après division par n, des résidus distincts, et qui sont contenus dans les nombres 1, 2, 3, ..., $n-1$; de plus, les puissances a^{n-1} et a^0 donnent pour résidu l'unité.

La formule $a^{n-1}-1$ est divisible par n, donc si on pose $n=2p+1$, alors une des deux formes a^p-1 ou a^p+1 est divisible par n. Or a^p ne peut donner 1 comme résidu puisque, comme a est premier à n, $n-1$ est le plus petit exposant x tel que a^x donne 1 pour résidu. Euler en déduit donc que c'est la formule a^p+1 qui est divisible par n. Donc la puissance a^p admet -1, soit $n-1$, pour résidu.

Il identifie alors les puissances a^0, a^1, a^2, ..., a^{n-2} aux résidus 1, 2, 3, ..., $n-1$ et observe que $1.2.3.\ldots.(n-1)$ donne le même résidu que la formule $a^0.a^1.\ldots.a^{n-2} = a^{0+1+2+\ldots+(n-2)}$ après division par n. Or $n-2=2p-1$ et donc :

$$a^{0+1+2+\ldots+(n-2)} = a^{2p^2-p} = a^{2p(p-1)+p} = a^{2p(p-1)} \times a^p.$$

Or, $a^{2p} = a^{n-1}$ donc a^{2p} donne pour résidu 1 après division par n d'après le petit théorème de Fermat, et il en est donc de même pour $a^{2p(p-1)} = (a^{p-1})^{2p}$. De plus, on a montré que a^p donnait pour résidu -1. On en déduit donc que a^{2p^2-p} donne pour résidu -1 après division par n, et que $a^{2p^2-p}+1$ est divisible par n. D'après ce qui a été dit précédemment, on peut alors en conclure que $1.2.3.\ldots.(n-1)$ donne pour résidu -1, c'est-à-dire que $1.2.3.\ldots.(n-1)+1$ est divisible par n.

Dans ce mémoire, Euler expose donc une démonstration basée uniquement sur les propriétés des résidus, démontrées dans des mémoires précédents et utilise une correspondance entre les puissances du nombre a et leurs résidus après division par n. Remarquons cependant qu'Euler, contrairement à Gauss, n'introduit pas de symbole et distingue dans son exposé les calculs sur les puissances de a, et les calculs sur l'expression initiale. Du point de vue des résidus, il utilise plusieurs propriétés fondamentales : les puissances a^k, $1 \leq k \leq n-2$ sont d'ordre $n-1$, et permettent d'obtenir, après division par n, tous les nombres entiers compris entre 1 et $n-1$. Il observe également que $a^{\frac{n-1}{2}}$ donne pour reste -1, après division par n. D'autre part, il ne rappelle pas les démonstrations de ces différentes propriétés et semble les supposer connues : il les a effectivement exposées plus tôt dans des mémoires consacrés à la théorie des résidus, dont nous donnons un aperçu dans la section suivante.

36. Nous donnons un aperçu de ce texte dans la section suivante.

VI Euler(, Lagrange) et la théorie des résidus

Dans les sections précédentes, nous avons étudié quelques textes de théorie des nombres d'Euler et Lagrange. Nous avons mis en avant leurs influences réciproques et leurs différences dans la pratique de ce domaine. Lagrange se tourne le plus souvent vers des méthodes algébriques et variées, tandis qu'Euler semble tenter progressivement d'unifier les méthodes employées pour certains résultats autour d'un nouvel outil : les résidus. Lagrange, de son côté, connaît les écrits d'Euler et s'y réfère très régulièrement ; pourtant, il ne considère que très peu de restes de divisions euclidiennes et donne de nouvelles preuves des théorèmes qu'Euler a démontré en utilisant sa théorie des résidus. C'est pourquoi nous avons placé Lagrange entre parenthèses dans le titre de cette section : il n'intègre à aucun moment la théorie des résidus dans ses publications. Il est cependant vrai que Lagrange a démontré des résultats dont les équivalents en termes de résidus ou de congruences sont des propriétés fondamentales sur ces objets. Par exemple, on attribue parfois à Lagrange la démonstration du théorème sur le nombre maximum de solutions d'une congruence de degré n : une congruence de degré n à coefficients entiers et à une indéterminée admet au plus n racines entières. Il démontre effectivement un résultat équivalent dans [Lagrange, 1770, p. 667] mais où les restes ne sont pas mentionnés. Il le formule en termes de divisibilité : si A est un nombre premier, et si α est une expression de degré n, de variable θ dont les coefficients sont des nombres entiers, alors il y a au plus n valeurs distinctes de θ inférieures ou égales à $\frac{1}{2}A$ telles que α soit divisible par A. De même, dans ses recherches sur les formes quadratiques, plus tardives, Lagrange n'utilise pratiquement pas les restes dans ses raisonnements.

Au contraire, Euler présente à l'Académie de Berlin plusieurs travaux dont l'objet principal est la théorie des résidus, et dont l'objectif est de prouver des propriétés sur ces objets. Il applique également à plusieurs reprises les propriétés ainsi obtenues pour prouver des résultats sur les formes quadratiques binaires et leurs diviseurs : c'est ce que nous avons par exemple observé dans le cadre de ses mémoires sur les sommes de quatre carrés[37]. Nous présentons donc ci-dessous quelques textes d'Euler sur les résidus de puissance, les résidus quadratiques, ... afin de dresser un panorama des résultats obtenus par Euler à ce sujet.

1 - Premiers résultats sur les résidus de puissances

Le premier mémoire d'Euler dont le thème est la théorie des résidus de puissances s'intitule *Theoremata circa residua ex divisione potestatum relicta* (*Théorèmes sur les résidus obtenus par la division de puissances*) et a été présenté le 13 février 1855 à l'Académie de Berlin, puis publié dans les *Novi Commentarii academiae scientiarum Petropolitanae*

37. Pour une analyse de plusieurs mémoires d'Euler sur les formes quadratiques : voir [Bussotti, 2006].

en 1761. Par rapport à [Euler, 1760b] où le terme "résidu" désigne ce que l'on nomme aujourd'hui "résidu quadratique", Euler utilise ici le mot "résidu" pour désigner le reste d'une puissance d'un nombre donné. Un point très important de ce mémoire est qu'Euler n'utilise pas le petit théorème de Fermat pour prouver les différents résultats sur les résidus de puissances ; il donne d'ailleurs une troisième démonstration de ce théorème, qui est en fait le théorème 14.

Euler considère un nombre premier p, et un nombre a, premier à p. Il démontre dans un premier temps que les puissances a^k, $k \geq 0$, ne sont pas divisibles par p en utilisant le fait que le produit de deux nombres premiers à p est également premier à p. Il annonce dans une scholie qu'il a décidé d'étudier les résidus provenant des divisions par p de la suite géométrique (a^k), $k \geq 0$. Il rappelle que tout résidu peut être ramené à un nombre inférieur à p et observe que tous les restes de la forme $r \pm np$ représentent le même résidu r. Euler insiste donc sur le fait que l'on peut considérer un seul représentant pour une infinité de nombres [38]. Pour l'instant, il travaille avec des résidus positifs plus petits que p mais indique que l'on peut également prendre des restes positifs ou négatifs dont la valeur absolue est inférieure à $\frac{p}{2}$. Il remarque que les résidus de la progression géométrique considérée apparaissent chacun plusieurs fois puisque le nombre de résidus distincts est nécessairement fini. Il rappelle également la définition du complément d'un résidu.

Dans le théorème 2, Euler montre que le produit de deux résidus est également un résidu. Il en déduit trois corollaires. Il montre en particulier que si a^μ a pour résidu l'unité, alors il en est de même pour $a^{k\mu}$.

Dans le théorème 3, Euler affirme qu'une infinité de puissances de a ont pour résidu l'unité. Il le démontre en termes de divisibilité en considérant deux puissances de a ayant le même résidu. De plus, il existe une puissance a^λ telle que son résidu soit 1 et telle que $\lambda < p$.

Le théorème 4 a pour objet la division dans le sens déjà considéré dans le cas des résidus quadratiques : si a^μ a pour résidu r et $a^{\mu+\nu}$ a pour résidu rs, alors a^ν a pour résidu s.

Il applique les résultats précédents pour prouver le théorème 5 : si a^λ est la plus petite puissance de a ayant pour résidu l'unité, alors les puissances de a dont le résidu est l'unité sont nécessairement de la forme $a^{k\lambda}$. Il indique dans un de ses corollaires que tous les nombres compris entre 1 et $p-1$ ne sont pas nécessairement des résidus de puissances, mais, comme on considère les restes après division par le nombre p, on obtient au maximum $p-1$ résidus différents.

Pour le théorème 6, Euler montre que si a^{2n} a pour résidu l'unité, alors a^n a pour résidu ± 1.

38. Euler observe : « Itaque omnia haec residua $r \pm np$ pro eodem residuo r reputantur » [Euler, 1761b, §3].

Le théorème 7 décrit l'ensemble des résidus que l'on obtient après division par p : si a^λ est la plus petite puissance dont le résidu est 1, alors tous les résidus de la suite géométrique (a^k) sont contenus dans les résidus des puissances 1, a a^2, ..., $a^{\lambda-1}$. Cela implique que la suite des résidus obtenue après division par p des termes de la suite (a^k) est périodique : c'est l'objet du théorème 8.

Les théorèmes 10 à 13 indiquent quels sont les nombres de résidus que l'on peut obtenir. Ainsi, si tous les nombres compris entre 1 et $p-1$ apparaissent dans la série des résidus, alors la plus petite puissance de a dont le résidu est l'unité est a^{p-1}. Mais s'il y a moins de $p-1$ résidus distincts, alors il existe un $\lambda < p-1$ tel que a^λ a pour résidu 1. Alors ce sont les résidus des puissances 1, a, a^2, ..., $a^{\lambda-1}$ qui sont dans l'ensemble des résidus. Soit k, un nombre n'apparaissant pas dans la série des résidus. Alors ak, a^2k, a^3k, ..., $a^{(\lambda-1)}k$ sont des nombres distincts et non-résidus. Il y a donc au moins λ non-résidus. Euler montre ainsi par itération que le nombre de résidus est égal ou strictement inférieur à un diviseur de $p-1$ en se basant sur la même méthode : on exhibe un non-résidu n'appartenant pas à la suite de non-résidus déjà considérés. Ainsi, il conclut que le plus petit exposant λ tel que a^λ laisse l'unité pour résidu est nécessairement un diviseur de $p-1$. De là, il déduit le petit théorème de Fermat, qu'il énonce en termes de résidus, puis en termes de divisibilité, et obtient ainsi une nouvelle preuve de ce résultat. Il remarque d'ailleurs qu'il considère cette preuve basée uniquement sur la théorie des résidus comme bien plus naturelle [39].

Les cinq derniers théorèmes ont pour objet les résidus obtenus pour certaines formes données. Certains de ces théorèmes sont énoncés en termes de divisibilité. Par exemple, d'après le théorème 17, si $a = c^n \pm \alpha p$,et si n est un diviseur de $p-1$, alors $a^{\frac{p-1}{n}}$ a pour résidu l'unité. Dans des corollaires, il applique ce résultat au cas où $n = 2$ et 3.

Dans ce mémoire, on voit qu'Euler semble suivre le même cheminement que lors de son exposé sur les résidus quadratiques : il établit les propriétés de base des résidus de puissance (stabilité par multiplication, division),montre que la suite des résidus est périodique de période λ qui est un diviseur de $p-1$. Il obtient une nouvelle preuve du théorème de Fermat et se félicite qu'elle soit plus "naturelle" : elle est effectivement fondée sur l'utilisation des résidus seulement. Remarquons d'ailleurs que pour aboutir à cette nouvelle preuve, d'un point de vue moderne, Euler utilise la décomposition d'un groupe en ses classes modulo un sous-groupe. Il reste néanmoins un outil clé que Gauss utilise dans ses *Disquisitiones Arithmeticae* : les racines primitives. Euler les introduit dans [Euler, 1774] , présenté le 18 mai 1772 à l'Académie de Saint-Pétersbourg.

39. « [...] unde haec demonstratio magis naturalis videtur, cum praeterea nobis alias insignes proprietas circa residua potestatum, quando per numeros primos dividuntur, maifestet » [Euler, 1761b, §53].

2 - Petit intermède : fonction d'Euler et une quatrième preuve du petit théorème de Fermat

Dans le mémoire *Theoremata arithmetica nova methodo demonstrata*, publié en 1763, Euler présente en particulier des propriétés de l'actuelle fonction d'Euler et donne une démonstration d'une version généralisée du petit théorème de Fermat. Pour cela, il donne des propriétés des résidus obtenus à partir des termes d'une progression arithmétique puis d'une progression géométrique.

Il considère tout d'abord un nombre n et montre que les termes issus d'une progression arithmétique dont le terme initial et la raison sont premiers à n donnent pour résidus après division par n tous les nombres inférieurs à n. Dans le théorème 2, Euler ajoute que si le terme initial n'est pas premier à n, alors il y aura autant de résidus distincts que de nombres inférieurs et premiers à n. Euler utilise ces théorèmes et leurs corollaires afin de déterminer combien il y a de nombres inférieurs et premiers à n, ce que l'on note aujourd'hui $\varphi(n)$. Il calcule $\varphi(n)$ dans le cas où n est la puissance d'un nombre premier et le produit de deux nombres premiers. Puis il montre que la fonction d'Euler est multiplicative : si A et B sont deux nombres premiers entre eux, s'il y a a (respectivement b) nombres inférieurs et premiers à A (respectivement B), alors il y a ab nombres inférieurs et premiers à AB, ce qui permet d'obtenir la quantité cherchée dans tous les cas.

À partir du théorème 6, Euler rappelle les propriétés des résidus de puissances. Tout d'abord, les résidus obtenus sont des nombres inférieurs et premiers au diviseur N, il y a donc au maximum $\varphi(N)$ distincts[40]. Soit x un nombre premier à N. Si x^ν est la plus petite puissance de x ayant l'unité pour résidu, alors on obtient ν résidus distincts, et les puissances de la forme $x^{\mu+k\nu}$, où μ est fixé et où k est un nombre entier, ont toutes le même résidu après division par N. Il démontre les propriétés habituelles de stabilité par puissance et multiplication. Il insiste à nouveau sur le fait qu'ainsi, on ramène une infinité de nombres à un ensemble très réduit. Ainsi, dans les corollaires 2 et 3 du théorème 8, Euler indique :

Corollaire 2

> 44. Et le nombre des résidus n'en devient pas indéterminé, car comme nous l'avons déjà vu, des résidus semblables naissent d'une infinité de puissances, ainsi, si tous ces résidus, provenant de la multiplication mutuelle, sont réduits à la plus petite forme, ils ne feront qu'une très petite quantité.

Corollaire 3

> 45. Ainsi si la plus petite puissance qui, divisée par N donne de nouveau l'unité,

40. Ici, φ représente la fonction d'Euler. $\varphi(N)$ est égal à la quantité de nombres inférieurs et premiers à N.

est x^ν, de sorte que le nombre des résidus 1, a, b, c, d, etc. est = ν, alors tous les produits qui proviennent de la multiplication des nombres a, b, c, etc., seront contenus dans le même nombre, si toutefois on leur enlève le diviseur N chaque fois qu'il est possible [41].

D'un point de vue moderne, Euler exprime très bien ici la stabilité par multiplication de l'ensemble des résidus. Il illustre ces résultats par le cas où $x = 2$ et $N = 15$.

Dans le théorème 9, Euler démontre que le nombre de résidus distincts ν est égal au nombre d'entiers inférieurs et premiers avec le diviseur et que le nombre de non-résidus est égal à un multiple de ν. Il utilise une méthode similaire aux précédentes en montrant à partir de critères de divisibilité que si les résidus distincts sont 1, a, b, ..., et si α est un non-résidu, alors $a\alpha$, $b\alpha$, ..., sont également des non-résidus distincts. Il en déduit dans un corollaire que le produit d'un résidu et d'un non-résidu est un non-résidu.

Dans le théorème 10, Euler affirme que si x^ν est la plus petite puissance de x ayant pour résidu l'unité après division par N, alors ν divise nécessairement $\varphi(N)$. La preuve de ce résultat est basée sur le théorème 10. Il en déduit le onzième et dernier théorème de ce mémoire, qui est également une version généralisée du petit théorème de Fermat : si N est le diviseur, x un nombre premier à N, alors $x^\varphi - 1$ est divisible par N. Dans un des corollaires qui suivent, Euler remarque que cela implique que si x et y sont des nombres premiers à N, alors $x^n - y^n$ est divisible par N. Il conclut en justifiant l'intérêt des premiers résultats en lien avec la détermination de $\varphi(N)$ par cette version du petit théorème de Fermat.

Dans ce mémoire, Euler, montre donc, à partir de critères de divisibilité, des propriétés des résidus, similaires aux précédentes, mais pour un diviseur composé. Il insiste une fois de plus sur des conséquences fondamentales de la considération des résidus de puissances : on ramène l'étude d'un ensemble infini de nombres à un ensemble fini de résidus, stable par multiplication. Chaque résidu représente donc une infinité de nombres. Enfin, ce mémoire contient également des résultats sur les propriétés de ce que l'on appelle actuellement la fonction d'Euler.

41. Cette traduction est inspirée d'un manuscrit conservé à la Bibliothèque de l'Observatoire National de Bruxelles. Voici le texte original :

Corollarium 2

44. Neque tamen ideo numerus residuorum indeterminatus euadit ; quemadmodum enim iam vidimus ex innumeris potestatibus paria residua provenire, ita, si omnia residua, ex mutna multiplicatione nata, ad formam minimam reducantur, ad multitudinem medicam revocabuntur.

Corollarium 3

45. Ita si minima potestas, quae per N divisa iterum unitatem relinquit fuerit x^ν, ita ut numerus residuorum 1, a, b, c, etc., sit = ν, tum in eodem numero omnia producta ex multiplicatione numerorum a, b, c, etc. nata continebuntur, siquidem ab iis divisor N toties, quoties fieri potest, auferatur [Euler, 1763, §44, 45].

3 - Introduction d'un outil clé : les racines primitives d'un nombre premier

Dans ce mémoire, intitulé *Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia* , Euler étudie à nouveau les résidus après division par un nombre premier P d'une progression géométrique de raison a, et de terme initial 1. Il note ces résidus 1, α, β, γ, ...et reprend des propriétés énoncées et démontrées dans [Euler, 1761b]. Comme ces résidus sont inférieurs à P, il y en a au plus $P-1$. La série des résidus est donc finie et plusieurs nombres de la progression géométrique ont le même résidu. À partir d'un résidu, il explique comment obtenir facilement le résidu suivant. En effet, si $\epsilon = a^5 - mP$ et $\zeta = a^6 - nP$, alors $\zeta = a\epsilon - (n - ma)P$. Il suffit donc de multiplier le résidu ϵ par a puis de l'abaisser en-dessous de P.

Il remarque que tous les nombres peuvent être rangés en périodes selon leur résidu après division par P.

I.	0,	P,	$2P$,	$3P$,	$4P$,	...	mP,
II.	1,	$P+1$,	$2P+1$,	$3P+1$,	$4P+1$,	...	$mP+1$,
III.	2,	$P+2$,	$2P+2$,	$3P+2$,	$4P+2$,	...	$mP+2$,
VI.	3,	$P+3$,	$2P+3$,	$3P+3$,	$4P+3$,	...	$mP+3$,
				etc.			

Euler en déduit des considérations générales sur les résidus des nombres après division par P et conclut que l'on peut exprimer tous les restes comme des nombres dont la valeur absolue est inférieure à $\frac{1}{2}P$. Il poursuit son mémoire avec plusieurs observations : selon la raison a choisie pour la progression géométrique, les résidus des puissances de ce nombre peuvent ou non décrire tous les nombres compris entre 1 et $P-1$. Il donne deux cas particuliers simples :

- Si $a = 1$, le seul résidu obtenu est l'unité.
- Si $a = P - 1$, les seuls résidus obtenus sont 1 et -1.

Dans d'autres cas, tous les nombres compris entre 1 et $p-1$ se trouvent dans les résidus. Il donne l'exemple de $P = 7$ et $a = 3$. Dans ce cas, Euler qualifie la série des résidus de *complète*. Dans les deux exemples précédents, les séries de résidus étaient *incomplètes*. Pour $P = 7$, et pour $a = 2, 3, 4, 5$, on a les séries de résidus suivants :

Progressio geometrica	1,	2,	2^2,	2^3,	2^4,	2^5,	2^6,	2^7,	2^8,	2^9,	etc.
Residua	1,	2,	4,	1,	2,	4,	1,	2,	4,	1,	etc.
Progressio geometrica	1,	3,	3^2,	3^3,	3^4,	3^5,	3^6,	3^7,	3^8,	3^9,	etc.
Residua	1,	3,	2,	6,	4,	5,	1,	3,	2,	6,	etc.
Progressio geometrica	1,	4,	4^2,	4^3,	4^4,	4^5,	4^6,	4^7,	4^8,	4^9,	etc.
Residua	1,	4,	2,	1,	4,	2,	1,	4,	2,	1,	etc.
Progressio geometrica	1,	5,	5^2,	5^3,	5^4,	5^5,	5^6,	5^7,	5^8,	5^9,	etc.
Residua	1,	5,	4,	6,	2,	3,	1,	5,	4,	6,	etc.

Il pose alors le problème suivant : peut-on toujours exhiber un nombre a tel que la série des résidus associés soit complète ?

Il introduit à ce moment-là le terme de *racine primitive* : c'est la raison d'une progression géométrique qui produit une série complète de résidus. Autrement dit, c'est un nombre a tel que l'ensemble des résidus des puissances 1, a, a^2, a^3, …, a^{p-2} contienne tous les nombres de 1 à $p-1$.

Ainsi, pour $P = 7$, les racines primitives sont 3 et 5.

Le problème précédent se réduit donc à la question : tous les nombres premiers P admettent-ils des racines primitives ?

Avant de répondre à cette question, Euler démontre une série de propriétés relatives aux résidus de puissances :

- Dans une série de résidus, c'est toujours l'unité qui se représente en premier.
- Ainsi, dans la série des résidus

$$1, \alpha, \beta, \gamma, \delta, etc.$$

  l'unité se présente une seconde fois, et les autres résidus se présente à la suite dans le même ordre qu'initialement.
- Si a est une racine primitive, alors la puissance a^{P-1} laisse l'unité après division par le nombre premier P.
- Si la progression géométrique

$$1, a, a^2, a^3, a^4, etc.$$

  produit une série de résidus incomplète, le nombre de résidus différents est une partie aliquote du nombre $P-1$, qui est le diviseur P diminué de l'unité.

Euler démontre ensuite un théorème important, qui sera repris par ses successeurs,

et qui est un cas particulier du théorème prouvé par Lagrange sur le nombre de racines d'une congruence mentionné au début de la section.

Théorème : *La forme $x^n - 1$, pour $x < P$, est divisible par le nombre premier P, par au plus n quantités.*

En termes modernes, on dirait que l'équation binôme $x^n - 1 \equiv 0$ admet au plus n racines dans $\mathbb{Z}/p\mathbb{Z}$.

Dans une scholie qui suit cette démonstration, Euler explique que la forme $x^n - 1$ est divisible par P pour n valeurs réelles exactement lorsque n divise $P - 1$. Dans le cas où $n = P - 1$, il y a toujours n solutions réelles. Néanmoins, Euler ne démontre pas ces dernières affirmations et c'est une des raisons pour lesquelles les démonstrations suivantes, en lien avec l'existence des racines primitives, ne sont pas complètes. Dans les articles 32-34, Euler tente de démontrer par induction qu'il y a exactement $\varphi(n)$ nombres x inférieurs à P tels que $x^n - 1$ soit divisible par P, et tels que $x^l - 1$ ne soit pas divisible par P pour tout l inférieur à n, et où n est un diviseur de $p-1$. Euler en déduit que le nombre premier P admet $\varphi(P-1)$ racines primitives. Dans les *Disquisitiones Arithmeticae*, Gauss insiste d'ailleurs sur les deux faiblesses de cette preuve d'Euler : « Cependant la démonstration de cet homme pénétrant présente deux défauts ; l'un tient à ce qu'il suppose tacitement, art. 31 et suivants, que la congruence $x^n - 1 \equiv 0$, (en ramenant ses raisonnements à notre notation) a réellement n racines différentes, tandis qu'il était seulement démontré que cette congruence ne peut en avoir davantage ; l'autre, à ce qu'il ne déduit que par induction la formule du n° 34 » [Gauss, 1801, art. 56]. Il faut attendre les travaux de Gauss et Legendre pour obtenir une démonstration correcte de l'existence des racines primitives pour tout nombre premier. Cette démonstration incomplète implique alors qu'à chaque fois qu'Euler considère sans justification une racine primitive, le raisonnement correspondant est également imparfait.

Il énonce et démontre ensuite des résultats liés aux racines primitives. Soit a une racine primitive du nombre premier $2n + 1$, il montre en particulier que a^n a pour résidu -1.

Puis il obtient des résultats sur les résidus quadratiques et cubiques. Ainsi, il montre que les résidus quadratiques sont la série des résidus des puissances 1, a^2, a^4, ... Il prouve un cas particulier de la loi de réciprocité quadratique : -1 est un résidu quadratique si le nombre n est pair, c'est-à-dire si le nombre premier considéré est de la forme $4k + 1$ et -1 est non-résidu dans le cas contraire. Il en déduit des preuves de résultats sur les sommes de deux carrés énoncés dans ses écrits précédents.

De même, il cherche à trouver tous les résidus cubiques après division par le nombre premier P. Il distingue deux cas : si P est de la forme $3n + 1$, les résidus cubiques sont dans la série 1, a^3, a^6, ..., a^{3n-3} ; si P est de la forme $3n+2$, alors les résidus cubiques sont dans la série 1, a^3, a^6, ..., a^{9n}. Il est déduit en particulier des résultats sur les sommes du type $p^2 + 3q^2$.

Il formule les mêmes questions dans le cas des résidus biquadratiques et des résidus d'ordre supérieur dans la suite du mémoire.

4 - D'autres travaux sur les résidus... dont un traité de théorie des nombres inachevé

Ainsi, à partir des deux mémoires résumés précédemment, on voit qu'Euler obtient des résultats divers sur les résidus qui sont ensuite repris et complétés par Gauss dans les *Disquisitiones Arithmeticae* de façon plus systématique pour fonder ses recherches en théorie des nombres. Euler étudie les résidus dans d'autres textes. Par exemple, trois mémoires publiés en 1783 contiennent des raisonnements sur les résidus. Ces textes sont présentés entre le 18 mai 1772 et le 25 janvier 1773 à l'Académie de Saint-Pétersbourg et ne sont publiés qu'après la mort d'Euler. Dans [Euler, 1783d], Euler rappelle les propriétés fondamentales des résidus quadratiques, et obtient des conclusions en lien avec la future loi de réciprocité quadratique [42]. Dans [Euler, 1783b], il revient sur les résidus quadratiques, les résidus de puissances et les racines primitives. Enfin, dans [Euler, 1783a], il résout notamment le problème suivant : pour un diviseur donné N, trouver le plus petit exposant n tel que a^n laisse pour résidu l'unité. Il reprend le problème avec un résidu quelconque r.

Certains textes publiés à titre posthume, et jamais présentés devant une Académie contiennent également des recherches sur les résidus. Par exemple, dans [Euler, 1787], Euler utilise les propriétés des résidus quadratiques afin d'étudier les diviseurs des formes $a^2 + ny^2$. Et le texte le plus important sur ce thème est sans doute le *Tractatus de numerorum doctrina capita sedecim, quae supersunt*, traité de théorie des nombres inachevé, publié en 1849. Ce texte ne constitue donc pas une source pour nos mathématiciens de la première moitié du XIX$^{\text{e}}$ siècle, mais il est néanmoins éclairant d'avoir une idée de son contenu. Les titres de neuf chapitres sur seize contiennent le mot "résidus". Dans le chapitre V, Euler introduit la notion de résidu à partir de la division euclidienne. Il illustre cette introduction par des exemples. Il indique ainsi que si l'on considère le diviseur 6, on obtient six classes différentes de nombres : $6m$, $6m + 1$, $6m + 2$, $6m + 3$, $6m + 4$ et $6m + 5$. Il rappelle que l'on peut également travailler avec des résidus négatifs. Dans le sixième chapitre, il aborde les résidus que l'on obtient à partir des termes d'une progression arithmétique et reprend en particulier des résultats déjà exposés dans [Euler, 1763]. Il étudie dans le septième chapitre les résidus de puissances, et le huitième est consacré aux nombres qui ont pour résidu l'unité. Les chapitres 10 à 13 contiennent respectivement des propriétés sur les résidus quadratiques, cubiques, biquadratiques et quintiques. Dans le chapitre 14, Euler commence un travail sur les résidus quadratiques pour un diviseur non premier, puis étudie les sommes de la forme $x^2 + y^2$ et $x^2 + 2y^2$ dans les deux derniers

42. Voir notamment [Lemmermeyer, 2000, p. 4-5].

chapitres.

Dans ce traité de théorie des nombres, Euler semble donc avoir tenté de regrouper tous les résultats obtenus précédemment en lien avec sa théorie des résidus, en les mettant en relation avec des résultats sur les diviseurs de certaines formes quadratiques notamment.

5 - Conclusion

Comme nous l'avons vu dans ce chapitre, les travaux d'arithmétique de Lagrange relèvent de l'analyse diophantienne et ses dernières recherches constituent une première approche de la théorie des formes quadratiques. Dans les deux cas, il démontre des propriétés importantes et achève des démonstrations recherchées depuis longtemps, sans intégrer la théorie des résidus, et en particulier celle des résidus quadratiques. On retrouve au contraire chez Euler plusieurs travaux contenant des résultats fondamentaux sur les résidus. Plus de la moitié de son traité inachevé de théorie des nombres est en lien avec ces outils, et cela montre bien qu'Euler semble leur donner une place centrale pour une partie de ses recherches en théorie des nombres, notamment celles en lien avec les formes quadratiques. Il faut néanmoins garder à l'esprit qu'Euler publie également d'autres textes d'arithmétique, qui ne sont pas basés sur les résidus.

Parmi les propriétés des résidus particulièrement mises en avant par Euler, nous trouvons la question de la représentation d'une infinité de nombres par un seul représentant. En effet, Euler insiste à plusieurs reprises sur le fait de ramener les nombres de la forme $r+np$ par exemple au seul résidu r. De même, il observe que les divers produits de résidus donnent une infinité de nombres qui sont également contenus dans un ensemble fini de résidus. Nous n'avons pas retrouvé de telles réflexions explicites dans les différents travaux du XIX$^{\text{e}}$ siècle.

Euler revient également plusieurs fois sur la classification des différents nombres entiers compris entre 1 et $p-1$, avec p premier par exemple, en résidus (quadratiques, de puissances, ...) et non-résidus. Il prouve les différentes propriétés opératoires de ces résidus du point de vue de la multiplication et de la division à quotient entier. Pour sa troisième démonstration du petit théorème de Fermat, il divise même ces nombres entiers en plusieurs ensembles en considérant les résidus de puissances d'une part, et les non-résidus qu'il partage également en sous-ensembles : d'un point de vue moderne, il s'agit pour un sous-groupe cyclique de $\mathbb{F}_p^*$ de construire explicitement les classes modulo ce sous-groupe (qui sont en fait les différentes classes de non-résidus chez Euler).

Enfin, nous avons vu qu'Euler met en place des schémas de démonstration pour obtenir des théorèmes sur les sommes de carrés. Nous avons également vu que, dans le cadre de ses études sur les résidus, il suit la plupart du temps la même démarche pour présenter

les propriétés des résidus considérés, en donnant des tables d'exemples puis en démontrant des résultats sur les produits de résidus, de non-résidus, ... Dans [Euler, 1849], Euler présente des résultats sous cette forme pour les résidus cubiques, biquadratiques, et de puissance cinquième. Il construit notamment des tableaux indiquant explicitement, à partir d'exemples, les classes de non-résidus cités précédemment. Par exemple, dans le cas des résidus cubiques, il liste, pour le diviseur 13, les résidus cubiques sur une ligne (1, 8, 5, 12), puis les deux classes de non-résidus sur deux autres lignes (2, 4, 3, 6 et 11, 9, 10, 7). Il fait le même travail dans le cas des résidus quintiques. Par exemple, dans le cas du diviseur 31, son tableau est formé de colonnes indiquant les résidus cinquièmes, les puissances de nombres qui donnent ces résidus cinquièmes, et les représentants de chacune des quatre classes de non-résidus (*Classes non-residuorum* [Euler, 1849, p. 60]), numérotées de I à IV.

L'étude des différentes publications d'Euler présentées dans ce chapitre permet de mettre en valeur une évolution du mathématicien par rapport aux résidus. Plusieurs sources secondaires interprètent en termes de théorie des groupes les raisonnements d'Euler[43] . Il est vrai que plusieurs résultats démontrés dans ses mémoires sur les résidus peuvent être transposés dans ce cadre, mais Euler n'introduit pas d'approche structurale en tant que telle : il étudie certaines propriétés d'ensembles de résidus afin d'obtenir, dans un premier temps, des résultats sur les sommes de carrés par exemple. Il est cependant remarquable qu'entre [Euler, 1760b] et les mémoires plus tardifs consacrés à la théorie des résidus, leur statut évolue sensiblement, dans le sens qui est décrit par Enrico Guisti sur le thème plus général de la naissance des objets mathématiques :

> On remarque même une caractéristique importante du processus de génération de nouveaux objets : ceux-ci entrent d'abord comme *instruments de recherche*, méthodes démonstratives tirées d'idées novatrices. Dans un second temps ils deviennent *solutions de problèmes* et aussi *objets d'étude*. C'est au terme de ce processus qu'ils acquièrent une véritable existence objective [Guisti, 2000, p. 33].

Dans le cadre des recherches d'Euler, les résidus ont passé l'étape d'être seulement des "instruments de recherche" en tant qu'outils efficaces pour obtenir des résultats sur les

43. Par exemple, dans [Weil, 1984], le titre d'un des paragraphes de l'étude des travaux d'Euler en théorie des nombres est « The multiplicative group modulo N » [Weil, 1984, p. xii] et l'auteur indique notamment :

> Whether or not these observations gave Euler the primary motive for exploring group-theoretical concepts further, he obviously gave much thought to them, from 1745 to the end of his life [Weil, 1984, p. 190].
>
> [...]Next in linecomes the paper entitled « *Theoremata arithmetica nova methodo demonstrata* » , based this time on Chapters 4 to 7 of the *Tractatus* ; the "new method" is here the group-theoretic investigation of the additive and multiplicative groups modulo an arbitrary integer N, with the calculation of the order $\varphi(N)$ of the latter group... [Weil, 1984, p. 196].

sommes de carrés, et sont devenus des "solutions de problèmes" ([Euler, 1783a]) et des objets d'étude (dans les mémoires consacrés aux résidus quadratiques ou aux résidus de puissances).

Euler met en avant l'intérêt de l'utilisation et de l'étude des résidus, qui permettent de traduire les problèmes en lien avec la divisibilité et ouvre ainsi la voie à de nouvelles méthodes et de nouveaux concepts en théorie des nombres. Mais on remarque que Lagrange parvient à prouver *in fine* les mêmes résultats initiaux sans les résidus, développant du même coup d'autres directions de recherche. Cette alternative est essentielle pour situer les travaux des mathématiciens français du début du XIX^{e} siècle.

CHAPITRE 6

La place des résidus dans deux traités de théorie des nombres (Legendre et Gauss) : 1798-1801

Dans ce chapitre, notre objectif n'est pas de décrire de manière approfondie ces traités de théorie des nombres de Legendre et de Gauss, mais de les resituer dans notre problématique : nous montrons d'une part que Legendre n'utilise pratiquement pas les résidus dans les différentes éditions de son traité, et nous détaillons d'autre part les sections de l'ouvrage de Gauss qui sont à la base des recherches arithmétiques de Poinsot et Cauchy [1].

I Les résidus dans l'*Essai sur la théorie des nombres* de Legendre (1798)

Lorsque Legendre (1752-1833) publie son premier *Essai sur la théorie des nombres*, il est déjà renommé en tant que mathématicien. Il est effectivement associé de l'Académie des Sciences de Paris depuis 1785 et obtient un des six postes de la section mathématique lors de la réouverture de l'Académie en 1795.

1 - Préface et plan de l'ouvrage

Le traité de Legendre commence par une préface où l'auteur dresse un panorama de l'histoire de la théorie des nombres. Il résume notamment les travaux d'Euler dans ce domaine, en indiquant par exemple que ce dernier a prouvé plusieurs théorèmes de Fermat, à savoir le petit théorème de Fermat et le théorème des deux carrés et qu'il a donné « la démonstration de beaucoup de Théorèmes sur les puissances des nombres, et particulièrement de ces propositions négatives avancées par Fermat, que la somme ou la différence de deux cubes ne peut être un cube[...] » [Legendre, 1798, p. vij]. Par contre, il ne fait référence à aucun moment aux résultats sur les résidus traités par Euler. Pourtant, Legendre connaît certains mémoires dans lesquels Euler étudie et utilise les résidus de puissances. En effet, dans son premier mémoire de théorie des nombres, présenté en 1785 à l'Académie puis publié en 1788, il indique dans son introduction que les premiers

1. Plus généralement, l'importance des congruences dans l'ouvrage de Gauss et sa réception dans la communauté savante au XIX^{e} siècle ont été étudiés dans [Goldstein et al., 2007]. Nous avons par ailleurs abordé les recherches d'Euler sur les résidus et qui sont en partie reprises par Gauss dans le chapitre précédent. Ces travaux ne constituent néanmoins pas l'unique source pour Gauss : Maarten Bullynck a également mis en avant l'influence qu'ont pu avoir sur Gauss les travaux de Lambert et de Hindenburg d'une part et les manuels allemands d'arithmétique qui contiennent des problèmes de reste d'autre part : voir [Bullynck, 2009] et [Bullynck, 2006].

théorèmes qu'il expose sont déjà contenus dans [Euler, 1761b] et [Euler, 1783c]. Or, comme nous l'avons vu dans le précédent chapitre, Euler utilise les résidus dans les énoncés et démonstrations exposés dans ces deux mémoires. Néanmoins, dans [Legendre, 1788], Legendre ne reprend pas les preuves d'Euler et énonce tous les résultats en termes de divisibilité.

Legendre fait d'ailleurs référence à ce mémoire publié en 1788, intitulé *Recherches d'analyse indéterminée*, à plusieurs reprises. Il rappelle par exemple qu'il y a déjà énoncé et démontré [2] la « loi générale qui existe entre deux nombres premiers quelconques, et qu'on peut appeler *loi de réciprocité* » [Legendre, 1798, p. viij].

Il donne également des indications sur sa vision de la théorie des nombres dans une note :

> Je ne sépare point la théorie des nombres de l'analyse indéterminée, et je regarde ces deux parties comme ne faisant qu'une seule et même branche de l'analyse algébrique. En effet, il n'est pas de Théorème sur les nombres qui ne soit relatif à la résolution d'une ou de plusieurs équations indéterminées. Ainsi, quand on assure, d'après Fermat, que tout nombre premier $4n+1$ est la somme de deux quarrés, c'est comme si on disait que l'équation $A = x^2 + y^2$ est toujours résoluble tant que A est un nombre premier de forme $4n+1$ [Legendre, 1798, p. ix].

Cette observation est très importance car elle permet de comprendre pourquoi Legendre, dans ses travaux de théorie des nombres, raisonne principalement en termes d'équations indéterminées et n'intègre pratiquement pas les méthodes de Gauss. D'autre part, ce lien théorie des nombres-équations indéterminées amène naturellement au lien congruences-équations que nous avons retrouvé dans les mémoires des savants français commentés dans la première partie.

Le traité de Legendre est composé de quatre parties. La première contient surtout des méthodes sur la résolution d'équations indéterminées, ainsi que des paragraphes sur les fractions continues. La seconde, intitulée *propriétés générales sur les nombres*, contient plusieurs théorèmes rencontrés fréquemment dans notre première partie, dont la loi de réciprocité quadratique, ainsi que des résultats sur les formes quadratiques. Dans la troisième partie, Legendre donne des résultats sur les nombres décomposables en une somme de trois carrés. La quatrième et dernière partie contient de nouveaux résultats sur les équations indéterminées. Un paragraphe est notamment consacré à la résolution en nombres entiers de l'équation indéterminée $x^n - b = ay$, qui correspond à la congruence binôme $x^n - b \equiv 0 \pmod{a}$.

Ici, nous allons commenter quelques extraits des deuxième et quatrième parties de Legendre afin de montrer quelles sont les formulations utilisées par ce savant avant la publication des *Disquisitiones Arithmeticae*.

2. Sa démonstration est néanmoins incomplète : voir [Lemmermeyer, 2000, p. 6-9].

2 - Deuxième partie (1) : quelques théorèmes sur les nombres

Dans cette deuxième partie, les premiers théorèmes énoncés par Legendre sont le petit théorème de Fermat (article 129), le théorème de Wilson (article 130) et le théorème de Lagrange sur le nombre maximum de racines entières d'une congruence en fonction de son degré (article 132). Comme Lagrange, Legendre énonce ces théorèmes en termes de divisibilité. Ainsi,le théorème de Wilson est énoncé ainsi : « *Si n est un nombre premier, le produit* $1.2.3\dots(n-1)$ *augmenté d'une unité sera divisible par* n » [Legendre, 1798, art. 130]. Pour démontrer ce théorème, il utilise des arguments de la forme : lorsqu'on néglige les multiples de n, on a $m^{n-1} = 1$ d'après le théorème précédent (le petit théorème de Fermat). Il fait cependant des commentaires sur les restes dans l'article suivant pour en déduire que $\left(1.2.3\dots\frac{n-1}{2}\right)^2 \pm 1$ est divisible par n selon que n est de la forme $4k+1$ ou $4k-1$: il observe que « les nombres $n-1$, $n-2$, $n-3$, &c. considérés comme restes de la division par n, sont équivalents aux restes -1, -2, -3, &c. ; d'ailleurs n étant supposé impair, le nombre des facteurs 1, 2, $3\dots n-1$ sera pair. Donc le produit $1.2.3\dots(n-1)$, divisé par n laissera le même reste que $\pm 1^2.2^2.3^2\dots\left(\frac{n-1}{2}\right)^2$, le signe ambigu étant + lorsque n est de la forme $4k+1$ et − lorsqu'il est de la forme $4k-1$ » [Legendre, 1798, art. 131].

Dans tout le traité, Legendre utilise à plusieurs reprises ce type d'observations sur les restes, mais il ne va jamais plus loin : il ne donne ou n'utilise aucune propriété opératoire des résidus par exemple.

3 - Deuxième partie (2) : symbole de Legendre et loi de réciprocité quadratique

Dans les articles 134 et 135, Legendre donne une caractérisation de ce que l'on appelle les résidus quadratiques, et introduit le symbole de Legendre. Il montre d'abord qu'un nombre premier c divise x^2+N si et seulement si $(-N)^{\frac{c-1}{2}}-1$ est divisible par c et justifie ensuite l'introduction du symbole qui lui est ensuite associé :

> Nous avons démontré que N étant un nombre quelconque, et c un nombre premier qui ne divise pas N, la quantité $N^{c-1}-1$ est toujours divisible par c ; cette quantité est le produit de deux facteurs $N^{\frac{c-1}{2}}+1$, $N^{\frac{c-1}{2}}-1$; il faut donc que l'un ou l'autre de ces deux facteurs soit divisible par c ; d'où nous conclurons que la quantité $N^{\frac{c-1}{2}}$ divisée par c, laissera toujours le reste +1 ou le reste −1.
>
> (135) *Comme les quantités analogues à* $N^{\frac{c-1}{2}}$ *se rencontreront fréquemment dans le cours de nos recherches, nous emploierons le caractère abrégé* $\left(\frac{N}{c}\right)$*, pour exprimer le reste que donne* $N^{\frac{c-1}{2}}$ *divisée par* c *; reste qui, suivant ce qu'on vient de voir, ne peut être que* +1 *ou* −1 [Legendre, 1798, art. 134-135]

Legendre utilise notamment ce nouveau symbole afin d'exprimer le théorème qu'il appelle lui-même *loi de réciprocité* le plus simplement possible.

En effet, le mémoire de 1785 contient déjà l'énoncé de la loi de réciprocité. Avant de formuler le théorème, Legendre précise quelques notations :

> Comme il sera principalement question des nombres premiers dans ce qui suit, & que leurs différentes formes donnent lieu à différentes propriétés, nous désignerons par A, a, α, A', & c. ceux de la forme $4n+1$, par B, b, β, B', & c. ceux de la forme $4n-1$, & par les autres lettres, ceux dont la forme n'est pas déterminée. Nous avertissons aussi que cette expression $\delta^{\frac{c-1}{2}} = 1$ ou -1 suppose qu'on a rejeté les multiples de c dans le premier membre [Legendre, 1798, p. 516].

L'énonce de la loi de réciprocité alors proposé par Legendre est composé de huit théorèmes différents de la forme : « Si $b^{\frac{a-1}{2}} = 1$, il s'ensuit que $a^{\frac{b-1}{2}} = 1$ » [Legendre, 1788, p. 516]. Il résume ensuite ces huit théorèmes en observant que les deux expressions intervenant dans chaque théorème donnent une valeur différente seulement lorsque les deux nombres sont de la forme $4n-1$.

En 1798, il donne une formulation beaucoup plus courte de la loi de réciprocité, en utilisant son symbole : si m et n sont des nombres premiers, alors $\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}.\left(\frac{n}{m}\right)$ Il reprend néanmoins son premier énoncé divisé en huit propositions pour donner une nouvelle démonstration incomplète du théorème.

Ainsi, Legendre introduit ici une notation qui lui permet de simplifier son énoncé. Il l'utilise d'ailleurs de nombreuses fois. Il détermine par exemple la valeur de $\left(\frac{2}{p}\right)$, c'est-à-dire le caractère quadratique de 2, mais sans utiliser la théorie des restes. Il n'utilise le mot "résidu" qu'une seule fois dans tout son traité, dans la section sur la résolution des « équations symboliques » [Legendre, 1798, p. 239]. Mais là encore, Legendre n'applique aucune opération sur ces résidus et emploie ce mot comme synonyme de reste de division euclidienne.

4 - Résolution des équations $x^n - b = ay$

Dans la quatrième partie, il consacre une section à ce que nous appelons les congruences binômes, qu'il note $x^n - b = ay$. Le théorème II concerne notamment le cas où $b = 1$, qui est un exemple fondamental pour la théorie de la cyclotomie développée par Gauss ensuite. Voici le théorème démontré par Legendre :

> Théorème II. Étant proposée l'équation $\frac{x^n-1}{a} = e$ dans laquelle a est un nombre premier, et n un diviseur de $a-1$, en sorte qu'on ait $a-1 = a'n$,
>
> 1°. On aura $x = u^{a'}$, u étant un nombre quelconque non divisible par a.
>
> 2°. Si θ est une valeur de x, θ^m en sera une aussi, quelque soit l'exposant m.
>
> 3°. Si le nombre θ est tel que $\theta^{\frac{n}{\nu}} - 1$ ne soit pas divisible par a, ν étant un diviseur premier de n, la formule $x = \theta^m$ contiendra toutes les solutions de l'équation

proposée, lesquelles seront 1, θ, $\theta^2 \ldots \theta^{n-1}$, ou les restes de ces quantités divisées par a.

4°. Non-seulement il y a plusieurs nombres θ qui jouissent de cette propriété, mais le nombre en est $n\left(1-\frac{1}{\nu}\right)\left(1-\frac{1}{\nu'}\right)\left(1-\frac{1}{\nu''}\right)$& c., ν, ν', ν'', & c. étant les différents nombres premiers qui peuvent diviser n [Legendre, 1798, art. 348].

Avec le vocabulaire d'Euler, le troisième point signifie que si θ^n est la plus petite puissance de θ dont le résidu est l'unité, alors toutes les puissances 1, θ, θ^2, ..., θ^{n-1} sont les solutions de l'équation initiale. Si $n = a-1$, le quatrième point du théorème revient à dire qu'il y a $\varphi(a)$ racines primitives du nombre a. Legendre obtient donc ici un théorème dont Euler n'a pas réussi à donner une démonstration complète dans [Euler, 1774]. Néanmoins, là encore, les formulations des deux mathématiciens sont très différentes. Dans [Euler, 1774], Euler étudie les résidus de puissances d'un nombre, c'est-à-dire les résidus d'une progression géométrique, et en déduit qu'il existe toujours un résidu tel que ses différentes puissances donnent la série complète de résidus, à savoir tous les nombres de 1 à $a-1$. Ici, Legendre donne des théorèmes sur la résolution d'une équation indéterminée, et ne met pas en avant la particularité du cas où $n = a-1$.

5 - Legendre et la théorie des résidus : un premier bilan

Finalement, la première édition du traité de Legendre est dans la ligné des travaux arithmétiques de Lagrange : ses recherches restent principalement centrées sur les équations indéterminées et les formes quadratiques ; il considère quelques fois des restes, ce qui permet de simplifier la formulation de certains énoncés, mais n'applique pas les propriétés propres aux résidus données précédemment par Euler. Enfin, les résultats énoncés par Euler en termes de résidus le sont par Legendre en termes de divisibilité (théorèmes de Fermat et de Wilson) et d'équations indéterminées.

II Les congruences et les résidus dans les *Disquisitiones Arithmeticae* de Gauss : un aperçu et quelques détails

1 - Contenu et structure de l'ouvrage

Les *Disquisitiones Arithmeticae*[3] de Gauss débutent précisément par l'introduction d'un nouvel objet : les congruences. Contrairement à Legendre qui ne reprend pas du tout les travaux d'Euler sur les résidus, Gauss reprend, traduit, développe et approfondit cette catégorie de résultats d'Euler à l'aide des congruences. De même, contrairement à

3. Rappelons que toutes nos citations des *Disquisitiones Arithmeticae* sont empruntées à la traduction française publiée en 1807.

Legendre, l'« arithmétique transcendante » ne se réduit pas à l'analyse indéterminée pour Gauss :

> Les Recherches contenues dans cet Ouvrage appartiennent à cette partie des Mathématiques où l'on considère particulièrement les nombres entiers, quelquefois les fractions, mais où l'on exclut toujours les nombres irrationnels. L'Analyse *indéterminée* ou de *Diophante*, qui apprend à distinguer, parmi les solutions d'un problème indéterminé, celles qui sont entières, ou du moins rationnelles et le plus souvent positives, ne constitue pas cette doctrine, mais elle en est une partie très-distincte ; elle a avec elle à-peu-près le même rapport que l'Algèbre, c'est-à-dire, l'art de réduire ou de résoudre les équations, avec l'Analyse universelle.
>
> [...]On voit par là que l'on doit distinguer deux parties dans l'Arithmétique, et que les considérations dont nous venons de parler se rapportent à l'Arithmétique élémentaire, tandis que les recherches générales sur les affections particulières aux nombres entiers sont revendiquées par l'*Arithmétique transcendante* [Gauss, 1801, Préface].

Le livre de Gauss, rappelons-le, se compose de sept sections. Dans la première section, Gauss définit la notion de congruence, puis en donne les premières propriétés. Dans la deuxième, il donne des théorèmes généraux sur les entiers, comme la propriété de décomposition unique en facteurs premiers, et aborde également les congruences linéaires ainsi que notre actuelle fonction d'Euler. Dans la troisième, Gauss expose différents résultats sur les résidus de puissances, en rappelant notamment la définition d'une racine primitive d'un nombre premier et en introduisant la notion d'indice. La section IV est intitulée *Des congruences du second degré* ; il énonce et démontre principalement des propositions sur les résidus quadratiques et donne une première démonstration complète de la loi de réciprocité ; il propose ensuite des méthodes de résolution pour des congruences du second degré.

La section V, qui est la plus importante avec plus de 150 articles, est intitulée *Des Formes, et des Équations indéterminées du second degré* ; elle est consacrée à la théorie des formes quadratiques. Les auteurs de [Goldstein et Schappacher, 2007a] observent que Gauss aborde ce sujet sous un autre jour que ses prédécesseurs :

> Leonhard Euler, Joseph-Louis Lagrange, and Adrien-Marie Legendre had forged tools to study the representation of integers by quadratic forms. Gauss, however, moved away from this Diophantine aspect towards a treatment of quadratic forms as objects in their own right, and, as he had done for congruences, explicitly pinpointed and *named* the key tools [Goldstein et Schappacher, 2007a, p. 8].

Ainsi, Gauss introduit dès le début de cette partie une nouvelle notation : la forme $ax^2 + 2bxy + cy^2$ est notée (a, b, c). Ici, Gauss utilise à de nombreuses reprises des congruences et la théorie des résidus quadratiques, et ce, dès le premier théorème : « *Si un nombre M peut être représenté par la forme (a, b, c), de manière que les valeurs des indéterminées soient*

premières entre elles ; $b^2 - ac$ sera résidu quadratique de M » [Gauss, 1801, art. 154]. Réciproquement, il applique les résultats obtenus sur la théorie des formes quadratiques pour obtenir une deuxième démonstration de la loi de réciprocité quadratique. Gauss observe d'ailleurs vers la fin de la section une analogie entre la composition des classes de formes quadratiques et les résidus de puissances :

> On remarquera sur-le-champ l'analogie de la démonstration du théorème précédent, avec les démonstrations des n^os^ 45, 49 ; et effectivement la théorie de la multiplication des classes a une grande affinité avec le sujet traité dans la section III [Gauss, 1801, art. 306].

Dans la section VI, *Applications des différentes Recherches précédentes*, Gauss aborde notamment la décomposition de fractions, la résolution des congruences de la forme $x^2 \equiv 1 \pmod{p}$ et les équations indéterminées $mx^2 + ny^2 = A$. Il donne également des critères de primalité. Enfin, dans la dernière section, *Des équations qui déterminent les Sections circulaires*, Gauss expose une méthode pour résoudre algébriquement les équations binômes $x^n = 1$, dont l'outil clé est une racine primitive de n. Gauss remarque d'ailleurs : « La théorie de la division du cercle, ou des polygones réguliers, qui compose la section VII, n'appartient pas *par elle-même* à l'Arithmétique, mais ses *principes* ne peuvent être puisés que dans l'Arithmétique transcendante » [Gauss, 1801, Préface].

Comme notre analyse de la première partie l'a montré, les *Disquisitiones Arithmeticae* sont un des points de départ des différentes recherches en arithmétique dans la première moitié du XIX^e^ siècle. La partie de l'ouvrage la plus rapidement connue et reprise est la section VII. Néanmoins, même celle-ci a été considérée, notamment par Lagrange, comme un sujet secondaire par rapport aux travaux de Gauss sur l'astronomie. Dans son *Rapport historique sur les progrès des sciences mathématiques depuis 1789 et sur leur état actuel*, publié en 1810, Delambre cite également l'ouvrage de Gauss :

> M. Frédéric Gauss, dans l'ouvrage déjà cité, a donné une forme nouvelle à la recherche des propriétés des nombres, en considérant, sous le nom de *congruence*, la relation qui lie entre eux tous les nombres qui laissent le même reste, lorsqu'on les divise par un nombre donné. Il établit aussi sur ce modèle des congruences du second degré ; il rattache à ses principes toute l'analyse indéterminée. Cette analyse se composant d'un grand nombre de propositions isolées et assujetties à des limitations particulières, il seroit difficile d'entrer ici dans le détail des résultats nouveaux annoncés dans l'ouvrage de M. Gauss[...] [Delambre, 1810, p. 70].

Pour lui, l'ouvrage de Gauss, et donc la théorie des nombres, sont formés «d'un grand nombre de propositions isolées». Or, l'objectif de Gauss est au contraire de construire une théorie complète. En effet, Gauss prévoit de compléter son traité par une huitième section traitant « des congruences algébriques de tous les degrés » [Gauss, 1801, Préface],

à laquelle il se réfère à plusieurs reprises dans les différentes sections de son traité[4]. La structure du traité, composé de ses huit sections prévues initialement aurait été ainsi cyclique sous plusieurs aspects[5] :

> The treatise would thus have come full circle in several respects : beginning with ordinary congruences and ending with higher congruences ; encountering various periodic structures along the way : prime residues, periods of reduced quadratic forms of positive discriminant, classes of quadratic forms which are all multiples of one class, cyclotomic periods and their analogues mod p ; and proving quadratic reciprocity four separate times in the process [Goldstein et Schappacher, 2007a, p. 16].

Gauss observe explicitement l'analogie existant entre les résidus de puissances et les classes de formes quadratiques. Le comportement des racines primitives de l'équation binôme traitée dans la section VII est également semblable à celui des racines primitives des congruences binômes, et donc des résidus de puissances. Cette deuxième analogie, comme nous le verrons dans la troisième partie, est particulièrement mise en avant quelques années plus tard par Poinsot.

Finalement, les résidus et les congruences sont omniprésents dans le traité de Gauss ; nous allons ici détailler trois passages clés pour la suite de notre étude : la définition des congruences, la définition et l'utilisation des racines primitives, et la méthode de résolution des équations binômes $x^n = 1$.

2 - Section I : Définition et premières propriétés des congruences

Commençons par citer un extrait du *Report on the Theory of Numbers* de Smith, lorsqu'il rappelle pourquoi l'outil des congruences a été aussi fructueux :

> [...] the definition of a congruence involves only one of the most elementary arithmetical conceptions, that of the divisibility of one number by another. But it expresses that conception in a form so suggestive of analogies with other parts of analysis, so easily available in calculation, and so fertile in new results, that its introduction into arithmetic (by Gauss) has proved a most important contribution to the progress of the science. It will be at once evident, from the definition, that congruences possess many of the properties of equations. Thus, congruences in which the modulus is the same may be added to one another ; a congruence may be multiplied by any number ; each side of it may be raised to any power whatever, and even may be divided by any number prime to the modulus [Smith, 1859-1865, p. 40].

4. Un manuscrit intitulé *Disquisitiones generales de congruentiis* datant apparemment de 1797 semble être une version provisoire de cette huitième section : voir [Frei, 2007].

5. Les auteurs de [Goldstein et Schappacher, 2007a] discutent l'importance des systèmes, et particulièrement ceux qui reposent sur une architecture cyclique, dans la science dans l'Allemagne de la seconde moitié du XVIII^{e} siècle : voir [Goldstein et Schappacher, 2007a, p. 16-18].

Comme nous l'avons vu dans la première partie, c'est également pour les mêmes raisons que plusieurs mathématiciens font l'éloge de cette heureuse notation et l'adoptent.

Gauss consacre la section I à introduire cet objet et ses propriétés fondamentales. Nous rappelons sa définition des *nombres congrus* ou *incongrus* :

> Si un nombre a divise la différence des nombres b et c, b et c sont dits *congrus* suivant a, sinon *incongrus*. a s'appellera le module ; chacun des nombres b et c, *résidus* de l'autre dans le premier cas, et *non résidus* dans le second.
>
> Les nombres peuvent être positifs ou négatifs, mais entiers. Quant au module il doit évidemment être pris absolument, c'est-à-dire sans aucun signe [Gauss, 1801, art. 1].

Il introduit ensuite le symbole ≡ pour désigner une congruence et remarque en note :

> Nous avons adopté ce signe à cause de la grande analogie qui existe entre l'égalité et la congruence. C'est pour la même raison que Legendre, dans des mémoires que nous aurons souvent l'occasion de citer, a employé le signe même de l'égalité, pour désigner la congruence ; nous en avons préféré un autre, pour prévenir toute ambiguïté [Gauss, 1801, art. 2, Note].

Il met donc en avant dès le début de son ouvrage cette analogie qui, comme nous avons commencé à l'observer dans la première partie de notre travail, est à la base de beaucoup de travaux en lien avec les congruences. Cette analogie est d'ailleurs utilisée dans les deux sens : on transpose les propriétés des équations à celles des congruences, on utilise la correspondance équation - congruence dans les deux sens sans toujours la justifier, ... Nous détaillons quelques exemples importants dans nos parties 3 et 4.

Gauss donne ensuite quelques propriétés fondamentales des congruences : la relation de congruence est transitive, les congruences peuvent être additionnées, soustraites, multipliées entre elles. Une congruence peut également être élevée à une puissance entière positive. Il ne donne que de très brèves justifications de ces propriétés et se justifie ainsi :

> Tous les résidus d'un nombre donné a suivant le module m, sont compris dans la forme $a + km$, k étant un entier indéterminé. Les plus faciles des propositions que nous allons exposer peuvent sans peine se démontrer par-là ; mais chacun en sentira la vérité au premier aspect [Gauss, 1801, art. 4].

Il rappelle ici la correspondance existant entre les congruences, et les raisonnements que l'on peut mener en termes de multiples et de diviseur. Dans cette section, Gauss ne revient à aucun moment sur un exposé en termes de divisibilité.

Il donne également un lien entre les racines des équations et des congruences :

> On voit en général que lorsque X est de la forme $x^n + Ax^{n-1} + Bx^{n-2} + \text{etc.} + N$; A, B, C, etc., étant entiers, et n entier positif, l'équation $X = 0$, (forme à laquelle toute équation algébrique peut se ramener) n'aura aucune racine rationnelle, s'il arrive que pour un certain module la congruence $X \equiv 0$ ne soit pas satisfaite ; mais ce

caractère qui se présente ici de lui-même, sera développé davantage dans la section VIII [Gauss, 1801, art. 11].

Des raisonnements liés à cette propriété amènent certains mathématiciens, comme Poinsot et Galois par exemple [6], à introduire les racines imaginaires pour les congruences.

Il conclut cette courte première section, en rappelant que beaucoup de résultats d'arithmétique sont fondés sur les principes exposés pour les congruences. Il donne deux exemples : il démontre les critères de divisibilité par 9 et 3, puis remarque que si une égalité est vraie, alors la congruence correspondante, en prenant un module quelconque, doit également être vérifiée, ce qui donne une méthode de vérification des calculs.

Ainsi, dans cette première section, Gauss introduit la notion de nombres congrus et de congruences, en basant ses raisonnements sur des analogies avec les égalités et les équations et établit des liens entre les premières et les secondes, ce qui est fondamental pour les travaux de ses successeurs.

3 - Section III : Résidus de puissances, racines primitives et indices

La troisième section s'ouvre avec des résultats, prouvés précédemment par Euler dans [Euler, 1761b] , mais formulés en termes de congruences. Ainsi, le premier théorème est énoncé ainsi :

> *Dans toute progression géométrique* $1, a, a^2, a^3$ *etc., outre le premier terme 1, il y en a encore un autre* a^t *congru à l'unité suivant le module* p *premier avec* a*, l'exposant* t *étant* $< p$ [Gauss, 1801, art. 45].

Il reprend de manière très rapide les raisonnements exposés par Euler. Tous les termes de la progression sont non nuls, congrus à un nombre entier compris entre 1 et $p-1$; plusieurs termes auront donc le même résidu, et par division, on obtient un terme dont le résidu est l'unité. Il rappelle ensuite que la progression géométrique est périodique, chaque période étant composée des termes $1, a, a^2, \ldots, a^{t-1}$, ce qu'il formule ainsi : si $r \equiv \rho \pmod{t}$, alors $a^r \equiv a^\rho \pmod{p}$, et réciproquement

Il démontre également que t est nécessairement une partie aliquote de $p-1$, et en déduit le théorème de Fermat comme un cas particulier. On remarque ici que Gauss suit exactement le même cheminement qu'Euler [7] . Il fait d'ailleurs référence aux démonstrations d'Euler dont l'une est semblable à la sienne.

Gauss introduit alors de nouvelles notations. ψd représente la quantité de nombres inférieurs à p, dont la puissance d est la plus petite congrue à l'unité. D'autre part, il dit qu' un « nombre a appartient à l'exposant d » [Gauss, 1801, art. 53] lorsque a^d est

6. Voir partie 3.
7. Sa démonstration correspond en effet aux théorèmes 10 à 14 de [Euler, 1761b].

la plus petite puissance congrue à l'unité. En termes modernes, ψd représente le nombre d'éléments de $\mathbb{Z}/p\mathbb{Z}$ d'ordre d. Il démontre que $\psi d = \varphi(d)$ dans les articles 53 et 54. Cette égalité est importante puisqu'elle permet d'en déduire l'existence des racines primitives :

> *il existe toujours des nombres dont aucune puissance plus petite que* $p-1$ *n'est congrue à l'unité ;* il y en a même autant entre 1 et $p-1$, qu'il y a au-dessous de $p-1$ de nombres qui lui soient premiers [Gauss, 1801, art. 55].
>
> [...] Nous nommerons avec Euler, *racines primitives* les nombres qui appartiennent à l'exposant $p-1$ [Gauss, 1801, art. 57].

Il donne une deuxième démonstration de ce résultat, car « la diversité des méthodes aide beaucoup à jeter du jour sur les points les plus obscurs » [Gauss, 1801, art. 55]. On retrouve donc ici la volonté de Gauss de donner plusieurs démonstrations des résultats fondamentaux, comme le théorème de Fermat ou la loi de réciprocité quadratique, basés sur des outils différents. Rappelons que la démonstration donnée par Euler dans [Euler, 1774] est incomplète.

Il compare alors l'introduction des racines primitives dans la théorie des nombres à celle des logarithmes dans l'arithmétique. Pour une racine primitive donnée a, qu'il nomme *base*, si $a^e \equiv b \mod p$, e est nommé l'*indice* de b (de la même façon que $\log 10^3 = 3$ lorsque l'on considère le logarithme en base 10 par exemple). Il donne ensuite une série de propriétés sur les indices, en indiquant l'analogie existant avec celles sur les logarithmes :

- *L'indice d'un produit de tant de facteurs qu'on voudra, est congru à la somme des indices des différents facteurs, suivant le module* $p-1$.
- *L'indice de la puissance d'un nombre est congru, suivant le module* $p-1$*, au produit de l'exposant par l'indice du nombre donné.*

Gauss explique comment ces propriétés, ainsi que d'autres, permettent de simplifier le calcul de l'indice d'un nombre donné. Il donne une table et donne également une méthode, à condition d'avoir deux sortes de tables, pour résoudre les congruences du premier degré.

Dans les articles 60-68, il commence l'étude de l'équation $x^n \equiv A \mod p$, en notant $\sqrt[n]{A}$ les racines de cette équation. Deux de ces racines seront considérées comme distinctes si elles ne sont pas congrues modulo p. Il donne certains résultats qui s'appuie sur les outils introduits précédemment, mais il ajoute également à plusieurs reprises que ce sujet sera traité de manière plus approfondie lors de la section VIII, qui ne verra pas le jour à proprement parler. Par exemple, en parlant de l'équation $x^n \equiv 1 \mod p$:

> Quand $A \equiv 1$, et que r sera une des valeurs de l'expression $\sqrt[n]{1}(\mod p)$, ou que $r^n \equiv 1(\mod p)$, toutes les puissances de r seront aussi des valeurs de cette expression ; et il y en aura autant de différentes qu'il y a d'unités dans l'exposant auquel r appartient (n° 48). Si donc r est une valeur appartenant à l'exposant n, les puissances r, r^2, r^3, ..., r^n (où l'unité peut remplacer la dernière) renfermeront toutes

> les valeurs de l'expression $\sqrt[n]{1}(\mod p)$. Nous expliquerons plus en détails dans la section VIII comment on peut trouver ces valeurs qui appartiennent à l'exposant n.[8] [Gauss, 1801, art. 65].

Il revient sur les *racines primitives*, sur les différents systèmes que l'on obtient en prenant l'une ou l'autre de ces racines primitives et précise comment on peut passer d'un système à un autre par de simples multiplications. Ces observations sont très importantes puisqu'elles montrent que le choix de la racine primitive n'est pas essentiel. Il donne également une méthode de recherche des racines primitives par tâtonnements dans les articles 73 et 74.

Gauss démontre le théorème de Wilson en utilisant la notion d'indice, en ajoutant que sa preuve se base sur les mêmes principes que celle d'Euler.

Gauss ajoute encore du vocabulaire à sa théorie : deux nombres sont dits *associés* lorsque leur produit est congru à l'unité. Gauss attribue cette définition à Euler. On peut remarquer que c'est la définition de deux nombres inverses dans le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$. Gauss affirme, d'après la section précédente, que tout nombre n'admet qu'un seul et unique nombre associé. À part 1 et $p-1$, les autres nombres seront associés deux à deux.

Gauss conclut la troisième section en renvoyant le lecteur souhaitant des démonstrations plus détaillées aux textes d'Euler à ce sujet : [Euler, 1761b], [Euler, 1774] et les parties 5 et 8 des *Opuscula Analytica*.

Dans la section III, Gauss reprend une grande partie des résultats exposés quelques années plus tôt sur la théorie des résidus des puissances, en les reformulant à l'aide des congruences et en les complétant. Il donne des démonstrations de tous les résultats, ce qui n'est pas le cas d'Euler, et parfois même plusieurs démonstrations, basées sur des raisonnements différents. Il les complète avec des références à celles données par Euler et Lagrange. Il démontre surtout rigoureusement l'existence systématique des racines primitives, outil clé pour la méthode développée dans la section VII.

4 - La section VII ou une application de la théorie des nombres à l'algèbre

Dans la section VII, Gauss propose une méthode pour résoudre algébriquement une classe infinie d'équations : les équations de la forme $x^n - 1 = 0$ pour tout nombre entier n. L'analyse plus générale que donne Gauss sur la résolubilité de ces équations pour tout n a constitué un modèle pour la théorie des équations du début du XIX$^{\text{e}}$ siècle. Ainsi, Gauss donne non seulement la solution d'un problème géométrique, mais il démontre également un résultat très important d'algèbre, et ceci dans un traité de théorie des nombres. Afin de comprendre pourquoi les « *principes* [de la théorie de la division du cercle] ne peuvent

8. Un nombre a appartient à l'exposant n lorsque l'élément a est d'ordre n dans $\mathbb{Z}/p\mathbb{Z}$

être puisés que dans l'Arithmétique transcendante » [Gauss, 1801, Préface], nous allons résumer les principales étapes de son raisonnement en prenant appui sur la résolution d'un cas particulier[9] : l'équation $x^{13} - 1 = 0$.

(a) Préliminaires

L'équation $x^{13}-1 = 0$ admet l'unité pour racine, comme toutes les équations considérées ici. Après division par $x-1$, on obtient l'équation $x^{12}+x^{11}+x^{10}+\ldots+x+1 = 0$, notée $X = 0$, appelée équation cyclotomique, et dont toutes les racines sont des nombres complexes. Ces racines de l'unité ont la propriété d'être liées entre elles : si on désigne par r une de ces racines, alors elles peuvent s'exprimer sous la forme r^k, pour un nombre entier k compris entre 1 et 12. Comme la notation r^k sera utilisée très régulièrement dans cette section, Gauss introduit la notation : $[k] = r^k$. Voici comment Gauss présente le fonctionnement général de sa méthode :

> Le but de nos recherches, qu'il n'est pas inutile d'annoncer ici en peu de mots, est de décomposer X *graduellement* en un nombre de facteurs de plus en plus grand, et cela de manière à ce que les coefficiens de ces facteurs puissent être déterminés par des équations du degré le plus bas possible, jusqu'à ce que, de cette manière, on parvienne à des facteurs simples, ou aux racines Ω. Nous ferons voir que si l'on décompose le nombre $p-1$ en facteurs entiers quelconques α, β, γ, etc. (pour lesquels on peut prendre les facteurs premiers), X est décomposable en α facteurs du degré $\frac{n-1}{\alpha}$, dont les coefficiens seront déterminés par une équation du degré α ; que chacun de ces facteurs est décomposable en β facteurs du degré $\frac{n-1}{\alpha\beta}$, à l'aide d'une équation de degré β, etc. De sorte que ν étant le nombre de facteurs α, β, γ, etc. la recherche des racines Ω est ramenée à la résolution de ν équations des degrés α, β, γ, etc [Gauss, 1801, art. 342].

En d'autres termes, l'objectif de Gauss est de décomposer l'équation cyclotomique en une suite d'équations résolubles, dont le degré est de plus en plus bas. Le principe général utilisé par Gauss est d'ordonner d'une certaine façon les racines de l'équation afin d'obtenir des équations auxiliaires correspondant à ce qui est annoncé ci-dessus.

(b) Réindexation des racines et formation des périoes

Pour obtenir une réindexation des racines, il va utiliser l'outil introduit dans la section III : les racines primitives. Par définition, une racine primitive d'un nombre premier p est un nombre g tel que la suite de ses puissances g^k (pour k allant de 1 $p-1$ ou de 0 à $p-2$) est congrue modulo p à la suite des nombres entiers de 1 à $p-1$ (sans tenir compte de l'ordre).

9. Gauss détaille dans sa section VII le cas où $n = 19$ et $n = 17$. Nous choisissons ici de présenter sa méthode à partir du cas où $n = 13$, car c'est cet exemple que Poinsot utilise dans certains de ses mémoires, que nous étudions dans la troisième partie.

Dans le cas où $p = 13$, $g = 2$ est une racine primitive. On détermine la suite des résidus obtenus après division par 13 :

Puissances	g^0	g^1	g^2	g^3	g^4	g^5	g^6	g^7	g^8	g^9	g^{10}	g^{11}
Résidus	1	2	4	8	3	6	12	11	9	5	10	7

On peut donc exprimer les racines de l'équation $X = 0$ à l'aide d'une puissance d'une racine primitive modulo p. Au lieu de considérer la suite [1], [2], ..., [12], on travaille sur la suite : $[g^0]$, $[g^1]$, $[g^2]$, ..., $[g^{11}]$.

La méthode de Gauss consiste maintenant à partager les racines en des ensembles ayant même cardinal pour former des sommes de racines appelées *périodes* (on utilise les diviseurs du nombre 12) et à obtenir des équations auxiliaires dont les racines sont ces *périodes*[10]. Par exemple, on peut former quatre périodes de trois racines en prenant les racines de quatre en quatre dans la liste ci-dessus. On obtiendra ainsi la période $[g^0]+[g^4]+[g^8]$. Dans cette période, grâce à la réindexation des racines à partir d'une racine primitive, si on substitue la racine $[g^4]$ à $[g^0]$, on obtient la période $[g^4]+[g^8]+[g^0]$ puisque $g^{12} \equiv 1 \pmod{13}$. De même, connaître une racine d'une période permet de connaître la période complète :

> Donc deux périodes, de même nombre de termes (que nous nommerons périodes *semblables*), seront identiques, si elles ont une seule racine commune, et par conséquent il est impossible que de deux racines contenus dans une certaine période, il ne s'en trouve qu'une seule dans une période semblable... [Gauss, 1801, art. 344].

À la fin de la décomposition, on obtient des *périodes* contenant un seul terme : la résolution de l'équation auxiliaire correspondante permet alors de trouver une des racines de l'équation. La notation de Gauss pour les périodes est : (nombre de termes, un terme de la période).

(c) Décomposition graduelle de l'équation

Nous allons maintenant présenter un exemple de décomposition de l'équation cyclotomique. Pour notre exemple, le premier ensemble considéré est composé des douze racines : la période correspondante (qui peut être notée (12, [2]) par exemple) est égale à −1 (puisqu'elle correspond à la somme de toutes les racines de l'équation).

On obtient ensuite deux périodes de six éléments, en considérant les racines de deux en deux :

$$(12,1)\begin{cases} (6,1) & \dots & [1]+[4]+[3]+[12]+[9]+[10] \\ (6,2) & \dots & [2]+[8]+[6]+[11]+[5]+[7] \end{cases}$$

On détermine ensuite l'équation dont ces deux périodes sont solutions, en utilisant les relations entre coefficients et racines d'une équation : :

10. C'est dans l'article 343 que Gauss définit les périodes ; il démontre également que leur formation est indépendante de la racine primitive choisie.

$(6,1)+(6,2)=(12,1)=-1$,
$(6,1)\times(6,2)=3(12,1)=-3$,
donc les deux périodes sont solutions de l'équation quadratique[11] : $x^2+x-3=0$. On obtient ainsi facilement les valeurs des deux périodes $(6,1)$ et $(6,2)$.

On continue en considérant quatre périodes de trois racines. On décompose donc les deux périodes (6,1) et (6,2) en deux périodes de trois racines. Par exemple :

$$(6,1)\begin{cases}(3,1) & \dots & [1]+[3]+[9]\\ (3,4) & \dots & [4]+[12]+[10]\end{cases}$$

En calculant la somme $(3,1)+(3,4)$ et le produit $(3,1)\times(3,4)$, on obtient une nouvelle équation du second degré à résoudre, $x^2-(6,1)x+3+(6,2)$, dont les solutions sont les deux périodes $(3,1)$ et $(3,4)$.

La dernière étape consiste à déterminer les douze périodes d'une racine, et donc à obtenir les solutions de l'équation proposée. Par exemple, en décomposant la période (3,1) en les trois périodes (1,1), (1,3) et (1,9), et en calculant la somme, la somme des produits deux à deux, et le produit de celles-ci, on obtient une équation du troisième degré, $x^3-(3,1)x^2+(3,4)x-1=0$ dont les solutions sont trois racines de l'équation initiale $x^{13}-1=0$.

Bien sûr, dans ce cas précis, on obtient des équations auxiliaires du deuxième et du troisième degrés que l'on sait résoudre par radicaux. Dans d'autres cas, pour l'équation $x^{11}-1=0$ par exemple, on obtient notamment des équations auxiliaires du cinquième degré qui, a priori, ne sont donc pas nécessairement résolubles par radicaux.

Gauss donne des précisions à ce sujet dans l'article 359 :

> Les recherches précédentes avaient pour but de trouver les équations auxiliaires ; nous allons maintenant exposer sur leur résolution une propriété digne de remarque. On sait que tous les travaux des plus grands géomètres ont échoué contre la résolution générale des équations qui passent le premier degré, ou pour mieux définir l'objet de la recherche, contre la réduction des équations complètes à des équations à deux termes, et il est à peine douteux si ce problème ne renferme pas quelque chose d'impossible, plutôt qu'il ne surpasse les forces actuelles de l'analyse.[...] Il est certain néanmoins qu'il y a une infinité d'équations composées dans chaque degré, qui admettent une telle réduction, et nous espérons faire plaisir aux géomètres, en prouvant que nos équations auxiliaires sont toujours dans ce cas. Mais à cause de l'étendue du sujet, nous ne présenterons que les principes les plus importants qui sont nécessaires pour démontrer cette possibilité, différant à un autre temps une "exposition plus complète" [Gauss, 1801, art. 359].

Enfin, il conclut la section VII en revenant à la résolution du problème géométrique

11. Pour obtenir le coefficient 3, il suffit d'effectuer le produit et de regrouper les puissances pour former des expressions dont on connaît les valeurs.

initial :

> Il suit de là généralement que pour la division géométrique du cercle en N parties soit possible, N doit être 2 ou une puissance de 2, *ou bien* un nombre premier de la forme $2^m + 1$, *ou encore* le produit d'une puissance de 2 par un ou plusieurs nombres premiers différens de cette forme ; ou d'une manière plus abrégée, il est nécessaire que N ne renferme aucun diviseur impair qui ne soit de la forme $2^m + 1$, ni plusieurs fois un même diviseur premier de cette forme[Gauss, 1801, art. 366].

(d) Premiers résultats sur les sommes de Gauss

Nous terminons la présentation de la section VII par les résultats contenus dans l'article 356. Gauss y considère toujours l'équation $x^n - 1 = 0$, où n est un nombre premier, r une racine primitive de cette équation, et g une racine primitive du nombre n. Il donne les valeurs de ce qui sera ensuite appelé les sommes de Gauss quadratiques, c'est-à-dire les sommes de la forme $\sum_{j=0}^{n-1} e^{i\frac{2j^2\pi}{n}} = \sum_{x \pmod n} \left(\frac{x}{n}\right) e^{i\frac{2x\pi}{n}}$, lorsque n est impair, sans facteur carré. Il insiste d'abord sur le lien existant entre les équations auxiliaires obtenues à partir de sa méthode et la théorie des nombres : « elles sont liées d'une manière étonnante avec les propriétés les plus abstraites du nombre n » [Gauss, 1801, art. 356]. Les sommes de Gauss quadratiques correspondent à l'équation auxiliaire obtenue lors de la première étape de la méthode, c'est-à-dire lorsque l'on considère deux périodes composées de $\frac{n-1}{2} = m$ termes. Une des périodes est composée des racines r^{g2k}, $0 \leq k \leq \frac{n-1}{2}$, où les résidus des exposants sont les résidus quadratiques de n, et l'autre période contient les autres racines, celles dont les exposants sont les non-résidus quadratiques de n. Il note donc : $(m,1) = [1] + [R] + [R'] + \ldots$ et $(m,g) = [N] + [N'] + [N''] + \ldots$, où R, R', $\ldots$, désignent les résidus quadratiques de n, et où N, N', $\ldots$, sont les non-résidus quadratiques de n.

Ces deux périodes sont donc racines de l'équation quadratique $x^2 - Sx + P$, où $S = (m,1) + (m,g) = -1$ et $P = (m,1) \times (m,g)$ Il détermine ensuite les différentes valeurs possibles de P en fonction de la forme du nombre n, et en s'appuyant sur le fait que le produit P est une fonction linéaire des deux périodes et de $(m,0)$, et symétrique des deux périodes $(m,1)$ et (m,g).

Il conclut alors :

> Ainsi, quelque soit la racine que l'on ait prise pour [1], si l'on désigne par $\sum[R]$ la somme de toues les racines [1], $[R]$, $[R']$, etc., et par $\sum[N]$ celle des racines $[N]$, $[N']$, etc. On aura
>
> $$\sum[R] - \sum[N] = \pm\sqrt{n}, \text{ ou } = i \pm \sqrt{n},$$
>
> suivant que $n \equiv 1$ ou $\equiv 3 \pmod 4$. Il suit facilement de là que k étant un nombre

entier quelconque non divisible par n, on a

$$\sum \cos \frac{kRP}{n} - \sum \cos \frac{kNP}{n} = \pm\sqrt{n}, \text{ ou } = 0,$$

$$\sum \sin \frac{kRP}{n} - \sum \sin \frac{kNP}{n} = 0, \text{ ou } = \pm\sqrt{n},$$

suivant que $n \equiv 1$ ou $\equiv 3 \pmod 4$, théorèmes remarquables par leur élégance[Gauss, 1801, art. 356].

Gauss termine en indiquant le signe de ces sommes selon que k est résidu quadratique ou non de n, sans donner de démonstration. Il publiera une preuve de ce dernier résultat dans [Gauss, 1811]. Comme nous l'avons observé dans notre première partie, ces résultats sont repris à de nombreuses occasions des années plus tard. Dirichlet en donne une preuve en 1835 à partir de méthodes d'analyse de Fourier. Parmi les mathématiciens ayant repris ces résultats, soit en essayant d'en obtenir de nouvelles preuves, basées sur des outils différents, soit pour en déduire d'autres résultats, on peut citer Jacobi, Cauchy, Eisenstein ou encore Hermite [12]. Nous reviendrons sur le travail de Cauchy en lien avec ces sommes dans la quatrième partie.

Finalement, à partir de la considération d'expressions construites à partir des racines primitives, Gauss obtient des résultats d'algèbre - la résolution algébrique des équations binômes - pour en déduire des résultats d'analyse - sur les sommes de fonctions circulaires - et de géométrie - sur la division du cercle.

(e) En guise de conclusion : les réceptions de la section VII

Ainsi, même si le principal résultat démontré dans cette section est un théorème d'algèbre permettant de résoudre un très ancien problème de géométrie, la théorie des nombres, représentée par les racines primitives, est fondamentale ici. C'est grâce à la structure cyclique de l'ensemble des racines de l'unité, et à leur réindexation à l'aide d'une racine primitive, que la méthode de résolution proposée par Gauss fonctionne.

Comme nous l'avons observé dans la première partie, la section VII a été reprise très rapidement en France : Lacroix intègre la méthode de résolution des équations binômes dans sa section *Des propriétés des nombres* de la troisième édition de ses *Compléments aux éléments d'algèbre* dès 1804. Lagrange en propose en 1808 une simplification dans la quatorzième note de la deuxième édition de son *Traité de la résolution des équations numériques de tous les degrés, avec des Notes sur plusieurs points de la Théorie des équations algébriques*, en la simplifiant : il utilise l'expression des racines de l'unité pour des degrés inférieurs, évite ainsi la considération d'équations auxiliaires et n'a donc pas à démontrer leur résolubilité. Lagrange met en valeur les propriétés particulières des racines

12. À ce sujet, voir [Patterson, 2007].

de l'unité construites à partir d'une racine primitive et s'appuie ensuite sur ce que Gauss appelle les périodes.

Dans ces deux reprises, la question de géométrie initiale n'est pas mise en avant : Lagrange n'y fait aucune allusion, et Lacroix y consacre une courte note à la fin de son exposé.

Dans les années 1810, la section VII est également reprise ou au moins citée dans plusieurs ouvrages. On peut penser [13] au traité de théorie des nombres de Barlow, publié en 1811, dont le chapitre VII de la deuxième partie est consacré à la *division du cercle analytique et géométrique* [Barlow, 1811, p. 479 - 505]. La méthode de Gauss est utilisée comme exemple par Hegel dans sa réflexion sur la nature des démonstrations dans *Wissenschaft der Logik*, publié entre 1812 et 1816. Les *Disquisitiones Arithmeticae*, et en particulier la section VII, font partie de la liste d'ouvrages recommandés par Babbage aux membres de la nouvelle Cambridge Analytical Society dans la préface du premier volume des *Memoirs of the Analytical Society*, publié en 1813. De plus, comme nous l'avons indiqué dans notre première partie, la réindexation des racines de l'unité utilisée dans la section VII est très souvent reprise dans beaucoup de travaux de théorie des nombres du XIX^{e} siècle [14].

5 - Après les *Disquistiones Arithmeticae* : des preuves supplémentaires de la loi de réciprocité quadratique

Trois mémoires de Gauss sont publiés en 1808, 1811 et 1818, dans les mémoires de Göttingen [15]. Ces trois textes tournent autour du même sujet : les résidus et les lois de réciprocité. Gauss ajoute quatre nouvelles démonstrations de la loi de réciprocité quadratique [16] aux deux premières déjà présentées dans les *Disquisitiones Arithmeticae*. Certaines de ces preuves sont élémentaires - basées uniquement sur des principes arithmétiques et sont notamment réinterprétées géométriquement par Eisenstein dans [Eisenstein, 1844b], une s'appuie sur la théorie des formes quadratiques. La quatrième démonstration donnée par Gauss est basée sur l'égalité, que l'on note (A) :

$$1 + r + r^4 + r^9 + \ldots + r^{(n-1)^2} = i^{\frac{1}{4}(n-1)^2}\sqrt{n},$$

où n est un nombre premier et r une racine primitive de l'équation $x^n = 1$. La démonstration de cette égalité, et la détermination du signe ambigu, a occupé pendant longtemps

13. Nous reprenons ici une partie de la liste donnée dans [Goldstein et Schappacher, 2007a, p. 21].
14. Nous le verrons particulièrement chez Poinsot et Cauchy dans nos troisième et quatrième parties.
15. Il est difficile d'avoir une idée précise la facilité d'accès à ces textes en France. Il semble néanmoins que ces livres aient été présents à Paris, au moins dans la bibliothèque Sainte-Geneviève, et ce assez rapidement après leur publication (d'après les informations données par les responsables de cette bibliothèque).
16. Voir [Smith, 1859-1865, art. 18-22] à ce sujet.

Gauss [17] et ses successeurs. La formule (A) permet également d'obtenir des égalités liant le symbole de Legendre et les fonctions circulaires, en fonction de la forme du nombre premier n. Comme on l'a vu précédemment, de nombreux travaux utilisent ou étudient ce type de formules. La sixième preuve proposée par Gauss s'appuie sur l'étude des expressions de la forme $\sum_{i=0}^{p-2}(-1)^i x^k g^i$, où p est un nombre premier, g est une racine primitive de p, k est un nombre premier avec p et x est une indéterminée. Ces expressions sont aujourd'hui appelées "sommes de Gauss". Là encore, de nombreux travaux - dont ceux de Jacobi et Cauchy pour ne citer qu'eux - ont pour thème l'étude de ces expressions, ou d'expressions similaires.

Gauss justifie cette recherche de preuves nouvelles sur la théorie des résidus quadratiques ainsi :

> C'est à partir de 1805 que j'ai travaillé sur la théorie des résidus cubiques et biquadratiques [...] J'ai trouvé des théorèmes par induction [...] qui montrent une analogie remarquable avec les théorèmes sur les résidus quadratiques. D'autre part, les tentatives pour obtenir des démonstrations complètes ont été inutiles. Cela a constitué la motivation pour essayer d'ajouter encore des preuves à celles déjà connues sur les résidus quadratiques, dans l'espoir que parmi les différentes méthodes données, l'une ou l'autre contribue à la découverte d'arguments proches [pour les résidus cubiques et quadratiques] [18].

Gauss tente ici de poser un cadre général afin de pouvoir étudier les résidus d'ordre supérieur. Ce thème est repris à sa suite et les textes qu'il publie entre 1808 et 1818 jouent le rôle, comme les *Disquisitiones Arithmeticae*, mais dans une moindre mesure, de point de départ pour de nombreuses recherches. C'est en 1825 que Gauss présente à l'Académie de Göttingen ses premiers travaux sur les résidus biquadratiques et sur les entiers complexes de la forme $a+b\sqrt{-1}$, où a et b sont des nombres complexes. Là encore, ce mémoire, publié en 1828, sera repris à partir des années 1830.

17. Un des mémoires sur ce sujet est [Gauss, 1811].
18. Cette traduction est issue de la traduction présentée dans [Cox, 1989, p. 87]. Voici l'extrait original :

> Scilicet quum inde ab anno 1805 theoriam residuorum cubicorum atque biquadraticorum [...] Protinus quidem theoremata ea, quae has quaestiones prorsus exhauriunt, et in quibus mira analogia cum theorematibus ad residua quadratica pertinentibus eminet, per inductionem detectafuerunt, quam primum via idonea quaesita essent : omnes vero conatus, ipsorum demonstrationibus ex omni parte perfectis potiundi, per longum tempus irriti manserunt. Hoc ipsum incitamentum erat, ut demonstrationibus iam cognitis circa residua quadratica alias aliasque addere tantopere studerem , spe fultus, ut ex multis methodis di- versis una vel altera ad illustrandum argumentum affine aliquid conferre posset. Quae spes neutiquam vana fuit , laboremque indefessum tandem successus pro- speri sequuti sunt [Gauss, 1818, p. 50].

III Les deux éditions suivantes de la *Théorie des nombres* de Legendre (1808-1830)

La deuxième édition de l'*Essai sur la théorie des nombres* de Legendre paraît en 1808. Puis, en 1830, Legendre en fait publier une troisième édition, alors intitulée *Théorie des nombres*[19] et composée de deux tomes. L'objectif de cette section est de comprendre l'influence de l'ouvrage de Gauss sur Legendre et de mettre en avant les principales différences entre ces deux éditions et la première, du point de vue des résidus et des congruences.

Remarquons enfin que dans ces deux nouvelles éditions, Legendre présente les travaux d'autres mathématiciens, souvent très rapidement : il reproduit ainsi, en utilisant son vocabulaire, deux démonstrations de la loi de réciprocité quadratique de Gauss et Jacobi et la démonstration du théorème de Fermat pour les nombres polygones donnée par Cauchy en 1815.

1 - L'Avertissement

Les deux éditions de 1808 et 1830 sont précédées d'un *Avertissement*. Dans celle de 1808, Legendre indique qu'il a intégré deux parties des *Disquisitiones Arithmeticae* de Gauss : la théorie de la cyclotomie, présentée dans une nouvelle cinquième partie, ainsi qu'une de ses démonstrations de la loi de réciprocité quadratique. Puis il ajoute :

> On aurait désiré enrichir cet Essai d'un plus grand nombre des excellens matériaux qui composent l'ouvrage de M. Gauss : mais les méthodes de cet auteur lui sont tellement particulières qu'on n'aurait pu, sans des circuits très-étendus, et sans s'assujétir au simple rôle de traducteur, profiter de ses découvertes [Legendre, 1808, Avertissement, p. vj].

L'*Avertissement* de la troisième édition ne contient plus ce commentaire. Néanmoins, dans ces ouvrages, Legendre ne mentionne à aucun moment la notion de *congruence* introduite par Gauss dans ses recherches que Legendre a étudiées. De même, il n'utilise que très peu de fois le terme "résidu".

Comme il l'annonce lui-même, les trois premières parties de son traité abordent les mêmes thèmes dans les trois éditions. En particulier, Legendre énonce toujours les théorèmes de Fermat, Wilson et Lagrange en termes de divisibilité.

19. Legendre justifie ce changement par les améliorations apportées à cette troisième édition :

> L'ouvrage ayant ainsi reçu tous les perfectionnements que l'auteur a pu lui procurer, tant par ses propres travaux que par ceux des autres géomètres dont il a pu profiter, on a cru devoir lui donner définitivement le titre de *Théorie des nombres*, au lieu de celui d'*Essai* sur cette Théorie qu'il avait porté jusqu'à présent [Legendre, 1830, vol. 1, Avertissement].

2 - La loi de réciprocité quadratique

Il introduit de la même manière son symbole $\left(\frac{a}{b}\right)$, mais prouve des propriétés opératoires supplémentaires. Ainsi, en 1808, Legendre détermine les valeurs de $\left(\frac{-a}{p}\right)$ et $\left(\frac{a}{p}\right).\left(\frac{b}{p}\right)$ en fonction de $\left(\frac{a}{p}\right)$ et $\left(\frac{b}{p}\right)$.

Il tente également d'achever sa propre démonstration de la loi de réciprocité quadratique, en vain. Il intègre donc d'autres démonstrations. Ainsi, dans l'édition de 1808, Legendre reprend une des démonstrations données par Gauss :

> Il [les *Disquisitiones Arithmeticae* de Gauss] contient particulièrement une démonstration directe et fort ingénieuse de la loi de réciprocité déjà citée ; démonstration qu'on se proposait d'insérer avec des développements plus étendus, dans cette seconde Édition. Mais l'Auteur étant parvenu depuis à en trouver une beaucoup plus simple et plus élégante, on a exposé de préférence cette dernière dans le §VII de la quatrième partie [Legendre, 1808, Avertissement, p. vj].

La démonstration de Gauss évoquée ici est celle de [Gauss, 1808], qui s'appuie sur ce qu'on appelle aujourd'hui le lemme de Gauss. Ainsi, Legendre intègre très rapidement les travaux de Gauss dans son traité, en les reformulant avec ses propres outils : il utilise les restes et quelques égalités dans lesquelles il ne tient pas compte des multiples de p, mais n'intègre pas les congruences et continue de raisonner en termes de divisibilité.

En 1830, il donne à nouveau cette preuve et ajoute également dans la sixième partie une autre démonstration qu'il attribue à Jacobi : en effet, ce dernier expose les principales étapes de cette nouvelle démonstration [20] dans une lettre adressée à Legendre [21]. Cette démonstration est fondée sur les principes de la méthode de résolution des équations binômes exposée par Gauss dans la septième section, et reprise par Legendre dans la cinquième partie de son traité. Avant de faire quelques remarques sur cette cinquième partie, nous revenons sur la résolution équations indéterminées que Legendre note $x^n - b = ay$.

3 - Une nouvelle notation pour symboliser certaines équations indéterminées

La résolution des congruences binômes est toujours traitée par Legendre sous la forme d'équations indéterminées $x^n - b = ay$ dans ses deux dernières éditions. Il donne les mêmes théorèmes que dans la première édition, mais introduit une notation qui est ensuite reprise, comme nous l'avons vu dans notre première partie, par Poinsot et Binet notamment :

20. Cette preuve est néanmoins très proche de la sixième démonstration proposée par Gauss dans [Gauss, 1818]. Nous revenons sur ce sujet dans notre quatrième partie, Cauchy ayant également présenté une version très proche de cette preuve en 1829 puis 1840.

21. Voir [Legendre et Jacobi, 1875].

il désigne par $M(a)$ un multiple quelconque du nombre a. Avec ce nouveau symbole, Legendre obtient ainsi des équations indéterminées, comme $x^n - 1 = M(a)$, où une seule inconnue apparaît, ce qui est bien plus proche des congruences de Gauss.

4 - Cinquième partie : la théorie de la cyclotomie de Gauss revue par Legendre

Dans les deux éditions, la présentation de la théorie de la cyclotomie par Legendre est proche de celle de Gauss[22] et il reprend des notations similaires : par exemple, si r est une racine complexe de l'équation binôme $x^n - 1 = 0$, alors (α) désigne la racine r^α. De même, si g est une racine primitive de n, il note que la suite (α), (αg), (αg^2), …, (αg^{n-2}) contient toutes les racines différentes de l'unité de l'équation $x^n - 1 = 0$. Néanmoins, en 1808, Legendre n'introduit pas les périodes en opérant sur les exposants de la racine primitive g, mais en observant que, si $n - 1 = mk$, l'« équation indéterminée $x^{n-1} - 1 = M(n)$, qui devient $x^{mk} - 1 = M(n)$, pourra se décomposer en un nombre k d'équations de la forme $x^m - A = M(n)$ » [Legendre, 1808, art. 444]. Il en déduit que les solutions de $x^{n-1} - 1 = M(n)$ sont « partagées en k groupes de chacun m termes » [Legendre, 1808, art. 444]. Il nomme ces différents groupes les *périodes* et remarque que chacune de ces périodes est « rentrante » [Legendre, 1808, art. 445]. Ainsi, une fois de plus, Legendre fonde sa méthode sur la décomposition d'équations indéterminées, plutôt que sur les puissances de la racine primitive considérée. En 1830, la manière dont il présente la formation des périodes, qu'il qualifie alors de « suite circulaire » [Legendre, 1830, vol. 2, art. 493], est plus proche de celle de Gauss.

5 - Legendre et la théorie des résidus et des congruences : un deuxième bilan

La lecture des deux éditions de 1808 et 1830 du traité de théorie des nombres de Legendre montre qu'il connaît bien les *Disquisitiones Arithmeticae* de Gauss, ainsi que certains de ses travaux ultérieurs : il intègre effectivement dès 1808 la preuve de la loi de réciprocité donnée par Gauss cette même année. De même, il reprend la méthode de résolution des équations binômes de Gauss en la modifiant légèrement. Néanmoins, il n'intègre pas dans ses travaux les congruences et l'étude des résidus, qui est pourtant au cœur du livre de Gauss. Comme il le dit lui-même dans sa préface, Legendre estime que la théorie des nombres et l'analyse indéterminée ne forment qu'une seule matière et ses travaux arithmétiques sont donc principalement axés sur la considération d'équations indéterminées.

22. Les différences entre ces deux éditions et l'ouvrage de Gauss du point de vue de la théorie de la cyclotomie sont particulièrement commentées dans [Maigre, 2007].

Conclusion

Cette partie nous a permis d'expliciter les sources auxquelles se réfèrent les différents écrits arithmétiques de la première moitié du XIX^{e} siècle. Du point de vue d'une histoire centrée sur les résidus et les congruences, la filiation Euler-Gauss apparaît évidemment essentielle. Leurs recherches de théorie des nombres intègrent de manière centrale ces deux outils. Euler met en avant des idées importantes, comme la représentation par un seul résidu d'une infinité de nombres de la même forme, et énoncent de nombreuses propriétés des résidus de puissances, notamment quadratiques. Il utilise des méthodes de plus en plus exclusivement arithmétiques. Gauss reprend les travaux d'Euler, et construit une théorie des nombres fondée sur les résidus et les congruences ; il complète les démonstrations d'Euler et établit ainsi une théorie centrée autour de ces deux outils sur des bases solides.

Du point de vue des résidus et des congruences, nous avons vu une approche arithmétique alternative qui n'assimile pas ces deux outils et se focalise surtout sur la résolution des équations indéterminées. Contrairement à Euler, qui intègre progressivement les résidus au cœur de ses recherches sur les formes quadratiques, les étudie pour eux-mêmes et (même s'il s'appuie encore sur des raisonnements formulés en termes de divisibilité) et emploie très rapidement des expressions de la forme $a = \alpha^2 \pm np$ au lieu de "$a - \alpha^2$ est divisible par p", Lagrange, qui développe pourtant des recherches importantes sur les formes quadratiques, n'utilise pratiquement jamais d'arguments basés sur les restes, raisonne toujours en termes de divisibilité, et introduit dans ses preuves des outils étrangers à la théorie des nombres. Par exemple, il emploie dans sa démonstration du théorème des quatre carrés les différences finies, outil qu'Euler n'utilise que dans les premiers écrits analysés ici. Ainsi, les deux mathématiciens abordent des thèmes communs, comme le théorème des quatre carrés et le théorème de Wilson par exemple, leurs recherches se répondent, ils reprennent les résultats ou les formes de démonstrations de l'autre, mais ils construisent systématiquement des preuves basées sur leurs propres outils.

Or cette alternative subsiste au début du XIX^{e} siècle, comme en témoignent les traités de théorie des nombres de Legendre et de Gauss. Ces ouvrages n'ont pas été écrits à la même période de leur carrière scientifique : en 1801, Gauss est un jeune savant de 24 ans tandis que Legendre est un géomètre établi, membre de l'Institut de France. L'ouvrage de Legendre contient notamment des résultats déjà obtenus par Euler et Lagrange. C'est également le cas du traité de Gauss, mais presque tous les théorèmes y sont reformulés à l'aide des nouvelles notions qui y sont introduites. Nous ne retrouvons pas le même phénomène de réponses successives entre Legendre et Gauss qu'entre Euler et Lagrange puisque Gauss ne publie qu'une édition des *Disquisitiones Arithmeticae* et les recherches

arithmétiques qu'il entreprend ensuite sont tout à fait étrangères aux sujets de recherche de Legendre. Néanmoins, nous avons observé des caractéristiques similaires à celles que nous avons trouvées chez Euler et Lagrange : Gauss fonde sa théorie des nombres sur les résidus et les congruences, tandis que Legendre assimile la théorie des nombres à l'analyse indéterminée. Il intègre totalement certaines des méthodes et démonstrations de Gauss (comme une preuve de la loi de réciprocité et la théorie de la cyclotomie) mais ne modifie pas la structure principale de son traité, toujours axé sur l'analyse indéterminée quelque soit l'édition. Par exemple, Legendre n'utilise *jamais* le mot "congruence" dans aucune des trois éditions de sa *Théorie des nombres* !

Au début du XIX^{e} siècle, nous retrouvons ces pratiques multiples pour la théorie des nombres. On remarque que ces différences sont aussi associées à des enjeux disciplinaires, car fondre l'arithmétique et l'algèbre plus étroitement peut être perçu comme un avantage ou un inconvénient selon les auteurs. La première forme de pratique, qui s'appuie sur les écrits de Lagrange et Legendre, base presque uniquement la théorie des nombres sur l'étude des équations indéterminées et des formes quadratiques. La seconde, issue des recherches d'Euler et Gauss, ajoute à ces thèmes, des outils centraux à la théorie des nombres : les résidus et les congruences. Les objets de la théorie des nombres se sont diversifiés, aux équations diophantiennes et formes s'ajoutent les résidus et les congruences. Plusieurs mathématiciens français se focalisent toujours sur les premiers objets, même s'ils intègrent les outils et idées fournis par l'étude des seconds. C'est ce que nous allons examiner en détail dans les travaux arithmétiques de deux de ces savants, Poinsot et Cauchy [23].

23. Nous avons justifié leur choix dans notre première partie.

PARTIE III

Louis Poinsot et la théorie de l'ordre (1808-1845)

Introduction

L'objectif de cette partie est d'analyser les travaux en théorie des nombres et en algèbre de Louis Poinsot (1777-1859). Ce savant [24] occupe plusieurs fonctions au sein de la communauté scientifique française au début du XIX^{e} siècle : professeur à l'École Polytechnique et inspecteur général de l'Université dès 1809, puis Inspecteur des études [25] en 1815, élu à l'Institut en 1813 dans la classe des mathématiques à la mort de Lagrange, collaborateur au *Bulletin de Férussac* à partir de 1824. Dans ses publications, peu nombreuses [26], Poinsot aborde essentiellement la mécanique, la géométrie de situation et la théorie des nombres. C'est surtout pour les deux premières qu'il est très connu : ses *Éléments de statique* connaîtront douze éditions par exemple [27] ; son premier mémoire de géométrie, publié en 1809, sur la théorie des polygones et des polyèdres, reçoit également des éloges, et est notamment repris par Cauchy.

Pourquoi étudier les travaux de Poinsot en algèbre et théorie des nombres ? Même si, à première vue, Poinsot semble faire pâle figure devant les Gauss, Cauchy, ou encore Niels Henrik Abel que l'on retrouve dans toutes les histoires des mathématiques, nous avons vu dans notre première partie que ses travaux de théorie des nombres entrent dans la perspective caractéristique de certains auteurs français où des analogies entre équations et congruences sont particulièrement mises en avant. Au cours de nos recherches, nous avons également rencontré plusieurs références à ce mathématicien qui laissent à penser que ses travaux en algèbre et théorie des nombres ne sont pas passés inaperçus au XIX^{e} siècle. Par exemple, en 1843, Liouville fait référence à l'analyse faite par Poinsot en 1808 du *Traité des équations numériques de tous les degrés* de Lagrange dans le cadre d'un conflit avec Libri [28] :

24. Il existe très peu d'informations sur la vie de Poinsot, que ce soit dans les archives ou dans les correspondances. Joseph Bertrand nous livre quelques anecdotes de la vie de Poinsot dans un éloge historique [Bertrand, 1890] mais il est difficile d'en tirer des conclusions totalement fiables.

25. Voir [Caplat, 1986, p. 557]. Il sera mis à la retraite le 22 septembre 1824 en tant qu'inspecteur général à l'avènement de Charles X. En 1840, il intégrera le Conseil royal de l'Université, puis sera chargé de la préparation de la réforme des études scientifiques en 1845, par le ministre Salvandy.

26. Dans [Crosland, 1992, p. 206], l'auteur commente ce fait en même temps que l'élection de Poinsot à l'Académie en remplacement de Lagrange en 1813 : « Poinsot lived on until 1859, proving to be one of the least productive membres of the Academy in the 1820s, 30s, 40s and 50s ». À côté de ses publications, la Bibliothèque de l'Institut de France possède 18 portefeuilles contenant des manuscrits de Poinsot. On y trouve des brouillons et textes de Poinsot relatifs à la mécanique, à l'enseignement, à l'algèbre et à la théorie des nombres. Dans la partie concernant la théorie des nombres, beaucoup de feuillets sont des réflexions sur la théorie des équations et des congruences ainsi que des recherches sur le dernier théorème de Fermat. Nous étudierons d'ailleurs ici un mémoire sur la théorie des permutations trouvé dans ces manuscrits.

27. La thèse de Patrice Bailhache est d'ailleurs une analyse de certains travaux de Poinsot en mécanique et statique. Voir [Poinsot et Bailhache, 1975].

28. Bruno Belhoste et Jesper Lützen détaillent les relations *détestables* entre Liouville et Libri - et en particulier le conflit dont il est question ici - dans [Belhoste et Lützen, 1984]. Ce n'était pas le premier heurt entre les deux hommes puisque dès 1838, Liouville a dénoncé à l'Académie des erreurs importantes

> Pour m'épargner la rédaction que j'aurais d'ailleurs beaucoup moins bien faite, je viens de copier le passage de la préface de M. Poinsot, publiée dès 1808 dans le *Magasin encyclopédique*. M. Poinsot avait spécialement en vue les équations binômes, mais le raisonnement est général, et, pour qui comprend bien cette théorie, il devait l'être. Aussi, c'est le cas de dire que la démonstration du théorème se trouvait d'*avance* dans l'article de M. Poinsot [29].

On retrouve également d'autres références à Poinsot jusqu'à la fin du XIX[e] siècle. Rappelons par exemple que Poinsot est inclus par Smith dans [Smith, 1859-1865] dans la liste des quelques savants, qui, selon lui, ont développé le domaine de la théorie des nombres à partir du traité de Gauss [30]. Poinsot est également cité dans *Les mathématiques en Portugal*[31], de Rodolphe Guimarães, à l'occasion d'un aperçu des sciences mathématiques de la première moitié du XIX[e] siècle :

> Nous sommes, donc, à la moitié du XIX[e] siècle : avec une théorie des nombres, dûe à Gauss, les groupant en classes moyennant les équations de congruence, qui s'élève jusqu'à la notion de nombre complexe ; avec les élégantes investigations de Poinsot, qui font dépendre l'Arithmétique et l'Algèbre de l'ordre et de la combinaison ; avec une Algèbre qui, en délaissant les fâcheuses et peu fécondes élucubrations que l'on devait appliquer dans la pratique, se renferme avec les théorèmes de Sturm et Cauchy, pour suivre une autre direction, soumise au concept de groupe des *substitutions*[Guimarães, 1900, p. 7].

Ces deux auteurs prêtent donc à Poinsot une place surprenante dans l'évolution de l'algèbre et la théorie des nombres au XIX[e] siècle. L'ouvrage de Smith est une source importante pour l'histoire de la théorie des nombres tandis que la seconde vient d'un livre

contenues dans un travail de Libri. Dans le cas présent, le litige s'est produit quelques semaines après l'élection de Libri au Collège de France - élection dont il était finalement le seul candidat après les démissions de Cauchy et Liouville. Le 14 août 1843, Liouville soumet à l'Académie un rapport sur un mémoire de Hermite relatif à la division des fonctions abéliennes. Hermite y développe une méthode analogue à celle utilisée par Abel en 1827 pour déterminer la division des intégrales elliptiques. À la fin de l'exposé, Libri prend la parole pour affirmer que c'est lui qui a démontré pour la première fois la division en parties égales de la lemniscate, et donc également résolu les équations relatives aux fonctions elliptiques. Une semaine plus tard, Liouville répond aux réclamations de Libri. Ce dernier base sa requête sur un théorème qu'il a énoncé sans démonstration devant l'Académie en 1825 - mais qui n'a été publié qu'en 1833 - et qu'il a développé en 1830 seulement. On trouvera les détails de l'argumentation de Liouville dans les *Comptes rendus hebdomadaires des séances de l'Académie des Sciences* de l'année 1843 (tome 17, pages 327 - 334). Liouville formule correctement le résultat en question ainsi : « Quand les racines d'une équation algébrique peuvent être *toutes* rangées en cercle de telle manière que chacune d'elles se déduise de la précédente et engendre la suivante par une seule et même opération rationnelle, cette équation est nécessairement résoluble à l'aide de radicaux. », résultat dont il paraphrase ensuite la démonstration donnée par Poinsot en 1808. Toujours dans le cadre de ce conflit, Liouville annonce également son intention de publier les écrits de Galois lors de la séance du 4 septembre 1843. Pour une étude du contexte de cette publication, voir [Ehrhardt, 2010].

29. *Comptes rendus hebdomadaires des séances de l'Académie des Sciences*, tome 17, année 1843, p. 332.

30. Voir page 122.

31. La première édition de cet ouvrage a été publiée en 1900, à l'occasion de l'Exposition Universelle de Paris.

certes beaucoup moins connu, mais qui, à la fin du XIX^{e} siècle, place Poinsot parmi les quelques mathématiciens marquants de l'évolution de l'arithmétique et de l'algèbre. Nous voulons donc essayer de comprendre pourquoi Poinsot semble être pour certains savants un chaînon non négligeable dans le développement de ces deux domaines.

Il existe cinq publications de Poinsot relatives à l'algèbre et la théorie des nombres :

- un commentaire publié dans le *Moniteur universel* du 21 mars 1807 à l'occasion de la traduction française par Poullet - Delisle des *Disquisitiones Arithméticae* de Gauss ;
- un commentaire du *Traité des équations numériques de tous les degrés* de Lagrange paru en 1808 dans le *Magasin encyclopédique* ;
- un *Extrait de quelques recherches nouvelles sur l'algèbre et la théorie des nombres* lu en 1817 à l'Académie des Sciences puis publié en 1818 dans les *Mémoires de la classe des sciences mathématiques et physiques de l'Institut de France* ;
- un *Mémoire sur l'application de l'algèbre à la théorie des nombres* publié en 1820 dans le *Journal de l'École Polytechnique* ;
- des *Réflexions sur les principes fondamentaux de la théorie des nombres*, publiées dans le *Journal de Mathématiques Pures et Appliquées* en 1845.

Dans l'ensemble de ses textes, Poinsot lie la théorie des nombres, l'algèbre et la géométrie autour d'une notion centrale : la théorie de l'*ordre*. Notre objectif est donc d'essayer de comprendre ce que signifie cette idée, son origine et en quoi la façon de voir de Poinsot a pu avoir une influence sur l'histoire de la théorie des nombres et de l'algèbre. Par exemple, en mettant en avant cette idée, Poinsot dégage explicitement la théorie des équations de la recherche des valeurs numériques des solutions pour se concentrer sur relations entre racines. On peut donc en particulier se demander quel rôle son travail joue dans le développement qui conduit du point de vue de Gauss à celui de Galois.

Pour cela, nous partageons cette partie en deux chapitres. Dans un premier chapitre, nous étudions en détails les textes de 1808, 1818, 1820, ainsi qu'un des manuscrits de Poinsot dans lequel il développe ses idées sur les permutations dans le cadre de la théorie algébrique des équations. Nous ne revenons pas sur le commentaire des *Disquisitiones Arithmeticae* par Poinsot qui montre surtout que ce dernier est un des lecteurs parisiens de l'ouvrage dès le tout début du XIX^{ème} siècle, comme Lagrange, Legendre ou S. Germain, et un promoteur de sa lecture dans les cercles lettrés. Nous analysons les écrits de Poinsot jusqu'en 1820 en prenant principalement les *Disquisitiones Arithmeticae* comme point de comparaison pour mettre en avant ce que Poinsot apporte par rapport au traité de Gauss. Cet examen nous permet ainsi de comprendre les pratiques arithmétiques et algébriques de Poinsot et de caractériser sa théorie de l'ordre. Le second chapitre est consacré aux différentes réceptions des travaux arithmétiques de Poinsot. Nous verrons ainsi qu'à partir de 1845, les références à la théorie de l'ordre de Poinsot sont plus nombreuses. C'est pourquoi nous entrecoupons ce chapitre par l'analyse de certains extraits du

mémoire de Poinsot publié en 1845. En effet, ce dernier texte, plus tardif, consiste en une synthèse approfondie sur plusieurs résultats de théorie des nombres. Poinsot n'y présente pas d'idées novatrices par rapport à ses travaux précédents : c'est la raison pour laquelle nous n'en donnons pas une étude détaillée comme pour les écrits publiés précédemment, mais n'abordons que certains points de ce travail.

CHAPITRE 7

Louis Poinsot et la théorie de l'ordre (1808 - 1820)

I 1808 : analyse du traité de Lagrange ou une première présentation "à la Poinsot" de la section VII des *Disquisitiones Arithmeticae*

Comme nous l'avons signalé dans notre première partie, la deuxième édition du *Traité de la résolution des équations numériques de tous les degrés* de Lagrange est publiée en 1808. Poinsot rédige un commentaire sur l'ouvrage, publié en 1808 dans le *Magasin encyclopédique, ou Journal des sciences, des lettres et des arts*[1]. Ce commentaire est d'ailleurs intégré au début de la troisième édition posthume publiée en 1826 du *Traité* de Lagrange, vraisemblablement par Poinsot[2], avec une note indiquant qu'il « a reçu l'approbation de M. Lagrange ». Nous étudions ici des extraits de l'analyse de Poinsot relatifs à la définition de l'algèbre, la résolution algébrique des équations puis au cas particulier de la résolution algébrique des équations binômes.

1 - Une première définition de l'algèbre

Au début de son analyse, Poinsot donne une définition de l'algèbre, domaine alors souvent assimilé à la théorie des équations[3] :

> D'abord si l'on jette un coup d'œil général sur l'Algèbre, on voit que cette science, abstraction faite des opérations ordinaires (au nombre desquelles on peut compter l'élimination), se partage naturellement en trois articles principaux. 1°. La théorie générale des équations, c'est-à-dire l'ensemble des propriétés qui leur sont communes à toutes. 2°. Leur résolution générale, qui consiste à trouver une expression composée des coefficiens de la proposée, et qui, mise au lieu de l'inconnue, satisfasse identiquement à cette équation, et que tout s'y détruise par la seule opposition des signes. 3°. La résolution des équations numériques, où il suffit de trouver des valeurs particulières qui satisfassent d'une manière aussi approchée qu'on le voudra, à une équation dont tous les coefficiens sont actuellement connus et donnés en nombre[Poinsot, 1808, p. 345 - 346].

1. Voir [Poinsot, 1808].
2. Poinsot lui-même semble être à l'origine de cette édition. En effet, l'ouvrage se termine par une note de Poinsot commentant une correction faite par Lagrange. De plus, seuls les noms de Lagrange et Poinsot apparaissent dans la présentation de l'ouvrage.
3. Par exemple, dans [Sinaceur, 1991, p. 51], l'auteur indique que cette définition restera la plus courante jusqu'à la fin du XIX^{e} siècle.

Dans l'introduction de son *Traité*, Lagrange expose un point de vue légèrement différent : il divise également la théorie des équations en trois parties mais, pour lui, la résolution numérique des équations n'est pas à proprement dit une partie de l'algèbre :

> Il faut bien distinguer la résolution des équations numériques de ce qu'on appelle en Algèbre la résolution générale des équations. La première est, à proprement parler, une opération arithmétique, fondée à la vérité sur les principes généraux de la théorie des équations, mais dont les résultats ne sont que des nombres, où l'on ne reconnaît plus les premiers nombres qui ont servi d'éléments, et qui ne conservent aucune trace des différentes opérations particulières qui les ont produits.
>
> [...] Aussi conviendrait-il de donner dans l'Arithmétique les règles de la résolution des équations numériques, sauf à renvoyer à l'Algèbre la démonstration de celles qui dépendent de la théorie générale des équations[Lagrange, 1808, p. 13-14].

La définition de l'algèbre qu'il donne ensuite est plus générale que celle de Poinsot :

> L'Algèbre plane pour ainsi dire également sur l'Arithmétique et sur la Géométrie ; son objet n'est pas de trouver les valeurs mêmes des quantités recherchées ; mais le système d'opérations à faire sur les quantités données pour en déduire les valeurs des quantités qu'on cherche, d'après les conditions du problème. Le tableau de ces opérations représentées par les caractères algébriques, est ce qu'on nomme en Algèbre une formule ; et lorsqu'une quantité dépend d'autres quantités, de manière qu'elle peut être exprimée par une formule qui contient ces quantités, on dit alors qu'elle est une fonction de ces mêmes quantités.
>
> L'Algèbre, prise dans le sens le plus étendu, est l'art de déterminer les inconnues par des fonctions des quantités connues, ou qu'on regarde comme connues ; et la résolution générale des équations consiste à trouver pour toutes les équations d'un même degré, les fonctions des coefficiens de ces équations qui peuvent en représenter toutes les racines[Lagrange, 1808, p. 14-15].

En 1808, pour Lagrange, Poinsot et certainement la plupart des mathématiciens, l'algèbre est donc considérée comme une science où l'on doit déterminer des inconnues en fonction de valeurs données. Ici, nous allons voir cette notion évoluer sensiblement chez Poinsot.

Dans son commentaire, Poinsot donne ensuite une présentation succincte des méthodes développées par Lagrange dans le cadre de la résolution numérique des équations dans les cinq premières pages de son analyse. Les neuf pages restantes sont consacrées au résumé et commentaire des réflexions de Lagrange et de Gauss sur « le problème si fameux de la résolution générale des équations »[Poinsot, 1808, p. 359]. Poinsot commence par citer des mathématiciens ayant produit des travaux dans le cadre de cette théorie, en insistant sur les écrits de Vandermonde et de Lagrange. Il donne notamment les idées générales développées par Lagrange pour la résolution générale des équations, ainsi que les principaux points du raisonnement de Gauss pour la résolution générale des équations

binômes. Nous allons dans chacun de ces deux cas résumer les raisonnements développés par Lagrange et Gauss dans leurs œuvres avant de considérer l'analyse qu'en fait Poinsot.

2 - La théorie générale des équations

(a) Les *Réflexions sur la résolution algébrique des équations* de Lagrange (1770)

En 1770 paraît l'ouvrage *Réflexions sur la résolution algébrique des équations* de Lagrange [4]. Son objectif est annoncé dès l'introduction de son mémoire :

> Je me propose dans ce Mémoire d'examiner les différentes méthodes que l'on a trouvées jusqu'à présent pour la résolution algébrique des équations, de les réduire à des principes généraux et de faire voir *a priori* pourquoi ces méthodes réussissent pour le troisième et le quatrième degré, et sont en défaut pour les degrés ultérieurs. Cet examen aura un double avantage : d'un côté il servira à répandre une plus grande lumière sur les résolutions connues du troisième et du quatrième degré ; de l'autre il sera utile à ceux qui voudront s'occuper de la résolution des degrés supérieurs, en leur fournissant différentes vues pour cet objet et en leur épargnant surtout un grand nombre de pas et de tentatives inutiles[Lagrange, 1772-1773, p. 206-207].

L'originalité de ce travail consiste en ce qu'il ne contient pas une suite de nouveaux résultats et méthodes ; il réside en un bilan critique des méthodes présentées jusque là pour les équations que l'on sait résoudre afin de dégager des principes communs pour guider les recherches ultérieures sur la théorie algébrique des équations. Les deux premières sections contiennent une analyse des méthodes connues pour la résolution des équations générales des troisième et quatrième degrés. Lagrange y observe que les méthodes déjà connues s'appuient sur la résolution d'une équation auxiliaire, appelée dans un premier temps *réduite*, et que l'on peut ramener à un degré inférieur à celui de l'équation proposée. La troisième section englobe des réflexions sur la résolution des équations de degré supérieur à 4. Dès le début, Lagrange revient entre autres sur la méthode exposée par Bézout. Dans ses travaux sur la théorie algébrique des équations [5], ce dernier obtient une *réduite* du cent-vingtième degré pour l'équation du cinquième degré, qui équivaut à une équation du vingt-quatrième degré. Selon lui, sa difficulté ne doit pas dépasser celle d'équations de degré inférieur à 5. Lagrange exprime son scepticisme à ce sujet :

> Mais cette conclusion, si j'ose le dire, me paraît un peu forcée, car j'avoue que je ne vois pas bien clairement ce qui pourrait empêcher que l'expression des racines

4. On pourra notamment se reporter à [Neumann, 2007a], [Neumann, 2007b], [Hamburg, 1976/77] et [Houzel, 2002, chap. 4 et 5] pour une analyse de certains passages de ce mémoire. Lagrange n'est pas le seul mathématicien à avoir publié un travail sur la résolution algébrique des équations à cette période. Edward Waring fait publier en 1770 les *Meditationes Algebricae* et Alexandre-Théophile Vandermonde, dans son *Mémoire sur la résolution des équations* paru en 1774, résume les différentes questions à résoudre pour la résolution générale des équations et propose une méthode de résolution pour l'équation binôme de degré 11.

5. Voir [Bézout, 1764] et [Bézout, 1765]. Nous renvoyons en particulier à [Alfonsi, 2005] pour une étude des travaux de Bézout.

de l'équation du vingt-quatrième degré dont il s'agit ne contint encore des radicaux cinquièmes ; du moins il n'est pas démontré que cela ne puisse absolument avoir lieu ; ainsi il pourrait bien arriver que cette équation du vingt-quatrième degré renfermât encore toutes les difficultés de l'équation proposée du cinquième degré ; auquel cas, après avoir trouvé cette équation par des calculs très-pénibles, on n'en serait que plus éloigné de la résolution de l'équation proposée.

[...] Il serait donc fort à souhaiter que l'on pût juger *a priori* du succès que l'on peut se promettre dans l'application de ces méthodes aux degrés supérieurs au quatrième... [Lagrange, 1772-1773, p. 307].

Lagrange doute donc de pouvoir arriver à la résolution algébrique des équations de degré supérieur à 4 à partir de sa méthode. Pour introduire la quatrième section, intitulée « Conclusion des réflexions précédentes, avec quelques remarques générales sur la transformation des équations, et sur leur réduction ou abaissement à un moindre degré »[Lagrange, 1772-1773, p. 355], Lagrange résume les principes généraux aboutissant à une méthode de résolution *a priori* :

On a dû voir par l'analyse que nous venons de donner des principales méthodes connues pour la résolution des équations, que ces méthodes se réduisent toutes à un même principe général, savoir à trouver des fonctions des racines de l'équation proposée, lesquelles soient telles : 1 ° que l'équation ou les équations par lesquelles elles seront données, c'est-à-dire dont elles seront les racines (équations qu'on nomme communément les *réduites*), se trouvent d'un degré moindre que celui de la proposée, ou soient au moins décomposables en d'autres équations d'un degré moindre que celui-là ; 2 ° que l'on puisse en déduire aisément les valeurs des racines cherchées.
L'art de résoudre les équations consiste donc à découvrir des fonctions des racines, qui aient les propriétés que nous venons d'énoncer ; mais est-il toujours possible de trouver de telles fonctions, pour les équations d'un degré quelconque, c'est-à-dire pour tel nombre de racines qu'on voudra ? C'est sur quoi il paraît très-difficile de se prononcer en général[Lagrange, 1772-1773, art. 86].

Voyons maintenant sur quels principes s'appuient la formation des équations auxiliaires[6]. Elles doivent être invariables sous toute permutation des racines de l'équation proposée[7]. Si l'équation initiale est de degré n, alors l'équation auxiliaire est de degré $n!$. Afin d'abaisser le degré de ces équations auxiliaires, Lagrange met en avant l'importance des racines de l'unité qui ont une particularité intéressante du point de vue des permutations : si l'on considère l'équation $x^n - 1 = 0$, il existe toujours une racine r de cette équation telle que ses différentes puissances r^i (pour i allant de 1 à n) donnent l'ensemble

6. On trouve dans les travaux de Lagrange les termes *réduite* et *résolvante*. La *réduite* désigne une équation auxiliaire formée à partir des coefficients de l'équation initiale et dont les racines sont des fonctions rationnelles des racines de l'équation proposée. La *résolvante* est une équation, ou un ensemble d'équations, donnant l'expression des racines de la *réduite* en fonction des racines de l'équation initiale. Selon [Vuillemin, 1993, p. 79], Lagrange confond parfois l'utilisation de ces deux termes.

7. Cela vient du fait que les coefficients d'une équation sont des fonctions symétriques de ses racines.

des solutions de l'équation $x^n - 1 = 0$, c'est-à-dire l'ensemble des racines n^e de l'unité. Ainsi, remplacer dans une expression r par une de ses puissances induit une permutation circulaire des différentes racines. Utiliser les racines de l'unité pour former les équations auxiliaires permet ainsi d'abaisser leur degré.

Les travaux de Lagrange mettent en avant non seulement les problèmes à résoudre pour la résolution algébrique des équations mais également l'importance des permutations et des racines de l'unité en tant qu'outils de cette résolution.

(b) L'analyse de Poinsot

Dans le commentaire de Poinsot relatif à la théorie générale des équations, on distingue deux parties : il commence par résumer quelques découvertes concernant la théorie générale des équations, avant de s'intéresser au cas particulier des équations pour lesquelles on connaît des relations entre les racines.

Après avoir donné une petite chronologie du sujet de Cardan à Bezout, Poinsot conclut :

> Toutes ces méthodes dépendent de l'exécution actuelle d'un calcul, et l'on n'y voit point qu'on doive arriver, à moins qu'on n'arrive effectivement : or, par la nature du problème, la longueur des calculs croît avec une telle rapidité, que la question ne peut plus être aujourd'hui de chercher la formule, mais simplement de prédire la suite des opérations qui y conduirait à coup sûr. Aucune de ces méthodes ne peut donc satisfaire l'esprit, et c'est à des idées plus hautes sur la nature des équations qu'il faut s'élever à présent pour découvrir s'il y a ou non une route certaine qui ferait parvenir à leur résolution générale[Poinsot, 1808, p. 360].

Poinsot donne ici les objectifs que doivent se fixer, selon lui, les mathématiciens travaillant sur la théorie générale des équations : il ne faut plus chercher une formule explicite donnant les solutions de l'équation générale de degré n en fonction de ses coefficients - comme cela a été fait pour les équations de degrés 2, 3 et 4 - mais plutôt trouver une méthode pour démontrer qu'une équation est résoluble sans pouvoir nécessairement développer des calculs explicites. Ces idées sont déjà mises en avant par Lagrange dès 1770, qui prône une méthode permettant de déterminer *a priori* afin d'éviter les calculs « pénibles »[8]. On retrouve d'ailleurs un commentaire très semblable[9] dans la préface écrite

8. Voir l'extrait cité plus haut, page 222.

9. Ce passage du texte de Galois est notamment commenté dans la thèse de Caroline Ehrhardt : [Ehrhardt, 2007, p. 92-93]. On peut d'ailleurs également citer un passage du *Discours Préliminaire* où Galois suit la même idée :

> Il existe, en effet, pour ces sortes d'équations, un certain ordre de considérations Métaphysiques qui planent sur tous les calculs, et qui souvent les rendent inutiles. Je citerai, par exemple, les équations qui donnent la division des fonctions Elliptiques et que le célèbre Abel a résolues. Ce n'est certainement pas d'après leur forme numérique que ce géomètre y est parvenu. Tout ce qui fait la beauté et à la fois la difficulté de cette théorie, c'est qu'on

par Galois des années plus tard pour ses mémoires : « Le moment arrivera où les spéculations des analystes ne trouveront plus ni le temps ni la place de se produire ; à tel point qu'il faudra se contenter de les avoir prévues »[Galois, 1908, p. 25-26].

Pour Poinsot et Galois, il faut donc *prévoir* ou *prédire* les calculs, sans les effectuer. Ainsi, en analysant les travaux de Lagrange sur la théorie des équations, Poinsot met en avant une idée générale sur la théorie des équations qui sera suivie quelques années plus tard par le jeune Galois : il faut adopter des raisonnements dont les fondements ne sont pas dans les calculs mais dans « des idées plus hautes sur la nature des équations ».

Poinsot présente ensuite les idées générales contenues dans les travaux de Vandermonde et Lagrange sur la théorie générale des équations. Il insiste notamment sur le lien mis en avant par Lagrange entre la résolution générale des équations et la théorie des permutations, ainsi que sur l'intérêt de considérer les racines de l'unité :

> Car, il est clair actuellement que le problème peut revenir à celui-ci : trouver des fonctions des racines qui soient telles d'abord qu'on en puisse aisément dégager ces racines, et en second lieu, qui ne dépendent que d'équations inférieures à la proposée dont les coefficients soient connus ou dépendent eux-mêmes d'équations aussi inférieures à cette proposée[10]. M. Lagrange choisit une fonction linéaire des racines : l'équation qui la donnerait et qu'on peut actuellement construire, s'élèverait au degré marqué par le nombre des permutations qu'on pourrait faire entre toutes ces racines, et passé le 2e degré, serait toujours plus haute que la proposée. Mais si l'on a soin de prendre pour les coefficients de cette fonction linéaire, les racines de l'unité du même degré que l'équation, ce que toutes les méthodes indiquent, la réduite s'abaissera, comme on peut le voir *a priori*, par la forme même de la fonction[Poinsot, 1808, p. 365].

Les réflexions générales de Poinsot exposées ici permettent de faire ressortir, de manière claire et précise, les principaux acquis sur la théorie générale des équations en ce début de XIXe siècle. À partir de l'exemple de l'équation générale du 5e degré, il explique pourquoi le fait de former la *réduite* à partir des racines de l'unité permet de faire diminuer son degré initial :

> Pour en donner une idée, qu'il s'agisse par exemple, de résoudre l'équation du 5e degré. L'équation résolvante qui donnera la fonction linéaire de ses cinq racines, s'élèvera au degré 1.2.3.4.5 ou 120, nombre de manières dont on peut permuter cinq choses entre elles. Mais si les coefficiens de cette fonction sont les racines cinquièmes de l'unité, on observera que cette fonction multipliée successivement par ces 5 racines, fournira 5 fonctions pareilles où les racines de la proposée auront changé de place. Cette multiplication équivaudrait donc à 5 permutations qu'on ferait entre

a sans cesse à indiquer la marche des calculs et à prévoir les résultats sans jamais pouvoir les effectuer.[Galois, 1908, p.22].

10. Pour Poinsot, une équation est inférieure à une autre équation lorsque son degré est inférieur.

> les racines. Donc, si la fonction simple a 120 valeurs, sa cinquième puissance n'en aura que la 5e partie ou 24. On cherchera donc la cinquième puissance de la fonction linéaire. Mais ces 24 valeurs se partageront encore en six groupes. Car, par la nature des racines imaginaires de l'unité, une seule, avec ses puissances successives, donne toutes les autres ; une autre avec ses puissances successives, les donne encore, mais rangées dans un ordre nouveau. Or, comme il y a ici quatre de ces racines, la même fonction où l'on emploierait successivement et de la même manière ces quatre racines, répondrait successivement à quatre de ses valeurs comme si l'on y eût permuté quatre fois les racines de la proposée. Toute expression semblable de ces quatre fonctions, telles que leur somme, la somme de leurs produits deux à deux, ou trois à trois, etc., n'aura donc que le quart de toutes les valeurs, ou simplement six valeurs différentes. La fonction pourra donc être regardée comme la racine d'une équation du 4e degré dont les coefficiens seront donnés par une équation du 6e qui sera entièrement connue[Poinsot, 1808, p. 365-366].

Ainsi, il arrive à la même conclusion que Lagrange : à l'aide de cette méthode, on ne peut pas réduire la résolution de l'équation générale du 5e degré à la résolution d'une équation de degré inférieur. Mais, on peut néanmoins, dans certains cas particuliers, résoudre des équations de degré supérieur à quatre : c'est le cas des équations où « les racines sont liées par quelque relation connue »[Poinsot, 1808, p. 367]. En effet, le fait de connaître des relations entre des ensembles de racines permet de réduire encore plus le degré des équations auxiliaires. Les racines des équations binômes $x^n = 1$ ont cette propriété et c'est dans les *Disquisitiones Arithmeticae* que Gauss expose pour la première fois une méthode pour les résoudre algébriquement, en utilisant les outils mis en avant par Lagrange et un recodage particulier des racines.

3 - La résolution algébrique des équations binômes : analyse de la méthode de Gauss par Poinsot

Après avoir exposé ses réflexions sur la théorie générale des équations, Poinsot remarque que l'on peut aller plus loin dans certains cas :

> Mais lorsque les racines sont liées par quelque relation connue, la difficulté descend toujours à celles des degrés inférieurs. Si une partie des racines est traitée d'une certaine manière, on pourra sur le champ dégager le polynome qui les renferme ; et s'il y a plusieurs groupes où les racines contenues soient semblablement traitées, on obtiendra un quelconque de ces groupes par une équation d'un degré marqué par leur nombre[Poinsot, 1808, p. 367-368].

Poinsot développe alors le cas des équations binômes en se référant à Gauss. Il illustre la méthode de ce dernier en prenant l'exemple de l'équation binôme du treizième degré :

> Ainsi, l'on verra sans peine que les douze racines imaginaires de l'équation binôme du 13e degré se partage en quatre groupes de trois racines, telles, dans chacun d'eux,

qu'en mettant l'une à la place de l'autre, ces trois racines ne se séparent pas ; et par conséquent, si l'on échange les racines d'un groupe à l'autre, les groupes ne feront que changer de place en conservant toujours leurs mêmes racines. Ensuite on verra que, parmi ces quatre groupes, il y en a deux qui sont tels que, tout échange qui fait passer l'un à la place de l'autre, ramène celui-ci à la place du premier ; ainsi, les deux autres groupes sont dans le même cas. Si donc vous demandez à l'équation du 12^{e} degré, le diviseur du 3^{e} qui rassemblerait les trois racines d'un groupe, vous aurez les coefficiens de ce diviseur par une équation du 4^{e} degré... [Poinsot, 1808, p. 370]

Poinsot ne donne donc aucun détail technique de la méthode de Gauss, il n'utilise pas la même terminologie que lui non plus. En effet, les *groupes de racines* de Poinsot désignent les *périodes* de Gauss. On retrouve d'ailleurs les quatre *périodes* de trois racines de l'exemple développé plus haut. Il retranscrit les propriétés des *périodes* énoncées par Gauss à l'aide du vocabulaire courant : « les racines ne se séparent pas ». Ici, son résumé met en avant le point fondamental de l'approche de Gauss : le fait que les racines de l'équation considérée soient liées entre elles permet de décomposer cet ensemble de racines en sous-ensembles dont dépendent des équations de degrés de plus en plus bas. Poinsot pointe du doigt l'outil qui permet de former ces *groupes de racines* ou *périodes* : l'utilisation des *racines primitives* pour ordonner les racines de l'équation proposée. Si l'on prend une racine n^{e} quelconque de l'unité, notée r, et qu'on calcule ses différentes puissances, r^2, r^3, r^4, ..., r^{n-1}, on obtient ainsi toutes les racines n^{e} de l'unité. Bien sûr, si l'on prend une autre racine quelconque n^{e} de l'unité, r', alors la série r', r'^2, r'^3, ..., r'^{n-1} contient également toutes les racines n^{e} de l'unité, mais dans un ordre complètement différent. Poinsot explique donc pourquoi le choix de Gauss, fait la différence :

Mais, au lieu de ranger ces exposants en progression arithmétique, M. Gauss, d'après le théorème de Fermat sur les résidus des puissances, eut l'idée heureuse de les ranger en progression géométrique, en prenant pour base un de ces nombres, qu'Euler nomme *racines primitives* , et qui sont tels que leurs puissances successives divisées par le nombre premier dont il s'agit, qui est ici onze, laissent des résidus successifs tous différents ; de cette manière, on a encore les dix même racines que si l'on eût pris les exposants 1, 2, 3, 4, etc. ; mais dans un ordre nouveau, ce qui est indifférent. Or, à présent l'on peut voir que cette disposition des racines est telle que, si l'on veut mettre une d'entre elles à la place d'une autre, et que par ce changement, une des racines s'avance d'une, de deux, de trois ou de quatre places, etc., toutes les autres s'avanceront en même temps d'une, de deux, de trois ou de quatre places, etc., de sorte que toutes les permutations possibles que vous voudriez faire entre ces dix racines, par le transport de l'une à la place de l'autre se réduiront uniquement aux dix permutations que vous obtenez en lisant de suite vos racines, d'abord à partir de la première, puis de la deuxième, puis de la troisième, etc., enfin de la dixième, exactement comme si elles étaient écrites en cercle[Poinsot, 1808, p. 372-373].

Son objectif est une fois de plus de mettre en lumière les raisons de la validité de la méthode : l'utilisation des racines primitives - outil de théorie des nombres - permet de ranger les racines de l'équation proposée dans un ordre où ces racines seront toujours placées de la même façon les unes par rapport aux autres, comme si elles étaient disposées régulièrement sur un cercle. Cette image avait déjà été utilisée par Gauss une première fois pour décrire le même type de structure dans une note de la section II des *Disquisitiones Arithmeticae*, dans le cadre de la démonstration d'un résultat sur les permutations. Gauss définit les *permutations semblables* :

> Lorsque dans deux permutations l'ordre des choses ne différera qu'en ce que celle qui tient la première place dans l'une, en occupe une différente dans l'autre, mais que du reste toutes les autres, à partir de celles-là, suivent le même ordre dans chacune des permutations, de manière que la dernière de l'une se trouve placée immédiatement avant la première dans l'autre ; nous les appellerons *permutations semblables* (*). Ainsi, $ABCDE$ et $DEABC$, $ABAAB$ et $ABABA$ seront semblables[Gauss, 1801, art. 41].

Gauss illustre ce type de permutations dans une note correspondant au symbole * de la citation précédente :

> Si l'on écrivait en cercle les permutations semblables, de manière que la dernière chose touchât à la première, il n'y aurait aucune différence entre elles, parce qu'aucune place ne peut s'appeler la première ni la dernière[Gauss, 1801, art. 41].

Nous verrons que cette image du cercle est récurrente dans les travaux de Poinsot et fondamentale dans ce qu'il appelle la *théorie de l'ordre*, développée dans chacun de ses travaux. De manière plus générale, on retrouve dans ce commentaire les prémisses des idées centrales que Poinsot va développer dans ses travaux ultérieurs. De plus, les ensembles analysés ici seront repris par Poinsot de manière plus approfondie, leurs caractéristiques communes avec d'autres ensembles seront mises en avant et ce sont celles-ci qui fonderont la notion d'*ordre* telle qu'elle est vue par Poinsot.

II 1813 : un manuscrit sur les permutations

Cette section est consacrée à l'étude d'un manuscrit de Poinsot qui n'a jamais été publié auparavant, dont nous avons inséré une transcription en annexe [11]. Nous avons trouvé ce texte lors de notre dépouillement des manuscrits de Poinsot présents à la Bibliothèque de l'Institut de France. Dès notre première lecture, nous avons supposé qu'il correspondait au travail présenté en 1813 à l'Académie sous le nom de *Mémoire sur les Permutations* pour plusieurs raisons que nous développons en annexe [12]. Ce mémoire est important car il diffère des autres mémoires contemporains sur le même thème.

11. Voir à partir de la page 499.
12. Voir en annexe, page 498.

L'outil des permutations [13] prend de l'importance avec la publication des travaux de Waring, Lagrange et Vandermonde sur la théorie algébrique des équations dans les années 1770. Au début du XIX^{e} siècle, deux mathématiciens publient des mémoires sur la théorie des permutations : Paolo Ruffini et Cauchy. Ruffini commence par publier un ouvrage d'algèbre en 1799, intitulé *Teoria generale delle equazione, in cui si domstra impossibile la soluzione algebrica delle equazioni generali di gradi superiore al quarto*, où il détaille les propriétés de l'ensemble des permutations d'un nombre de racines donné dans le but de démontrer l'impossibilité de la résolution de l'équation générale du cinquième degré. Celui-ci sera suivi, entre 1802 et 1813, de six autres versions et ajouts, principalement pour répondre aux remarques et propositions de son ami Pietro Abbati et aux critiques De Gian - Francesco Malfatti, qui, selon [Wussing, 1984], ne voulait pas admettre la non-existence d'une solution générale de l'équation du cinquième degré. De son côté, Cauchy [14] publie dans un premier temps deux mémoires concernant la théorie des permutations en 1815, puis attendra 1840 pour faire évoluer sa théorie des permutations. Dès 1815, Cauchy donne de nouvelles notations et définitions. Il y introduit par exemple la notion de *substitution*, qui désigne le procédé permettant de passer d'une permutation à une autre, ainsi que la notation utilisée encore aujourd'hui. Il définit ensuite le produit de plusieurs substitutions, etc [15].

1 - Étude et analyse du manuscrit

Dans ce texte, Poinsot essaie de comprendre comment on peut partager les permutations en différents ensembles, toujours dans le cadre de la résolution générale des équations. Nous nous intéressons ici prioritairement aux raisonnements concernant l'ordre et les relations entre les différents objets considérés. Dès les premières lignes (voir page 499), il introduit une fonction φ des racines a, b, c, d, ... Il pose $\varphi = (a, b, c, d, \ldots)$, qu'il simplifie à l'aide de la notation $abcd\ldots$, appelée *permutation*. On peut supposer que Poinsot se base ici les travaux de Lagrange sur les équations algébriques exposés dans [Lagrange, 1772-1773] ou [Lagrange, 1808].

(a) Une première méthode pour classer les permutations

Poinsot choisit de travailler avec l'exemple de l'équation générale du 5^{e} degré, il note les racines a, b, c, d, e. On obtient ainsi $5 \times 4 \times 3 \times 2 \times 1 = 120$ valeurs pour la fonction φ. Il

13. Au début du XIX^{e} siècle, une permutation est un ensemble ordonné d'objets. Pour une discussion plus approfondie sur les notions de permutation et de substitution, voir par exemple [Dahan Dalmedico, 1980].

14. Voir [Cauchy, 1815a] et [Cauchy, 1815b]. Ces deux textes sont précédemment lus devant l'Académie le 30 novembre 1812.

15. Une analyse des travaux de ces deux mathématiciens à ce sujet est donnée dans [Wussing, 1984], [Dahan Dalmedico, 1980] pour Cauchy, dans [Cassinet, 1988] et [Houzel, 2002, chap. 4 et 6] pour Ruffini.

affirme alors un résultat qu'il va ensuite justifier en rangeant les différentes permutations dans des tableaux :

> Or, ces 1.2.3.4.5. permutations peuvent être partagées en 5 groupes principaux de 1.2.3.4 permutations chacun et tels que les permutations d'un même groupe ne se séparent jamais malgré tous les échanges qu'on pourrait faire entre les lettres a, b, c, d, e. (page 500)

Comme précédemment, Poinsot ne définit pas les termes *permutation* et *groupe*. Nous pouvons supposer que, pour lui, une *permutation* est un ensemble ordonné de lettres[16]. D'autre part, le mot *groupe* paraît être associé à un ensemble d'objets *inséparables*. L'adjectif *inséparable* semble signifier que l'on peut passer d'un objet à un autre par un procédé semblable - ici, un échange de lettres - et que l'on ne peut pas de cette façon obtenir un objet d'un autre groupe. De même, plus loin, l'utilisation de la notion de *groupe* s'accompagne d'une mention similaire : « dont les permutations respectives ne pourront jamais se mêler » (voir page 501).

Poinsot illustre ses raisonnements en regroupant toutes les permutations possibles des cinq racines dans un tableau (voir page 500). Poinsot remarque que le premier groupe est stable lorsque l'on échange les lettres b, c, d, e d'une manière quelconque, c'est-à-dire, en utilisant le vocabulaire de Cauchy, lorsqu'on applique à toutes les permutations une substitution laissant fixe la lettre a. Si on échange la lettre a avec une autre lettre, on obtient un des quatre groupes suivants. Il qualifie ces cinq groupes de *groupes principaux*. Puis il continue à partager ces permutations en sous-ensembles - les *groupes secondaires* - en s'appuyant sur le même principe :

> Actuellement, chaque groupe qui est de 1.2.3.4 permutations pourra se partager en 4 groupes secondaires composés de 1.2.3 permutations. (page 501)

Dans le premier groupe de 24 permutations, il forme un premier groupe contenant les permutations telles que b soit à la deuxième place, puis un groupe tel que les permutations soient de la forme $ac\ldots$, et ainsi de suite : il forme ainsi quatre *groupes secondaires* de 6 éléments. Il continue en formant des *groupes ternaires* composés de deux permutations chacun, tels que ces permutations aient les mêmes trois premières lettres.

Enfin :

> [...] chaque groupe ternaire, tel que le premier, se décomposera en deux permutations simples *abcde*, *abced* qui seront toujours conjuguées dans tous les échanges possibles des lettres entre elles. (page 501)

Ici, le terme *conjugué* n'a pas le sens de la conjugaison actuelle : deux permutations *conjuguées* semblent être pour Poinsot des permutations qui appartiennent au même *groupe*, quels que soient les échanges de lettres entre elles que l'on peut y faire.

16. Nous verrons que, dans son manuscrit, il n'introduit pas le concept de substitution, c'est-à-dire l'opération qui permet de passer d'une permutation à une autre. On retrouve ce concept dans les mémoires de Cauchy de 1815, puis dans les travaux de Galois, puis enfin, de façon beaucoup plus aboutie, dans les travaux de Cauchy de 1844.

Poinsot utilise ensuite ces réflexions pour raisonner sur le degré des fonctions des racines de l'équation proposée (voir page 501). L'exposé de Poinsot est un résumé partiel des travaux de Lagrange dans [Lagrange, 1772-1773], basé sur la façon dont on peut ranger les permutations. On sait que la fonction φ admet 5! valeurs sous les permutations des racines a, b, c, d et e. Poinsot ne donne aucune condition pour le choix de cette fonction. Ensuite, il considère les fonctions φ' qui n'auront que 3.4.5 valeurs, et qui sont invariables (c'est-à-dire symétriques). On peut par exemple utiliser les fonctions $\varphi'_{1.1} = \varphi(a,b,c,d,e) + \varphi(a,b,c,e,d)$ et $\varphi'_{1.2} = \varphi(a,b,c,d,e) \times \varphi(a,b,c,e,d)$. On aurait deux autres couples équivalents de fonctions φ', avec les permutations (a,b,d,c,e) et (a,b,e,c,d). Dans ce cas, φ est bien racine d'une équation de degré 2 dont φ' est coefficient : $x^2 - \varphi'_{1.1}X + \varphi'_{1.2}$. On raisonnera de même avec les fonctions symétriques ayant trois variables pour obtenir les expressions des fonctions φ'', et ainsi de suite. Ainsi, la résolution d'une équation de degré n dépendrait de la résolution de plusieurs équations de degrés de 1 à n. On remarque qu'ici, Poinsot donne une idée générale de cette résolution, mais qu'il n'applique pas sa méthode à une équation particulière, et qu'il ne détaille pas comment choisir les fonctions φ, φ', etc. Son objectif ne semble pas être de trouver une méthode de résolution - ou une démonstration de l'impossibilité de la résolution générale du cinquième degré - mais bien de comprendre le fond des réflexions de Lagrange en analysant le comportement des permutations.

Pour conclure cette partie, Poinsot considère les différentes manières de partager les permutations et indique que la méthode de partage choisie ici ne « peut rien apprendre sur la résolution ». En effet, ici, Poinsot classe les différentes permutations pour former des *groupes* mais n' "opère" pas sur les permutations. Il raisonne à partir d'échanges de lettres seulement. Dans la partie suivante, Poinsot présente une nouvelle classification fondée sur l'utilisation d'une *loi*.

(b) Une seconde méthode basée sur l'utilisation d'une *loi*

La deuxième partie du manuscrit consiste à partager les permutations d'une nouvelle façon, qui se rapproche des calculs sur les permutations que l'on peut connaître aujourd'hui. Cette nouvelle manière consiste à considérer une permutation quelconque, et à utiliser une *loi* pour modifier l'ordre de ses lettres afin d'obtenir une nouvelle permutation. La *loi* correspond en fait à la façon de modifier les lettres les unes par rapport aux autres. Par exemple, une *loi* pourrait consister à échanger la première lettre avec la seconde lettre. Cela correspond en fait à ce que Cauchy appelle *substitution*, c'est-à-dire le procédé permettant de passer d'une permutation initiale à une seconde permutation. Les *lois* utilisées par Poinsot sont toujours d'un type particulier : elles vont lui permettre d'obtenir exclusivement des ensembles qui correspondent à ce que l'on appelle aujourd'hui des groupes cycliques d'ordre n. Il applique cette même *loi* à la permutation obtenue afin d'en obtenir une troisième et continue ainsi jusqu'à revenir à la *permutation primitive* :

La manière générale de trouver les permutations qui s'assemblent est de prendre une quelconque de ces permutations, et d'y appeler toutes les lettres dans un nouvel ordre, ce qui fournira une nouvelle permutation, ensuite de tirer de celle-ci, par la même loi, une troisième permutation qui sera dérivée de la $2^{\text{ème}}$ comme la $2^{\text{ème}}$ est dérivée de la $1^{\text{ère}}$; on continuera de cette manière jusqu'à ce que l'on retombe sur la permutation primitive d'où l'on était parti, et l'on repassera ensuite dans les mêmes à l'infini.

Ces différentes permutations dérivées successivement l'une de l'autre par la même loi seront conjuguées ; c'est-à-dire ne se sépareront jamais malgré tous les échanges possibles entre les lettres [...](page 504)

Il obtient ainsi le groupe de permutations :

$$\begin{array}{ccccc} a & b & c & d & e \\ b & c & d & e & a \\ c & d & e & a & b \\ d & e & a & b & c \\ e & a & b & c & d \end{array}$$

On ne peut s'empêcher de penser ici aux raisonnements développés par Poinsot - à partir des travaux de Gauss et Lagrange - autour des racines des équations binômes et des racines primitives, qui engendrent également des ensembles correspondant à des groupes cycliques. Les racines primitives permettent d'obtenir la *loi* pour opérer sur les racines des équations binômes qui ont le même rôle que les permutations.

Poinsot observe ensuite que l'on peut obtenir le même groupe de permutations conjuguées en utilisant des lois semblables, c'est-à-dire en prenant les lettres de deux en deux, de trois en trois, ... En termes modernes, si on considère la substitution $\sigma = (a\ b\ c\ d\ e)$, une loi semblable est d'appliquer à la permutation initiale, et à celles obtenues ensuite, la substitution σ^2, ou σ^3, ... Si le nombre m est premier, les groupes inséparables que l'on obtient en appliquant une substitution circulaire (la *loi* utilisée par Poinsot) sont composés de m éléments, et à partir de l'un de ces éléments quelconques et avec une des $m-1$ lois équivalentes, on obtiendra toujours le groupe de m éléments. Par contre, si m est composé, et si on considère un groupe de m éléments, obtenu à partir d'une permutation quelconque, et en y appliquant la substitution $(a\ b\ c\ d\ e\ldots)$, alors ce groupe peut être décomposé en plusieurs sous-groupes dont le cardinal sera un diviseur de m (voir page 505). Poinsot partagera de la même façon les groupes de racines de l'unité. Il donne d'ailleurs des exemples plus concrets :

Ainsi pour $m = 12$ par exemple, les douze permutations se pourraient partager en deux groupes de six, et chacun de ces groupes en deux autres de trois permutations.

Voilà donc une manière très simple de partager le système des $1.2.3.4\ldots m$ permutations de m lettres, en $1.2.3.4\ldots m-1$ groupes de m permutations conjuguées

par la même loi, et qui sont inséparables malgré tous les échanges qu'on pourrait faire entre les m lettres proposées. (page 506)

Lorsque Poinsot prend l'exemple $m = 12$, il obtient quatre groupes de trois permutations. On peut faire le lien avec son commentaire de 1808, où il considère l'équation binôme du treizième degré, qui se ramène à la résolution d'une équation du douzième degré (après division par $x - 1$), et où « les douze racines imaginaires [...] se partagent en quatre groupes de trois racines »[Poinsot, 1808, p. 370]. On reconnaît donc ici des raisonnements très similaires à la méthode de Gauss pour la résolution des équations binômes. Poinsot ne l'indique pas explicitement ici, mais il essaie, comme en 1808, de faire ressortir les mécanismes qui font fonctionner les méthodes de Gauss et Lagrange sur la résolution des équations.

(c) *Conjugaison mutuelle des groupes*

Après avoir exploré les différentes manières possibles de *conjuguer* les permutations, Poinsot reprend des raisonnements similaires pour *conjuguer* les groupes entre eux. Pour former un groupe de permutations, Poinsot applique la même loi à une permutation, puis aux permutations successivement obtenues, jusqu'à ce que l'on obtienne à nouveau la permutation initiale. En d'autres termes, il a pris les différentes puissances d'une substitution circulaire σ, qui correspond à prendre « toutes les lettres de n en n ». Pour obtenir des *groupes conjugués*, il utilise un *principe analogue* : il applique la même loi à chacune des permutations d'un même groupe pour obtenir un *groupe conjugué*, puis il fait de même avec ce nouveau groupe, et ainsi de suite jusqu'à obtenir de nouveau le groupe initial. Il donne également une méthode pour passer directement du premier groupe au troisième groupe par exemple : il suffit d'appliquer la substitution σ^2, ce qui revient à prendre les lettres de n^2 en n^2 (voir page 507). Il conclut en faisant un lien avec les racines primitives :

> Ce théorème est très remarquable, il donne une espèce de définition géométrique de ces nombres qu'Euler nomme racines primitives, et qui sont tels que toutes leurs puissances successives laissent par rapport au nombre premier μ que l'on considère des restes tous différents 1, 2, 3, 4, ... $\mu-1$ et qui reparaissent ensuite périodiquement à l'infini.
>
> Si μ lettres sont rangées en cercle comme les angles d'un polygone, il y a toujours des nombres n tels qu'en joignant les points de n en n, ce qui donne un nouveau polygone, puis ceux-ci de n en n, ce qui forme un troisième polygone, et ainsi de suite, vous formez toutes les espèces de polygones de l'ordre μ ; et il y a juste autant de ces nombres ou racines primitives qu'il y a de nombres premiers à $\mu-1$ et inférieurs à $\mu - 1$. (page 507)

Ainsi, Poinsot reprend cette image du cercle, et lie l'algèbre, la théorie des nombres, et la géométrie avec les permutations, les racines primitives et les polygones. Par exemple, une *loi* qui permet de générer toutes les permutations du groupe considéré correspond

à une racine primitive, qui, en considérant ses puissances successives, permet d'obtenir toutes les racines complexes d'une équation binôme. Les différents groupes que l'on obtient à partir du groupe initial et en le composant avec une substitution circulaire correspondent aux différentes *périodes* de Gauss que l'on peut obtenir à partir d'une même racine primitive. En effet, une *période* est constituée de certaines puissances d'une racine de l'équation donnée, et on obtient les périodes semblables en multipliant les exposants de chacune de ces racines par un même nombre.

Poinsot va encore plus loin en expliquant comment on peut former une suite de *systèmes* et de *systèmes partiels* : il applique aux permutations ce que Gauss a fait dans les *Disquisitiones Arithmeticae*, et que lui-même appliquera aux équations binômes plus tard, c'est-à-dire qu' il subdivise ces groupes en *systèmes partiels* encore conjugués, en utilisant les facteurs du nombre $m-1$ qui est un nombre composé puisque m est un nombre premier. En effet, prendre successivement les lettres de n en n dans chaque nouveau groupe obtenu revient à prendre, dans le groupe initial, les lettres de n^k en n^k pour k allant de 1 à $m-2$. On retrouve alors dans le raisonnement de Poinsot des points très semblables à la théorie de la cyclotomie de Gauss [17] :

> Mais la première manière de déduire successivement ces groupes l'un de l'autre par la même loi est plus avantageuse en ce qu'elle nous découvre encore une décomposition de ces $m-1$ groupes entre eux, et par l'ordre où elle les fait naître successivement[...] or supposez que α soit un facteur de $m-1$, et dans l'ordre où sont actuellement vos groupes, essayez de les déduire les uns des autres par la loi d'où le $\alpha+1^{\text{ème}}$ dérive du 1^{er}, ce qui revient à prendre toutes les lettres de n^α en n^α, vous irez ainsi de l'un à l'autre, en sautant de α en α, et comme α est diviseur de $m-1$, vous ne passerez jamais que sur une même partie $\frac{m-1}{\alpha}$ de vos $m-1$ groupes, de sorte que le système sera partagé en α systèmes partiels de $\frac{m-1}{\alpha}$ groupes aussi conjugués entre eux. Et de même si $\frac{m-1}{\alpha}$ a pour diviseur β, vous pourrez subdiviser encore chacun des $\frac{m-1}{\alpha}$ systèmes partiels en β systèmes de $\frac{m-1}{\alpha\beta}$ groupes aussi conjugués entre eux, et ainsi de suite, jusqu'à ce que le système entier n'offre plus dans toutes ses subdivisions que les nombres premiers α, β, ... qui entrent dans la composition du nombre $m-1$; alors il y aura une dépendance mutuelle toute semblable 1°. entre les m permutations d'un même groupe ; 2°. entre les groupes d'un même système

17. Voici le passage correspondant dans les *Disquisitiones Arithmeticae* :

> Le but de nos recherches [...] est de décomposer X *graduellement* en un nombre de facteurs de plus en plus grand, et cela de manière à ce que les coefficients de ces facteurs puissent être déterminés par des équations du degré le plus bas possible[...] Nous ferons voir que si l'on décompose $p-1$ en facteurs entiers quelconques α, β, γ, etc. X est décomposable en α facteurs du degré $\frac{n-1}{\alpha}$ [...] ; que chacun de ces facteurs est décomposable en β facteurs du degré $\frac{n-1}{\alpha\beta}$[...][Gauss, 1801, art. 342].

partiel ; 3 °. entre les systèmes partiels d'un même système supérieur ; et ainsi de suite. (page 508)

Ici, Poinsot parle de « dépendance mutuelle toute semblable ». Aujourd'hui, on pourrait dire que l'on retrouve des structures semblables.

Pour finir, et comme nous l'avons indiqué précédemment, Poinsot « passe à une exposition plus claire et plus rapide » (page 511) en mettant en avant une fois de plus « une liaison intime » entre la théorie des polygones, la résolution générale des équations et la théorie des nombres. Ainsi, il reprend très rapidement ses raisonnements sur les ensembles de permutations que l'on peut faire entre 3, 4 et 5 racines, en illustrant ses propos à l'aide des polygones réguliers à 3, 4 et 5 côtés.

2 - Les apports de ce texte

Dans ce texte, Poinsot n'a pas les mêmes objectifs que Ruffini et Cauchy : il n'essaie pas de construire une théorie des permutations. Il n'étudie pas techniquement le groupe symétrique comme peuvent le faire les deux autres mathématiciens. Il ne définit pas les termes particuliers qu'il utilise régulièrement - on peut penser à *groupe* et *conjugaison* par exemple - comme Cauchy peut le faire dès le début de ses travaux. Il ne perfectionne pas les techniques de calcul sur les permutations. Quand Cauchy définit précisément ce qu'est une substitution, Poinsot parle de *loi* pour passer d'une permutation à une autre, sans en donner une définition ou les caractéristiques. De plus, les *lois* abordées par Poinsot ne correspondent qu'aux *substitutions circulaires* de Cauchy : son étude de l'ensemble des permutations est donc très partielle.

Sur le fond, ce mémoire reste au niveau de ce que l'on peut retrouver quelques années auparavant chez Gauss ou Lagrange. Néanmoins, si l'on place ce texte dans l'ensemble des écrits de Poinsot à ce sujet, on retrouve des caractéristiques intéressantes et plus originales. En particulier, il met en avant la *liaison intime* (page 511) qui existe selon lui entre la géométrie (avec la théorie des polygones), l'algèbre (avec la résolution des équations) et la théorie des nombres (avec les racines primitives et les congruences). D'autre part, Poinsot présente une partie de la structure du groupe symétrique, en faisant ressortir le type de relations qui existent entre certaines permutations, et entre certains sous-groupes du groupe symétrique. Bien sûr, Poinsot n'a pas en tête les notions de structure ou de groupe telles qu'elles seront définies à partir de la fin du XIX^{e} siècle, mais sa façon de présenter l'ensemble des permutations est originale dans le sens où elle se focalise sur la manière dont on peut relier et classer ces objets entre eux à l'aide d'une *loi*.

Ce texte n'ayant jamais été publié, il est vraisemblable qu'une grande majorité des mathématiciens de l'époque ne l'ait pas connu en détail. Certains ont certainement assisté

à sa lecture en 1813, d'autres ont peut-être eu accès à une copie écrite [18]. Néanmoins, Poinsot présente ses réflexions sur la théorie des permutations en quelques paragraphes en 1817 à l'Académie, dont le mémoire correspondant est publié en 1818 dans les *Mémoires* de l'Académie. On peut donc supposer que les idées générales développées dans ce manuscrit sont connues, et que l'étude de ce texte permet de comprendre plus en détails ce que Poinsot résume quelques années plus tard.

L'intérêt de ce texte se situe donc dans la façon nouvelle dont Poinsot expose des idées déjà développées par Gauss et Lagrange. La théorie des permutations vue par Poinsot a-t-elle été reprise au cours du XIX^{e} siècle ? Un mathématicien au moins se réfère à la théorie des permutations de Poinsot : Théodore Despeyrous [19]. Dans un mémoire intitulé *Sur la détermination des nombres de valeurs que prennent les fonctions par les permutations des lettres qu'elles renferment*, paru en 1865 dans le *Journal de Mathématiques pures et appliquées* , il explique qu'il ne travaille pas avec les principes de Cauchy mais à partir de la *théorie de l'ordre* de Poinsot[Despeyrous, 1865b, p. 56]. Dans ce même volume, on trouve un autre texte de Despeyrous : *Classifications des permutations d'un nombre quelconque de lettres en groupes de permutations inséparables.* Il y travaille avec les polygones étoilés, comme l'avait fait Poinsot, et considère les permutations de m objets « qui sont relatives aux polygones de Poinsot, c'est-à-dire toutes celles qu'on déduit de cette permutation en prenant successivement les lettres, à partir de la première, de p_1 en p_1, de p_2 en p_2, ... »[Despeyrous, 1865a, p. 179], où les p_i considérés sont les nombres inférieurs et premiers à m. De même, dans un mémoire antérieur, intitulé *Mémoire sur la théorie générale des permutations*, publié en 1861 dans le même journal, Despeyrous se réfère déjà aux polygones de Poinsot, et rappelle que Poinsot avait promis, en 1817, un travail sur la théorie des permutations :

> Telles sont les deux lois générales de classification que notre travail démontre. Le profond géomètre dont nous avons parlé, Poinsot, avait, dès l'année 1817, entrevu une partie de ces résultats, et avait promis sur cette matière plusieurs Mémoires. Les géomètres regretteront sans doute qu'il n'ait pas réalisé sa promesse : loin de nous la prétention d'y suppléer[Despeyrous, 1861, p. 417 - 418].

18. Nous avons par exemple retrouvé une version de ce texte dans les manuscrits de Joseph Bertrand à l'Institut de France.

19. Nous remercions Norbert Verdier pour nous avoir fait connaître les textes de ce mathématicien. Caroline Ehrhardt a également commenté le point de vue de Despeyrous en lien avec Poinsot dans sa thèse : voir [Ehrhardt, 2007, p. 400-402]. Le *Cours de Mécanique de Théodore Despeyrous*, publié en 1884, est précédé d'une *Notice sur la vie et les travaux de M. Despeyrous*, écrite par l'éditeur A. Hermann, et dont nous extrayons les informations qui suivent. Ce mathématicien originaire de la région de Toulouse arrive à Paris en 1842 afin de poursuivre ses études à la Faculté des Sciences. C'est à cette même époque qu'il se laisse séduire par les idées de Charles Fourier et Saint-Simon et collabore au journal *La Phalange*, fondé par Fourier. À partir de 1844, il commence à fréquenter des mathématiciens tels Charles - François Sturm, Libri et Poinsot. Il remplace Libri à la Faculté des Sciences de 1845 à 1847, est nommé à la Faculté des sciences de Dijon jusqu'en 1865, puis revient à Toulouse pour enseigner l'astronomie à l'Observatoire. Il meurt d'un accident de voiture en 1883.

III 1818 : présentation des recherches centrées autour de la notion d'ordre

Le texte que nous allons présenter ici est intitulé *Extrait de quelques recherches nouvelles sur l'algèbre et la théorie des nombres*, et a été lu le 5 mai 1817 à l'Académie des Sciences, puis publié en 1818 dans les *Mémoires* de l'Académie. Poinsot l'introduit en rappelant deux sujets de recherche qu'il a abordés quelques années plus tôt, et qui ont pour lui un point commun avec ses recherches en théorie des nombres : *la science de l'ordre*[20].

> Il y a déjà quelques années[21] que nous avons lu à l'Académie un Mémoire assez étendu sur la théorie générale des permutations. Nous tâchions d'approfondir cette théorie, d'y ajouter de nouveaux principes, et d'en faire quelques applications importantes à l'algèbre et à l'analyse indéterminée. Les mêmes principes se retrouvaient encore en géométrie, dans les propriétés de ces nouvelles figures que nous avons fait connaître[22], et que nous avons rapportées, avec plusieurs spéculations du même genre, à cette partie singulière de la science de l'étendue que Leibnitz à nommée la Géométrie de situation.
>
> Nous avons repris et continué toutes ces recherches qui sont liées entre elles de la manière la plus intime, et qui ont en général pour objet, *la théorie de l'ordre et de la situation des choses sans aucune considération de la grandeur* : théorie neuve et profonde, dont les éléments nous sont à peine connus, mais qu'on doit regarder comme le premier fondement de l'algèbre, et la source naturelle des principales propriétés des nombres[Poinsot, 1818, p. 382-383].

Il utilise notamment cette notion d'*ordre* pour faire des parallèles entre les relations existant entre différents objets mathématiques : les racines primitives et les permutations, les racines primitives de l'unité et les racines primitives modulo un nombre premier p. Il place ici l'*ordre* comme fondement de l'algèbre. Sa définition de l'algèbre commence donc à évoluer vers un domaine plus large que la seule théorie des équations. De plus, ici, l'*ordre* est également présenté comme un point commun entre l'algèbre et la théorie des nombres. Enfin, remarquons que Poinsot est l'un des rares à insister sur le fait que la section VII des *Disquisitiones Arithmeticae* lie la géométrie, l'algèbre et la théorie des nombres[23].

20. L'association des mathématiques à l'ordre n'est bien sûr pas nouvelle. Rappelons Descartes : « [...] j'ai découvert que toutes les sciences qui ont pour but la recherche de l'ordre et de la mesure, se rapportent aux mathématiques[...] »[Descartes, 1701, p. 223].

21. Il précise une date en note : Mai 1813. Comme annoncé précédemment, il est vraisemblable que cela corresponde au manuscrit étudié dans la partie précédente.

22. Il se réfère ici à son *Mémoire sur les polygones et les polyèdres* publié en 1809. Il y décrit notamment deux polyèdres réguliers étoilés. En 1812, Cauchy publie également un mémoire à ce sujet, dans lequel il démontre que tous les polyèdres réguliers étoilés ont été découverts. L'auteur y rappelle également les résultats de Poinsot, mais ne reprend pas du tout les passages qui s'appuient sur la notion d'ordre et sur la théorie des nombres.

23. La géométrie est effectivement souvent mise de côté. Poinsot insiste sur ce lien dès 1807 dans son commentaire sur les *Disquisitiones Arithmeticae*, publié dans le *Moniteur universel ou Gazette nationale*,

Poinsot donne l'objectif de son intervention :

> Comme nous nous proposons de donner successivement plusieurs[24] Mémoires sur cette matière, nous avons cru qu'il pouvait être utile, en attendant, de présenter à l'Académie une analyse rapide des principaux résultats que nous avons obtenus[Poinsot, 1818, p. 383].

Nous allons donc suivre sa présentation afin d'avoir un aperçu des sujets que Poinsot lie à l'*ordre*.

1 - L'*ordre* et la géométrie de situation

Dans le texte lu à l'Académie en 1817, Poinsot ne revient pas précisément sur son mémoire de géométrie. Nous allons néanmoins ici reprendre quelques passages de ce *Mémoire sur les Polygones et les Polyèdres*[25] pour montrer comment il utilise l'*ordre* dans ses raisonnements d'une part et comment il lie géométrie et théorie des nombres d'autre part. Ainsi :

> On rapporte les questions suivantes à la géométrie de situation, parce qu'on y considère moins la grandeur et la proportion des figures, que l'ordre et la situation des divers éléments qui la composent.
>
> Cette espèce de géométrie, qui ne regarde que les lieux dans l'étendue, est à-peu-près, à la géométrie ordinaire, ce que la science des propriétés des nombres est à l'algèbre, qui est la science des grandeurs[Poinsot, 1810, p. 26].

Poinsot donne une définition de la théorie des nombres très semblable dans ses écrits ultérieurs. C'est pour cela, selon lui, que c'est la théorie des nombres qui peut s'appliquer à la géométrie de situation, « comme l'analyse ordinaire s'applique naturellement aux problèmes déterminés de la géométrie, et le calcul différentiel à la théorie des courbes[...] » [Poinsot, 1810, p. 17]. Ici, il ne donne pas de définition précise de ce qu'il entend par la notion d'*ordre*. Il cite notamment Euler, Vandermonde et Marie - Jean Condorcet en tant que mathématiciens ayant travaillé sur la géométrie de situation, dans le sens qu'il

vol. 80, p. 312 : « On pourrait s'étonner d'abord de trouver dans ce livre des problèmes de géométrie, et de les voir résolus par les nombres. Mais dans les sciences mathématiques toutes les vérités se tiennent par une chaîne nécessaire. Aucune idée n'y peut éclore sans éclairer la plupart des théories qui, à leur tour, perfectionnent les arts qui leur répondent[...] ».

24. Seuls deux mémoires de Poinsot seront publiés à ce sujet : le mémoire publié en 1820 que nous étudions dans la quatrième partie de cet article, et le mémoire intitulé *Réflexions sur les principes fondamentaux de la théorie des nombres* publié en 1845. Dans ce dernier, Poinsot indique : « J'avais jeté sur le papier ces réflexions et ces démonstrations relatives à la théorie des nombres, dans la seule intention d'éclaircir, pour quelques personnes, les premiers principes de cette importante théorie. On m'a persuadé qu'il pouvait être utile de les publier[...] » [Poinsot, 1845, p. 1]. Il semble donc que Poinsot ait changé d'idée, ou qu'il n'ait pas pu écrire les mémoires prévus.

25. Ce texte a été lu à l'Académie en 1809, et publié en 1810 dans le *Journal de l'École Polytechnique*. Un rapport positif sur ce mémoire est lu par Legendre lors de la séance du lundi 16 octobre 1809 à l'Académie. On peut néanmoins remarquer que Legendre n'y fait aucune référence au fait que Poinsot y lie la géométrie de situation à la théorie des nombres.

lui donne[26]. On peut d'ailleurs citer la définition donnée par Euler de la *géométrie de situation* dans un mémoire sur le problème des ponts de Köenigsberg, et qui correspond totalement aux vues de Poinsot :

> Outre cette partie de la Géométrie qui s'occupe de la grandeur et de la mesure, et qui a été cultivée dès les temps les plus reculés, avec une grande application, Leibniz fait mention, pour la première fois, d'une autre partie encore très inconnue actuellement, qu'il a appelée *Geometria situs*. D'après lui, cette branche de la science s'occupe uniquement de l'ordre et de la situation, indépendamment des rapports de grandeurs[27].

Dans son mémoire de 1810, Poinsot commence par donner des définitions aux objets étudiés puis il étudie les différentes sortes de polygones ayant un nombre donné de côtés, en obtenant des résultats proches de la théorie des racines primitives :

> [...] dans l'ordre des polygones de m côtés, il y a autant d'espèces différentes qu'il y a de nombres premiers à m, depuis l'unité jusqu'au nombre $\frac{m-1}{2}$.
>
> Soit en effet un nombre h inférieur et premier à m, et considérez vos m points ou sommets rangés en cercle à égales distances dans l'ordre a, b, c, d, e, etc.. Si, à partir du premier a, vous les joignez successivement par des droites, en les prenant de h en h ; comme le nombre h n'a point avec m d'autre commune mesure que l'unité, vous serez obligé de passer par tous les points avant de revenir au premier ; alors vous aurez formé un polygone régulier de m côtés, avec m angles distincts a, b, c, d, e, etc[Poinsot, 1810, p. 21].

Poinsot reprend cette image des racines rangées autour d'un cercle, utilisée dès 1808 dans son commentaire du *Traité* de Lagrange. Il lie également son raisonnement sur les polygones à la théorie des équations binômes, en rapprochant des cas particuliers, ce qui peut laisser supposer que les idées développées par Poinsot dans ses travaux ultérieurs lui sont familières dès 1809. En effet :

> Dans l'analyse algébrique des polygones réguliers, ce cas répondrait à l'un de ceux où l'équation binôme se décompose, et où toutes les racines imaginaires ne sont pas propres à reproduire, par leurs puissances successives, toute la série des racines. Mais on reviendra là-dessus, comme on l'a dit : on a eu dessein de séparer ces considérations analytiques, pour ne faire ici qu'un mémoire de pure géométrie... [Poinsot, 1810, p. 27]

De plus, on trouve également dans ce mémoire une définition géométrique de nombre premier :

26. Poinsot remarque également que la définition donnée par d'Alembert dans l'*Encyclopédie* de la géométrie de situation selon Leibniz lui semble fausse, ou du moins incomplète (Voir [Poinsot, 1810, p. 16-17]) et que la *Géométrie de position* de Condorcet n'a pas les mêmes objectifs.

27. Cette traduction est issue de [Lucas, 1891, p. 21-22] et sa version originale se trouve dans le mémoire d'Euler intitulé *Solutio problematis ad geometriam situs pertinentis*, publié en 1741 [Euler, 1741a, p. 128].

> Nous avons dit que, si h est un nombre premier à m, et qu'on joigne de h en h, m points rangés en cercle dans l'ordre a, b, c, d, e, etc., on passera nécessairement par tous ces points avant de revenir au premier ; on peut voir également la réciproque de ce théorème, c'est-à-dire que, si, joignant de h en h, m points a, b, c, d, e, etc., on passe par tous ces points avant de revenir au point de départ, le nombre h sera nécessairement premier à m. Si donc, en unissant ainsi plusieurs points par des intervalles quelconques égaux, on ne peut jamais revenir au premier sans avoir passé par tous les autres, on pourra assurer que tous ces points sont en nombre premier absolument : ce qui donne une espèce de définition géométrique d'un nombre *premier*[POINSOT, 1810, p. 27-28].

On voit donc ici une construction de relations réciproques entre deux domaines des mathématiques que Poinsot étend également à l'algèbre avec la théorie des permutations et la théorie algébrique des équations. Il reprendra d'ailleurs cette image géométrique du nombre. Par exemple, dans le chapitre III de [POINSOT, 1845], intitulé *Démonstrations nouvelles tirées de la considération de l'ordre*, il démontrera certaines propriétés fondamentales des nombres à partir de cette définition géométrique. Par exemple, il prouvera que si deux nombres a et b sont premiers à un troisième nombre c, alors le produit ab est également premier au nombre c.

2 - L'*ordre* et la théorie des permutations

Après l'introduction générale, Poinsot consacre les trois premiers points de son texte à résumer son travail sur la théorie des permutations [28]. Le premier paragraphe ci-dessous correspond à un résumé de la première partie du manuscrit :

> Et d'abord, nous avons fait voir comment le système de toutes les permutations possibles de plusieurs choses, peut-être partagé en plusieurs groupes de permutations associées entre elles de manière que, malgré tous les échanges qu'on voudrait faire de ces choses, les permutations d'un même groupe ne pussent jamais se séparer. Et de même on a montré comment chacun de ces groupes principaux pouvaient se partager en groupes secondaires de permutations également inséparables ; et ainsi de suite pour les groupes successifs qui se subdivisent d'après les diviseurs du nombre total des permutations. On forme ainsi des tableaux qui offrent sur-le-champ plusieurs conséquences remarquables. Et, par exemple, on sait en algèbre que si l'on cherche à déterminer une fonction quelconque des racines d'une équation proposée, la résultante qui la donne s'élève au degré marqué par le nombre de toutes les permutations que ces racines pourraient offrir sous la fonction que l'on considère : or il résulte

28. En parcourant les publications de Poinsot relatives à l'algèbre ou la théorie des nombres, on trouve des références générales relatives à la théorie des permutations dans le commentaire du *Traité* de Lagrange analysé précédemment. Or, comme on va le voir, les idées présentées par Poinsot ici sont bien plus détaillées que dans son texte de 1808 mais sont souvent de simples paraphrases de ce qui se trouve dans le manuscrit étudié précédemment : nous n'analyserons donc que certains extraits.

de la théorie précédente que cette équation élevée n'a point de difficulté supérieure à celle de la proposée elle-même, et qu'elle peut actuellement se résoudre à l'aide d'équations de degrés marqués par les diviseurs de son exposant[Poinsot, 1818, p. 382-383].

En comparaison avec la publication de 1808, Poinsot réutilise le même vocabulaire : les *groupes de racines* sont remplacés par les *groupes de permutations* pour travailler sur le même sujet, la théorie générale des équations. La caractéristique du *groupe* pour les permutations reste la même que précédemment : « malgré tous les échanges qu'on voudrait faire de ces choses, les permutations d'un même groupe ne [peuvent] jamais se séparer ». Par contre, Poinsot ne précise pas quelle est la nature de ces *échanges*. L'étude des permutations pour la résolution des équations est une idée commune, mais la particularité de Poinsot est de mettre en avant les mécanismes validant les méthodes. On retrouve les idées fondamentales développées dans le manuscrit avec le partage des permutations d'une part, et la formation des groupes secondaires d'autre part.
Après avoir remarqué, comme dans le manuscrit, que cette première manière de partager les permutations ne permet pas d'en tirer des conséquences sur la résolution générale des équations, Poinsot signale sa deuxième façon de ranger les permutations : « en les faisant naître l'une de l'autre par une même loi ». Cela permet de comprendre très facilement les résultats obtenus par Lagrange concernant les équations du cinquième degré dans [Lagrange, 1772-1773] et d'obtenir des informations supplémentaires sur l'équation générale du 4^{e} degré. Néanmoins, dans sa présentation de 1817, il ne donne aucune précision sur la nature des *lois* utilisées pour classer les permutations. Pour finir, il tisse un lien entre ce sujet et la géométrie des polygones :

Or, le point le plus essentiel dans les spéculations de ce genre, étant la simplicité de la représentation de tant de formules, nous avons cherché, dans les nouveaux polygones que nous avons fait connaître, un moyen de les réduire et de les peindre avec une extrême facilité : de sorte que, par ces figures, on peut très-brièvement exposer, et, pour ainsi dire, montrer aux yeux, tout ce qu'on a trouvé jusqu'ici de plus général et de plus profond sur la résolution des équations algébriques[Poinsot, 1818, p. 385].

L'utilisation de la géométrie de situation sert donc ici à comprendre les résultats obtenus sur la théorie des permutations, et donc plus généralement la théorie générale des équations.

La transition entre la théorie des équations et la théorie des nombres est faite par Poinsot à l'aide d'un objet déjà cité précédemment : les racines primitives.

4. Cette théorie des permutations nous fait voir encore pourquoi toutes les équations binômes, et celles qui en dépendent, peuvent se résoudre algébriquement. Elle apprend à classer leurs racines imaginaires, de manière qu'elles se conjuguent entre elles d'après les diviseurs du nombre de ces racines ; etc., etc.
5. Elle conduit naturellement à la considération de cette espèce de nombres qu'Euler

a nommés *racines primitives*, et dont la nature et la détermination lui paraissaient l'un des points les plus difficiles de la théorie des nombres[Poinsot, 1818, p. 385].

Là encore, Poinsot ne détaille pas vraiment ses affirmations : ces résultats sont supposés maîtrisés par le lecteur. Le fait que ses réflexions sur la théorie des permutations permettent de justifier la résolubilité des équations binômes vient des *lois* indiquées plus tôt, et est à relier aux relations particulières existant entre les racines des équations binômes : elles sont toutes engendrées par les puissances successives d'une quelconque d'entre elles. Le lien avec les racines primitives s'explique par l'utilisation de ces dernières pour ranger les racines des équations binômes dans un ordre particulier : cet ordre permettra d'utiliser une même *loi* pour passer d'une racine à l'autre.

3 - L'*ordre* et la théorie des nombres

Poinsot justifie les travaux qu'il va résumer dans la suite de son exposé par l'étude des racines primitives : « nous nous sommes particulièrement appliqués à l'étude de ces nombres , et nous sommes parvenus à en découvrir l'expression analytique [29], en suivant une analogie singulière dont nous allons parler »[Poinsot, 1818, p. 385-386]. Poinsot explique comment il a eu l'idée de cette analogie : il a remarqué des faits analogues entre les racines primitives d'un nombre premier p, qui sont en fait certaines racines de la congruence $x^{p-1}-1 \equiv 0 \pmod{p}$, et les racines complexes de l'équation binôme $x^{p-1}-1=0$. Par exemple, les puissances successives d'une racine primitive r du nombre premier p donnent tous les résidus de 1 à $p-1$ après division par p. De manière analogue, la série des puissances successives de certaines racines imaginaires de l'équation $x^{p-1}-1=0$ donne toutes les racines de cette équation. Poinsot en déduit ainsi une analogie entre l'ensemble des racines de l'équation binôme $x^n - 1 = 0$ et l'ensemble des racines des congruences binômes $x^n - 1 \equiv 0 \pmod{p}$, où p est un nombre premier :

> Cette analogie remarquable, qu'il est facile d'étendre plus loin, et qui est complète, nous a fait penser que ces racines imaginaires devaient être la représentation analytique des racines primitives du nombre premier dont il s'agit : que, vues simplement comme résidus relatifs à ce nombre premier, elles leur devaient être tout-à-fait équivalentes : que, par conséquent, si l'on ajoutait aux nombres qui sont sous les radicaux, des multiples convenables de ce nombre premier (ce qui ne peut jamais altérer les valeurs résidues), ces expressions imaginaires deviendraient réelles, rationnelles et entières, donneraient exactement les racines primitives, et ne produiraient que ces seuls nombres. C'est en effet ce que nous avons établi de plusieurs manières, et confirmé par une foule d'exemples curieux[Poinsot, 1818, p. 386 - 387].

Cette analogie et la manière dont on peut passer des racines primitives de l'unité aux racines primitives modulo un nombre premier p est détaillée dans [Poinsot, 1820].

29. L'adjectif *analytique* utilisé par Poinsot semble indiquer que, grâce à sa méthode, les racines primitives d'un nombre premier vont être déterminées à l'aide d'une formule algébrique.

Poinsot y explique comment, à partir d'une racine complexe primitive de l'unité, on peut trouver les racines primitives du nombre p. A posteriori, on remarque que Poinsot construit une analogie entre deux domaines - théorie des équations et théorie des nombres - en remarquant des similarités entre les relations liant les objets qui composent des ensembles relatifs à ces deux domaines. Il met donc en avant des structures semblables, sans travailler avec la forme des objets. Il n'est pas le premier mathématicien à avoir eu l'idée de développer cette analogie, même s'il semble être le premier à l'avoir exposée dans une publication. En effet, comme nous l'avons indiqué dans l'introduction, les *Disquisitiones Arithmeticae* de Gauss aurait dû être composées d'une huitième section traitant des polynômes modulo un nombre premier p. Une version manuscrite de cette section VIII, qui aurait été rédigée au cours de l'année 1797 et qui est intitulée *Disquisitiones Generales de Congruentiis*, a été retrouvée en 1855 dans les papiers de Gauss, puis publiée en 1863 par Richard Dedekind dans le second tome des *Werke* de Gauss [30]. Selon Günther Frei, les recherches relatives à la section VII, où Gauss expose sa théorie de la cyclotomie, ont été initiées par l'étude des congruences binômes $x^n - 1 \equiv 0 \pmod{p}$, où p est un nombre premier. Nous pouvons ainsi citer plusieurs passages où l'auteur montre que Gauss utilise l'analogie entre les équations algébriques et les congruences pour construire sa théorie des polynômes modulo p :

> Gauss's theory of polynomials mod p in the *Caput Octavum* was planned to run parallel to the theory of rational integers as treated in the seven sections of the D.A. In particular, it was also to contain a theory of cyclotomy (division of the circle) modulo p. For these reasons, many proofs in the *Disquisitiones Arithmeticae* are formulated in such a way that they are not only valid for the domain of rational integers but also for the domain of polynomials over the integers or rationals or over a "finite field" with p elements, and even, as we would say today, for integral domains. This is one reason why the *Disquisitiones Arithmeticae* appeared so advanced and abstract for many readers[Frei, 2007, p. 164].
>
> [...]
>
> He announces that in the present section he will try to base the theory of congruences, at least as far as this is possible at present, on higher principles, following the salient analogy with the theory of [algebraic] equations, an analogy he has observed many times... [Frei, 2007, p. 178]
>
> [...]
>
> Gauss studies in detail how to find the roots of the cyclotomic polynomial $X^m - 1$ modulo a prime number p in terms of Gaussian periods, all expressed by means of a primitive root $\pmod{p}$[Frei, 2007, p. 188].

Ces affirmations sont très intéressantes puisque l'on retrouve des ressemblances frappantes avec les idées présentées par Poinsot, même si ce dernier les développe de façon

30. Les informations relatives à la section VIII des *Disquisitiones Arithmeticae* sont extraites de [Frei, 2007].

moins détaillée et moins technique que Gauss. Comme on le verra d'ailleurs lors de notre étude du *Mémoire sur l'application de l'algèbre à la théorie des nombres* de Poinsot, la justification du passage des équations binômes algébriques aux congruences binômes reprend la méthode utilisée par Gauss dans la section VII des *Disquisitiones Arithmeticae*.

Après quelques détails supplémentaires sur l'analogie construite, Poinsot commente le fait d'utiliser des nombres complexes en théorie des nombres :

> C'est au premier coup-d'œil, un étrange paradoxe que d'employer des imaginaires à la représentation actuelle de certains nombres entiers. Mais, quand on songe qu'il ne s'agit uniquement que de valeurs résidues, le paradoxe s'évanouit. Car si l'on remplace les nombres soumis aux radicaux par les puissances mêmes dont ils ne sont que les moindres résidus, toute l'expression devient claire et parfaitement égale aux nombres entiers dont il s'agit... [Poinsot, 1818, p. 387-388]

Là encore, plusieurs mathématiciens ont été confrontés à l'utilisation de nombres complexes dans le cadre de la théorie des congruences à cette époque. Gauss les utilise peu dans les *Disquisitiones Arithmeticae* et dans les *Disquisitiones Generales de Congruentiis*[31], mais s'appuie sur certaines classes de nombres complexes dans ses travaux sur les résidus biquadratiques, publiés entre 1825 et 1832. Il y introduit les nombres de la forme $a + bi$, où a et b sont des nombres entiers relatifs, que l'on appelle aujourd'hui *entiers de Gauss* et qui forment l'anneau $\mathbb{Z}[i]$. Il justifie ainsi l'introduction des nombres complexes en théorie des nombres :

> So leicht sich aber alle dergleichen specielle Theoreme durch die Induction entdecken lassen, so schwer scheint es, auf diesem Wege ein allgemeines Gesetz für diese Formen aufzufinden, wenn auch manches Gemeinschaftliche bald in die Augen fällt, und noch viel schwerer ist es, für diese Lehrsätze die Beweise zu finden.
>
> [...] Man erkennt demnach bald, dass man in dieses reiche Gebiet der höhern Arithmetik nur auf ganz neuen Wegen eindringen kann,[...] dass für die wahre Begründung der Theorie der biquadratischen Reste das Feld der höhern Arithmetik, welches man sonst nur auf die reellen ganzen Zahlen ausdehnte, auch über die imaginären erstreckt werden, und diesen das völlig gleiche Bürgerrecht mit jenen eingeräumt werden muss. Sobald man diess einmal eingesehen hat, erscheint jene Theorie in einem ganz neuen Lichte, und ihre Resultate gewinnen eine höchst überraschende Einfachheit[Gauss, 1863, p. 170 - 171][32].

31. Pour les références relatives à la théorie des résidus biquadratiques de Gauss, nous nous appuyons sur les analyses de [Goldstein et Schappacher, 2007a] et [Frei, 2007].

32. Ce passage est extrait de l'annonce (*Anzeige*) du texte *Theoria residuorum biquadraticorum. Commentatio secunda*, publié pour la première fois en 1832. Voici une traduction possible de ces paragraphes :

> Il est aussi facile de découvrir tous ces théorèmes particuliers par induction qu'il est difficile de trouver une loi générale pour ces formes de cette même manière, même si plusieurs caractéristiques communes sont évidentes.
>
> [...] On reconnaît bientôt que des approches totalement nouvelles sont nécessaires pour pénétrer ce riche domaine qu'est l'arithmétique supérieure, [...] que, pour le fondement réel de la théorie des résidus biquadratiques, le champ de l'arithmétique supérieure, qui s'était

Ainsi, l'utilisation des nombres complexes en théorie des nombres apporte de la simplicité, de la clarté pour les deux mathématiciens. Néanmoins, les nombres imaginaires considérés par Gauss et Poinsot en théorie des nombres sont très différents. L'étude des entiers de Gauss mène des années plus tard à la théorie des nombres algébriques, développée notamment par Kummer et Dedekind. Les nombres imaginaires introduits par Poinsot ne sont pas des entiers de Gauss. Comme nous le verrons dans notre étude de son *Mémoire sur l'application de l'algèbre à la théorie des nombres*, les nombres considérés par Poinsot font partie pour nous d'extensions algébriques des corps $\mathbb{Z}/p\mathbb{Z}$. D'autres mathématiciens vont introduire ce type de nombres dans leurs travaux de théorie des nombres dans les années 1820, c'est-à-dire peu de temps après la publication des mémoires en question de Poinsot. On peut évoquer Jacobi dont un article de quatre pages est publié dans le deuxième tome du *Journal de Crelle* en 1827. Ce texte s'intitule *De residuis cubicis commentatio numerosa* et contient des résultats sans démonstration donnant des indications sur les relations des caractères cubiques de deux nombres premiers, en considérant des nombres imaginaires de la forme $a + b\sqrt{-3}$, où a et b sont des nombres entiers, modulo un nombre premier. Comme nous l'avons évoqué plus haut, Cournot en résume le contenu dans le *Bulletin de Férussac*, après avoir remarqué que des travaux de Gauss à ce sujet sont attendus depuis quelques années déjà :

> A son imitation, M. Jacobi, qui a beaucoup médité sur le même sujet, nous fait part, sans les démontrer, de trois théorèmes principaux découverts par lui, mais en y joignant quelques éclaircissements et notamment l'annonce d'une théorie neuve et piquante, celle des racines imaginaires des congruences et de leurs racines primitives. Depuis long-temps nous avions pensé (et les derniers mémoires de M. Poinsot l'indiquaient assez clairement) que la considération de cette sorte de racines était nécessaire pour compléter la théorie des nombres et étendre ses rapports avec l'analyse algébrique[Cournot, 1827].

Rappelons que Galois étudie ces nombres imaginaires dans son article *Sur la théorie des nombres* publié en 1830 dans le treizième tome du *Bulletin de Férussac*. Ce texte porte sur l'étude de toutes les racines des congruences de degré supérieur à 2. Galois réduit ses recherches au cas particulier où la congruence est irréductible modulo p et il indique alors une analogie possible entre les nombres complexes et les racines de la congruence ainsi considérée :

> Dans ce cas, la congruence n'admettra donc aucune racine entière, ni même aucune racine incommensurable de degré inférieur. Il faut donc regarder les racines de cette congruence comme des espèces de symboles imaginaires, puisqu'elles ne

auparavant prolongé aux entiers réels uniquement, doit être étendu pour inclure également les entiers imaginaires et que l'on doit donner exactement le même droit de citoyenneté à ces derniers qu'aux premiers. Dès que l'on a intégré cela, cette théorie apparaît sous une lumière totalement nouvelle, et ses résultats acquièrent une étonnante simplicité.

satisfont pas aux questions de nombres entiers, symboles dont l'emploi dans le calcul sera souvent aussi utile que celui de l'imaginaire $\sqrt{-1}$ dans l'analyse ordinaire. [...]

C'est la classification de ces imaginaires et leur réduction au plus petit nombre possible, qui va nous occuper[Galois, 1830, p. 428].

Rappelons également que le travail de Galois relatif à ces nombres, qualifiés aujourd'hui d'« imaginaires de Galois », est notamment repris par Serret dans la troisième édition du *Cours d'algèbre supérieure*[33], dans un paragraphe intitulé *De point de vue sous lequel Galois a envisagé les congruences suivant un module premier et une fonction modulaire.* Serret indique d'ailleurs : « Ainsi peuvent s'introduire dans l'analyse de nouvelles imaginaires dont l'emploi offre certains avantages, bien qu'il ne soit pas indispensable. Cette conception est entièrement due à Galois, qui l'a exposée succinctement dans le *Bulletin des Sciences mathématiques de Férussac* »[Serret, 1866, p. 178]. Néanmoins, même si l'étude de ces nombres par Galois est bien plus approfondie que celle de Poinsot, c'est bien ce dernier qui les utilise plusieurs années auparavant dans son *Mémoire sur l'application de l'algèbre à la théorie des nombres* lu en 1818 à l'Académie des Sciences.

Dans ce texte, Poinsot nous livre bien un tour d'horizon des sujets qu'il aborde dans le cadre de sa *théorie de l'ordre*. Il indique les principales idées qu'il développe plus précisément dans ses textes : cela lui permet d'annoncer à l'Académie ses recherches en géométrie, algèbre et théorie des nombres articulées autour de la notion fondamentale d'*ordre* (qu'il ne définit toutefois pas de manière explicite). Les sujets abordés sont étudiés par d'autres mathématiciens dans ce premier tiers du XIX^{e} siècle. Nous allons maintenant examiner un mémoire plus original.

IV 1820 : analogies entre les équations et les congruences binômes

Le mémoire que l'on va étudier ici a été présenté en 1818 à l'Académie sous le nom de *Représentation analytique des résidus des puissances par la formule des racines imaginaires de l'unité*, publié en 1820 dans le *Journal de l'École Polytechnique* et en 1824 dans les *Mémoires* de l'Académie sous la forme d'un texte intitulé *Mémoire sur l'application de l'algèbre à la théorie des nombres*, puis présenté par Cournot dans le *Bulletin de Férussac* en 1825. Le contenu de ce mémoire était déjà annoncé dans le texte présenté en 1817 à l'Académie, commenté précédemment.

33. Voir [Serret, 1866, p. 178-188].

1 - Sur le sens du résultat

L'objectif de ce mémoire est d'utiliser une analogie entre les équations binômes $x^n - 1 = 0$ et les congruences $x^n - 1 \equiv 0 \pmod{p}$, où p est un nombre premier et n est, dans un premier temps, un diviseur de $p - 1$, afin de résoudre ces dernières :

> J'ai observé les propriétés analogues de ces nombres entiers et de ces racines imaginaires ; et, suivant jusqu'au bout cette analogie, j'ai avancé que la formule générale qui résout l'équation binôme $x^n - 1 = 0$, est, dans le sens que je vais dire, la représentation analytique de chacun des nombres entiers qui résolvent l'équation semblable, $x^n - 1 = Mp$, mais où le second membre, au lieu d'être nul, désigne un multiple du nombre premier p ou du module que l'on considère.
> Ce théorème remarquable est la base de toute la théorie des *résidus des puissances*... [Poinsot, 1820, p. 343]

Pour justifier cela, nous allons voir que Poinsot s'appuie une fois de plus sur les travaux de Gauss dans les *Disquisitiones Arithmeticae*, et plus particulièrement sur la section VII. Avant de donner l'énoncé exact de son théorème et d'en donner une démonstration, Poinsot illustre à l'aide d'exemples la façon dont on peut passer d'égalités absolues à des égalités modulo un nombre premier p, après avoir explicité le lien entre ces deux types d'égalités : « Cette égalité consiste proprement dans celle des restes que laisseraient les deux membres relativement à ce module ; de manière qu'en l'ajoutant une ou plusieurs fois aux divers nombres qui se trouvent engagés dans la proposée, on rendrait les membres parfaitement égaux entre eux, et que cette égalité relative dont nous parlions deviendrait une égalité absolue »[Poinsot, 1820, p. 343]. Poinsot présente trois exemples : $\sqrt{-1} = \pm 2$ «relativement au module 5» (car $\sqrt{-1+5} = \sqrt{4} = \pm 2$). Puis : $\sqrt{-1}$ modulo 13, qui revient à $\sqrt{-1+2\times 13} = \sqrt{25} = \pm 5$ modulo 13. Enfin, il utilise la formule d'une des racines cubiques de l'unité : $\dfrac{-1+\sqrt{-3}}{2}$, avec $p = 7$. Comme, dans $\mathbb{Z}/7\mathbb{Z}$, $-3 = -3 + 7 = 4$, l'expression précédente revient à $\dfrac{-1+7+\sqrt{-3+7}}{2}$, ce qui est égal à 2 ou 4 selon le signe choisi pour $\sqrt{4}$. Pour les deux premiers exemples, le module est un nombre premier de la forme $4n+1$, ce qui correspond au cas où le nombre -1 est un résidu quadratique modulo p. Il est donc certain que l'on puisse trouver un multiple np de p tel que $-1 + np$ soit un carré. De même, on peut démonter facilement que le nombre -3 est un résidu quadratique modulo 7. Mais Poinsot ne précise à aucun moment pourquoi il a choisi ces exemples. La raison de ce silence peut être que, depuis la publication des ouvrages de théorie des nombres de Legendre et Gauss, les résultats liés aux résidus quadratiques et en particulier à la loi de réciprocité quadratique font partie du "bagage nécessaire" pour qui veut lire des travaux de théorie des nombres[34].

34. De même, Poinsot ne revient pas sur la définition de la notation $\sqrt{4}$ modulo p. En effet, dans une égalité absolue, c'est-à-dire en considérant les nombres réels, l'équation $x^2 = 4$ a deux solutions mais la

Enfin, Poinsot fait quelques remarques générales autour de cette analogie. D'une part, il insiste sur la puissance de cette propriété qui met en avant des relations entre une infinité d'ensembles de nombres, les solutions de l'équation $x^n = 1$ et les solutions des équations $x^n \equiv 1 \pmod{p}$ pour n'importe quel nombre premier p :

> Sous ce point de vue donc, je dis que l'expression algébrique imaginaire qui rend nul le binôme $x^n - 1$, représente les divers nombres entiers qui rendent ce même binôme multiple d'un nombre premier p.
>
> [...]C'est en cela sur-tout que consistent la nouveauté et l'étendue de notre théorème : car on n'aperçoit aucune relation, ni entre les divers nombres qui résolvent la proposée pour un module particulier, ni entre les différentes classes des nombres qui la peuvent résoudre pour des modules différens ; et pourtant nous voyons que tous ces nombres sont réductibles à une même expression imaginaire, composée de nombres actuellement déterminés et connus, qui ne dépendent point des modules, mais uniquement du degré de la proposée. Cette réduction si frappante, cette même représentation analytique de tant de nombres différens, et qui ne paraissent soumis à aucune loi, nous indique de nouvelles routes dans l'analyse indéterminée, et nous offre, comme on l'a dit, le premier et singulier exemple de l'application de l'algèbre à la théorie des nombres[Poinsot, 1820, p. 344].

Il ajoute que ce résultat peut d'ailleurs se généraliser, mais que la démonstration en est bien plus difficile. L'intérêt d'exposer cette théorie pour les équations binômes est qu'elles forment une classe d'équations qui est la base de la résolution des équations générales. Il rappelle enfin que, comme il l'a déjà indiqué en 1817, son théorème permet de déterminer les racines primitives d'un nombre premier p : on les obtient en effet à partir de l'expression des racines complexes primitives de l'équation $x^{p-1} - 1 = 0$. Mais la méthode de Gauss pour résoudre les équations binômes se base sur l'utilisation des racines primitives modulo un nombre premier p. Poinsot remarque donc que son théorème peut sembler amener à « une espèce de cercle vicieux »[Poinsot, 1820, p. 345], ce qui n'est pas le cas : en effet, pour déterminer les racines primitives du nombre premier p, il faut résoudre la congruence $x^{p-1} - 1 \equiv 0 \mod p$, qui correspond à l'équation binôme $x^{p-1} - 1 = 0$. Or, résoudre cette équation à l'aide de la méthode de Gauss revient à résoudre des équations binômes de la forme $x^k - 1 = 0$, où k est un diviseur premier du nombre $p - 1$: cela nécessite donc de connaître une racine primitive du nombre premier $k < p$. Il observe également que sa méthode, qui permet de déterminer les racines primitives d'un nombre premier, est très indirecte mais que l'intérêt est ici de mettre en avant «la théorie et les méthodes

notation $\sqrt{4}$ désigne le nombre 2, c'est-à-dire la racine positive de l'équation. Par contre, la notation $\sqrt{4}$ modulo p, désigne ici une des racines de l'équation $x^2 \equiv 4$ modulo p. Gauss, dans les *Disquisitiones Arithmeticae*, explicite cette différence : « et comme $\sqrt[n]{A}$ ne signifie autre chose que la racine de l'équation $x^n = A$; en ajoutant le module, $\sqrt[n]{A} \pmod{p}$ représentera une racine quelconque de la congruence $x^n \equiv A \pmod{p}$ »[Gauss, 1801, art. 60].

générales»[Poinsot, 1820, p. 346] [35].

Poinsot explique enfin les fondements de sa démonstration en abordant la résolution de l'équation réciproque $x^{n-1} + x^{n-2} + x^{n-3} + \ldots + x + 1 = 0$. Il se réfère alors à Lagrange, Vandermonde et Gauss, qui a rangé les racines telles que leurs exposants forment « la suite naturelle des puissances d'une racine primitive du nombre premier n ». La considération des racines primitives permet en effet la résolution systématique des équations binômes : en utilisant l'ordre de Gauss obtenu à l'aide des racines primitives, toute substitution de racines induit une permutation simultanée de ces racines qui est de plus circulaire.

2 - Théorème et démonstration

Après ces généralités, Poinsot énonce le théorème qui permet de déterminer les racines des congruences $x^n \equiv 1 \pmod{p}$ à partir des racines de l'équation $x^n = 1$:

> Considérons donc l'équation binôme indéterminée, $x^n - 1 = Mp$, où Mp désigne un multiple quelconque du nombre premier p, et n un exposant quelconque premier, que je supposerai d'abord diviseur de $p - 1$, afin que l'équation $x^n - 1 = Mp$ ait n racines ou solutions en nombres entiers inférieurs à p. Je dis que si l'on prend, à la place de cette équation indéterminée, l'équation binôme déterminée $x^n - 1 = 0$, et qu'on la résolve, l'expression algébrique de ses n racines, qui, excepté l'unité, sont toutes imaginaires, sera la représentation analytique des n nombres entiers qui résolvent l'équation $x^n - 1 = Mp$; c'est-à-dire qu'en ajoutant aux nombres qui sont sous les divers radicaux de cette formule imaginaire, des multiples convenables de p, on fera disparaître les imaginaires et les irrationnelles, on rendra toutes les opérations indiquées parfaitement exécutables, et l'on parviendra précisément aux n nombres entiers qui satisfont à la proposée $x^n - 1 = Mp$[Poinsot, 1820, p. 349].

Dans ce texte, il n'aborde que le cas des congruences binômes où le module p est un nombre premier. Il considère dans un premier temps le cas où le nombre n est premier et divise $p - 1$, puis il justifie le cas plus général où n est un nombre composé. Enfin, il donne des exemples pour le cas où $n - 1$ ne divise pas le nombre p. Il étudiera des cas plus généraux dans [Poinsot, 1845] [36].

35. Il donne d'ailleurs des méthodes de recherche de racines primitives plus efficaces dans ses textes de 1817 et 1845.

36. Dans les *Disquisitiones Arithmeticae*, Gauss indique le nombre de racines de l'équation $x^n \equiv 1 \pmod{p}$. Il trouve cette quantité à l'aide de la notion d'*indice*, mais annonce qu'il compte démontrer ces résultats à l'aide de « considérations plus profondes »[Gauss, 1801, art. 61] dans la section VIII. Gauss étudie également cette équation pour un module de la forme p^k à l'aide des outils qu'il a introduits précédemment, tout en ajoutant qu'il en proposera une preuve plus simple dans la section VIII. De son côté, Poinsot détermine, dans son texte de 1845, le nombre de racines de l'équation $x^n \equiv 1 \pmod{p}$ en démontrant que l'équation $x^n \equiv 1 \pmod{p}$ admet les mêmes racines que l'équation $x^\theta \equiv 1 \pmod{p}$, où θ est le plus grand diviseur commun de n et de $p - 1$. C'est la méthode qui est reprise par Serret dans son *Cours d'Algèbre Supérieure*.

Pour démontrer le cas où n est un nombre premier [37] diviseur de $p-1$, Poinsot transpose les étapes fondamentales de la méthode de Lagrange, exposée dans la Note XIV de son *Traité de la résolution des équations numériques de tous les degrés*, pour la résolution des équations binômes en termes de congruences. Comme dans son *Analyse du traité*, il commence par insister sur la forme des racines des équations binômes et sur la « considération ingénieuse »[Poinsot, 1820, p. 348] de Gauss, à savoir l'utilisation des racines primitives. Ainsi, la résolution de l'équation $x^n - 1 = Mp$ se ramène à la résolution de l'équation $x^{n-1} + x^{n-2} + x^{n-3} + \ldots + x + 1 = Mp$, où les racines sont des nombres entiers supérieurs à l'unité (car $n < p$). Si r est solution de cette équation, alors r^2, r^3, r^4, $\ldots$, r^{n-1} le seront également. Il considère alors la suite, déjà considérée par Gauss dans la section VII des *Disquisitiones Arithmeticae*, r, r^a, r^{a^2}, r^{a^3}, $\ldots$, $r^{a^{n-1}}$, où a est une racine primitive du nombre n. Ainsi :

> [...] les racines de la proposée, non-seulement sont représentées par les différentes puissances d'une *même* racine, mais encore elles sont rangées dans un ordre où chacune d'elles est une *même* puissance de celle qui la précède.
>
> [...] cet ordre ingénieux, dont rien ne paraît d'abord nous indiquer le choix entre tous les autres, est au fond un ordre analytique déterminé par la nature même des choses. Car, comme il s'agit de racines qui jouissent toutes également de la même propriété, et qu'il n'y a aucune raison de préférer l'une à l'autre, il est clair que l'ordre le plus naturel est celui qui conviendrait également à toutes les racines, et qui par conséquent ne changerait point, quelle que fût la racine r d'où l'on voulut partir. Ainsi, par la nature même de la question, on est porté à chercher, s'il est possible, un ordre où les racines naîtraient successivement l'une de l'autre par la même fonction, et où il serait alors indifférent d'y changer une racine en une autre quelconque à volonté.
>
> [...] aucun échange de racines ne pourra troubler l'ordre ; les racines ne feront que s'avancer toutes à la fois d'un même nombre de places, et elles garderont toujours entre elles la même disposition, exactement comme si elles étaient rangées en cercle[Poinsot, 1820, p. 350-351].

Une fois de plus, Poinsot met ici la notion d'*ordre* en avant en détaillant pourquoi l'ordre obtenu à partir de l'utilisation des racines primitives permet d'obtenir la solution du problème et comment on peut y penser *a priori*. Il donne au lecteur une définition très précise de l'*ordre* auquel il semble se référer dans sa *théorie de l'ordre* : non seulement, chaque élément est représenté par une puissance d'un même objet primitif, mais ces objets sont rangés de telle sorte que pour passer de l'un à l'autre, on applique toujours la même *loi* ou la même *fonction*. Cela caractérise bien les ensembles étudiés par Poinsot - racines des équations binômes, permutations - et également par Gauss. De plus, en utilisant à

37. Le cas où n est composé et diviseur de $p-1$ se déduit de celui où n est premier et Poinsot l'aborde sans le justifier à la fin de la démonstration ; il le détaillera dans son mémoire de 1845.

nouveau l'image du cercle, Poinsot met encore en avant le fait que ces ensembles sont cycliques pour la *loi* choisie.

Poinsot expose alors sa démonstration en s'appuyant sur les travaux de Gauss revus par Lagrange et en transposant les égalités absolues en des égalités modulo p dans les raisonnements des deux mathématiciens. Il justifie cette transposition par l'addition ou la soustraction d'un certain multiple du nombre premier p, puis conclut enfin sur le contenu de son théorème :

> Mais il est évident que cette supposition de $r^n = 1$, au lieu de $r^n = 1 + Mp$, et de $r + r^2 + r^3 + \&c. = -1$ au lieu de $r + r^2 + r^3 + \&c. = -1 + Mp$, revient à supprimer dans les expressions θ, θ', θ'', & c. qui sont sous les radicaux, certains multiples du nombre premier p que l'on considère. Donc, puisque par cette suppression de multiples p, on passe de l'expression du nombre entier r, à l'expression de la racine imaginaire n^{e} de l'unité, il s'ensuit que, par la restitution dans celle-ci de ces mêmes multiples de p, on reviendrait à l'expression exacte du nombre entier r[Poinsot, 1820, p. 354].

En énonçant son théorème, Poinsot construit une analogie entre les racines complexes de l'équation $x^n - 1 = 0$ et les racines des congruences $x^n - 1 \equiv 0$ modulo un nombre premier p, qu'il prolonge sans justification dans sa démonstration.

Poinsot considère ensuite une autre décomposition , en utilisant des *groupes* particuliers des racines :

> [...] au lieu de considérer à la fois toutes les racines r, r^2, r^3, r^4, r^5, & c. r^{n-1}, il faudra les partager en plusieurs groupes de racines liées entre elles de la même manière. On formera immédiatement chacun de ces groupes au moyen de la suite ordonnée,
>
> $$r, r^a, r^{a^2}, r^{a^3}, r^{a^4}, \&c.,\ r^{a^{n-2}},$$
>
> en y prenant les racines de h en h, si h est un diviseur de $n - 1$. On aura ainsi h groupes composés de $\frac{n-1}{h}$ racines ; et ces divers groupes seront aussi ordonnés entre eux, de manière que chacun d'eux produira le suivant, en y changeant la racine r en r^a.
>
> On décomposera de même chaque groupe, en y prenant les racines de k en k, si k est un diviseur de leur nombre $\frac{n-1}{h}$, et ainsi de suite. Et si l'on applique enfin à la représentation des racines de ces groupes partiels, et des sommes de racines contenues dans ces groupes eux-mêmes, une analyse toute semblable à celle qu'on a suivie plus haut pour l'ensemble de toutes les racines, on parviendra facilement à une formule qui ne présentera point de radicaux d'exposans supérieurs aux facteurs 2, h, k, &c. du nombre composé $n - 1$... [Poinsot, 1820, p. 356]

Comme précédemment, Poinsot s'appuie sur le travail que Gauss a exposé pour la résolution de l'équation $x^n - 1 = 0$, les *périodes* de Gauss devenant des *groupes de racines*. Cet extrait est également similaire à ce que l'on trouve dans le manuscrit de Poinsot sur

les permutations, lorsqu'il décompose les groupes de permutations en *groupes secondaires*, *groupes ternaires*, ... On retrouvera des raisonnements similaires à la fin de ce *Mémoire*.

Poinsot aborde alors le cas où n n'est pas un diviseur de $p-1$:

> Lorsque n ne divise pas $p-1$, l'équation indéterminée $x^n - 1 = Mp$ n'a qu'une seule racine ou solution entière, qui est l'unité ; et toutes les autres sont impossibles ou irrationnelles. Mais la formule des racines $n.^{\text{mes}}$ de l'unité n'en est pas moins encore l'expression analytique de ces racines même impossibles[Poinsot, 1820, p. 357].

En effet, ces racines vérifient les mêmes conditions (leur somme doit être égale à $-1 + Mp$), et on peut donc reproduire le raisonnement précédent. Cette remarque est importante dans le sens où la considération de ces racines *impossibles* est une première introduction des nombres complexes dans la théorie des congruences. Poinsot avait d'ailleurs déjà insisté sur ce point dans son exposé de 1817.

Pour illustrer son théorème et donner un exemple de ces racines *impossibles*, Poinsot prend l'exemple de l'équation $x^3 - 1 = Mp$ pour $p = 43$, cas où le nombre 3 divise le nombre $p-1$, puis pour $p = 29$, qui est un cas où 3 ne divise pas $p-1$. Dans les deux cas, il utilise l'expression des deux racines complexes de l'équation $x^3 - 1 = 0$: $\frac{-1\pm\sqrt{-3}}{2}$. Dans le cas où $p = 43$, -3 est résidu quadratiques modulo 43, et on obtient donc trois racines entières qui « existent réellement »[Poinsot, 1820, p. 358] : -7 et 6 à partir de la formule ci-dessus et l'unité [38]. Dans le cas où $p = 29$, -3 n'est pas un résidu quadratique, donc le radical $\sqrt{(-3)}$ ne deviendra jamais un nombre entier modulo 29. Poinsot explique comment on peut néanmoins obtenir une expression des racines imaginaires de l'équation considérée :

> Mais si $p-1$ n'est pas divisible par 3, comme dans le cas de $p = 29$, alors il n'y a que le seul nombre entier 1 à chercher, et les deux autres racines sont impossibles ; mais on peut toujours supposer ces racines également représentées par la formule $\frac{-1\pm\sqrt{-3}}{2}$, que l'on changera, si l'on veut , en $\frac{-1+ip\pm\sqrt{(-3+op)}}{2}$, en ajoutant aux nombres les multiples ip et op du module p. A la vérité, on ne pourra jamais, par cette addition, rendre le nombre -3 un carré parfait, et la quantité $\frac{-1+ip\pm\sqrt{(-3+op)}}{2}$ sera toujours une incommensurable, quelque soit le multiple de p que l'on veuille introduire : mais cette expression irrationnelle, pouvant toujours satisfaire à l'équation $x^3 - 1 = Mp$ (comme on le voit en supposant i et o tous deux nuls, ou même seulement, $3i^2p - 6i + o = 0$), sera l'expression analytique de ces racines même impossibles. Cette expression sera donc aussi parfaite que celle des imaginaires dans l'analyse ; je veux dire qu'on pourra, sans crainte, l'employer dans le calcul, et que si, par une combinaison quelconque de semblables valeurs, les irrationnelles viennent à se détruire, le résultat final sera

38. En effet : $-3+4\times43 = 169 = 13^2$ donc $\frac{-1\pm\sqrt{-3}}{2} = \frac{-1\pm13}{2} = 6$ ou -7. On vérifie d'ailleurs facilement que ces deux nombres sont bien solutions de la congruence binôme $x^3 - 1 \equiv 0 \bmod 43$. Dans son texte, Poinsot indique que les solutions de cette congruence sont -6 et 7 : on suppose qu'il s'agit d'une erreur de signe.

> aussi exact, et la démonstration aussi bien établie, que si l'on eût point passé par ces valeurs irrationnelles[Poinsot, 1820, p. 359].

Poinsot donne de façon explicite l'expression des racines complexes d'une congruence, de manière analogue aux nombres complexes. Néanmoins, il ne justifie ni l'existence ni la validité des opérations pour ces nombres imaginaires dans $\mathbb{Z}/p\mathbb{Z}$, et ne fait aucun commentaire sur les difficultés que l'introduction de ces nombres peut impliquer. Il admet pourtant que l'on peut « sans crainte, [les] employer dans le calcul [...] », ce qu'il fait plus loin pour analyser des exemples particuliers où l'on retrouve des expressions des racines faisant apparaître des nombres imaginaires qui s'annulent entre eux[39]. D'autre part, comme on l'a observé précédemment, Poinsot ne cite à aucun moment les travaux d'Euler, Legendre ou Gauss relatifs à la théorie des résidus quadratiques, alors qu'il doit s'en servir pour construire les exemples convenables. Ces résultats peuvent effectivement être supposés connus des lecteurs de Poinsot. Cette absence de référence reste cependant surprenante puisque Poinsot fait régulièrement référence aux travaux de ses prédécesseurs pour la théorie algébrique des équations.

Après avoir détaillé quelques exemples, montré comment l'on peut déterminer les racines primitives d'un nombre premier à l'aide de sa méthode, et déduit des théorèmes généraux, Poinsot conclut :

> Je reviendrai ailleurs sur ce rapprochement curieux de l'algèbre et de la théorie des nombres ; et je ferai voir que les principes généraux de l'analyse mathématique ont leur source naturelle dans la simple considération de l'*ordre*, ou de la disposition mutuelle qu'on peut observer actuellement entre plusieurs objets : ce qui me paraît le plus haut point d'abstraction et de généralité où il soit permis de porter la science[Poinsot, 1820, p. 402].

Ce passage résume bien les idées fondamentales des travaux de Poinsot en algèbre et en théorie des nombres. Ici, Poinsot raisonne de manière plus générale : l'*ordre* devient le fondement de l'*analyse mathématique*. Poinsot ne précise pas ce qu'il entend par cette expression. Au XIX^{e} siècle, l'*analyse mathématique* peut désigner une méthode générale ou une discipline incluant la théorie des équations[40]. La notion d'*ordre* est également utilisée de manière plus générale que précédemment : ici, Poinsot ne relie pas l'*ordre* à des structures cycliques comme on a pu le voir jusqu'ici, mais à la *disposition mutuelle qu'on peut observer actuellement entre plusieurs objets*. Poinsot insiste ainsi sur l'importance de l'étude des relations qui peuvent exister entre les objets d'un même ensemble.

39. Poinsot étudie dans ce mémoire (pages 116-120) l'équation $x^7 - 1 = Mp$ pour $p = 43$ et $p = 29$ que nous ne détaillerons pas dans ce texte. Dans le deuxième cas, on retrouve des racines cubiques incommensurables modulo p qui se simplifient entre elles.

40. On pourra notamment se reporter à [Sinaceur, 1991, p. 51]

3 - Un retour sur la notion d'ordre

Le mémoire se termine par une addition sur les différentes manières dont on peut partager les racines des équations binômes. Poinsot y montre dans un premier temps pourquoi l'ordre dans lequel sont rangées les racines de l'équation binôme à partir d'une racine primitive ne dépend ni de la racine r de l'équation binôme de degré n que l'on prend pour commencer, ni de la racine primitive a choisie [41].

En effet, si on considère l'ordre

$$r, r^a, r^{a^2}, r^{a^3}, \ldots, r^{a^{n-1}},$$

et que l'on parcourt les racines de h en h, où h est un nombre inférieur et premier à n. On passera alors par toutes les racines avant de revenir à celle de départ. On obtient ainsi un nouvel ordre :

$$r, r^{a^h}, r^{a^{2h}}, r^{a^{3h}}, \ldots, r^{a^{(n-2)h}}.$$

Si on pose $b = a^h$, b est également une racine primitive du nombre n, et l'ordre précédent peut s'écrire :

$$r, r^b, r^{b^2}, r^{b^3}, \ldots, r^{b^{n-1}}.$$

Poinsot nous explique alors pourquoi ces deux suites peuvent être considérées comme dans le même ordre :

> Ainsi, les différens ordres qu'on peut former en employant les différentes racines primitives de n sont comme un seul et même ordre, mais où l'on regarderait les $n-1$ racines r, r^a, r^{a^2}, r^{a^3}, & c. soit de suite ou de 1 en 1, soit de h en h, soit de h' en h', & c. ; & , h ,h', & c., étant les différens nombres inférieurs et premiers à $n-1$. Et comme l'idée de cet intervalle plus ou moins grand , par lequel on va de l'une à l'autre, ne peut entrer dans l'idée de l'*ordre*, qui, par sa nature, ne dépend point de la *grandeur*, il s'ensuit que ces différens ordres coexistent tous dans un seul quelconque d'entre eux, comme les racines d'une même équation, sans qu'on puisse les distinguer ou les isoler par aucune analyse[Poinsot, 1820, p. 404].

Poinsot approfondit encore les concepts de *grandeur* et d'*ordre* dans son mémoire de 1845. On peut donc considérer les différents ordres obtenus à partir de racines primitives différentes comme équivalents si l'on ne prend en compte que la notion d'ordre. Par exemple, on peut obtenir la suite de racines $r, r^b, r^{b^2}, r^{b^3}, \ldots, r^{b^{n-1}}$ donnée par Poinsot ci-dessus en considérant les racines de la suite $r, r^a, r^{a^2}, r^{a^3}, \ldots, r^{a^{n-1}}$ de h en h. Avant de développer cette idée sur l'exemple $x^{13} - 1 = 0$, Poinsot fait à nouveau un parallèle entre

41. Gauss démontre également cette indépendance : on pourra se reporter à l'article 343 des *Disquisitiones Arithmeticae*.

la théorie des nombres et la géométrie, en reliant la disposition des racines les unes par rapport aux autres à celle des sommets d'un polygone régulier.

Après avoir donné les différents ordres équivalents que l'on peut obtenir à partir des racines de l'équation $x^{13} - 1 = 0$, Poinsot remarque que l'intérêt de prendre cet ordre pour les racines est que cela montre que les racines sont liées deux à deux, mais plus généralement d à d, où d est un diviseur de $p - 1$, soit 12 dans l'exemple actuel. Cela revient à représenter les périodes que Gauss a défini dans les *Disquisitiones Arithmeticae* pour la résolution de l'équation cyclotomique. En effet, il considère l'ordre des racines que l'on obtient à partir de la racine primitive 2 :

$$r, r^2, r^4, r^8, r^3, r^6, r^{12}, r^{11}, r^9, r^5, r^{10}, r^7.$$

On a $12 = 4 \times 3$, donc en prenant les racines de 4 en 4, on forme 4 groupes de 3 racines (ce qui correspond aux 4 périodes de Gauss formées de 3 éléments) :

$$(r, r^3, r^9) \quad (r^2, r^6, r^5) \quad (r^4, r^{12}, r^{10}) \quad (r^8, r^{11}, r^7).$$

Ces quatre groupes sont en fait constitués des racines (r^h, r^{h+4}, r^{h+8}), où h est un des nombres 1, 2, 4, 8 selon les groupes. Donc, si on remplace par exemple r^h par r^{h+4}, on obtient le groupe : $(r^{h+4}, r^{h+8}, r^{h+12})$. Or, $r^{h+12} = r^h r^{12} = r^h$, et on obtient bien le groupe de départ. Poinsot développe ici les relations existant entre les différents *groupes*, ce qui rappelle la partie *Conjugaison mutuelle des groupes* de son manuscrit sur la théorie des permutations.

Ainsi, si l'on construit une fonction φ symétrique des trois racines r, r^3, r^9, notée $\varphi(r)$, cette fonction ne prendra que quatre valeurs : $\varphi(r)$, $\varphi(r^2)$, $\varphi(r^4)$, et $\varphi(r^8)$. Donc cette fonction sera déterminée par une équation du quatrième degré. Ainsi, tout polynôme symétrique élémentaire de ces quatre fonctions sera symétrique en r, r^2, r^3, ... et pourra être déterminé.

On peut réitérer ce raisonnement en rassemblant les groupes[42] 2 à 2 : $(\varphi(r), \varphi(r^4))$ et $(\varphi(r^2), \varphi(r^4))$. Poinsot en conclut donc que la résolution de l'équation du quatrième degré se réduit à celle de deux équations quadratiques.

4 - Conclusion

Même s'il l'avait auparavant présenté dans son *Extrait de quelques recherches nouvelles...*, Poinsot expose pour la première fois un nouveau résultat de théorie des nombres. De plus, la méthode exposée ici pour résoudre les congruences binômes est très différente de l'approche utilisée par Gauss dans les *Disquisitiones Arithmeticae*, où il raisonne à

42. Poinsot confond ici les écritures des groupes de racines avec celles des fonctions symétriques en ces racines. On peut observer que Gauss faisait de même dans les *Disquisitiones Arithmeticae*, lorsqu'il n'y avait pas d'ambiguïté possible.

partir de la notion d'*indice*. La méthode de Poinsot s'appuie notamment sur une analogie entre la structure de l'ensemble des racines de l'équation binôme $x^n - 1 = 0$ d'une part et celle des racines des congruences $x^n - 1 \equiv 0$ modulo un nombre premier d'autre part. C'est cette analogie qui l'autorise (bien sûr sans aucune justification) à transposer des raisonnements des nombres complexes aux résidus modulo p. D'autre part, il considère également des racines imaginaires modulo un nombre premier p, ce qui est un autre point original de son travail puisque celui-ci est une des premières publications sur la théorie des congruences contenant des raisonnements sur les nombres complexes.

Poinsot présente donc au lecteur un texte développant des outils innovants de théorie des nombres. Néanmoins, ce *Mémoire sur l'application de l'algèbre à la théorie des nombres* est surtout basé, comme les travaux précédents de Poinsot, sur les résultats déjà obtenus par Gauss. Poinsot s'intéresse au sujet de la section VIII inédite des *Disquisitiones Arithmeticae* : les congruences supérieures développées en parallèle avec les équations. D'autre part, comme nous l'avons indiqué précédemment, Poinsot se réfère régulièrement à Gauss et Lagrange dans ses raisonnements autour de la théorie algébrique des équations et utilise explicitement leurs méthodes. Par contre, il est étonnant de ne trouver pratiquement aucune référence [43] sur les résultats relatifs à la théorie des résidus quadratiques lorsqu'il travaille sur les racines carrés modulo un nombre premier p. On peut également remarquer que Poinsot n'utilise pas la notation $\equiv$ des congruences, introduite par Gauss en 1801 dans les *Disquisitiones Arithmeticae*, mais celle de Legendre.

Comme dans ses textes précédents, Poinsot insiste sur la notion d'*ordre*, notamment dans son *Addition*. On y retrouve une étude de la structure de l'ensemble des racines des équations binômes et des congruences binômes, très semblable à ce qui est exposé dans son manuscrit sur la théorie des permutations. De plus, la notion d'*ordre* est caractérisé de manière plus précise dans son mémoire. On y retrouve des définitions claires à deux reprises. La première fois, il est défini dans le cadre de l'étude de structures cycliques : les objets considérés doivent *naître successivement les uns des autres par la même loi, ou même fonction*. La seconde caractérisation est plus générale : « la disposition mutuelle qu'on peut observer actuellement entre plusieurs objets »[Poinsot, 1820, p. 402].

Le travail de Poinsot sur la résolution des congruences binômes n'est pas cité dans le cours d'*Algèbre supérieure* de Serret par exemple, bien que ce manuel contienne un chapitre sur les congruences dans chaque édition. Serret fait référence à Poinsot en ce qui concerne des méthodes exposées dans son mémoire de 1845 mais ne fait aucune allusion à son travail sur l'analogie que l'on peut retrouver entre la résolution des équations et celle des congruences. Il cite par contre Galois et l'utilisation des imaginaires dans les congruences.

D'un autre côté, ce même travail est cité en exemple par Smith dans son article *Solution*

43. Poinsot renvoie à Euler pour l'introduction des racines primitives. Cette référence est néanmoins faite dans le cadre de la résolution des équations binômes.

of the Congruence $x^n \equiv 1$, *mod* p que l'on retrouve dans le *Report on the Theory of Numbers* :

> The methods of Gauss, Lagrange, and Abel for the solution of the binomial equation $x^n - 1 = 0$ are in a certain sense applicable to binomial congruences of this special form. It is evident, from a comparison of several passages in the Disquisitiones Arithmeticae [Smith cite les articles 61, 73 et 335], that Gauss himself contemplated this arithmetical application of his theory of the division of the cercle, and that he intended to include it in the 8th section of his work, which, however, has never been given to the world.[...] When, for any prime modulus, an Abelian equation admits of being considered as an Abelian congruence, , so precise is the correspondance of the equation and the congruence, that (as Poinsot has observed in a memoir in which he has occupied himself with the comparative analysis of the equation $x^n - 1 = 0$, and the congruence $x^n \equiv 1 \pmod{p}$) we may consider the analytical expression of the roots of the equation as also containing an expression of the roots of the congruence ; and by giving a congruential interpretation to the radical signs which occur in that expression, we may elicit from it the actual values of the roots of the congruence. An exemple taken from Poinsot's memoir will rend this intelligible[Smith, 1859-1865, p. 141-142].

Après avoir détaillé l'exemple développé par Poinsot, Smith conclut : « Theorically, however, the relation between the analytical expression of the equation-roots and the values of the congruence-roots is of considerable importance, and the subject would certainly repay a closer examination than it has yet received »[Smith, 1859-1865, p. 144].

V Une première conclusion : qu'est-ce que la théorie de l'ordre ?

1 - L'utilisation des analogies chez Poinsot

L'analogie joue un rôle important dans la recherche mathématique. Selon Eberhard Knobloch, « les mathématiques sont le domaine légitime de l'analogie »[Knobloch, 1991, p. 217] et poursuit :

> [...] les mathématiciens les plus créateurs et les plus féconds comme Johannes Kepler, John Wallis, Leibniz, Isaac Newton, Leonhard Euler, Pierre Simon de Laplace ont mis en évidence le rôle éminent de l'analogie pour la découverte de nouvelles vérités mathématiques.
>
> Ils distinguaient le contexte de la découverte du contexte de la justification : d'après cela, l'analogie guide la connaissance mais ne la justifie pas[Knobloch, 1991, p. 217-218].

En particulier, les analogies jouent un rôle significatif dans les travaux de Poinsot. Bien sûr, son *Mémoire sur l'application de l'algèbre à la théorie des nombres* est basé sur l'étude de l'analogie entre les équations et les congruences binômes. Mais on remarque également qu'il produit des raisonnements très analogues pour décrire d'une part les ensembles de permutations en 1808 et 1818 et d'autre part les ensembles de racines d'équations binômes de 1808 à 1820. Ces deux types d'analogies développées par Poinsot entrent bien dans le *contexte de découverte* annoncé par Knobloch comme nous allons le voir ci-dessous.

(a) Analogies dans les procédés opératoires

Le *Mémoire sur l'application de l'algèbre à la théorie des nombres*, publié en 1820, Poinsot annonce qu'il a « observé [des] propriétés analogues » entre deux types de nombres - les racines des congruences binômes et les racines des équations binômes - et que cela l'a amené à considérer une analogie entre les expressions des solutions de ces congruences et équations. À partir de cette analogie, il en déduit son théorème qu'il démontre en transposant les opérations[44] valables pour les nombres complexes aux nombres modulo un nombre premier p.

D'une part, Poinsot affirme que l'analogie à partir de laquelle il a obtenu son résultat sur les congruences binômes peut être étendue à toutes les équations résolubles. À ce sujet, Smith remarque que le principe de Poinsot est effectivement valide pour les équations et congruences jusqu'au quatrième degré mais que pour les équations de degré supérieur résolubles, la démonstration de Poinsot n'est plus suffisante :

> But this reasoning ceases to be applicable to equations of an order higher than the fourth, because no general formula exists representing the roots of an equation of the fifth or any higher order. If, therefore, $F(x) = 0$ be an equation of the nth order, the roots of which can be expressed by a radical formula, and which is also completely resoluble when considered as a congruence for the modulus p, so that $F(x) \equiv (x - a_1)(x - a_2) \dots (x - a_n)$, mod. p, it will not necessarily follow that the formula which gives the roots of $F(x) = 0$ is also capable (when we add multiples of p to the numbers contained in it) of giving the roots of $(x-a_1)(x-a_2) \dots (x-a_n) = 0$, *i. e* the roots of the congruence $F(x) \equiv 0$, mod p ; and thus the principle enunciated by M. Poinsot is, it would seem, not rigorously demonstrated[Smith, 1859-1865, p. 145].

Poinsot donne d'ailleurs une précision à ce sujet dans son mémoire de 1820, mais sans soulever le problème de savoir si on peut supposer a priori que les formules donnant les expressions des racines d'une équation de degré n, $n > 4$, peuvent être dans tous les cas transposées pour donner les expressions des racines de la congruence correspondante :

> Quant à notre démonstration considérée en elle-même, on verra qu'elle réside, au fond, bien plutôt dans la supposition d'une formule générale qui résoudrait la pro-

44. Sur la question des analogies utilisées au XIX^{e} siècle pour transférer des processus opératoires, voir [Durand-Richard, 2008]. Une originalité de Poinsot est la place accordée à la cyclicité dans ce transfert.

posée, que dans la manière d'obtenir cette formule ; et même les géomètres sentiront d'abord comment le théorème que je propose s'étendrait à une équation complète, dont la résolution algébrique serait supposée connue. Il suffirait de considérer que les coefficiens de cette équation sont les mêmes, aux multiples près du module, que ceux de l'équation semblable déterminée qui aurait les mêmes racines ; que par conséquent la formule générale qui résoudrait la première équation, conviendrait à la seconde, en restituant aux coefficiens les multiples du module et nous donnerait ainsi les racines entières de la proposée[Poinsot, 1820, p. 348].

D'autre part, dans sa démonstration, il traduit une démonstration valable dans $\mathbb{C}$ en une démonstration dans $\mathbb{Z}/p\mathbb{Z}$, une fois de plus sans justifier rigoureusement les propriétés de cet ensemble et poser explicitement des questions à ce sujet. Il reproduit simplement des suites d'égalités algébriques en argumentant que l'on peut ajouter ou supprimer des multiples de p. Quelques années plus tard, Libri produit le même type de raisonnement dans son mémoire, intitulé *Mémoire sur la théorie des nombres*, publié en 1825. Il affirme que le théorème de Poinsot sur l'analogie des équations $x^n - 1 = 0$ et $x^n - 1 \equiv 0 \pmod{a}$, où a est un nombre quelconque, est évident « dans tous les cas », c'est-à-dire pour toutes les équations algébriques. En effet : « si l'on ajoute des multiples de a sous les radicaux compris dans l'expression des racines de cette équation, on aura les racines de la congruence proposée. »[Libri, 1838, p. 21]. Dans ces deux cas, Poinsot et Libri manipulent des expressions algébriques, les transforment sans poser explicitement la question de la légitimité des opérations.

D'un point de vue moderne, Poinsot transpose donc des raisonnements sur des équations valables dans $\mathbb{C}$ à des raisonnements analogues sur des congruences dans $\mathbb{Z}/p\mathbb{Z}$, où p est un nombre premier. $\mathbb{C}$ et $\mathbb{Z}/p\mathbb{Z}$ ont à la fois des propriétés communes (par exemple, ce sont des corps), et des différences profondes. Poinsot, pas plus que Libri plus tard, ne semble jamais s'interroger sur les propriétés qui permettent (ou non) le transfert d'un ensemble à l'autre.

Dans son *Report on the Progress and Present State of certain Branches of Analysis*[45], George Peacock résume et analyse également le travail de Poinsot sur l'équation $x^n - 1 = Mp$:

> Poinsot has given a very remarkable extension to the theory of the solution of the binomial equation $x^n - 1 = 0$, by showing that its imaginary roots may be considered in a certain sense as the analytical representation of the whole numbers which satisfy the congruence or equation $x^n - 1 = M(p)$ whose *modulus* (a prime number) is p [...]
>
> These views of Poinsot are chiefly interesting and valuable as connecting the theory of indeterminate with that of ordinary equations. It has, in fact, been too much the custom of analysts to consider the theory of numbers as altogether separated from that of ordinary algebra. The methods employed have generally been

45. Ce rapport est contenu dans le *Report of the Third Meeting of the British Association for the Advancement Of Science*. Cette rencontre à eu lieu à Cambridge en 1833.

> confined to the specific problem under consideration, and have been altogether incapable of application when the known quantities employed were expressed by general symbols and not by specific numbers. It is to this cause that we may chiefly attribute the want of continuity in the methods of investigation which have been pursued, and the great confusion which has been occasioned by the multiplication of insulated facts and propositions which were not referable to, nor deducible from, any general and comprehensive theory[Peacock, 1834, p. 320 - 322].

Peacock défend donc également une théorie générale, qui ne s'applique pas seulement aux nombres entiers, ou rationnels, mais également à des quantités symboliques qui n'ont pas le statut de nombre, comme les congruences par exemple. En effet, ces réflexions de Poinsot correspondent en partie aux idées de Peacock sur l'algèbre, comme nous le préciserons plus loin.

Dans son mémoire de 1820, Poinsot ne développe pas l'analogie entre les équations et les congruences binômes uniquement dans le but de transposer la méthode de Gauss aux congruences. Il met également en avant des analogies dans la structure des ensembles des deux types de racines, analogies que l'on retrouve dispersées dans tous les textes étudiés ici.

(b) Analogies dans les structures étudiées et la notion d'ordre

D'un point de vue moderne, si l'on liste les structures étudiées par Poinsot dans ses textes - permutations, raisonnements sur les polygones, racines des équations et congruences binômes, elles correspondent toutes à des groupes et sous-groupes cycliques. Dans chacun de ces cas, Poinsot met en avant des analogies entre ces ensembles : les relations existant entre les objets des ensembles considérés (permutations ou racines d'une équation binôme par exemple) sont similaires - elles permettent de passer d'un objet à un autre en utilisant toujours le même procédé et d'obtenir ainsi tous les objets composant l'ensemble. Il utilise cette particularité pour partager ces ensembles en *groupes*, qui correspondent aujourd'hui à des groupes et sous-groupes cycliques. Pour décrire ces structures cycliques, Poinsot utilise d'ailleurs la même image dans tous ses textes de géométrie, d'algèbre et de théorie des nombres de 1808 à 1820 (image qu'il reprend en 1845) : celle d'objets disposés régulièrement autour d'un cercle. Cela permet à plusieurs reprises à Poinsot d'illustrer les structures qu'il étudie et d'appuyer ses décompositions en groupes et sous-groupes sur cette image de cercle. Bien sûr, Poinsot n'a pas en tête les notions de structure ou de groupe telles qu'elles seront définies à partir de la fin du XIX^{e} siècle, mais sa façon de présenter l'ensemble des permutations ou des racines des équations binômes est originale dans le sens où elle se focalise sur la manière dont on peut relier et classer ces objets entre eux à l'aide d'un même procédé opératoire qu'il nomme dans certains cas une *loi*. Ces analogies sont notamment mises en avant par le fait qu'il utilise toujours

le même vocabulaire (*groupes*, *inséparables*, ...) pour produire ses raisonnements sur ce thème entre 1808 et 1820.

Revenons ici sur l'utilisation du mot *groupe* par Poinsot dans le cadre de son étude des structures cycliques. Lors de l'examen de celles-ci, Poinsot classe les objets étudiés en ensembles et sous-ensembles qu'il nomme systématiquement *groupes*. À la lecture du commentaire de Poinsot sur le *Traité* de Lagrange, publié en 1808, le lecteur moderne peut être surpris de retrouver à plusieurs reprises l'expression *groupe de racines* pour désigner ce qui correspond aujourd'hui à des groupes ou sous-groupes cycliques. Il peut cependant estimer que Poinsot emploie le mot *groupe* pour désigner un ensemble quelconque d'objets, sans lui donner une caractéristique particulière et que cette utilisation n'a aucun lien avec celle qu'en fera notamment Galois et ses lecteurs des années plus tard. De plus, il ne donne aucune définition de ce qu'il appelle *groupe* ou de ce qu'il qualifie d'*inséparable* dans ce texte, ni dans ses écrits ultérieurs.

Cependant, il est difficile d'ignorer le fait que Poinsot utilise ensuite ce même terme dans tous ces textes d'algèbre et de théorie des nombres, pour désigner à chaque fois un ensemble d'objets qui ne se *séparent* jamais, que ce soit pour désigner des *groupes de racines* ou des *groupes de permutations*. D'un point de vue moderne, les *groupes* de Poinsot désignent invariablement des groupes ou sous-groupes cycliques. Certes, comme à de nombreuses reprises, Poinsot ne donne aucune définition de ce terme, comme s'il l'utilisait dans son sens courant, sans aucune caractéristique supplémentaire, c'est-à-dire une réunion quelconque d'objets dans un ensemble. Cette hypothèse semble cependant peu plausible. Il nous paraît juste d'affirmer que pour Poinsot, un *groupe* désigne un ensemble d'objets tel que l'on peut obtenir tous ces objets à partir d'un seul, en lui appliquant à plusieurs reprises un même procédé et tel qu'il est impossible d'obtenir un objet n'appartenant pas à ce groupe en appliquant ce procédé à un objet appartenant au groupe. On est donc encore très loin de la définition mathématique actuelle du mot *groupe*, ou même du *groupe cyclique*. Néanmoins, Poinsot utilise ce terme du vocabulaire courant dans un sens technique qu'il n'explicite pas. On observe donc le début d'une transformation sémantique : un terme du vocabulaire courant commence à prendre une signification technique nouvelle ; ce même mot désignera quelques dizaines d'années plus tard une notion mathématique abstraite, définie rigoureusement. Par contre, il semble à l'heure actuelle impossible d'affirmer qu'il y a une quelconque relation entre l'utilisation du mot *groupe* par Poinsot dans ce cadre bien particulier et le fait que, quelques années plus tard, ce même mot sera également utilisé dans un sens mathématique, plus général. Enfin, quelques auteurs commente les travaux de Poinsot en lien avec la notion de groupe. Par exemple, une note sur Poinsot et sur son utilisation du mot *groupe* est insérée dans l'*Encyclopédie des sciences mathématiques pures et appliquées*[46] :

46. Ce paragraphe est écrit par E. Bortoletti. La référence donnée ci-dessous semble inexacte : lors de la séance du 17 mai 1813, Poinsot a lu un *Mémoire sur les Permutations*, ce qui ne correspond pas au

> *L. Poinsot* [Recherches sur l'Algèbre et sur la Théorie des nombres, mémoire présenté à la classe des sciences de l'Institut de France en mai 1813, publié Mém. classe sc. math. phys. Institut France 14 (1813/5), éd. 1818, p. 382] fait déjà usage du mot "groupe" dans un sens technique. Il y parle de "groupes de permutations associées entre elles", de "groupes principaux et secondaires de permutations" et de "groupes semblables" [Meyer et Molk, 1904 - 1916, *Tribunes publiques*, p. 141].

Bachmann, dans la préface de son traité *Die Elemente der Zahlentheorie*, relie également les recherches de Poinsot sur les congruences au concept de groupe en observant :

> The theory of congruences bases itself substantially upon the fundamental concept of mathematics, which is already the foundation of Poinsot's method, the concept of group [47].

Ce sont ces particularités qui rendent les travaux de Poinsot différents. Néanmoins, la considération de ces structures cycliques et de ces analogies, cette vision de l'algèbre se retrouvent déjà en partie dans ce qui est la source principale des écrits de Poinsot en algèbre et en théorie des nombres : les *Disquisitiones Arithmeticae* de Gauss. En effet, dans son traité de théorie des nombres, Gauss étudie de façon récurrente des structures cycliques : dans le cadre des théories des résidus, des formes quadratiques et de la cyclotomie [48]. Les analogies sont également mises en avant, par exemple à propos de démonstrations sur des résultats relatifs aux formes quadratiques et aux résidus :

> On remarquera sur-le-champ l'analogie de la démonstration du théorème précédent, avec les démonstrations des n^{os} 45, 49 ; et effectivement, la théorie de la multiplication des classes a une grande affinité avec le sujet traité dans la Section III[Gauss, 1801, art. 306].

L'analyse des relations a également une place importante chez Gauss. José Ferreirós précise d'ailleurs ce point dans [Ferreirós, 2007] en donnant plusieurs citations de Gauss issue de ses œuvres ultérieures démontrant que pour Gauss, les mathématiques sont la « science des relations »[Ferreirós, 2007, p. 254]. Ainsi, Gauss écrit en 1825 :

> Les mathématiques sont ainsi, dans le sens le plus général, la science des relations dans laquelle on isole les relations de tous les contenus. [49]

titre donné ici. Par contre, lors de la séance du 5 Mai 1817, Poinsot a bien lu un Mémoire intitulé *Extrait de quelques recherches nouvelles sur l'algèbre et la théorie des nombres.*

47. Cette traduction de Miller est donnée dans [Miller, 1903, p. 88]. Voici la citation originale : « Die Lehre von den Congruenzen gründet sich sodann wesentlich auf jenen Fundamentalen Begriff der Mathematik, der im Grunde auch schon bei dem Poinsot'schen Verfahren zur Geltung kommt, auf den Begriff der Gruppe »[Bachmann, 1892, p. iv].

48. L'étude des structures périodiques par Gauss est notamment commentée dans [Goldstein et Schappacher, 2007a, p. 17-18].

49. Nous avons traduit la phrase originale : « Die Mathematik ist so im allgemeinsten Sinne die Wissenschaft der Verhältnisse, indem man von allem Inhalt der Verhältnisse abstrahirt. », issue de la page 396 du volume X-1 des *Werke* de Gauss, *Nachträge zur reinen Mathematik*, publié en 1917.

Ces points communs entre les idées générales des deux mathématiciens et le fait que de nombreux passages des travaux de Poinsot consistent en des reformulations des méthodes de Gauss peuvent pousser à se demander si les travaux de Poinsot apportent réellement quelque chose par rapport aux *Disquisitiones Arithmeticae* de Gauss, publiées en 1801. Il nous semble que la formulation des travaux de Gauss par Poinsot est justement un des points-clés des travaux de ce dernier. En effet, pour comprendre l'importance des structures, de l'étude des relations, des analogies dans le travail de Gauss, il est nécessaire d'étudier attentivement un ouvrage volumineux de théorie des nombres. Par contre, dans ses différentes publications, Poinsot insiste explicitement sur ces points fondamentaux puisqu'il centre ses réflexions autour de la *théorie de l'ordre*.

2 - La théorie de l'ordre au cœur de l'algèbre et de la théorie des nombres

C'est dans le texte publié en 1818 que Poinsot utilise pour la première fois la notion d'*ordre*, et l'expression *théorie de l'ordre*, qu'il place au cœur de l'algèbre, de la théorie des nombres et de la géométrie de situation. Ce vocabulaire est toujours employé dans le cadre de l'étude des relations entre des objets, que ce soit pour les permutations ou les racines d'équations et de congruences. Bien qu'il définisse l'ordre comme la « disposition mutuelle qu'on peut observer actuellement entre plusieurs objets » [Poinsot, 1820, p. 402], la structure des ensembles étudiés est toujours cyclique : en usant des termes de Poinsot, ces objets *naissent successivement l'un de l'autre* à partir d'une même *loi*.

Lors de notre étude, nous avons signalé à plusieurs reprises la façon dont Poinsot définit l'algèbre. Ainsi, en 1808, il assimile l'algèbre à la théorie des équations. En 1817, l'algèbre est fondée sur « *la théorie de l'ordre et de la situation des choses sans aucune considération de la grandeur* »[Poinsot, 1818, p. 383]. En 1818, « les principes généraux de l'analyse mathématique [qui inclut vraisemblablement l'algèbre et la théorie des nombres] ont leur source naturelle dans la simple considération de l'*ordre*, ou de la disposition mutuelle qu'on peut observer actuellement entre plusieurs objets »[Poinsot, 1820, p. 402]. L'algèbre et la théorie des nombres doivent donc être basées sur cette notion d'*ordre*, c'est-à-dire sur l'étude des relations existant entre les objets étudiés. Cette caractérisation de l'algèbre, plus générale et plus moderne *a posteriori* que celle donnée par Poinsot en 1808, est remarquable. Nous verrons plus loin qu'il donne d'ailleurs dans son mémoire de 1845 une définition semblable.

Comme nous l'avons remarqué plus haut, Peacock développe des idées que l'on peut rapprocher de celles de Poinsot sur la partie de l'algèbre qu'il nomme *Algèbre symbolique*. Il fait partie d'un groupe de mathématiciens que Novy appelle *École Algébrique Anglaise* dans [Nový, 1968] et développe une *Algèbre symbolique*[50] dans les années 1830. Il aborde

50. Nous nous appuyons sur l'analyse de Marie-José Durand-Richard pour les références aux travaux de

la notion d'*Algèbre symbolique* dans le *Report*[51] de 1833 :

> [...] we do necessarily arrive at a new science much more general than arithmetic, whose principles, however derived, may be considered as the immediate, though not the ultimate foundation of that system of combinations of symbols which constitutes the science of algebra.
>
> [...]the real distinction between them [arithmetical algebra and symbolic algebra] will arise from the *supposition or assumption that the symbols in symbolical algebra are perfectly general and unlimited both in value and representation, and that the operations to which they are subject are equally general likewise*[Peacock, 1834, p. 194-195].

Pour Peacock, l'Algèbre arithmétique et l'Algèbre symbolique sont indépendantes :

> En définissant l'Algèbre symbolique comme science de l'esprit, G. Peacock affirme l'indépendance de la rationalité de ses opérations vis-à-vis des objets sur lesquels elle s'exerce. L'Algèbre arithmétique et l'Algèbre symbolique sont donc deux sciences indépendantes, l'une est science des quantités, l'autre est science des opérations[Durand-Richard, 1990, p. 146].

Ainsi, on retrouve bien une similitude entre les deux hommes sur leurs définitions de l'algèbre : l'algèbre de Peacock a pour but l'étude des opérations quand Poinsot prône une algèbre qui se base sur les relations entre les objets. Néanmoins, les opérations de Peacock et les *lois* utilisées de Poinsot ne sont pas de même nature. En effet, les procédés opératoires caractérisant l'Algèbre symbolique de Peacock sont limités à quatre opérations : addition, soustraction, multiplication et division. Les *lois* de Poinsot sont plus générales : par exemple, dans ses travaux sur les permutations, Poinsot considère une *loi* permettant de passer d'une permutation à une autre qui correspond en fait à une substitution et non pas à une des quatre opérations considérées par Peacock[52].

Comme nous le verrons à la fin du chapitre suivant, c'est dans la deuxième moitié du XIX^{e} siècle que l'on retrouve chez plusieurs auteurs des réflexions autour de la définition de l'algèbre de Poinsot en particulier et sur sa théorie de l'ordre en général. Avant d'en commenter quelques-unes, nous allons nous arrêter sur les références aux travaux de Poinsot publiées à la suite des mémoires étudiés ici, puis nous nous arrêterons sur quelques extraits de son mémoire publié en 1845.

Peacock. On pourra notamment se reporter à [Durand-Richard, 1990] et [Durand-Richard, 1996].

51. Il la développe ensuite de manière plus approfondie dans la deuxième édition de son *Treatise of Algebra*.

52. Marie-José Durand-Richard discute cette limitation par Peacock aux quatre opérations dans [Durand-Richard, 1990] notamment.

CHAPITRE 8

La théorie de l'ordre et ses réceptions (1820 - . . .)

I Une première réception timide (1820 - 1845)

Comme nous l'avons vu dans la section précédente, les travaux de Poinsot en algèbre et en théorie des nombres ne contiennent que très peu de résultats nouveaux et il utilise régulièrement des objets ou des raisonnements dont il ne démontre pas la validité. Il développe des idées déjà présentes dans les *Disquisitiones Arithmeticae* mais son originalité consiste en sa façon de présenter les différentes notions étudiées autour d'un concept fondamental : l'*ordre*, c'est-à-dire l'étude des relations entre des objets. Il pose l'*ordre* comme fondement de trois disciplines : la théorie des nombres, l'algèbre et la géométrie de situation, ce qui constitue un lien fort entre elles. Dans la section VII des *Disquisitiones Arithmeticae*, Gauss introduit un outil de théorie des nombres - les racines primitives - pour résoudre un problème d'algèbre. Comme on peut le lire dans [Goldstein et Schappacher, 2007a], à partir des années 1820, beaucoup de travaux liés à la théorie des nombres s'appuient sur un autre domaine des mathématiques. On retrouve déjà une utilisation d'outils algébriques et analytiques dans les travaux en théorie des nombres de Lagrange, mais cela deviendra plus systématique avec la génération de mathématiciens ayant étudié très tôt les *Disquisitiones Arithmeticae* de Gauss. On peut par exemple citer Dirichlet qui utilise les séries infinies dans ses travaux de théorie des nombres, Abel et Jacobi avec leurs travaux relatifs aux fonctions elliptiques, ou encore Kummer, Hermite, Eisenstein et Kronecker. Ces travaux font partie de ce que les auteurs de [Goldstein et Schappacher, 2007a] appellent l'*arithmétique algébrique analytique*. L'œuvre de Poinsot est donc originale par rapport à ce courant, car il lie l'algèbre et l'arithmétique à la géométrie et non à l'analyse réelle ou complexe. Cela s'explique par sa vision des mathématiques liée à la notion d'*ordre* : cela l'incite à rapprocher des sujets dont l'étude est simplifiée en se basant sur cette idée.

Évaluer la portée réelle de la singularité des travaux de Poinsot reste néanmoins très difficile et ce, pour plusieurs raisons. D'une part, les travaux de Poinsot à ce sujet sont en nombre restreint. D'autre part, le peu d'indications biographiques, de correspondances à ce sujet rend plus ardu l'établissement d'un réseau autour de Poinsot. La quasi-absence de résultats nouveaux par rapport à ses prédécesseurs immédiats, en particulier Gauss, complique encore la mesure de son influence éventuelle : comment décider de celle d'un point de vue, d'une manière de voir ?

Nous nous appuyons dans ce chapitre sur les références de plusieurs auteurs aux travaux de Poinsot pour proposer une évaluation de la portée de la théorie de l'ordre.

Avant la publication de son traité de 1845, plusieurs auteurs remarquent l'intérêt des publications de Poinsot. Comme nous l'avons signalé précédemment, son mémoire de 1820 est cité et commenté à plusieurs reprises dans des rapports. Ainsi, Cournot remarque les « aperçus plus nouveaux et plus piquants »[Cournot, 1825, p. 144] de Poinsot dans son compte rendu de [Poinsot, 1820] inséré dans le *Bulletin de Férussac*. Dans le même périodique, il cite également Poinsot en lien avec l'utilisation des racines imaginaires des congruences dans son commentaire du mémoire de Jacobi sur les résidus cubiques. D'autre part, Peacock insiste également sur l'intérêt de la vision de Poinsot dans son *Report on the Progress and Present State of certain Branches of Analysis* en 1833 : nous en avons cité quelques extraits dans le chapitre précédents.

Plusieurs auteurs se réfèrent également à Poinsot dans leurs recherches mathématiques. Ainsi, dans ses recherches de théorie des nombres présentées à l'Académie des Sciences en 1825, Libri suit explicitement Poinsot lorsqu'il ajoute des multiple de p afin de transposer un résultat de la théorie des équations à la théorie des congruences [1]. En 1829, dans son premier mémoire de théorie des nombres, Lebesgue évoque également les idées de Poinsot lorsqu'il présente sa section sur les congruences dont le module est composé, et souligne l'« analogie parfaite »[Lebesgue, 1829, p. 24] existant entre la théorie des récaines égales des équations et celle des congruences [2]. Liouville cite littéralement Poinsot en 1843 pour donner l'esprit de la méthode de la résolution des équations binômes.

Les méthodes de Poinsot sont également mises en avant par au moins deux autres mathématiciens, même si leurs références à Poinsot n'ont alors pas été publiées. Nous avons indiqué dans notre première partie que Sophie Germain connaît le texte de Poinsot publié en 1820, et s'y réfère notamment dans une lettre à Gauss. Dans une lettre à Poinsot datée du 2 juillet 1819, Sophie Germain le remercie de lui avoir envoyé son mémoire publié en 1820 [3], lui annonce qu'elle en a fait envoyer un exemplaire à Gauss et le félicite pour ses apports [4] :

> Je prévoyois dès lors que j'y trouverois, en quelque sorte, la métaphysique des procédés que j'employois à la détermination de l'ordre des restes considerés dans la série des nombres naturels. La lecture de votre mémoire inseré dans l'un des derniers volumes publiés par l'académie a justifié mon attente.
>
> [...]L'emploi des racines imaginaires dans les recherches arithmétiques m'a paru fort lumineux. C'est un phanal placé sur la grand route : il éclaire les sentiers détournés.

1. Voir page 259.
2. Nous donnons la citation correspondante page 77.
3. Rappelons que ce travail a été présenté en 1818 à l'Académie des Sciences.
4. Nous reproduisons ici des extraits de la transcription de la lettre de Germain donnée dans [Del Centina, 2005, p. 5].

> [...]Les théorèmes nouveaux et vos remarques sur la coexistence des ordres qui n'en forment qu'un seul m'ont fait un grand plaisir. Les premiers sont pleins de finesse les secondes soulagent l'esprit en lui permettant d'embrasser à la fois un grand nombre d'analogies.

Ainsi, Sophie Germain insiste particulièrement sur les points fondamentaux des travaux de Poinsot : la considération des racines imaginaires des congruences, qui découle des analogies mises en avant par Poinsot et ses observations sur « les ordres qui n'en forment qu'un » existant entre les racines des équations binômes, qu'il développe particulièrement dans l'*Addition* de [Poinsot, 1820]. Elle insiste également auprès de Gauss dans sa lettre de 1819 sur le rôle du mémoire de Poinsot dans ses recherches [5] :

> Je suppose que vous avez sous les yeux le mémoire ou plutôt le projet de mémoire de M^r^ Poinsot car il faut faire soi-même le travail que l'auteur s'est épargné. Quoiqu'il en soit son idée m'a paru fort heureuse. J'ai admiré comment étant parti de principes si différens, il m'avoit fourni en quelque sorte la [métaphysique] de ma méthode. En effet en [faisant] usage de la remarque de cet auteur on voit comment j'ai dû arriver aux résultats que je viens d'exposer car il s'agit ici de traiter les racines de l'équation binome du degré $2N$, et quoique les quantités résultantes de la combinaison de ces racines [...] ne puisse devenir réelles que pour certaines valeurs de $2Np+1$ et par conséquent aussi de p, leurs rapports entr'elles sont indépendants des valeurs de p.

Elle propose également plus loin une nouvelle méthode pour déterminer le caractère quadratique du nombre 2. Ici, pour ses recherches, Sophie Germain s'appuie donc sur l'analogie décrite par Ponsot entre les équations et les congruences binômes. Les auteurs de [Laubenbacher et Pengelley, 2010] insistent sur la manipulation par Sophie Germain d'idées que l'on peut aujourd'hui relier aux groupes et -sous-groupes cycliques [6]. Après analyse des travaux de Poinsot, et puisqu'elle les connaît et les a étudié, il est vraisemblable qu'ils aient eu un rôle dans les réflexions de Sophie Germain en lien avec la structure de l'ensemble des racines de l'unité.

Enfin, pour l'instant, aucune référence publiée avant 1845 ne nous indique que les mémoires de Poinsot sont connus en Allemagne. On sait déjà que Gauss a reçu au moins un des textes de Poinsot par l'intermédiaire de Sophie Germain ; nous n'avons néanmoins pas retrouvé de références à Poinsot de la part de Gauss sur ses recherches arithmétiques. Par contre, Jacobi donne un cours avancé de théorie des nombres à l'université de Königsberg pendant le premier semestre de l'année 1836-1837 : comme nous l'avons indiqué précédemment, ce cours, composé de 52 leçons, a récemment été publié et contient notamment des développements sur la théorie de la cyclotomie et les lois de réciprocité. Dans sa quatrième leçon, Jacobi donne des résultats sur les congruences en général, et démontre

5. Ces extraits sont issus de [Del Centina, 2008, p. 360-361].
6. Voir notre citation page 66.

notamment le théorème de Lagrange sur le nombre maximum d'une congruence de degré n pour un module premier. Il observe ensuite :

> Für den seltenen Fall, daßman eine Gleichung algebraisch auflösen kann, lassen sich hieraus auch Mittel ziehen, die Kongruenz aufzulösen. Dies ist zuerst bemerkt und durchgeführt von meinem Freunde Poinsot in einer Abhandlung in polytechnischen Journal, welche ihres deutlichen Vortrags und einiger grober Fehler wegen zum eigenen Studium zu empfehlen ist[Jacobi, 2007, p. 36].

Il poursuit en donnant un exemple : la résolution de la congruence $x^3 \equiv 1 \pmod{19}$ en utilisant l'expression des racines de l'équation $x^3 = 1$, et en ajoutant le module 19 sous la racine de cette expression. Jacobi ne précise pas à quelle date il a pris connaissance de cette méthode mais cette citation montre que les deux hommes se connaissent, et que l'analogie entre équations et congruences mise en avant par Poinsot est utilisée par Jacobi, au moins dans ses cours.

Ces références montrent que les mémoires de théorie des nombres de Poinsot sont connus voire utilisés en partie par un groupe restreint de savants. La méthode qui est souvent mise en avant dans les articles mathématiques que l'on a cités est la correspondance ayant lieu entre les équations et les congruences correspondantes. Seule Sophie Germain se réfère également aux réflexions de Poinsot sur l'ordre existant entre les racines primitives, même si elle n'emploie dans ses recherches que les résultats qu'il expose sur l'analogie entre les racines des équations et des congruences binômes. Nous allons voir qu'à partir de 1845, Poinsot est au contraire mis en avant pour sa théorie de l'ordre.

II La synthèse de 1845

1 - Une introduction qui place l'ordre au cœur des mathématiques

L'objectif de ce mémoire est de revenir sur des résultats fondamentaux de la théorie des nombres, et d'en donner des démonstrations diverses, fondées sur des principes différents. Comme nous l'avons signalé dans notre première partie, Poinsot annonce que les développements qu'il expose ici devraient faire partie des ouvrages élémentaires destinés à l'enseignement de la théorie des nombres et de l'algèbre.

Poinsot introduit ce texte par des réflexions générales sur la théorie des nombres et l'algèbre notamment. Il rappelle les principes déjà exposés avant 1820 sur les mathématiques en général :

> Les mathématiques ne sont pas seulement la science des rapports, je veux dire que l'esprit n'y a pas uniquement en vue la *proportion* ou la *mesure* ; il peut encore considérer le *nombre* en lui-même, l'*ordre* et la *situation* des choses, sans aucune idée de

leurs rapports, ni des distances plus ou moins grandes qui les séparent[Poinsot, 1845, p. 3].

Il applique ensuite ce principe à la théorie des nombres, l'algèbre, lé géométrie et la mécanique. Par exemple, pour l'Arithmétique, il différencie l'*arithmétique ordinaire*, qui est l'« art de la numération »[Poinsot, 1845, p. 3] et qui dépend de la base choisie pour la numération, de la *théorie des nombres*, qui a pour objet les propriétés des nombres indépendamment du système de numération considéré. De même, concernant l'Algèbre :

> Si vous considérez l'Algèbre, vous y voyez également deux parties très-distinctes. Et d'abord, l'algèbre ordinaire, qu'on peut très bien nommer *arithmétique universelle*. Cette algèbre, en effet, n'est autre chose qu'une arithmétique généralisée, c'est-à-dire étendue des nombres particuliers à des nombres quelconques[...] Mais il y a une algèbre supérieure, qui repose toute entière sur la théorie de l'ordre et des combinaisons, qui s'occupe de la nature et de la composition des formules considérées en elles-mêmes, comme de purs symboles, et sans aucune idée de valeur ou de quantité. C'est à cette partie qu'on doit rapporter la théorie profonde des équations [...] et c'est même cette seule partie élevée de la science qui mérite, à proprement parler, le nom d'*algèbre*[Poinsot, 1845, p. 4].

Poinsot continue avec la géométrie : la géométrie de situation est l'équivalent de la théorie des nombres ou de l'algèbre supérieure pour la géométrie ; il rappelle d'ailleurs que son mémoire publié en 1810 sur les polygones et les polyèdres appartient à cette géométrie de situation. Une fois de plus, Poinsot donne ici des structures analogues pour les domaines de l'arithmétique, l'algèbre et la géométrie : l'étude de la mesure d'une part et de l'ordre d'autre part.

2 - Démonstrations diverses basées sur des principes variés

Les trois premières parties de ce mémoire sont consacrées à des preuves de théorèmes fondamentaux de la théorie des nombres, tels les théorèmes de Fermat et de Wilson, et le théorème de Lagrange sur le nombre maximum de racines d'une congruence. Poinsot présente quelques démonstrations inédites mais reprend à plusieurs des anciennes preuves de lui-même ou d'autres savants.

Poinsot n'expose pas de résultats inédits mais insiste particulièrement sur les fondements des démonstrations proposées. Par exemple, lorsqu'il propose une preuve du théorème de Lagrange, il revient sur l'importance de l'analogie existant entre les équations et les congruences :

> Ces transformations [pour obtenir les multiples voulus] sont tout à fait analogues à celles qu'on emploie dans les équations algébriques pour faire disparaître les fractions et réduire le premier coefficient à l'unité[Poinsot, 1845, p. 16].

Poinsot remarque que sa démonstration ne s'appuie que sur des fondements du calcul, à savoir la division algébrique et sur le fait que si deux nombres entiers a et b sont premiers à un nombre entier c, alors leur produit ab est également premier à c. Poinsot semble donc porter une attention toute particulière à présenter des démonstrations qui s'appuient sur un nombre restreint de principes, qu'il explicite. Dans le deuxième chapitre, intitulé *Démonstrations de ces mêmes propriétés à l'aide de nouveaux principes*, il suit la même démarche. Il y donne de nouvelles démonstrations des théorèmes de Fermat et Wilson, cette fois-ci fondée uniquement sur deux propriétés arithmétiques, qu'il démontre également :

- le résultat d'un produit est toujours le même dans quelque ordre que l'on multiplie les facteurs ;
- si deux nombres sont premiers par rapport à un troisième alors leur produit est également premier par rapport au troisième nombre.

Enfin, dans le chapitre III, intitulé « Démonstrations nouvelles tirées de la considération de l'ordre », Poinsot considère alors N objets de l'espace, dans l'ordre a, b, c d, e, etc., et tels qu'ils soient égaux et à égale distance l'un de l'autre (puisque seuls l'ordre et le nombre importe ici). Poinsot modélise donc cette situation comme « N points a, b, c, d, e, etc., rangés en cercle, et formant ainsi les sommets d'un polygone régulier de N côtés »[Poinsot, 1845, p. 46]. Il emploie cette caractérisation pour donner de nouvelles preuves de résultats fondamentaux de la théorie des nombres. Poinsot indique pourquoi il propose une fois de plus d'autres démonstrations :

> Mais il me semble que ces théorèmes ont une source plus profonde dans la science des mathématiques, et qu'ils doivent tenir à des principes d'un ordre plus élevé, de manière à ce qu'on voie que ce n'est point par hasard que l'esprit s'est attaché à ces spéculations, qu'elles ne sont point de pure curiosité, mais puisées dans la nature même des choses, et qu'elles forment une partie fondamentale de la science mathématique considérée de la manière la plus générale : et, pour en donner une idée, je vais présenter de nouvelles démonstrations, uniquement tirées de la considération de l'*ordre* qu'on peut observer actuellement entre plusieurs objets[Poinsot, 1845, p. 45].

3 - Des théorèmes fondamentaux de la théorie des nombres démontrées à partir de la considération de l'ordre

Nous nous arrêtons sur cette partie du mémoire car elle contient des preuves nouvelles de résultats abordés précédemment. Ces nouvelles preuves sont basées sur la considération des sommets d'un polygone régulier à N côtés. À partir de ce principe, il obtient notamment une définition géométrique de deux nombres premiers entre eux :

> *Si l'on a N points rangés en cercle, et qu'on les joigne de h en h, h étant*

premier à N, on passe nécessairement par tous les N points avant de retomber sur le point de départ ; et l'on fait nécessairement h fois le tout entier e la circonférence.

Réciproquement, *si en joignant N points de h en h, on passe par tous ces points avant de revenir au premier, h sera nécessairement premier à N* [Poinsot, 1845, p. 46].

Pour justifier ce théorème, il considère un nombre h premier au nombre N. Si on ne passait pas par tous les points de polygones avant de retomber sur le sommet de départ en se déplaçant de h points en h points, on passera sur n points, où $n < N$. Et on aurait donc parcouru nh points en tout, et le nombre nh serait dans ce cas égal à un multiple de N, ce qui est impossible puisque h est supposé premier à N, et n est inférieur à N. Réciproquement, si on passe par tous les points en allant de h en h, alors le plus petit multiple commun de h et de N est $N \times h$, et donc N et h sont premiers entre eux. En choisissant pour h les différents intervalles possibles, et dans le cas où on doit toujours passer par tous les points avant de revenir au sommet initial, on obtient ce que Poinsot qualifie de *définition géométrique de nombre premier*. Il avait déjà utilisé ce type de définition dans son mémoire sur les polygones et les polyèdres en 1809.

Il donne également une caractérisation du plus grand diviseur commun de deux nombres, lorsque ceux-ci ne sont pas premiers entre eux :

Si h et N ne sont pas premiers entre eux, je dis qu'en joignant les N points de h en h, on ne passera que par $\frac{N}{\theta}$ d'entre eux ; θ étant le plus grand commun diviseur des deux nombres h et N [Poinsot, 1845, p. 47].

Nous allons détailler sa démonstration, pour montrer à nouveau sur quelles considérations il s'appuie.

On reporte h sur la circonférence N du cercle jusqu'à ce que l'on revienne au point initial. Soit q le nombre de tours effectués. Le nombre qN est donc le plus petit multiple de N que l'on peut diviser par h. Si on pose $\theta = \frac{h}{q}$, θ est donc le PGCD de h et de N.

Soit x le nombre de sommets par lesquels on est passé pour former le polygone précédent. On a donc $xh = NQ$. Or $q = \frac{h}{\theta}$ donc $xh = \frac{Nh}{q}$. On obtient donc : $x = \frac{N}{\theta}$.

Poinsot conclut :

On peut remarquer encore que cette démonstration ne suppose aucune propriété des nombres ni aucun théorème d'arithmétique, pas même cette théorie du plus grand commun diviseur que nous devons à Euclide. Elle donnerait même, au besoin, pour la recherche de ce commun diviseur, une règle nouvelle qu'on pourrait suivre en arithmétique et en géométrie, et qui ne paraît pas moins élégante[Poinsot, 1845, p. 48].

Poinsot donne alors un nouvel algorithme géométrique pour déterminer le plus grand commun diviseur de deux nombres. Dans les *Éléments*, Euclide propose, pour déterminer le PGCD de deux grandeurs A et B de reporter la plus petite sur la plus grande. Si la plus petite est reportée un nombre exact de fois, on a le PGCD. Dans le cas contraire, on réitère le procédé en essayant de reporter la grandeur qui reste sur B, etc. Poinsot, de son côté, propose, plutôt que de considérer un reste dans le cas où B ne peut être reportée un nombre exact de fois pour obtenir A, d'essayer de la reporter un nombre exact de fois sur $2A$, puis $3A$, et ainsi de suite.

Bien sûr, cette méthode peut être traduite en un raisonnement équivalent sur les nombres.

Poinsot explique ensuite pourquoi sa méthode est plus simple que celle d'Euclide. En effet, avec celle de Poinsot, on ne considère pas de reste, et, si l'on se place à nouveau dans la situation d'un polygone régulier à B côtés, tout se réduit à compter le nombre de tours nécessaires pour revenir au point de départ. Si on ne revient jamais au point de départ, cela signifie que les grandeurs A et B sont *incommensurables*.

Il donne ensuite la démonstration de la propriété *si α et β sont deux nombres premiers à un même nombre N, alors le produit $\alpha\beta$ est également premier à N* selon les mêmes principes : on prend un sommet de départ, puis on parcourt le polygone de N sommets de α en α. Comme, par hypothèse, α et N sont premiers entre eux, on forme ainsi un nouveau polygone à N côtés. Sur ce polygone à N côtés, on va de β sommets en β sommets : comme β et N sont premiers entre eux, on obtient à nouveau un autre polygone de N côtés, en étant passé une unique fois sur chaque sommet. Or, considérer des intervalles de α sommets, puis, à partir de ces intervalles, considérer des intervalles de β sommets, revient à considérer des intervalles de $\alpha\beta$ sommets. Comme on obtient un polygone de N côté, en passant une seule fois par chaque sommet, le produit $\alpha\beta$ est bien premier à N.

Il poursuit en proposant ensuite une démonstration, basée sur les mêmes principes, du théorème de Fermat généralisé :

$$x^n - 1 = \mathcal{N},$$

où $n = \varphi(N)$, le nombre de nombres inférieurs et premiers à N.

Il conclut :

> Ainsi l'on a de ce beau théorème une démonstration puisée dans les premiers principes de la chose, et rendue, pour ainsi dire, sensible par la considération des divers polygones réguliers d'un même nombre de côtés. Cette idée simple de passer, par la même loi, d'un polygone à l'autre, en y marchant toujours par le même intervalle, nous mène directement à l'idée des *puissances*, des *résidus*, des *multiples racines* de l'unité, etc. D'où il paraît, comme je l'ai déjà remarqué dans d'autres mémoires, que la théorie de l'ordre est la source

naturelle des propriétés des nombres... [Poinsot, 1845, p. 54]

Poinsot revient ici sur la signification de sa notion d'ordre : les groupes d'objets qu'il construit en considérant l'ordre dépendent toujours d'une même loi.

4 - Théorie des équations binômes

Dans le quatrième chapitre, Poinsot revient sur la théorie des équations binômes. Cette partie ne contient pas de nouveaux résultats, mais consiste en une synthèse sur ce cas particulier de congruences, où les modules considérés peuvent être premiers ou composés. Smith commente d'ailleurs :

> The work of Poinsot (Reflexions sur la Theorie des Nombres, cap. iv. p. 60) contains a very full and elegant exposition of the theory of binomial congruences; but neither he nor any other writer subsequent to Gauss has been able to add any other direct method to that which we have just mentioned [Smith, 1859-1865, p. 141].

Il donne notamment une méthode permettant de déterminer les racines primitives d'un nombre premier donné. Il revient également sur la notion d'ordre, dans l'article *Sur l'ordre naturel dans lequel doivent être rangées les équations binômes* Poinsot y reprend les arguments qu'il a développés dans son mémoire de 1820 à propos de l'ordre dans lequel on peut ranger les racines n^{e} de l'unité et conclut de manière similaire :

> Ainsi, soit qu'on change, la racine r d'où l'on part, soit qu'on change l'exposant a à l'aide duquel on produit les racines l'une après l'autre, la disposition mutuelle de ces racines n'en peut être troublée; elles demeurent toujours équi-distantes, comme si elles étaient rangées en cercle. C'est à cet ordre remarquable que tient la résolution algébrique des équations binômes, et, en général, celle de toute équation où l'inconnue est une fonction des racines de l'unité : ce qui comprend au fond, comme on peut le démontrer, toutes les équations possibles à racines périodiques (voyez le tome IV des *Mémoires de l'Académie des Sciences*)[Poinsot, 1845, p. 77].

5 - Conclusion

Dans ce mémoire, Poinsot développe des résultats élémentaires de théorie des nombres en mettant en avant le fondement des démonstrations qu'il propose. Il tente de donner des preuves basés sur un nombre restreint au maximum de principes élémentaires. Il insiste à nouveau sur l'importance de la considération de l'ordre en mathématiques de façon générale, et pour la théorie des nombres en particulier. D'autre part, remarquons que, contrairement à [Poinsot, 1818] et [Poinsot, 1820], Poinsot ne considère pas ici de racines imaginaires de congruences.

Remarquons enfin que les preuves fondées sur les principes de l'ordre proposées par Poinsot dans sa troisième partie, sont reprises dans des textes de théorie des nombres

élémentaires. C'est par exemple le cas de l'article [Aubry, 1907], dans lequel l'auteur donne plusieurs démonstrations des théorèmes de Fermat et Wilson : les démonstrations de Poinsot fondées sur la considération de l'ordre y sont détaillées. De même, Paul Bachmann, dans son traité de théorie des nombres élémentaires, reprend cette méthode basée sur la considération de polygones réguliers et la qualifie de *très instructive*[7] dans le paragraphe dont le titre est *Ableitung des Euclidischen Fundamentalsatzes nach Poinsot*[8]. Les idées exposées dans ce mémoire sont reprises à la fin du XIX^{e} et au début du XX^{e} siècle dans certains textes liés à la théorie des nombres élémentaires en France et en Allemagne. Nous allons voir dans la dernière section que, plus généralement, Poinsot et sa théorie de l'ordre sont régulièrement cités à partir de 1845, soit après la publication de ce texte, dont un compte-rendu d'une vingtaine de pages est d'ailleurs donné par Grunert dans le périodique *Archiv der Mathematik und Physik* en 1846.

III La théorie de l'ordre dans la deuxième moitié du XIX^{e} siècle

Même s'il serait difficile de trouver chez Poinsot un résultat nouveau dû à la théorie de l'ordre, celle-ci semble avoir eu un impact à moyen terme : nous en donnons un aperçu dans cette section.

En 1847, Cournot, dont les comptes rendus du *Bulletin de Férussac* contiennent déjà quelques commentaires sur Poinsot, reprend la définition de l'algèbre par Poinsot dans le cadre de la théorie de l'ordre dans *De l'origine et des limites de la correspondance entre l'algèbre et la géométrie* :

> Enfin, pour ne pas abuser des citations, suivant M. Poinsot, l'algèbre est la science de l'ordre : idée fine et profonde, mais qui a besoin de commentaire, et que l'auteur lui-même, dans un de ces derniers écrits, a lucidement commenté[Cournot, 1847, p. 61].

Il cite ensuite la définition de l'algèbre donnée par Poinsot en 1845. Cournot se réfère à plusieurs reprises à Poinsot dans ses travaux. Dans [Martin, 1996], la philosophie de Cournot est d'ailleurs présentée comme « philosophie de l'ordre ». L'auteur ajoute :

> C'est dire notamment qu'elle se propose de mettre à jour la diversité des relations qui unissent les différents objets qu'elle envisage, afin d'y déceler l'organisation interne qui leur confère leur unité sur la base de leurs différences[Martin, 1996, p. 24].

7. Voir [Bachmann, 1892, p. 19] : « Diese sehr instruktive Methode, der wir hier uns anschliessen, stammt von Poinsot her ».

8. Nous remercions Frédéric Brechenmacher pour avoir attiré notre attention sur cette références.

Cela correspond bien, de façon plus générale, aux idées développées par Poinsot dans ses travaux d'algèbre et de théorie des nombres [9].

La définition de l'algèbre par Poinsot citée par Cournot est également reprise dans le *Vocabulaire technique et critique de la philosophie* de Lalande : « Algèbre [...] D. Science de l'ordre (Poinsot). Cette définition a été louée par Cournot pour sa profondeur, dans un chapitre où il recueille une série de définitions de l'Algèbre (*Correspondance*, ch. IV) mais lui-même adopte finalement le sens C »[Lalande, 1932, p. 28].

Le philosophe Louis Couturat cite Poinsot dans le cadre de la *théorie de l'ordre* dans son article *Sur les rapports du nombre et de la grandeur*, publié en 1898 dans la *Revue de Métaphysique et de Morale*. Il y explique que la notion d'ordre est déjà utilisée dans les travaux de Descartes, qui définit les mathématiques comme la « recherche de l'ordre et de la mesure » [10] et qui explique : «Toute la méthode consiste dans l'ordre et la disposition des objets». On retrouve des traces de l'importance de cette notion chez Fermat, Pascal, Leibniz et Bernoulli mais :

> ce n'est que dans ce siècle qu'elle [la science de l'ordre] a véritablement été fondée par Galois. Depuis lors (1832), elle a pris un développement extraordinaire, non seulement en prenant place dans la mathématique à côté des sciences traditionnelles et classiques, mais encore en les envahissant et en les transformant presque toutes. Cette science, que Sylvestre et Cayley appelaient la *Tactique*, et Cournot la *Syntactique*, consiste principalement dans la théorie des substitutions[Couturat, 1898, p. 437].

Galois est ici mis en avant par rapport à ses travaux de 1832, puis Couturat ajoute plus loin :

> Voyons maintenant quels sont les rapports de la théorie des substitutions avec l'algèbre. C'est à Cournot, après Poinsot[Couturat donne pour références [Cournot, 1847] et [Poinsot, 1845].], que revient le mérite d'avoir mis en lumière l'importance de l'idée d'ordre comme fondement des sciences mathématiques. Ces auteurs distinguent dans l'algèbre deux parties : 1 ° une arithmétique universelle, fondée sur la généralisation des opérations élémentaires et sur l'extension corrélative de l'idée de nombre ; 2 ° la science de l'ordre et des combinaisons, science formelle et abstraite, applicable à toutes sortes d'objets et d'opérations. Cette distinction est juste et profonde ; seulement, elle est trop

9. Nous tenons à remercier Bernard Bru et Thierry Martin pour avoir répondu à nos interrogations sur Cournot, notamment dans le cadre de sa collaboration au *Bulletin de Férussac*, et pour nous avoir fourni des documents sur les écrits de jeunesse du philosophe. D'autre part, signalons que Poinsot a également été très proche d'Auguste Comte : il fait partie des savants ayant assisté aux premières leçons de philosophie positiviste de Comte et l'a soutenu dans sa carrière. Les idées de Poinsot semblent également avoir été reprises par des savants proches du réseau saint-simonien, comme Despeyrous par exemple. Il serait donc intéressant de faire une analyse approfondie des liens entre Poinsot et Comte d'une part, et entre Poinsot et les saint-simoniens d'autre part.

10. Les citations de Descartes données par Couturat sont tirées de [Descartes, 1701].

radicale pour qu'on puisse confondre sous le même titre deux sciences tout à fait hétérogènes. Nous réserverons donc le nom d'algèbre à l'arithmétique universelle, science du nombre généralisé, comprenant la théorie des équations, qui a pour but de déterminer des nombres inconnus par leurs relations arithmétiques avec des nombres connus ; et nous verrons dans la théorie de l'ordre une science à part, indépendante des sciences du nombre et de la grandeur, quoique pouvant leur prêter un précieux concours.

Mais si l'algèbre est bien distincte de la science de l'ordre, si même elle en est en principe indépendante, il n'en est pas moins vrai qu'elle a du y avoir recours pour la résolution algébrique des équations ; et le mérite de Galois a précisément consisté à apercevoir le secours que l'algèbre pouvait tirer de la notion d'ordre, en apparence étrangère à ses spéculations[Couturat, 1898, p. 438-439].

C'est néanmoins Poinsot qui place explicitement la notion d'ordre au cœur de l'algèbre et de la théorie des nombres dès 1818.

La théorie de l'ordre de Poinsot est également mise en avant dans des manuels d'algèbre. Par exemple, on peut citer la préface du *Cours d'algèbre élémentaire* de Léon Lecointe, publié en 1859, dans laquelle l'auteur tente de définir l'algèbre :

> Je définis l'algèbre : la science qui s'occupe de la détermination du nombre représentant une grandeur et de la recherche des propriétés de ce nombre, abstraction faite de toute détermination d'unité. J'aurais pu ajouter : et qui traite des relations qui existe entre ces grandeurs, indépendamment des valeurs particulières dont elles sont susceptibles et des unités arbitraires l'expression numérique.
> Je justifie cette définition par une autorité :
> M^r^ Poinsot [Il renvoie au mémoire de Poinsot publié en 1845], après avoir établi qu'il existe une première algèbre, qu'il appelle arithmétique universelle, ajoute : « *il y a une algèbre supérieure qui repose toute entière sur la théorie de l'ordre et des combinaisons, qui s'occupe de la nature et de la composition des formules considérées en elles-mêmes comme de purs symboles et sans aucune idée de valeur ou de quantité[...] c'est même cette seule partie élevée de la science qui mérite, à proprement parler, le nom d'*Algèbre »[Lecointe, 1859, Préface].

On retrouve également l'association entre la notion d'*ordre* et Poinsot dans le *Cours de Mathématiques à l'usage des candidats à l'École Polytechnique, ...* publié en 1890, où De Comberousse indique dans le cadre de son exposé sur la résolution algébrique des équations :

> Nous sommes forcés d'indiquer seulement ces résultats et de renvoyer le lecteur aux écrits mêmes des savants illustres qui ont commencé à élucider ces questions si vastes et si difficiles. Lagrange et Gauss, Abel et Galois, Cauchy et

J. -A. Serret, MM. Bertrand, Hermite, E. Mathieu, Camille Jordan, ainsi que d'autres célèbres géomètres étrangers, ont jeté les fondements de cette Algèbre transcendante, où l'*ordre* a pris la place prédominante que lui assignait Poinsot [11][De Comberousse, 1890, p. 619].

Mais cet impact ne semble pas limité aux philosophes et aux ouvrages élémentaires : des mathématiciens se réclament également de Poinsot dans leurs travaux. Nous avons cité précédemment des extraits des mémoires de Théodore Despeyrous. Charles-Ange Laisant semble également avoir utilisé la notion d'ordre dans le sens développé par Poinsot dans ses travaux et cite par exemple [Poinsot, 1845] [12]. Camille Jordan associe Poinsot à la théorie de l'ordre dans son *Mémoire sur le nombre des valeurs d'une fonction* : « L'étude de ces diverses sortes de symétries offre un grand intérêt car c'est la base et le point de départ naturel de ce genre de recherches que M. Poinsot a distingué de tout le reste des mathématiques,sous le nom de *théorie de l'ordre* : elle présente en outre d'importantes applications »[Jordan, 1861, p. 113].

Ainsi, Poinsot est régulièrement associé à l'*ordre* après la publication de son mémoire de 1845. De plus, il semble clair que, parmi les mathématiciens qui travaillent dans la suite de Galois en France, certains se réclament de l'ordre et de Poinsot. En particulier, Jordan que nous avons cité précédemment insiste à nouveau sur le rôle de la théorie de l'ordre de Poinsot dans la *Notice sur les travaux de Camille Jordan* où il présente ses propres travaux en vue d'une élection à l'Académie des Sciences pour la section géométrie. En effet, dans l'avant-propos, il cite partiellement les définitions des mathématiques, de l'algèbre et de la géométrie de situation données par Poinsot dans le mémoire de 1845 puis indique :

Ces réflexions de Poinsot, qui ont servi d'épigraphe à mes premiers essais, caractérisent assez nettement la tendance générale de mes recherches.
Elles ont presque constamment pour but d'approfondir la *théorie de l'ordre* au double point de vue de la Géométrie pure et de l'Analyse[Jordan, 1881, p. 8].

Plus généralement, Frédéric Brechenmacher suggère que ce point de vue de la théorie de l'ordre est non seulement partagé par Jordan et Galois notamment pour l'algèbre et la théorie des nombres, mais qu'il semble également avoir induit une certaine approche des mathématiques dans d'autres domaines comme la mécanique par exemple :

The fact that Jordan had presented his reduction [of imprimitive groups to primitive groups] in the framework of Poinsot's theory of order suggests that Jordan and Galois shared a specific perspective on the roles played by relations in both algebra and number theory. Little is nevertheless known about the role played by the theory of order in the 19th century. Jordan's early works suggest that a specific approach to mathematics might have circulated within cristallography and mechanical investigations of motions of solid bodies (such as polyhedrons)[Brechenmacher, 2011].

11. L'auteur donne comme référence le mémoire de 1845.
12. À ce sujet, voir notamment [Auvinet, 2011, p. 305, 324 et 340].

Finalement, Poinsot témoigne d'une réflexion théorique sur ce qui permet la résolubilité des équations, insiste sur les relations entre les racines au détriment des calculs explicites et suggère une théorie des imaginaires pour les congruences. Toutes ces incitations jouent vraisemblablement un rôle dans le développement des mathématiques de Galois notamment, même s'il est difficile de le préciser davantage. Les mentions récurrentes à la théorie de l'ordre de Poinsot tout au long du XIX^{e} siècle montre que sa façon de voir a eu un impact sur un ensemble de mathématiciens et de philosophes. Prendre en compte Poinsot et sa théorie de l'ordre incite finalement à mieux situer l'originalité de Galois dans la théorie des équations : en particulier, l'intérêt pour la forme des relations entre racines et non pour leur calcul, le transfert de la notion de racines complexes aux congruences sont des idées déjà en discussion dans les publications des premières décennies du XIX^{e} siècle.

PARTIE IV

La théorie des nombre de Louis-Augustin Cauchy (1829 - 1847)

Introduction

Cauchy (1789-1857) [13] est bien sûr connu pour ses travaux en analyse [14], en particulier pour sa théorie des fonctions holomorphes, et pour ses mémoires sur la théorie des substitutions, souvent cités dans le cadre de la théorie algébrique des équations et de la naissance de la théorie des groupes [15]. Par contre, dans le domaine de la théorie des nombres, Cauchy est le plus souvent décrit dans les sources secondaires [16] comme un mathématicien obtenant des résultats similaires à ceux de Gauss, Jacobi ou Kummer, mais de manière totalement disparate. Comme nous l'avons indiqué dans l'introduction générale, Lemmermeyer observe par exemple que Cauchy obtient moins de résultats que Jacobi sur les lois de réciprocité notamment car il n'en comprend pas la nature profonde [17]. Notre objectif est ici de montrer au contraire que les différents résultats donnés par Cauchy dans ses travaux arithmétiques entre 1829 et 1840 ne sont pas disparates, mais obéissent à une perspective différente et répondent dans une certaine mesure aux travaux des mathématiciens allemands cités précédemment.

Né en 1789, l'enfant Cauchy vit très mal la période révolutionnaire : son père, ayant une importante place administrative, doit fuir Paris pour Arcueil avec sa famille en 1794. Peu de temps après, celui-ci obtient néanmoins un poste au Sénat sous le nouveau régime et revient à Paris. Louis-Augustin reçoit une initiation aux lettres et sciences par son père jusqu'en 1802, date à laquelle il entre à l'école centrale du Panthéon, où il se distingue particulièrement par ces capacités pour le latin et le grec. Il prépare néanmoins en 1804 le concours d'admission à l'École Polytechnique et y est admis l'année suivante à l'âge de seize ans. En 1807, il intègre l'École des Ponts et Chaussées. Malgré des dispositions certaines à l'ingénierie [18], Cauchy se consacre finalement aux mathématiques, et, sous les conseils de Lagrange, présente ses premiers travaux sur les polyèdres à l'Institut en 1811 et 1812. Ces premières recherches sont très bien accueillies et Cauchy est élu correspondant de la Société Philomatique. Jusqu'en 1816, il se présente en vain à plusieurs élections, notamment celle pour remplacer Lagrange à l'Académie, remportée par Poinsot, et une élection en 1814 pour combler un poste vacant à la société Philomatique. Pendant cette période, Cauchy publie plusieurs travaux dont ses mémoires sur les substitutions, sur les

13. Se reporter à [Belhoste, 1985] pour une biographie détaillée de Cauchy. Les indications biographiques que nous donnons ci-dessous sont issues de cet ouvrage. Voir également [Dhombres et Gilain, 1992] pour une liste de travaux concernant Cauchy.
14. Voir notamment [Peiffer, 1978] et [Gilain, 1989].
15. Voir par exemple [Dahan Dalmedico, 1980] ou [Wussing, 1984].
16. Par exemple, voir [Lemmermeyer, 2000] ou [Edwards, 1977].
17. Voir [Lemmermeyer, 2009, p. 171].
18. Voir [Belhoste, 1985, p. 23-31].

nombres de même forme et sur le théorème de Fermat pour les nombres polygonaux [19]. En 1815, la chute de Napoléon est définitive et la Restauration se met en place en juillet 1815. En novembre de la même année, Cauchy est nommé professeur à l'École Polytechnique à la place de Poinsot. De plus, avec la réorganisation de l'Institut consécutive à l'ordonnance royale de 21 mars 1816, plusieurs savants, dont Carnot et Monge pour la section mécanique, sont exclus de l'Institut. Cauchy est nommé à la place de l'un d'eux et, malgré ces nominations assez mal vues par ses collègues, il devient rapidement un mathématicien reconnu.

Ses travaux arithmétiques suivants sont publiés dans le *Bulletin de Férussac* entre 1829 et 1831 et dans ses *Exercices de mathématiques* en 1829. Il présente également sur cette période plusieurs autres mémoires sur la théorie des nombres qui ne sont pas publiés. Dans les articles du *Bulletin de Férussac*, Cauchy donne des résultats assez généraux, avec des démonstrations à peine esquissées, autour des lois de réciprocité et certaines formes quadratiques de la forme $p^\mu = x^2 + ny^2$, où p est un nombre premier, et n un diviseur de $p - 1$. Dans les écrits insérés dans ses *Exercices*, Cauchy expose des propriétés générales des congruences, qu'il nomme équivalences, souvent en lien avec des propriétés analogues des équations [20]. Mais en 1830, la Révolution de juillet éclate, Charles X abdique et ce tournant politique pousse Cauchy à s'exiler volontairement pendant huit années. Le savant ne produit que très peu de textes pendant cette période et aucun n'aborde la théorie des nombres.

À son retour en France en 1839, Cauchy refuse de se soumettre à l'obligation d'un serment politique envers le régime en place, et doit donc attendre la proclamation de la seconde République en février 1848 pour avoir une chance d'obtenir un poste scientifique, ses tentatives antérieures restant vaines [21]. Il obtient la chaire d'astronomie mathématique à la Sorbonne en mars 1849. De 1839 à 1850, non seulement Cauchy use, et abuse, de la possibilité de publier dans les *Comptes Rendus* des séances de l'Académie, mais, il fait également paraître son propre périodique dès 1839, intitulé cette fois les *Exercices d'analyse et de physique mathématique*. Avec ces deux périodiques, Cauchy publie de nombreux mémoires et notes de théorie des nombres, répartis principalement sur deux très courts intervalles de temps : 1839-1840 et 1847. Entre 1839 et 1840, dix notes sont insérées dans les *Comptes Rendus* et un *Mémoire sur la théorie des nombres* de plus de quatre cent pages est publié en 1840 dans les *Mémoires* de l'Académie. Tous ces textes reprennent et développent les thèmes abordés dans les articles du *Bulletin de Férussac* de 1829 et 1831 ; la partie principale du *Mémoire sur la théorie des nombres* correspond d'ailleurs selon Cauchy à un travail présenté en 1830 à l'Académie. Entre 1841 et 1845, on retrouve deux mémoires de théorie des nombres dans ses *Exercices*, contenant des

19. Voir notre première partie, p. 49.
20. Voir notre première partie, p. 72.
21. Voir [Belhoste, 1985, p. 153-178].

résultats généraux sur les congruences et les équations indéterminées[22]. Le mémoire sur les équations indéterminées est également reproduit dans les *Comptes Rendus* des séances de l'Académie. En 1847, Cauchy publie plus de dix notes aux *Comptes Rendus*. Cette fois-ci, ses travaux sont en lien avec les recherches en cours sur le dernier théorème de Fermat et traitent des *polynômes radicaux*, qui sont aujourd'hui appelés les entiers cyclotomiques. Cette même année, Cauchy expose également une nouvelle théorie des imaginaires, basée sur l'utilisation de congruences. Il insère également un mémoire à ce sujet en 1847, intitulé *Mémoire sur la théorie des équivalences algébriques substituées à la théorie des imaginaires* dans ses *Exercices d'analyse et de physique mathématique*.

Dans cet ensemble de textes[23], nous distinguons deux formes principales d'apparition des congruences : dans plusieurs mémoires, que nous avons commentés dans la première partie, Cauchy étudie les congruences en général et s'appuie le plus souvent sur des analogies entre la théorie des équations et celle des congruences pour démontrer des théorèmes sur les congruences. Les autres textes constituent la grande majorité de sa production arithmétique : il y utilise les congruences et les résidus pour obtenir des résultats sur d'autres thèmes, de théorie des nombres principalement. C'est cette deuxième catégorie de mémoires que nous allons étudier ici.

Plusieurs difficultés se sont présentées dans l'étude de ces textes arithmétiques de Cauchy. D'une part, ses *Œuvres complètes* se composent de 27 volumes : comme le remarque Amy Dahan dans sa thèse sur les travaux en algèbre de Cauchy, sa production « n'est dépassée en volume que par celle d'Euler »[Dahan Dalmedico, 1979, p. 1]. Cauchy utilise plusieurs moyens de publication. Par exemple, lors de son retour en France, Cauchy fait une utilisation intensive[24] des *Comptes Rendus hebdomadaires des séances de l'Académie des Sciences*. Même si ses travaux en théorie des nombres représentent une part très minoritaire de son œuvre, le nombre de textes publiés dans ce domaine reste donc important[25]. À ce volume important de matériau s'ajoutent des difficultés de lecture des productions de Cauchy. Par exemple, pour les années 1839 et 1840, Cauchy publie dans les *Comptes Rendus* de nombreuses notes de théorie des nombres où il aborde des idées variées qui ne se suivent pas nécessairement. D'ailleurs, à ce sujet, Biot est très critique envers Cauchy au sujet de ses nombreuses publications dans les *Comptes Rendus* de l'Académie des

22. Voir notre première partie, p. 84 et 87.

23. La liste de textes de Cauchy en rapport avec les résidus et les congruences est donnée en annexe : voir à partir de la page 513.

24. Considérée comme abusive par beaucoup : selon [Belhoste, 1991, p. 191], Cauchy présente environ 240 notes aux *Comptes Rendus* entre 1838 et 1848. À la suite de Bruno Belhoste dans [Belhoste, 1982], on peut par exemple citer un article du *National* du 19 octobre 1942, à propos de la quantité de notes publiées de Cauchy dans les *Comptes Rendus* : « Y aurait-il réellement une maladie attachée à la culture de la géométrie, et la noble espèce d'intelligence qui s'y consacre serait-elle exposée à des accès chroniques d'une fièvre particulière dont chaque accès n'aurait d'autre issue qu'une sorte d'évacuation algébrique sous forme d'un Mémoire ?[...] ». La violence de cette attaque peut également s'expliquer par les différences d'opinions politiques entre Cauchy et le journaliste. Mais, dans le *Journal des savants* de novembre 1842, c'est au tour de Biot d'être très critique envers son collègue : nous le citons juste après.

25. Voir liste en annexe.

Sciences et observe dans le *Journal des savants* de novembre 1842 :

> Un géomètre, assurément très habile, a profité de l'opportunité des comptes rendus pour publier, presque dans chaque numéro, une série de mémoires entiers, hérissés de symboles, sans connexion entre eux, reproduisant plusieurs fois les mêmes résultats ou les mêmes idées sous diverses formes, à mesure qu'elles se présentent à son esprit, brisés aussi de renvois qui se rapportent à une multitude de publications éparses ; de sorte qu'aujourd'hui, s'ils se correspondent dans la pensée de l'auteur, comme je n'en fais aucun doute, il semblerait être à peu près le seul qui puisse en profiter, ou qui soit capable d'en suivre le fil.

C'est effectivement la première impression qui ressort lors de la lecture de ces notes. D'autre part, Cauchy publie également un *Mémoire sur la théorie des nombres* de plusieurs centaines de pages dans les *Mémoires* de l'Académie en 1840, dans lequel il intègre un travail présenté à l'Académie en 1830 et qu'il enrichit de notes représentant plus de 350 pages. Ce texte reprend les différents résultats exposés par Cauchy dans le *Bulletin de Férussac* et les *Comptes Rendus* de l'Académie : le lecteur pourrait donc supposer que ce texte va permettre d'éclaircir les différents travaux de Cauchy sur la théorie des nombres. Sa partie principale montre que le mémoire exposé initialement en 1830 est effectivement très succinct, et de nombreux raisonnements nécessitent d'importants compléments afin d'être autonomes. Ces compléments sont en grande partie contenus dans les quatorze notes imprimées à la suite du texte principal. Cependant, à part pour les deux premières notes, explicitement destinées à compléter certains calculs des deux premiers paragraphes, Cauchy n'indique pas dans le corps principal du mémoire à quelle(s) note(s) le lecteur doit se référer pour obtenir la justification de chaque résultat : il faut donc commencer par lire les ajouts pour ensuite tenter de relier les différents résultats exposés dans le texte, ce qui ajoute au manque de lisibilité du mémoire. De plus, comme le remarque Amy Dahan dans sa thèse, les raisonnements de Cauchy contiennent de nombreuses erreurs, ce qui est un obstacle supplémentaire dans l'étude des mémoires de Cauchy [26].

Enfin, comme nous l'avons signalé dans notre brève biographie de Cauchy, celui-ci quitte la France pendant huit ans et ne publie quasiment pas de travaux pendant cette période. Il est donc très difficile de se faire une idée précise de ses occupations mathématiques d'alors : poursuit-il ses recherches en théorie des nombres, ou les résultats exposés entre 1839 et 1840 sont-ils déjà totalement présents dans son esprit au début des années 1830 ?

Par ailleurs, Amy Dahan justifie le fait que son étude exclut les travaux arithmétiques de Cauchy ainsi :

> Indiquons que nous avons poussé l'arbitraire jusqu'à séparer les recherches de Théorie des Nombres, des recherches algébriques, ce qui sans doute peut être considéré comme une aberration. Pourtant, il nous est apparu que l'étude des écrits de

26. Nous signalerons certaines de ces erreurs au cours de notre étude, qu'elles soient des fautes de frappe ou de calcul.

> Cauchy relatifs à la Théorie des nombres, ne saurait constituer seulement un chapitre supplémentaire de notre monographie, mais qu'elle appelait, à elle seule, un travail d'égale envergure. En effet, les travaux de Cauchy en théorie des nombres, à l'inverse de bien d'autres de ce mathématicien, ne peuvent être considérés de façon autonome. Ils doivent être étudiés dans un premier temps en relation avec les œuvres de Legendre et Gauss, et dans un deuxième temps, avec les travaux de nombreux contemporains (Lamé, Kummer, ...)[Dahan Dalmedico, 1979, p. 4].

Dans notre partie sur Louis Poinsot, nous avons principalement analysé ses mémoires avec comme point de repère les *Disquisitiones Arithmeticae* de Gauss. Ici, les textes de théorie des nombres de Gauss suffisent également pour comprendre le contenu des mémoires de Cauchy, mais ils ne permettent certainement pas de comprendre la chronologie et les résultats qui y sont mis en avant. Effectivement, contrairement à Poinsot, les recherches de Cauchy sont en lien étroit avec des recherches de ses collègues contemporains (Jacobi, Dirichlet, Kummer, Lamé, ...) qu'il cite régulièrement. De plus, les "vides" de plusieurs années observés dans sa production arithmétique sont également des périodes où les autres savants publient sur des thèmes similaires : il est donc indispensable de connaître les idées et méthodes générales avancées par ceux-ci pour comprendre les évolutions des recherches de Cauchy, et pour mettre en avant les différences de perspectives entre les premiers et le dernier. C'est pourquoi nous replaçons les textes de Cauchy analysés dans le contexte des différentes publications sur le même thème contenues dans notre corpus.

Nous nous concentrons ici sur l'analyse de deux groupes de textes, qui correspondent à deux utilisations différentes des congruences par Cauchy. Dans un premier chapitre, nous étudions les différents mémoires de Cauchy publiés entre 1829 et 1840 sur les formes quadratiques indiquées précédemment. Dans un deuxième chapitre, nous considérons ses trois textes de 1847 sur sa théorie symbolique des imaginaires fondée sur une nouvelle utilisation des congruences. Nous avons également listé une dizaine de notes de Cauchy, publiées en 1847, en lien avec des recherches sur le dernier théorème de Fermat et les entiers cyclotomiques. L'étude de ces textes est un travail en soi, à placer dans le contexte des écrits de Lamé, Wantzel, Kummer, ..., sur ce théorème en particulier, et sur les nombres entiers complexes en général, afin de dégager clairement les implications des réflexions de Cauchy sur ces sujets. Nous ne nous arrêtons pas sur ce thème dans le cadre de notre étude, car Cauchy y utilise les résultats obtenus dans ses recherches sur les formes quadratiques, et n'y développe donc pas un nouvel usage des congruences.

CHAPITRE 9

1829 - 1840 : des notes sur les formes quadratiques de la forme $p^\mu = x^2 + ny^2$

I Présentation des sources

Comme nous l'avons indiqué dans l'introduction, la quasi-totalité des textes de théorie des nombres publiés par Cauchy entre 1829 et 1840 ont pour objet l'étude des formes quadratiques $p^\mu = x^2 + ny^2$ ou $4p^\mu = x^2 + ny^2$ où où p est un nombre premier et n un diviseur de $p - 1$. On retrouve déjà chez Fermat des résultats sur les nombres premiers que l'on peut mettre sous la forme $x^2 + ny^2$. Euler, Lagrange, Legendre et Gauss développent des méthodes pour démontrer les conjectures formulées par Fermat, puis par Euler. Ainsi, à l'occasion de recherches sur ce thème, Euler développe sa théorie des résidus quadratiques, Lagrange travaille sur les formes quadratiques, étudiées ensuite par Legendre et Gauss. Ce dernier va également considérer les résidus cubiques et biquadratiques dans les cas où la théorie des formes quadratiques est insuffisante[1]. Dans ses travaux sur les formes quadratiques, Cauchy ne se réfère jamais à la théorie des formes quadratiques développée par Gauss dans la section V de son ouvrage. Ses écrits se fondent en effet tout particulièrement sur les expressions que l'on nomme les sommes de Gauss, et sur lesquelles nous revenons dans la section suivante ; l'origine des recherches de Cauchy peut être trouvée dans l'ouvrage de Gauss, mais dans la section VII. Gauss y présente sa théorie de la cyclotomie avec la résolution des équations binômes, et y obtient également des résultats sur les sommes de Gauss. Dans l'article 358, il montre par exemple que tout nombre de la forme $3m + 1$ peut se mettre sous la forme $x^2 + 27y^2$ en utilisant certains cas particuliers de périodes introduites dans la section VII. Il observe d'ailleurs :

> Il suit de là que le nombre $4n$, c'est-à-dire le quadruple de tout nombre premier de la forme $3m+1$, peut être représenté par la forme x^2+27y^2 ; et quoique ce résultat puisse se tirer sans difficulté de la théorie générale des formes binaires, il n'en est pas moins étonnant qu'une telle décomposition soit liée si intimement avec les nombres a, b, c...[2][Gauss, 1801, art. 358].

Entre 1829 à 1831, nous avons listé deux mémoires de Cauchy sur les congruences dans les *Exercices de Mathématiques* et deux mémoires sur les lois de réciprocité et les formes quadratiques publiés dans le *Bulletin de Férussac*. D'autre part, sept mémoires de Cauchy en lien avec la théorie des nombres sont annoncés dans les *Procès Verbaux* des séances de l'Académie des Sciences sur cette période : par exemple, Cauchy présente quatre mémoires

1. Voir [Cox, 1989].
2. Les nombres a, b et c sont définis en fonction des sommes cubiques de Gauss.

sur la détermination des racines primitives[3] en 1829 et 1830 qui ne sont pas publiés. Deux *Mémoires sur la théorie des nombres* sont également listés dans les *Procès Verbaux*, pour les séances du 9 novembre 1829 et du 31 mai 1830. Ce dernier texte est publié en 1840 avec plusieurs notes dans les *Mémoires* de l'Académie sous la forme d'un texte de plus de quatre cents pages. Enfin, Cauchy propose lors de la séance du 14 septembre 1829 à l'Académie un texte intitulé *Théorie générale des puissances qui comprend comme cas particuliers tout ce que l'on sait sur la théorie des résidus quadratiques et biquadratiques, etc.*, qui semble correspondre au mémoire *Sur la théorie des nombres* publié dans le douzième tome du *Bulletin de Férussac*.

D'autre part, entre 1839 et 1840, les recherches de Cauchy en théorie des nombres sont présentées dans une dizaine de notes des *Comptes Rendus* de l'Académie des Sciences. Ces notes contiennent des résultats du *Mémoire* publié en 1840, que nous analysons dans le prochain chapitre, exposés de façon plus générale et sans démonstrations détaillées.

Dans un premier temps, nous étudierons le contenu des deux mémoires de Cauchy publiés entre 1829 et 1831 dans le *Bulletin de Férussac*. Nous donnerons ensuite un aperçu des méthodes exposées par Jacobi dans ses recherches traitant notamment du même sujet et développées entre 1827 et 1840. Dans une troisième section, nous dégagerons la méthode générale donnée par Cauchy sur les formes quadratiques considérées, à partir de l'analyse de ses notes parues aux *Comptes Rendus* des séances de l'Académie. Enfin, nous analyserons dans le chapitre suivant son *Mémoire* publié en 1840 en le mettant en relation avec les notes commentées précédemment. Nous commençons par faire le point sur les notations et formulations utilisées par Cauchy dans les différents textes commentés ci-après.

II Préliminaires : notations et formulations récurrentes

Dans ses différentes publications en lien avec les formes quadratiques, Cauchy utilise presque toujours les mêmes notations pour les outils qu'il utilise régulièrement. Nous nous proposons donc d'en donner ici un aperçu, pour faciliter la lecture de ce chapitre et du suivant, et éviter les répétitions ; sauf indication contraire, ces notations seront valables pour ces deux chapitres.

Dans l'introduction du mémoire publié en 1829 dans le *Bulletin de Férussac* et dans la première note de son grand mémoire de 1840, Cauchy rappelle la notion de congruence, qu'il nomme équivalence, et l'attribue à Gauss. D'autre part, il introduit des racines primitives d'équations et d'équivalences et se réfère uniquement à Poinsot à ce sujet en 1829 : « je dirai avec M. Poinsot que ρ est une racine primitive »[Cauchy, 1829a, p. 89]. Dans la note [Cauchy, 1839] publiée en 1839 dans les *Comptes Rendus*, Cauchy se réfère de la même façon à Poinsot pour les racines primitives d'une équation binôme.

3. Séances des 14 septembre 1829 et 25 janvier, 31 mai et 5 juillet 1830.

Cela semble a première vue étonnant puisque c'est Euler qui introduit la notion de racine primitive en théorie des nombres dans [Euler, 1774], et Gauss qui la développe dans les *Disquisitiones Arithmeticae* mais peut s'expliquer par le fait que Poinsot, en 1820, insiste particulièrement sur les propriétés des racines primitives de congruences d'une part, mais aussi sur les racines primitives d'équations. Dans la première note de son grand mémoire, Cauchy cite d'ailleurs Euler et Poinsot :

> De plus, p étant un nombre premier, nous disons avec Euler d'une part et de l'autre avec M. Poinsot, que r est une *racine primitive* de l'équivalence
>
> $$x^n \equiv 1 \pmod{p}$$
>
> et ρ racine primitive de l'équation
>
> $$x^n = 1.$$
>
> [Cauchy, 1840a, p. 84]

Ces références indiquent au moins que Cauchy connaît le contenu des travaux de Poinsot.

Les recherches de Cauchy, pour la période 1829-1840, sont centrées sur l'étude des formes quadratiques de nombres premiers p, de la forme $n\varpi + 1$. Le nombre n, qui peut être premier ou composé, est donc un diviseur de $p-1$ et Cauchy note $\varpi = \dfrac{p-1}{n}$. Les lettres h et k désignent généralement des nombres entiers quelconques. Dans certains cas, les nombres h, h', ... représentent les résidus quadratiques de p, tandis que les nombres k, k', ..., représentent les non-résidus quadratiques de p.

Cauchy introduit ensuite des racines primitives : les lettres grecques désignent des racines primitives d'équations tandis que les lettres latines désignent des racines primitives d'équivalences. Nous pouvons d'ailleurs observer que, par le choix de ces notations, Cauchy met une fois de plus en avant la correspondance entre racines d'équations et de congruences. Ainsi :

- θ est une racine primitive de $x^p = 1$;
- τ est une racine primitive de l'équation $x^{p-1} = 1$;
  t est une racine primitive de l'équivalence $x^{p-1} \equiv 1 \pmod{p}$;
- $\rho = \tau^{\varpi}$ est une racine primitive de $x^n = 1$;
  $r = t^{\varpi}$ est une racine primitive de l'équivalence $x^n \equiv 1 \pmod{p}$.

Avec ces notations, les racines de l'équation $x^p = 1$, différentes de l'unité, sont de la

forme θ^k, où k est compris entre 1 et $p-1$. On obtient ainsi la suite des racines de cette équation :

$$\theta, \theta^2, \theta^3, \ldots, \theta^{p-1}.$$

Ces racines peuvent également être réordonnées à l'aide de la racine primitive t, de manière à ce que les exposants forment une progression géométrique :

$$\theta, \theta^t, \theta^{t^2}, \ldots, \theta^{t^{p-2}}.$$

Cauchy reprend ainsi la réindexation des racines utilisée par Gauss, particulièrement mise en avant par Poinsot ; cette façon de ranger les différentes racines de l'unité est fondamentale dans les recherches de Cauchy, tout spécialement dans la définition des expressions que l'on appelle aujourd'hui les sommes de Gauss :

$$\Theta_h = \theta + \rho^h \theta^t + \rho^{2h} \theta^{t^2} + \rho^{p-2} \theta^{t^{p-2}} = \sum_{i=0}^{p-2} \rho^{ih} \theta^{t^i}.$$

Cauchy ne donne à ces expressions aucun nom particulier, et ne se réfère à aucun texte de Gauss. Mais, comme nous l'avons déjà observé, ces expressions sont introduites par Gauss dans la section VII des *Disquisitiones Arithmeticae*. Gauss revient également sur le calcul de ces sommes dans le cas où $n = 2$, soit le cas où $\rho = -1$, dans [Gauss, 1811]. Cauchy considère d'ailleurs régulièrement ce cas particulier et note :

$$\Delta = \theta - \theta^t + \theta^{t^2} - \ldots + \theta^{t^{p-3}} - \theta^{t^{p-2}}.$$

Comme ρ est une racine primitive de $x^n = 1$, $\Theta_h = \Theta_{h+in}$, pour tout i entier relatif.

Cauchy démontre que l'on a l'égalité :

$$\Theta_h \Theta_k = R_{h,k} \Theta_{h+k},$$

où $R_{h,k}$, appelé aujourd'hui une somme de Jacobi, est une expression de la forme $a_0 + a_1\rho + a_2\rho^2 + \ldots + a_{n-1}\rho^{n-1}$, où les a_i sont des nombres entiers. Là encore, Cauchy n'attribue la définition de l'expression $R_{h,k}$ à aucun savant. Cela n'est pas étonnant puisque, comme nous le verrons par la suite, Jacobi n'utilise pas ces expressions dans le seul article de théorie des nombres qu'il publie avant 1829. L'appellation "somme de Jacobi" se justifie néanmoins par une lettre de Jacobi à Gauss, datée du 27 octobre 1826, dans laquelle il utilise ces sommes, et insiste sur leur importance dans la théorie des nombres. De plus, dans [Jacobi, 1837], le mathématicien axe également son article sur les propriétés de ces sommes et sur leurs conséquences.

Manipuler ce type d'expressions conduit Cauchy à raisonner très souvent sur des sommes finies, qu'il symbolise indifféremment par S ou Σ, et dont il délimite généralement les bornes dans le texte. Par exemple :

$$R_{h,k} = (-1)^{\varpi(h+k)} \Sigma \left(\frac{u}{p}\right)^h \left(\frac{v}{p}\right)^k,$$

le signe Σ s'étendant à toutes les valeurs entières de u, v comprises entre les limites 1 et $p-1$,et qui vérifieront l'équivalence

$$1 + u + v \equiv 0 \pmod{p}.$$

[Cauchy, 1840a, p. 8]

Dans notre analyse, nous utilisons la notation moderne (ici : $\sum_{\substack{1\leq u,v\leq p-1 \\ 1+u+v\equiv 0 \pmod p}}$) lorsque Cauchy indique explicitement les conditions à prendre sur les variables.

Comme Cauchy, dans les travaux considérés ici, travaille également avec des produits de sommes, par exemple, avec les expressions $R_{h,k}$, il introduit ce qui correspond aujourd'hui à des combinaisons :

$$\Pi_{h,k} = \frac{1.2.3.\ldots[(h+k)\varpi]}{(1.2.3\ldots h\varpi)(1.2.3\ldots k\varpi)}.$$

Enfin, Cauchy utilise très régulièrement le symbole de Legendre [4], qu'il note $\left(\frac{k}{p}\right)$ ou $\left[\frac{k}{p}\right]$, qu'il définit parfois de manière plus générale. Ainsi, dans [Cauchy, 1829a], $\left(\frac{k}{p}\right) \equiv k^{\frac{p-1}{n}} \pmod{p}$. Cauchy utilise également le symbole de Jacobi [5], qui est la généralisation du symbole de Legendre pour les nombres composés : si la décomposition en facteurs premiers d'un nombre n est $\nu^a \nu'^b \ldots$, alors $\left(\frac{k}{n}\right) = \left(\frac{k}{\nu}\right)^a \left(\frac{k}{\nu'}\right)^b \ldots$.

III 1829-1831 : énoncés de résultats généraux

Comme nous l'avons vu dans notre première partie, avant 1825, peu de mathématiciens, Gauss et Poinsot principalement, publient régulièrement des textes en théorie des nombres en lien avec les résidus et les congruences. À partir de 1827, le nombre de publications autour de ces objets augmente rapidement avec la création du *Journal de Crelle*, avec notamment les travaux de Jacobi et Dirichlet qui sont insérés dans le *Journal de Crelle*. Des mémoires de Cauchy, Lebesgue, Galois, Libri paraissent également dans le *Bulletin de Férussac*.

4. Rappelons que Legendre introduit cette notation dans sa première édition de son *Essai sur la théorie des nombres*, en 1798.

5. Jacobi définit pour la première fois son symbole en 1837 dans [Jacobi, 1837].

1 - Un premier *Mémoire sur la théorie des nombres* (1829) : lois de réciprocité et formes quadratiques

Comme nous l'avons indiqué dans la première partie[6], Cauchy annonce dans le premier paragraphe de ce mémoire, *Considérations générales*, des résultats généraux sur les résidus et les lois de réciprocité, thème qui est central dans les recherches arithmétiques de Gauss à cette époque. Gauss a présenté en 1825 la première partie de ses recherches sur les résidus biquadratiques, et une note de Jacobi sur les résidus cubiques est publiée dans le *Journal de Crelle* en 1827. Si l'on s'en tient à son introduction[7], le travail de Cauchy semble donc contenir un cas général des lois de réciprocité incluant les questions des deux savants allemands.

Dans son deuxième paragraphe, Cauchy introduit les notations présentées dans notre préliminaire, puis expose sans démonstration certaines propriétés des sommes de Gauss et de Jacobi :

- Si h n'est pas divisible par $p-1$: $\Theta_h\Theta_{-h} = (-1)^{\varpi h}p$. Cauchy ne l'indique pas explicitement, mais ce résultat permet d'obtenir $p-2$ décompositions du nombre $\pm p$ en un produit de deux nombres complexes. Nous verrons que Jacobi par exemple insiste sur ce point dans certains de ses écrits.
- Il donne la relation existant entre les sommes de Gauss et les sommes de Jacobi : $\Theta_h\Theta_k = R_{h,k}\Theta_{h+k}$. Il note de plus que les expressions $R_{h,k}$ sont de la forme $a_0 + a_1\rho + a_2\rho^2 + \ldots + a_{n-1}\rho^{n-1}$, où les a_i sont des nombres entiers inférieurs à p tels que leur somme est égale à $p-1$.
- Cauchy introduit également les produits

$$P_m = \frac{((2n-i-j)\varpi)!}{((n-i)\varpi)!((n-j)\varpi)!},$$

où m est un nombre quelconque entier compris entre 0 et $n-1$, $mh \equiv i \pmod n$ et $mk \equiv j \pmod n$. Ces produits lui permettent d'obtenir des équivalents modulo p des a_i, et donc un équivalent modulo p des sommes de Jacobi $R_{h,k}$ grâce à la congruence :

$$a_m \equiv \left(2 + P_{n-1}r^m + P_{n-2}r^{2m} + \ldots + P_{n-1}r^{(n-1)m}\right)\varpi \pmod p.$$

Pour déterminer les valeurs des expression $R_{h,k}$, remarquons que Cauchy substitue

6. Voir page 57.

7. Nous avons commenté cette introduction dans notre première partie. Cauchy observe notamment « Dans la science des nombres, l'une des propriétés les plus importantes et les plus fécondes en conséquences dignes de remarque, est le théorème connu sous le nom de *loi de réciprocité* entre deux nombres premiers »[Cauchy, 1829a, p. 88].

à la racine primitive ρ de l'équation $x^n = 1$, la racine primitive r de la congruence binôme $x^n \equiv 1 \pmod{p}$. Il utilise cette méthode à plusieurs reprises dans ses travaux suivants, et nous verrons que, là aussi, Jacobi met en avant l'importance de cette substitution. Il pose également $\Pi_{n-m} = P_m$ et traduit les formules précédentes en fonction de Π_m. Il donne ensuite des résultats sur les coefficients a_i.

Cauchy continue en appliquant les résultats obtenus précédemment à certaines formes quadratiques. Ainsi, il démontre que les nombres premiers p de la forme $3\varpi + 1$ peuvent être mis sous la forme $x^2 + 3y^2 = p$, et détaille des cas particuliers où il détermine les valeurs de x et y à l'aide des formules précédentes. Il considère ensuite l'exemple où n est égal à 4 : les nombres premiers p de la forme $4\varpi + 1$ peuvent être mis sous la forme $p = x^2 + y^2$. Là encore, sa méthode permet de déterminer les valeurs de x et de y. Ces résultats particuliers ont été démontrés précédemment par Euler et Gauss notamment [8]. Même si les exemples traités par Cauchy sont déjà connus, il développe ici une méthode générale, basée sur les sommes de Jacobi et de Gauss pour déterminer des représentations des nombres premiers de la forme $nk+1$ par des expressions de la forme x^2+ny^2. Il donne également les formules permettant de déterminer les nombres x et y.

La troisième partie du mémoire, *Nouvelles formules déduites des principes exposés dans le second paragraphe*, traite dans un premier temps de différentes propriétés des sommes de Gauss et de Jacobi ; Cauchy donne en particulier une méthode permettant de calculer $R_{h,k}$ en fonction des $R_{1,i}$, $i = 1 \ldots n-1$. La fin du mémoire contient les étapes d'une démonstration de la loi de réciprocité quadratique, basée également sur les sommes de Gauss. Cauchy la détaillera dans la note IV du *Mémoire sur la théorie des nombres* de 1840. Cette démonstration est assez proche de la sixième preuve de la loi de réciprocité donnée par Gauss en 1818, et semblable à celle de Jacobi, publié dans la troisième édition de la *Théorie des nombres* de Legendre en 1830.

Cauchy introduit pour cela la notation $\left[\frac{k}{p}\right]$ qui est

> une expression équivalente à
>
> $$0 \text{ ou } 1 \text{ ou } \rho \text{ ou } \rho^2 \text{ ou } \rho^3 \text{ ou } \ldots \text{ ou } \rho^{n-1}$$
>
> suivant que l'on aura
>
> $$k^{\varpi} \equiv 0 \text{ ou } 1 \text{ ou } \rho \text{ ou } \rho^2 \text{ ou } \rho^3 \text{ ou } \ldots \text{ ou } \rho^{n-1} \pmod{p}.$$

8. Comme nous l'avons étudié dans notre deuxième partie, Euler propose une première démonstration du théorème des deux carrés dans [Euler, 1758]. Gauss prouve également ce théorème une première fois dans la section sur les formes quadratiques des *Disquisitiones Arithmeticae* : voir [Gauss, 1801, art. 182]. On pourra également se reporter au chapitre 1 de [Cox, 1989] pour un exposé des méthodes utilisées par Euler, Lagrange, Legendre et Gauss pour traiter ce type de problèmes.

[Cauchy, 1829a, p. 104].

Comme $\varpi = \frac{p-1}{n}$, cette définition est une version généralisée dans le cadre des résidus d'ordre supérieur à 2 du symbole de Legendre. Cependant, seuls les nombres entiers naturels sont considérés ici[9]. Ainsi, même si Cauchy aborde les mêmes thèmes que Gauss et Jacobi, l'approche est différente puisqu'il n'utilise à aucun moment les nombres entiers complexes comme les deux savants allemands. Nous verrons par exemple que Jacobi définit le symbole de Legendre dans le cas cubique pour tous les nombres de la forme $a + b\sqrt{-3}$, où a et b sont des nombres entiers.

Il considère dans un premier temps le cas où $n = 2$ et donne ainsi les étapes de la démonstration de la loi de réciprocité quadratique :

$$\left[\frac{q}{p}\right] = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} p^{\frac{q-1}{2}}.$$

Pour finir, il reprend son raisonnement dans le cas où n est un nombre quelconque et aboutit à l'égalité :

$$p^{\frac{q-\varsigma}{n}}(b_0 + b_1\rho + \ldots + b_{n-1}\rho^{n-1}) = \left[\frac{q}{p}\right]^{n-\varsigma} + qQ,$$

où ς est le reste de la division de q par n, Q est un polynôme de la forme $c_0 + c_1\rho + c_2\rho^2 + \ldots + c_{n-1}\rho^{n-1}$, où les c_i sont des nombres entiers. Les b_i sont également des nombres entiers. Il annonce la suite de ces résultats dans ses recherches arithmétiques ultérieures. C'est néanmoins la dernière fois que Cauchy aborde les lois de réciprocité d'ordre supérieur dans ses travaux.

Cauchy conclut son mémoire en faisant référence à Jacobi :

> J'observerai en finissant qu'ayant donné à M. Jacobi communication de mes formules, j'ai appris de cet habile géomètre qu'il était parvenu de son côté, et en s'appuyant sur les mêmes principes à des résultats du même genre. Il a donné quelques-uns de ses résultats, mais sans indiquer la méthode qui les lui avait fournis, dans le tome II du *Journal* de M. Crelle [Cauchy, 1829a, p. 107].

Effectivement, comme nous allons le voir dans la prochaine section, Jacobi travaille à la même époque sur le même thème avec des outils similaires.

9. En effet, aujourd'hui, dans le cas de la théorie des résidus cubiques par exemple, on se place dans l'anneau $\mathbb{Z}[\omega] = \{a+b\omega : a, b \in \mathbb{Z}\}$, où $\omega = e^{2i\pi/3}$ est une racine cubique primitive de l'unité. On munit cette anneau euclidien de la norme $N(\alpha) = \alpha\overline{\alpha}$, où $\overline{\alpha}$ désigne le conjugué de α. On définit alors le caractère cubique d'un nombre α modulo π, que l'on peut noter $\left(\frac{\alpha}{\pi}\right)_3$, ainsi :

- $\left(\frac{\alpha}{\pi}\right)_3 = 0$ si π divise α ;
- $\left(\frac{\alpha}{\pi}\right)_3 \equiv \alpha^{\frac{N(\pi)-1}{3}} \pmod{\pi}$, où $\left(\frac{\alpha}{\pi}\right)_3$ est égal à 1, ω, ou ω^2.

Voir par exemple [Ireland et Rosen, 1990, p. 108-137]. La définition de Cauchy coïncide bien avec cette définition lorsque α et π sont des entiers.

2 - Un deuxième *Mémoire sur la théorie des nombres* (1831) et un premier résultat général sur les formes quadratiques de la forme $p^m = x^2 + ny^2$

Le deuxième mémoire *Sur la théorie des nombres* publié dans le quinzième tome du *Bulletin de Férussac* en 1831 est le dernier texte de théorie des nombres de Cauchy avant son exil [10]. Dans les trois pages qui le composent, Cauchy veut « donner une idée [des] propositions »[Cauchy, 1831, p. 137] qu'il a exposées dans les différents mémoires présentés à l'Académie depuis 1829. Ces feuilles contiennent un théorème général sur les formes quadratiques traitées dans son mémoire précédent :

> Théorème 1er. Soit p un nombre premier [11], n un diviseur premier de $p-1$, ϖ la valeur du rapport $\dfrac{p-1}{n}$
>
> $$\mathscr{A}_1 = \frac{1}{6},\ \mathscr{A}_2 = \frac{1}{30},\ \mathscr{A}_3 = \frac{1}{42},\ \textit{etc.}$$
>
> les nombres de Bernoulli [12], et m le plus petit nombre entier équivalent, suivant le module n, à $\pm 2A_{\frac{n+1}{4}}$. Enfin, soit s une racine primitive de l'équivalence
>
> $$x^{n-1} \equiv 1 \pmod{n};$$
>
> P_s, le produit des nombres entiers 1, 2, 3, . . s ; n' le nombre des racines [13] de l'équivalence $x^{\frac{n-1}{2}} \equiv 1 \pmod{n}$, qui sont inférieures à $\dfrac{n-1}{2}$, et $n'' = n - n' - 1$, le nombre des racines de l'équivalence $x^{\frac{n-1}{2}} \equiv -1 \pmod{n}$ qui remplissent la même condition.
> Si n est de la forme $4k+3$, l'équation
>
> $$x^2 + ny^2 = 4p^m,$$
>
> sera résoluble en nombres entiers, et on la vérifiera en prenant
>
> $$x \equiv P_{\varpi} P_{s^2\varpi} P_{s^4\varpi} \dots P_{s^{n-3}\varpi}, \quad \pmod{p}$$

10. Voir [Belhoste, 1985].
11. Nous corrigeons ici ce qui semble être une faute de frappe dans le mémoire : n est défini comme un diviseur de p, ce qui est incohérent avec la définition de ϖ.
12. Les $\mathscr{A}_i$ ainsi définis correspondent aux B_{2i} actuels, si B_i désigne le i^e nombre de Bernoulli. Cela vient du fait que $B_k = 0$, pour k impair et différent de 1. Par ailleurs, Cauchy considère ici les valeurs absolues des nombres de Bernoulli actuels. Les nombres de Bernoulli interviennent dans de nombreuses formules mathématiques ; citons par exemple celle d'Euler-Mac-Laurin. Pour des résultats sur ses nombres, voir [Nielsen, 1923]. Cauchy revient sur l'utilisation de ces nombres dans la démonstration du théorème énoncé ici dans son *Mémoire sur la théorie des nombres* de 1840.
13. Ces nombres sont donc les résidus quadratiques de n.

ou bien

$$x \equiv P_{s\varpi} P_{s^3\varpi} P_{s^5\varpi} \dots P_{s^{n-2}\varpi}, \quad (\text{mod } p)$$

suivant que l'on aura $n' < n''$ ou $n' > n''$. De plus, on trouvera dans le premier cas

$$m = \frac{n-1-4n'}{2} \text{ ou } m = \frac{n-1-4n'}{6},$$

et dans le second cas

$$m = \frac{4n'-n+1}{2} \text{ ou } m = \frac{4n'-n+1}{6}$$

suivant que n est de la forme $8k+7$ ou $8k+3$ [Cauchy, 1831, p. 137-138].

Aucune justification n'est donnée. Cauchy illustre son théorème par un exemple, en considérant les nombres premiers p de la forme $7n+1$. L'équation $4p^m = x^2 + 7y^2$ est donc résoluble en nombres entiers pour $m \equiv \mathscr{A}_2 \pmod 7$. Or, comme $\mathscr{A}_2 = \frac{1}{30}$, alors $m \equiv \frac{1}{15} \equiv 1 \pmod 7$ puisque $15 \equiv 1 \pmod 7$. Finalement, on peut toujours résoudre en nombres entiers l'équation $x^2 + 7y^2 = 4p$, lorsque p est un nombre de la forme $7k+1$. Ces résultats sont développés et démontrés dans le *Mémoire* de 1840 (lu en 1830 à l'Académie).

Remarquons qu'ici, Cauchy ne justifie pas l'existence de l'inverse du nombre 15 modulo 7 ; il ne commente pas non plus le fait que si le dénominateur du nombre de Bernoulli est un multiple du module considéré, alors cette méthode n'est plus valide. Cette manière de présenter au lecteur un exemple bien choisi sans en commenter sa sélection rappelle une pratique de Poinsot observée dans notre partie précédente.

L'intérêt de ce théorème est sa généralité : en effet, les résultats vus précédemment concernaient toujours des cas particuliers où n était fixé : ainsi, les exemples donnés en 1829 par Cauchy concernent les nombres de la forme $3k+1$ ou $4k+1$. Ici, les conditions sur n sont moins restrictives. De plus, Cauchy donne une expression équivalente au nombre x et la valeur de m. Ainsi, même s'il ne démontre pas ces résultats - ce texte semble avoir pour simple rôle d'annoncer le résultat obtenu par le mathématicien, peut-être en vue d'éviter de futures querelles de priorité - Cauchy semble posséder déjà les principaux outils que l'on retrouve dans ses textes de 1839-1840. Remarquons d'ailleurs que dans cette note, Cauchy ne fait plus aucune allusion aux lois de réciprocité.

D'autre part, il introduit ici les nombres de Bernoulli dans son théorème sur les formes quadratiques ; ces nombres sont reliés à l'aide d'une congruence aux nombres de résidus et non-résidus quadratiques. Comme nous l'expliquerons à la fin de cette partie, cette première utilisation des nombres de Bernoulli dans ce cadre peut être associée aux résultats développés par Kummer sur le dernier théorème de Fermat en 1847, via les recherches de Jacobi et Dirichlet notamment.

IV 1827-1839 : Jacobi et la théorie des nombres

1 - Les travaux de Jacobi sur les résidus cubiques publiés en 1827

Des résultats en lien avec la forme quadratique $p = x^2 + 27y^2$ sont conjecturés par Euler dans son traité posthume sur la théorie des nombres[14] publié en 1849. Gauss aborde également ce cas dès les *Disquisitiones Arithmeticae* dans la section VII, article 358, lorsqu'il considère les nombres premiers de la forme $3k+1$. Néanmoins, c'est Jacobi qui donne explicitement des résultats sur les résidus cubiques dans son court mémoire de quatre pages, intitulé *De residuis cubicis commentatio numerosa*, et publié en 1827 dans le *Journal de Crelle*. Son texte traite de la forme quadratique $4p = x^2 + 3y^2$, où p est de la forme $3k+1$: si $p = 3n+1$ est un nombre premier, alors $4p = a^2 + 27b^2$ où a est le résidu compris entre $\frac{1}{2}p$ et $-\frac{1}{2}p$ modulo p de $\dfrac{-(n+1)(n+2)\dots(2n)}{1.2.\dots n}$. Ce résidu est également équivalent à 1 modulo 3. Cependant, comme Cauchy le remarque, Jacobi ne donne pas de démonstration de ce résultat.

Même si cette note de Jacobi ne permet pas de connaître les méthodes qu'il a utilisées, on sait grâce à sa correspondance avec Gauss que les méthodes de Jacobi et Cauchy sont similaires. En effet, dans une lettre adressée à Gauss datée du 8 février 1827, Jacobi s'appuie lui aussi sur la cyclotomie. Il définit les sommes de Gauss et de Jacobi, en les faisant cependant dépendre de la variable ρ (si on reprend les notations utilisées par Cauchy), et non de l'indice h. Reprenons les notations de Jacobi : p est un nombre premier, x une racine primitive de l'équation[15] $x^p = 1$, g une racine primitive de $x^{p-1} \equiv 1 \pmod{p}$, l un diviseur de $p-1$ et r une racine primitive de $x^l = 1$. Jacobi pose

$$\xi(r) = x + rx^g + r^2x^{g^2} + \dots + r^{p-2}x^{g^{p-2}},$$

ce qui correspond bien aux expressions Θ_h définies par Cauchy. Jacobi considère ensuite les différentes sommes de la forme $\xi(r^k)$, où k est un nombre entier. Il affirme que $\dfrac{\xi(r)\xi(r^m)}{\xi(r^{m+1})}$ est une fonction entière de la racine r et est donc de la forme

$$A + A'r + A''r^2 + \dots + A^{l-1}r^{l-1},$$

où les nombres A, A', $\dots$, sont des nombres entiers.

Il énonce ensuite une égalité qu'il qualifie de *fondamentale* pour la théorie de la cyclo-

14. Voir [Euler, 1849] et [Cox, 1989, p. 20].

15. qu'il note $\dfrac{x^p - 1}{x - 1} = 0$: toutes les équations et congruences binômes que Jacobi considère sont notées sous cette forme.

tomie [16] :

$$\xi(r)\xi(\frac{1}{r}) = (-1)^{\frac{p-1}{l}}p.$$

Elle est équivalente à l'égalité $\Theta_h\Theta_{-h} = (-1)^{\varpi h}p$ de Cauchy.

Il introduit ensuite les sommes portant son nom :

$$\frac{\xi(r)\xi(r^m)}{\xi(r^{m+1})} = \psi(r),$$

ce qui donne $\psi(r)\psi(\frac{1}{r}) = p$. Il considère alors plusieurs cas particuliers, puis introduit deux nouvelles notations : $a_i \equiv i(m+1) \pmod{l}$ et $\left(\frac{\alpha}{\beta}\right) = \frac{\alpha(\alpha-1)\dots(\alpha-\beta+1)}{1.2\dots\beta}$, ce qui correspond au β^{e} coefficient binomial, comme le fait remarquer Cauchy. Lorsque $p = ln+1$, et lorsque l'on considère l'égalité $\frac{\xi(r)\xi(r^m)}{\xi(r^{m+1})} = \psi(r)$ où r est une racine primitive de l'équivalence $x^l \equiv 1 \pmod{p}$ (et non plus une racine primitive de l'équation $x^l = 1$), alors $\psi(r^i) \equiv -\left(\frac{a_i n}{in}\right) \pmod{p}$, où $1 \leq i \leq l-1$. Il en déduit ensuite des cas particuliers.

Dans la suite de sa note publiée en 1827 dans le *Journal de Crelle*, Jacobi utilise les nombres complexes de la forme $a+b\sqrt{-3}$ pour établir des résultats sur les résidus cubiques. Par exemple, soit p un nombre premier de la forme $6n+1$ tel que $4p = L^2+27M^2$ et q un nombre premier de la forme $6n-1$. Alors Jacobi établit un lien entre le caractère cubique de q par rapport à p et celui du quotient $\frac{L+M\sqrt{-3}}{L-M\sqrt{-3}}$ par rapport à q. Il obtient donc des résultats sur les formes quadratiques et des résultats sur les résidus cubiques en lien avec la loi de réciprocité associée.

Cauchy n'a vraisemblablement pas eu accès à la correspondance entre Gauss et Jacobi avant d'écrire son mémoire publié en 1829 sur le même sujet. C'est pourquoi les similitudes entre les travaux des deux hommes sont remarquables : ils travaillent, obtiennent et mettent en avant les mêmes résultats sur les sommes de Gauss et de Jacobi afin d'exprimer le nombre premier p considéré. Aussi, ils utilisent tous deux la méthode consistant à remplacer une racine d'équation par la racine de la congruence correspondante afin d'obtenir des équivalents d'expressions en lien avec les sommes considérées. Comme nous allons le voir plus loin, ces résultats et méthodes seront les bases des travaux ultérieurs sur les nombres premiers de la forme x^2+ny^2 et sur la genèse de la théorie des nombres idéaux de Kummer notamment. Il existe néanmoins une différence importante entre les travaux des deux hommes : Jacobi considère explicitement des nombres complexes de la forme $a+b\sqrt{-3}$, où a et b entiers dans ses théorèmes sur les résidus cubiques, tandis que

16. « Dieser Fundamentalsatz für die Theorie der Kreistheilung machte mir eine dunkele Andeutung zu den Disq. Ar. pag. 651 klar »[Jacobi, 1881-1891, p. 394]. Cela correspond à l'article 360 de l'ouvrage de Gauss.

Cauchy ne donne pas de commentaire sur la forme et la nature des nombres considérés dans ses travaux.

2 - Un mémoire de Jacobi sur la théorie de la cyclotomie

Comme nous venons de le voir, certains thèmes de recherches en théorie des nombres et les méthodes associées sont similaires chez Cauchy et Jacobi. Le dernier, contrairement au premier, publie plusieurs textes dans les années 1830. Les trois premiers, publiés dans le *Journal de Crelle* en 1828, 1832 et 1834, traitent de sommes quadratiques mais ne s'appuient pas sur la cyclotomie, les sommes de Gauss et de Jacobi [17]. Le dernier texte, publié en 1840, traite de résultats de théorie des nombres déduits de recherches sur les séries.

Nous allons donc nous intéresser aux deux textes publiés pour la première fois en allemand en 1837 et 1839 et traduits en français pour publication dans les *Nouvelles Annales de Mathématiques* et dans le *Journal de Liouville* respectivement [18]. Leur point commun est d'approfondir les recherches que Jacobi aborde dix ans plus tôt dans sa correspondance avec Gauss et dans son article de 1827. Remarquons qu'en 1839, Jacobi publie également le *Canon Arithmeticus*, qui contient une table de racines primitives et d'indices à laquelle Cauchy se référera dans ses textes.

Dans [Jacobi, 1837] [19], l'auteur énonce les différentes formules fondamentales sur les sommes de Gauss et de Jacobi et met en avant l'importance de ce que Franz Lemmermeyer appelle les *Jacobi's maps* dans [Lemmermeyer, 2009]. Ainsi, il pose : $F(\alpha) = x + \alpha x^g + \alpha^2 x^{g^2} + \ldots + \alpha^{p-2} x^{g^{p-2}}$, où p est un nombre premier, x une racine primitive de $x^p = 1$ et g une racine primitive de p. De plus, on a $F(\alpha^m)F(\alpha^n) = \psi(\alpha)F(\alpha^{m+n})$, $\psi(\alpha)$ est une fonction entière de α. Enfin, si α^m, α^n et α^{m+n} sont différents de l'unité, alors $\psi(\alpha)\psi(\alpha^{-1}) = p$. La correspondance entre les égalités exprimées en fonction d'une racine primitive de $x^{p-1} = 1$ et les congruences exprimées en fonction d'une racine primitive de p (soit de l'équivalence $x^{p-1} \equiv 1 \pmod{p}$) est présentée dès la deuxième page :

> Désignons par r une racine primitive de l'équation
>
> $$r^{p-1} = 1 = 0,$$

17. Jacobi se réfère en particulier aux fonctions elliptiques et à la théorie des formes quadratiques développée par Legendre, et par Gauss dans la section V des *Disquisitiones Arithmeticae*.

18. Le mémoire [Jacobi, 1837] est reproduit dans le trentième volume du *Journal de Crelle* en 1846, puis traduit en 1856 dans le quinzième tome des *Nouvelles Annales de Mathématiques*. Une traduction du texte [Jacobi, 1839b] est publiée en 1843 dans le huitième tome du *Journal de Liouville*.

19. À plusieurs reprises, Jacobi indique dans ce mémoire que les résultats exposés font partie de son cours de théorie des nombres, exposé en 1836-1837. Dans une note ajoutée en octobre 1845 [Jacobi, 1837, p. 348], Jacobi remarque d'ailleurs que Kummer et Dirichlet connaissaient déjà les démonstrations exposées ici.

et dans l'expression

$$\psi(r) = \frac{F(r^{-m}).F(r^{-n})}{F(r^{-m-n})}$$

remplaçons la quantité r par le nombre g ; il viendra, si m et n sont des nombres positifs plus petits que $p-1$,

$$\psi(g) \equiv -\frac{\Pi(m+n)}{\Pi(m)\Pi(n)} \pmod{p},$$

équation dans laquelle

$$\Pi(n) = 1.2.3 \ldots n.$$

Mais si $m+n$ est plus grand que $p-1$, on aura

$$\psi(g) \equiv 0 \pmod{p};$$

cette dernière proposition constitue dans les applications un des théorèmes les plus féconds de la théorie des nombres.[Jacobi, 1837, p. 338]

C'est la correspondance équation - congruence utilisée dans ce résultat que Lemmermeyer appelle les *Jacobi's maps*[20].

Jacobi donne également d'autres formules importantes de la théorie de la cyclotomie et remarque une analogie entre les relations qui existent entre les fonctions F et ψ d'une part et celles liant les intégrales eulériennes de première et deuxième espèces d'autre part[21]. Après avoir établi des relations supplémentaires entre les fonction F et ψ, Jacobi conclut que ses résultats permettent d'obtenir des « théorèmes particuliers [...] concernant le nombre de formes quadratiques réduites des diviseurs de la forme $y^2 + pz^2$, p étant un nombre premier de la forme $4n+3$ » et de former « un lien entre les deux parties principales de la haute arithmétique, la division du cercle et la théorie des formes quadratiques » [Jacobi, 1837, p. 346].

Jacobi indique ensuite des propriétés qu'il a déduit de ses recherches sur la cyclotomie concernant la théorie des résidus cubiques. Ainsi, il définit un équivalent du symbole de Legendre, pour les nombres complexes de la forme $\frac{L+M\sqrt{-3}}{2}$, et donne la loi de réciprocité cubique associée :

Soient

$$\frac{L+M\sqrt{-3}}{2} \text{ et } \frac{L'+M'\sqrt{-3}}{2}$$

deux nombres complexes premiers (M et M' sont divisibles par 3 et peuvent être

20. Voir en particulier [Lemmermeyer, 2009, p. 171 - 172].

21. En effet, ces intégrales, données par Euler dans [Euler, 1755], sont définies ainsi : $\Gamma(x) = \int_0^\infty e^{-t}t^{x-1}dt$ et $\beta(x,y) = \int_0^1 t^{x-1}(1-t)^{y-1}dt$ et sont liées par l'égalité : $\Gamma(x)\Gamma(y) = \beta(x,y)\Gamma(x+y)$.

zéro) ; désignons par

$$\left[\frac{x+y\sqrt{-3}}{\frac{1}{2}(L+M\sqrt{-3})}\right]$$

celle des quantités

$$1,\ \frac{-1+\sqrt{-3}}{2},\ \frac{-1-\sqrt{-3}}{2},$$

qui est congrue à la puissance

$$(x+y\sqrt{-3})^{\frac{\frac{1}{4}(L^3+3M^2)-1}{3}}$$

suivant le module $L+M\sqrt{-3}$, on aura

$$\left(\frac{\frac{1}{2}(L'+M'\sqrt{-3})}{\frac{1}{2}(L+M\sqrt{-3})}\right)=\left(\frac{\frac{1}{2}(L+M\sqrt{-3})}{\frac{1}{2}(L'+M'\sqrt{-3})}\right)$$

[Jacobi, 1837, p. 347].

Un point fondamental ici est que Jacobi définit le symbole de Legendre pour tous les nombres de la forme $x+y\sqrt{-3}$, et obtient ainsi une loi de réciprocité cubique analogue au cas quadratique. Jacobi rappelle qu'il a développé les démonstrations des lois de réciprocité cubique et biquadratique dans ses leçons données pendant l'hiver 1836-1837, puis indique qu'il a étendu les méthodes données par Gauss pour l'utilisation de la loi de réciprocité quadratique aux lois de réciprocité cubique et biquadratique en introduisant notamment ce que l'on appelle aujourd'hui le symbole de Jacobi : $\left(\frac{x}{p}\right)=\left(\frac{x}{f}\right)\left(\frac{x}{f'}\right)\left(\frac{x}{f''}\right)\ldots$ si p est un nombre composé dont les facteurs premiers (égaux ou distincts) sont f, f', f'', ... Il conclut en annonçant des recherches sur les résidus du huitième et du cinquième degré qu'il communiquera ultérieurement.

Dans ce texte, Jacobi développe une théorie des sommes de Gauss et de Jacobi pour en déduire des résultats sur les formes quadratiques. Remarquons d'ailleurs que, comme Gauss dans sa section VII, Jacobi met en avant l'intérêt du lien ainsi souligné entre la cyclotomie et la théorie des formes quadratiques. Là encore, l'exposé de Jacobi s'accorde avec les mémoires de Cauchy de 1829 et 1831 dans le sens où il travaille avec la cyclotomie pour obtenir des résultats généraux sur certaines formes quadratiques. Néanmoins, Jacobi établit également un lien entre la cyclotomie et les résidus cubiques, et redéfinit le symbole de Legendre dans ce cas en considérant des nombres complexes de la forme $a+b\sqrt{-3}$.

3 - Les résidus de cinquième, huitième et douzième puissances

Ce texte est publié pour la première fois en 1839, dans un mémoire dont la traduction du titre est *Sur les nombres premiers complexes que l'on dit considérer dans la théorie des*

résidus de cinquième, huitième et douzième puissances[22]. Il commence par indiquer que, selon lui, la théorie des résidus biquadratiques de Gauss a été inspirée par des résultats obtenus dans le cadre des fonctions elliptiques, en particulier avec les recherches sur la division de la lemniscate. La théorie des résidus biquadratiques s'appuie donc, comme les recherches de calcul intégral liées à la lemniscate, sur les nombres de la forme $a + b\sqrt{-1}$. De même pour la loi de réciprocité cubique :

> Il n'était pas besoin d'idées nouvelles pour trouver les lois de la réciprocité cubique ; il suffisait pour cela d'introduire d'une manière tout à fait analogue, comme modules ou comme diviseurs, les nombres complexes de la forme $\frac{a + b\sqrt{-3}}{2}$ ou d'autres semblables qui sont composés des racines cubiques de l'unité. On peut aussi rattacher ces recherches à la théorie de quelques intégrales ellpitiques particulières.[Jacobi, 1839b, p. 269]

Jacobi indique alors une question cruciale : « il reste encore à démêler parmi les méthodes et les solutions de l'arithmétique celles qui peuvent s'appliquer aussi à ces nombres complexes [ceux de la forme $a + b\sqrt{-1}$] »[Jacobi, 1839b, p. 269]. Il met ainsi en avant la nécessité de déterminer les propriétés de ces entiers complexes. Il observe par exemple que la méthode de Lagrange de réduction des formes quadratiques pour les entiers naturels est également valable pour les nombres complexes, et que la démonstration est analogue pour les deux ensembles de nombres. Comme nous l'avons souligné dans notre première partie, les recherches de Gauss et Dirichlet contiennent également des résultats liés à cette problématique : le premier développe dans [Gauss, 1828] et [Gauss, 1832] une étude approfondie des nombres de la forme $a + b\sqrt{-1}$ et le second démontre par exemple la loi de réciprocité quadratique pour les entiers complexes.

En se basant sur cette théorie des formes quadratiques, et en indiquant que des résultats similaires peuvent être obtenus par des méthodes « ordinaires de l'arithmétique » [Jacobi, 1839b, p. 270], Jacobi montre comment on peut décomposer les nombres premiers de la forme $8n + 1$ (respectivement $12n + 1$) en un produit de quatre nombres complexes composés des racines huitièmes (respectivement douzièmes) de l'unité. Par exemple, dans le cas des racines huitième de l'unité, Jacobi utilise l'équivalent d'un résultat d'Euler sur les sommes de deux carrés pour les entiers complexes $a + b\sqrt{-1}$: tout diviseur $a + b\sqrt{-1}$ d'une expression de la forme $y^2 - \sqrt{-1}z^2$ est de la même forme. Ainsi, le diviseur $a + b\sqrt{-1}$ est également de la forme $m^2 - \sqrt{-1}n^2$, soit $(m - \sqrt[4]{-1}n)(m + \sqrt[4]{-1}n)$, où m et n sont également des entiers complexes de la forme $a' + b'\sqrt{-1}$. Le nombre $a + b\sqrt{-1}$ est donc décomposé en un produit de deux nombres dépendants d'une racine huitième de l'unité. Ainsi, tout nombre premier p de la forme $8n + 1$ et $a^2 + b^2$ peut être décomposé en un produit de quatre facteurs composés de racines huitièmes de l'unité.

22. Ce mémoire est traduit en français et inséré dans le *Journal de Liouville* en 1843 : voir p. 90.

Il explique ensuite comment il a été conduit à rechercher des décompositions de ces ensembles de nombres premiers en facteurs complexes premiers : dans ses recherches sur la cyclotomie, il a montré que tout nombre premier p de la forme $\lambda k+1$ peut être décomposé de plusieurs manières comme un produit de deux nombres complexes formés des racines λ^{e} de l'unité. Ces décompositions correspondent aux formules démontrées par Jacobi et Cauchy sur les sommes de Gauss et de Jacobi[23] . À partir de manipulations sur ces expressions complexes, Jacobi est arrivé à la conclusion suivante :

> Je me suis convaincu, en considérant directement cette circonstance remarquable, que ces facteurs complexes du nombre premier p doivent être, en général, combinés de nouveau, de telle sorte que si on les décompose en vrais nombres premiers complexes, alors ceux qui forment les facteurs du dénominateur se laissent détruire isolément par les facteurs du numérateur [Jacobi, 1839b, p. 271].

Il justifie ensuite pourquoi les facteurs obtenus dans ce cadre sont nécessairement des nombres premiers et conclut sur la recherche de lois de réciprocité d'ordre supérieur. Comme nous l'avons déjà observé dans notre première partie, et même si les raisonnements de Jacobi ne sont qu'esquissés, ce texte est le point de départ de recherches sur les résidus d'ordre supérieur pour des mathématiciens comme Kummer par exemple.

4 - Le cours non publié de 1836-1837 : *Vorlesungen über Zahlentheorie*

Franz Lemmermeyer et Herbert Pieper ont édité en 2007 un cours de théorie des nombres de Jacobi, donné pendant le semestre d'hiver 1836-1837 à l'Université de Königsberg. Les leçons données par Jacobi sont annotées et précédées d'une table des matières détaillée construite par les éditeurs. Dans [Lemmermeyer, 2009], l'auteur insiste sur l'importance de ces leçons dans le développement de la théorie des nombres et de celles des nombres idéaux complexes de Kummer. Nous présentons ici les grandes lignes de ce cours pour mettre en avant les thèmes arithmétiques qui y sont développés.

Ce cours contient 52 leçons, partagées dans l'édition de 2007 en trois parties : *Elementare Zahlentheorie*, *Theorie der Kreistheilung oder Auflösung der reinen Gleichungen* et *Anwendung der Kreistheilung auf die Zahlentheorie*. Dans la première leçon, Jacobi commence par donner une caractérisation de l'arithmétique supérieure : « Die höheren Arithmetik beschäftigt sich nicht mit den Zahlen als Größen, sondern als Qualitäten »[Jacobi, 2007, p. 3]. Il résume brièvement une histoire de ce domaine, et indique que la théorie des nombres est actuellement divisée en deux parties principales : la théorie des équations (« Theorie der Auflösung der reinen Gleichungen »[Jacobi, 2007, p. 8]) et

23. Ainsi, d'après les notations de Jacobi, on a par exemple $\psi(\alpha)\psi(\alpha^{-1}) = p$, où α est une racine de l'équation $x^{p-1} = 1$.

la théorie des formes quadratiques. Ce cours est principalement consacré à la première, dont il attribue la découverte à Gauss.

Après avoir rappelé les résultats fondamentaux de la théorie des nombres, comme le petit théorème de Fermat ou encore le théorème de Wilson, il énonce les premières propriétés sur les congruences binômes et les racines primitives, puis rappelle également des résultats sur la loi de réciprocité quadratique. C'est à partir de la dixième leçon que Jacobi introduit ce que l'on nomme aujourd'hui les sommes de Gauss. Il pose :

$$(\alpha, x, g) = x + \alpha x^g + \alpha^2 x^{g^2} + \alpha^3 x^{g^3} + \ldots + \alpha^{p-2} x^{g^{p-2}},$$

où p est un nombre premier, x est une racine p^{e} de l'unité, α une racine n^{e} de l'unité, où n est un diviseur de $p-1$ et g une racine primitive de p (soit une racine primitive de la congruence $x^{p-1} \equiv 1 \pmod{p}$). Cette notation peut être réduite à (α, x) lorsque la racine primitive g est fixée, voire même à (α). Dans les leçons suivantes, Jacobi démontre plusieurs propriétés de ces expressions, déjà données dans sa lettre à Gauss ou encore dans [Jacobi, 1837]. Dans la onzième leçon, il prouve notamment un premier *Fundamentaltheorem*[Jacobi, 2007, p. 84] : $(\alpha, x, g)(\alpha^{-1}, x, g) = \pm p$. Il prouve également que le produit de deux sommes de Gauss (r^m, x) et (r^n, x), où r est une racine primitive de $x^{p-1} = 1$, est égal à la somme de Gauss (r^{m+n}, x) multipliée par une expression dépendant de la racine r. Il utilise cette propriété pour introduire dans la treizième leçon les sommes maintenant qualifiées de sommes de Jacobi en posant : $(r^m, x)(r^n, x) = \psi r(r^{m+n}, x)$, où ψr est une fonction entière rationnelle de r. Avec la deuxième égalité $(r^{-m}, x)(r^{-n}, x) = \psi r^{-1}(r^{-m-n}, x)$, il déduit un deuxième théorème qu'il qualifie de fondamental : $\psi r \psi(r^{-1}) = p$.

Jusqu'à la leçon 33, la majorité des résultats sont des propriétés des sommes de Gauss et de Jacobi, des calculs de sommes dans des cas particuliers (il obtient par exemple les sommes de Gauss d'ordre 5 et 8 dans le cas où $p = 41$ dans la 23^{e} leçon). Il obtient également quelques résultats particuliers sur les formes quadratiques traitées par Cauchy. Par exemple, dans le cas où le nombre p est de la forme $7n + 1$, Jacobi montre que $4p = m^2 + 7n^2$ en manipulant les racines septièmes de l'unité et en montrant que $\psi\alpha$ est de la forme $\frac{m+n\sqrt{-7}}{2}$. Il montre également que les nombres de la forme $20n + 1$ peuvent se mettre sous la forme $f^2 + 5g^2$. Comme nous le verrons lors de notre analyse du grand mémoire de Cauchy, c'est un exemple qui est également donné par ce dernier.

À partir de la leçon 34, Jacobi applique les résultats de la théorie de la cyclotomie obtenus précédemment à deux thèmes principaux : les lois de réciprocité cubiques et quartiques d'une part et les formes quadratiques traitées également par Cauchy d'autre part. Les éditeurs remarquent également que Jacobi donne des résultats en lien avec la formule de Dirichlet sur le nombre de classes des formes quadratiques de déterminant négatif : Jacobi ne fait cependant aucune référence à la théorie des formes quadratiques de Gauss, et aux travaux de Dirichlet à ce sujet. Par exemple, dans la table des matières,

les éditeurs indiquent pour la leçon 48 :

> Seien $\lambda \equiv 3 \pmod 4$ und $p = \lambda n + 1$ prim, sowie $-\lambda$ quadratischer Rest modulo p. Dann ist p im quadratischen Zahlkörper $\mathbb{Q}(\sqrt{-\lambda}$ zerlegt, und es gilt $4p^h = x^2 + \lambda y^2$, für $x, y \in \mathbb{N}$, wo h die ungerade Klassenzahl von k bedeutet[Jacobi, 2007, p. xxiv].

Jacobi montre effectivement que, pour un nombre premier p de la forme $\lambda n + 1$, où λ divise $p-1$ et est de la forme $4n+3$, on a l'égalité : $p^{2t-\frac{\lambda-1}{2}} = \frac{k^2+\lambda k'^2}{4}$, où $2t-\frac{\lambda-1}{2} = t-\left(\frac{\lambda-1}{2} - t\right)$ est la différence entre le nombre de résidus quadratiques et le nombre de non-résidus quadratiques compris en 1 et $\frac{\lambda-1}{2}$. Cependant, Jacobi ne fait pas le lien entre cette différence et le nombre de classes de formes quadratiques de déterminant $-\lambda$. Comme nous le verrons dans la section suivante, Jacobi s'appuie sur des principes similaires à ceux utilisés par Cauchy dans la démonstration de ce résultat : il considère le produit des sommes de Gauss [24] de la forme (α^a), où a parcourt les résidus quadratiques de λ et ceux des sommes de la forme (α^{-a}). Observons de plus que ce résultat est très proche de celui énoncé par Cauchy dans son article publié en 1831 dans le *Bulletin de Férussac*.

Finalement, dans les textes commentés ici, nous voyons que Jacobi développe de nombreux résultats sur les sommes de Gauss et de Jacobi pour en déduire des propriétés des lois de réciprocité et des formes quadratiques. Ces thèmes sont également abordés par Cauchy dans ses articles de 1829 et 1831. Néanmoins, par rapport à ce dernier, Jacobi témoigne d'une réflexion sur les propriétés que l'on peut attribuer aux nombres entiers complexes qui interviennent dans ces résultats sur la cyclotomie, à savoir les expressions faisant intervenir des racines de l'unité. Ces questions n'apparaissent par contre pas du tout dans les écrits de Cauchy publiés avant 1839. Nous allons maintenant faire ressortir les principes généraux exposés par Cauchy dans ses travaux arithmétiques parus entre 1839 et 1840 afin de mettre en évidence les points communs et les divergences entre les recherches des deux mathématiciens.

V 1839-1840 : retour de Cauchy sur la théorie des nombres avec les *Comptes Rendus* des séances de l'Académie des Sciences

Cauchy publie plusieurs travaux entre 1839 et 1840 dans lesquels il revient sur ses recherches sur les formes quadratiques abordées en 1829 et 1831. D'une part, il publie

24. Jacobi indique :

> Bildet man daher das Product aus den $\frac{\lambda-1}{2}$ Funktionen(α^a), wo für a alle quadratischen Reste zu setzen sind, so hat dieses die Eigenschaft, daß, wenn α^m statt α gesetzt wird, es ungeändert bleibt, wenn m quadratischer Rest von λ ist, und in das Produkt aus den $\frac{\lambda-1}{2}$ Funktionen (α^{-a}) übergeht, wenn m quadrtischer Nichtrest ist.[Jacobi, 2007, p. 254]

neuf notes où il considère des résidus et des congruences aux *Comptes Rendus de l'Académie des Sciences* dans lesquelles il présente notamment des méthodes autour des formes quadratiques $p^\mu = x^2 + ny^2$, où n est un diviseur de $p - 1$. D'autre part, il complète le mémoire de théorie des nombres présenté le 31 mai 1830 à l'Académie des Sciences de Paris par quatorze notes ; ce travail d'environ 450 pages est inséré en 1840 dans le dix-septième tome des *Mémoires* de l'Académie des Sciences, sous la forme d'un *Mémoire sur la théorie des nombres*. Les notes contiennent des commentaires explicites sur la méthode générale employée mais les résultats exposés ne sont généralement pas démontrés. Le mémoire renferme par contre des raisonnements bien plus complets, mais ceux-ci sont le plus souvent disséminés entre la partie principale du mémoire et les ajouts postérieurs. De plus, Cauchy n'y donne pratiquement aucune indication sur les principes généraux de sa méthode. Ces deux sources sont donc complémentaires : nous étudions donc les différentes notes présentées à l'Académie dans cette section et consacrons le chapitre suivant au grand mémoire.

Le titre et les références de chaque note sont indiqués en annexe. Parmi ces notes, deux ont été reproduites en 1840 dans le *Journal de Liouville*. Remarquons également qu'entre le 13 janvier et le 11 mai 1840, on retrouve douze notes de Cauchy dans les *Comptes Rendus* de l'Académie ; seules trois d'entre elles ne sont pas directement en lien avec le sujet. Nous ne détaillons pas les raisonnements employés lorsque Cauchy les développe sous la même forme dans son grand mémoire de 1840.

1 - 14 octobre 1839 : présentation des recherches

C'est le 14 octobre 1839 que Cauchy intervient à nouveau à l'Académie pour présenter ses recherches sur les formes quadratiques de la forme $p^\mu = x^2 + ny^2$. Lors de cette séance, il rappelle que Libri a récemment découvert des manuscrits de Fermat à ce sujet et se réfère à Gauss et Jacobi pour leurs recherches liées à la représentation d'un nombre premier par une expression de la forme $x^2 + ny^2$. Cauchy revient enfin sur ses propres travaux des années 1829-1830 dans lesquels il a développé des méthodes plus générales permettant la « recherche directe des formes quadratiques des nombres premiers », c'est-à-dire les formes quadratiques de la forme $p^m = x^2 + ny^2$ ou $4p^m = x^2 + ny^2$, où p est un nombre premier de la forme $nk + 1$ et où m peut être calculé à partir des nombres de Bernoulli. Cauchy demande finalement l'autorisation de rendre compte de ses recherches lors des prochaines séances de l'Académie. Dans chacune de ses interventions suivantes, Cauchy expose un point particulier de sa méthode, ou en donne des applications.

2 - 28 octobre 1839 : définition des facteurs primitifs et principe général de la méthode

Le 28 octobre 1839, Cauchy commence par rappeler ce que sont les *fonctions principales* de Lagrange, qui sont des fonctions linéaires des différentes puissances d'une racine de n^{e} de l'unité utilisées par ce dernier dans la théorie algébrique des équations, les équivalences et les racines primitives d'équations. Il considère ensuite une *fonction principale* particulière définie par $\Theta_h = \theta + \tau^h \Theta^h + \tau^{2h}\theta^{t^2} + \ldots + \tau^{(p-2)h}\theta^{t^{p-2}}$, où τ est une racine primitive de $x^{p-1} = 1$, et où θ et t sont définis comme précédemment. Cette expression, déjà utilisée par Cauchy en 1829, correspond aux sommes de Gauss. Comme en 1829, il en rappelle une des propriétés fondamentales : $\Theta_h \Theta_{-h} = (-1)^h p$ lorsque h n'est pas divisible par $p-1$. Ici, Cauchy insiste de plus sur la signification de cette égalité :

> [...] le produit des deux valeurs obtenues
>
> $$\Theta_h, \quad \Theta_{-h}$$
>
> sera égal au nombre p pris avec le signe + ou avec le signe −, suivant que l'indice h sera pair ou impair, pourvu toutefois que h ne soit pas divisible par p.[...]
>
> Pour cette raison, nous désignerons les deux expressions imaginaires
>
> $$\Theta_h, \quad \Theta_{-h}$$
>
> sous le nom de *facteurs primitifs* de $\pm p$, et nous dirons que ces deux facteurs sont *conjugués* l'un de l'autre[Cauchy, 1839, p. 510].

La formule "facteur primitif" apparaît ici pour la première fois dans les travaux de Cauchy, et peut rappeler l'expression "facteur premier". Cauchy ne fait néanmoins aucune remarque sur l'existence d'une analogie de la sorte, et ne détaille pas les propriétés de ces facteurs primitifs. Il est cependant remarquable que Cauchy utilise à plusieurs reprises l'adjectif "primitif" pour définir des objets mathématiques. Il reprend bien sûr l'appellation *racine primitive* introduite par Euler. Dans son mémoire plus tardif sur *les arrangements donnés que l'on peut former avec des lettres données et sur les permutations ou substitutions à l'aide desquelles on passe d'un arrangement à un autre* [Cauchy, 1846], il introduit également ce qu'il nomme les *substitutions primitives* et les *facteurs primitifs des substitutions*. Dans ce mémoire, Cauchy définit l'*ordre*[25] d'une substitution comme l'exposant de la plus petite puissance de cette substitution équivalente à l'unité, c'est-à-dire à la substitution identité. Il démontre plus loin que si l'on considère une substitution P d'ordre i dont la décomposition en facteurs premiers est $i = p^f q^g r^h \ldots$, alors il existe des substitutions U, V, W, ..., dont les ordres respectifs sont p^f, q^g, r^h et telles que $P = U^\alpha V^\beta W^\gamma \ldots$, où α, β, γ, ..., sont des nombres entiers déterminés à partir des fac-

25. Notons que, dans son mémoire, Cauchy ne commente pas le choix du terme *ordre*.

teurs premiers du nombre i. Cauchy met d'ailleurs en avant l'analogie existant entre les substitutions U, V, W, ..., les facteurs premiers du nombre i et les racines primitives des équations binômes :

> Cela posé, les substitutions
>
> $$U, V, W, \ldots$$
>
> joueront, par rapport à la substitution P de l'ordre i, un rôle analogue à celui des facteurs
>
> $$p^f, q^g, r^h, \ldots,$$
>
> dont chacun est une puissance d'un nombre premier, jouent aux-mêmes par rapport au nombre entier i. On peut remarquer aussi que les substitutions U, V, W, ... représentent des puissances de P desquelles on peut déduire toutes les autres [...] Elles offrent donc encore, pour cette raison, une certaine analogie avec certaines racines des équations binômes, savoir, avec celles qui sont désignées sous le nom de primitives, et qui, élevées à des puissances diverses, reproduisent toutes les autres racines. Pour conserver le souvenir de ces diverses analogues, nous dirons que les substitutions
>
> $$U, V, W, \ldots,$$
>
> [...] sont les *facteurs primitifs* de la substitution P.
>
> De plus, nous appellerons *substitution primitive* celle qui n'aura d'autres facteurs primitifs qu'elle-même, ou, en d'autres termes, celle dont l'ordre sera une puissance d'un nombre premier [Cauchy, 1846, p. 204-205].

Cauchy met donc en avant les analogies que l'on retrouve entre les racines primitives et les substitutions primitives. Il est donc étonnant qu'il ne justifie pas plus en détails l'introduction de la notion de *facteurs primitifs* dans le cas présent.

À l'aide de l'égalité liant les expressions Θ_h et le nombre premier p, Cauchy déduit une égalité démontrée par Gauss [26] :

$$\Delta^2 = (-1)^{\frac{p-1}{2}} p,$$

où $\Delta = \theta - \theta^t + \theta^{t^2} - \ldots + \theta^{t^{p-3}} - \theta^{t^{p-2}}$. Cette expression, en tant que somme alternée de la racine θ, sera à la base de beaucoup de ses raisonnements sur les résidus quadratiques. Après un rappel sur les résidus et les non-résidus quadratiques, Cauchy revient sur le lien entre les sommes de Gauss et les sommes de Jacobi :

> Une propriété remarquable des facteurs primitifs de p, c'est que le produit de deux ou plusieurs facteurs de cette espèce est proportionnel à un semblable facteur. En d'autres termes, on a
>
> $$\Theta_h \Theta_k = R_{h,k} \Theta_{h+k}$$

26. Voir [Gauss, 1801, art. 356]

... [Cauchy, 1839, p. 512]

où les $R_{h,k}$ sont des fonctions symétriques de τ^h et τ^k. Cette propriété jointe à la propriété précédente des Θ_h permet de transformer des puissances d'un nombre premier p en sommes de la forme $x^2 + ny^2$, où n est un diviseur de $p - 1$:

> il suffit, en effet, pour y parvenir, de multiplier l'un par l'autre, dans un certain ordre, les facteurs primitifs du nombre p... [Cauchy, 1839, p. 513]

Cet extrait est fondamental pour la suite : en effet, lorsqu'il donne des résultats sur les formes quadratiques à partir des sommes de Gauss, sa méthode s'appuie sur la façon dont on peut multiplier les différents facteurs primitifs afin d'obtenir les expressions voulues. Les prochaines notes sont consacrées à montrer comment on peut multiplier ces facteurs primitifs dans certains cas particuliers et comment abaisser au maximum la valeur de l'exposant μ une fois l'expression $p^\mu = x^2 + ny^2$ obtenue.

3 - 13 janvier 1840 : théorème général et méthode de démonstration

Le 13 janvier 1840, Cauchy revient sur le théorème énoncé dans le mémoire *Sur la théorie des nombres* publié dans le *Bulletin de Férussac* en 1831, et qui a « particulièrement attiré l'attention des géomètres » [27] : « une puissance d'un nombre premier p, ou le quadruple de cette puissance, peut toujours être converti en un binôme de la forme $x^2 + ny^2$ lorsque, n étant un diviseur de $p - 1$, et de la forme $4x + 3$ » [Cauchy, 1840d, p. 52]. Il rappelle d'ailleurs que la puissance du nombre premier p dépend des nombres de Bernoulli, et de la différence entre le nombre de résidus quadratiques et de non-résidus quadratiques inférieurs à $\frac{1}{2}n$. Cauchy propose alors un résultat similaire encore plus général, où n est toujours un nombre de la forme $4x + 3$, mais composé. Il y distingue les deux formes possibles pour le nombre n ($8x + 3$ et $8x + 7$) :

> Supposons que, n représentant toujours un diviseur impair de $p - 1$, ce diviseur n soit encore de la forme $4x + 3$, mais cesse d'être un nombre premier. Soit d'ailleurs h l'un quelconque des nombres entiers, premiers à n et inférieurs à $\frac{1}{2}n$. Lorsqu'on prendra successivement pour modules les divers facteurs premiers de n, que nous

27. À partir de notre corpus de textes, les auteurs qui citent Cauchy dans leurs travaux en lien avec les résidus et les congruences sont Legendre, Dirichlet, Libri, Grunert, Crelle et Lebesgue. Le seul se référant explicitement au mémoire de Cauchy publié en 1831 dans le *Bulletin de Férussac* et à son théorème général sur les formes quadratiques est Dirichlet dans son mémoire *Sur l'usage des séries infinies dans la théorie des nombres* publié en 1838 dans le *Journal de Crelle*. Dans cet article, Dirichlet détermine le nombre de classes de formes quadratiques de déterminant négatif $-p$ en fonction du nombre de résidus et de non-résidus quadratiques de p, en se référant à la théorie des formes quadratiques développée par Gauss dans la section V des *Disquisitiones Arithmeticae*. Il note à cette occasion le « théorème très remarquable sur les nombres premiers $4\nu + 3$ » [Dirichlet, 1838, p. 270]. Rappelons également que Jacobi expose des résultats du même type dans son cours donné en 1836-1837 à l'université de Königsberg : voir notre section précédente et [Jacobi, 2007].

> supposerons premiers entre eux, h pourra devenir plusieurs fois un non-résidu quadratique, et ce nombre de fois pourra être ou pair ou impair. Cela posé, comptons les valeurs de h qui se trouvent dans l'un des cas, et, du nombre de ces valeurs, retranchons le nombre de celles qui se trouvent dans l'autre. Le quadruple de la puissance de p qui aura pour exposant, ou la différence obtenue, si n est de la forme $8x+7$, ou le tiers de cette différence dans le cas contraire, pourra toujours être converti en un binôme de la forme x^2+ny^2 ; et l'on pourra effectuer immédiatement cette conversion en multipliant l'un par l'autre, dans un certain ordre, les facteurs primitifs du nombre premier p [Cauchy, 1840d, p. 53].

Cauchy indique qu'il existe des théorèmes semblables pour des formes différentes du nombre n, qu'il aborde dans la suite de cette note.

Après l'énoncé de son résultat, Cauchy développe son raisonnement dans une partie intitulé *Analyse*. Il réintroduit les mêmes notations et résultats fondamentaux que dans ses mémoires précédents. Il considère le nombre n impair, composé de facteurs premiers distincts ν, ν', ν'', ... « pour plus de simplicité », puis rappelle la signification $\left(\frac{h}{n}\right)$, lorsque n n'est pas premier, en se référant à Jacobi :

$$\left(\frac{h}{n}\right) = \left(\frac{h}{\nu}\right)\left(\frac{h}{\nu'}\right)\left(\frac{h}{\nu''}\right)\dots$$

Comme il le fait très régulièrement dans ses mémoires, il partage les nombres inférieurs et premiers à n en deux groupes : d'une part, les nombres notés h, h', h'', ... tels que $\left(\frac{h}{n}\right) = 1$ et d'autre part, les nombres notés k, k', k'', ... tels que $\left(\frac{k}{n}\right) = -1$. Cela lui permet de définir deux produits de facteurs primitifs distincts :

$$I = \Theta_h\Theta_{h'}\Theta_{h''}\dots \text{ et } J = \Theta_k\Theta_{k'}\Theta_{k''}\dots$$

.

Il pose également $N = \varphi(n) = n\left(1-\frac{1}{\nu}\right)\left(1-\frac{1}{\nu'}\right)\left(1-\frac{1}{\nu''}\right)\dots$, où φ représente la fonction d'Euler : N est donc le nombre de nombres inférieurs et premiers à n.

Il distingue alors deux cas :

- Si n est de la forme $4x+1$, alors $\left(\frac{-1}{n}\right) = 1$ et donc $\left(\frac{-h}{n}\right) = \left(\frac{h}{n}\right)$, $\left(\frac{-k}{n}\right) = \left(\frac{k}{n}\right)$. Ainsi, le produit I sera composé de couples de la forme $\Theta_h\Theta_{-h}$. Comme $\Theta_h\Theta_{-h} = (-1)^{\varpi h}p$, alors $I = p^{\frac{N}{4}}$. De même, $J = p^{\frac{N}{4}}$.
- Si n est de la forme $4x+3$, on a $IJ = p^{\frac{N}{2}}$, mais les nombres I et J ne sont plus réduits à une puissance de p. Pour déterminer une expression des produits I et J, il utilise une propriété de la somme alternée $\Delta = \theta - \theta^t + \theta^{t^2} - \dots + \theta^{t^{p-3}} - \theta^{t^{p-2}}$: $\Delta^2 = (-1)^{\frac{p-1}{2}}p$. Ici, il note Δ, Δ', Δ'', ..., la somme alternée définie précédemment, où p est remplacé par ν, ν', ν'', ... et où θ représente une racine primitive de $x^\nu = 1$, $x^{\nu'} = 1$, $x^{\nu''} = 1$, ..., et t représente une racine primitive de $x^\nu \equiv 1 \pmod{\nu}$, $x^{\nu'} \equiv 1$

$(\mathrm{mod}\ \nu')$, $x^{\nu''} \equiv 1\ (\mathrm{mod}\ \nu'')$, ... Il donne alors les deux égalités[28] :

$$2I = A + B\Delta\Delta'\Delta'' \ldots \quad 2J = A - B\Delta\Delta'\Delta'' \ldots,$$

où A et B sont des nombres entiers qui peuvent être divisibles par une puissance de p. L'intérêt de cette transformation est qu'ainsi, on obtient une nouvelle expression du produit IJ :

$$IJ = A^2 - B^2\Delta^2\Delta'^2\Delta''^2 \ldots$$

De plus, $\Delta^2 = (-1)^{\frac{\nu-1}{2}}\nu$, ..., et on obtient ainsi $\Delta^2\Delta'^2\Delta''^2 \ldots = (-1)^{\frac{n-1}{2}}n$. Finalement, en égalant les deux expressions obtenues pour le produit IJ, on obtient, lorsque n est de la forme $4x+3$:

$$4p^{\frac{N}{2}} = A^2 + nB^2.$$

Cauchy reproduit ensuite des raisonnements similaires pour obtenir des résultats analogues pour les formes quadratiques $p^{\frac{N}{2}} = A^2 + \frac{n}{4}B^2$ lorsque le nombre n est de la forme $4\nu\nu'\nu'' \ldots$ ou $8\nu\nu'\nu'' \ldots$ en adaptant dans chaque cas la définition de $\left(\frac{h}{n}\right)$.

Ici, Cauchy met donc en avant la méthode permettant d'obtenir une égalité de la forme $4p^\mu = x^2 + ny^2$: il utilise les propriétés des sommes de Gauss (qu'il développe et démontre en partie dans les notes suivantes, puis complètement dans son *Mémoire sur la théorie des nombres*), et en particulier l'égalité $\Theta_h\Theta_{-h} = \pm p$, pour avoir d'une part une puissance de p et d'autre part une expression de la forme $x^2 + ny^2$.

Dans un deuxième temps, il développe une méthode permettant de déterminer la plus petite valeur de μ telle que l'on ait $4p^\mu = x^2 + ny^2$. Il pose $A = p^\lambda x$, $B = p^\lambda y$, où p^λ est la plus grande puissance de p qui divise A et B et obtient ainsi $\mu = \frac{N}{2} - 2\lambda$. Il rappelle alors sans les démontrer des résultats contenus dans le mémoire présenté à l'Académie le 31 mai 1830, et qui sera reproduit dans le *Mémoire* de 1840, relatifs à la différence entre le nombre de résidus quadratiques de n inférieurs à $\frac{n}{2}$ et le nombre de non-résidus quadratiques de n inférieurs à $\frac{n}{2}$. Cela permet d'obtenir la valeur de μ.

Cauchy explique enfin comment calculer les valeurs entières de x vérifiant les équations $4p^\mu = x^2 + ny^2$ et $p^\mu = x^2 + \frac{n}{4}y^2$. Dans le cas où n est impair, il observe que l'on a $x^2 = p^\mu\left(2 + \frac{I}{J} + \frac{J}{I}\right)$. Il pose $P = R_{h,h}R_{h',h'} \ldots$ et $P = R_{k,k}R_{k',k'} \ldots$ et remarque, par exemple,

28. Ici, Cauchy ne donne pas de démonstration de ces égalités ; des preuves en sont données ultérieurement dans une note aux *Comptes Rendus* de la séance du 3 février 1840 et dans le *Mémoire sur la théorie des nombres*.

que si n est de la forme $8x+7$, alors $\frac{I}{J}=\frac{P}{Q}$. L'intérêt de faire le lien avec les sommes de Jacobi est que le quotient $\frac{I}{J}$ peut être représenté par une fonction rationnelle de ρ. Cauchy peut alors appliquer le principe déjà abordé en 1829 consistant à substituer à la racine primitive ρ de l'équation $x^n=1$, une racine primitive r de l'équivalence $x^n \equiv 1 \pmod{p}$. On peut alors obtenir directement la valeur de x lorsque $\mu=1$. Dans le cas contraire, on remplace ρ par une racine primitive r de l'équivalence $x^n \equiv 1 \pmod{p^\mu}$.

Pour conclure, il applique sa méthode au cas où $n=8$ et remarque que la méthode pour déterminer la valeur de μ dans les cas où n est égal à 3 ou 4 n'est plus valable : il résout ces cas en rappelant qu'ils donnent des formules démontrées par Jacobi en 1827 et Gauss en 1825.

4 - 20 janvier 1840 : propriétés des fonctions symétriques et alternées des racines primitives de l'équation $x^n=1$

Lors de son intervention du 20 janvier 1840, Cauchy donne des résultats sur les fonctions symétriques et alternées des racines primitives de l'équation $x^n=1$, et en déduit la valeur de Δ^2.

Donnons les principales étapes[29] du cas particulier où n est un nombre premier impair. D'une part, Cauchy démontre qu'une fonction symétrique des racines primitives de l'équation $x^n=1$ (qui sont $\rho, \rho^2, \ldots, \rho^{n-1}$) est de la forme $f(\rho)=a_0+a_1(\rho+\rho^2+\ldots+\rho^{n-1})$, où a_0 et a_1 sont des nombres entiers. D'autre part, une fonction alternée des racines primitives de $x^n=1$, est proportionnelle à $\Delta=\rho^h+\rho^{h'}+\rho^{h''}+\ldots-\rho^k-\rho^{k'}-\rho^{k''}+\ldots$, où h, h', h'', $\ldots$ sont les résidus quadratiques de n, et k, k', k'', $\ldots$, les non-résidus quadratiques de n, et est donc de la forme $f(\rho)=a\Delta$. Enfin, $\Delta^2=(-1)^{\frac{n-1}{2}}n$. Cauchy indique le signe de Δ en fonction de la forme de n. On en déduit que $[f(\rho)]^2=\pm na^2$, selon la forme de n.

À l'aide de ces résultats, Cauchy reprend la méthode développée dans son intervention précédente : il remarque que $I+J$ est une fonction symétrique des racines primitives de $x^n=1$, tandis que $I-J$ est une fonction alternée de ces mêmes racines. Donc, d'après ce qui précède :

$$(I+J)^2-(I-J)^2=A^2-(\pm nB^2),$$

soit

$$4IJ=A^2\mp nB^2.$$

On obtient ainsi les formes quadratiques $4p^{\frac{N}{2}}=A^2\mp nB^2$. Dans le cas où $\Delta^2=n$, soit n divisible par 8, ou de la forme $4x+1$, ou $4(4x+3)$, on a $I=J=p^{\frac{N}{4}}$, $B=0$. Dans le cas contraire, lorsque $\Delta^2=-n$, on obtient bien une forme quadratique de la forme

29. Nous revenons sur les démonstrations détaillées dans notre analyse du *Mémoire sur la théorie des nombres* de 1840.

$4p^\mu = x^2 + ny^2$, où x et y ne sont pas nuls.

Dans cette note, Cauchy expose donc des résultats très généraux sur les formes quadratiques, et donne les principes de sa méthode pour obtenir les égalités voulues : multiplier les facteurs primitifs dans un certain ordre lui permet d'obtenir des égalités de la forme $p^\mu = x^2 + ny^2$. Mais contrairement à Jacobi, il ne fait aucun commentaire sur les nombres complexes en jeu et n'aborde plus du tout les questions liées aux résidus d'ordre supérieur et aux lois de réciprocité associées.

5 - 3 et 10 février 1840 : calcul de l'exposant μ dans l'égalité $4p^\mu = x^2 + ny^2$

Dans la note intitulée *Suite des observations sur les formes quadratiques de certaines puissances des nombres premiers. Théorèmes relatifs aux exposants de ces puissances* présentée à l'Académie des Sciences le 3 février 1840, le travail de Cauchy est principalement consacré[30] à la détermination de l'exposant μ. Pour cela, Cauchy utilise les formules $\Theta_0 = -1$ et $\Theta_l\Theta_{l'} = R_{l,l'}\Theta_{l+l'}$, ainsi que l'équivalence $h + h' + h'' + \ldots \equiv k + k' + k'' + \ldots \equiv 0 \pmod{n}$. Il en déduit :

$$\begin{cases} I = -R_{h,h'}R_{h+h',h''}R_{h+h'+h'',h'''}\ldots, \\ J = -R_{k,k'}R_{k+k',k''}R_{k+k'+k'',k'''}\ldots, \end{cases}$$

Il remarque également que $R_{l,l'}R_{-l,-l'} = R_{l,l'}R_{n-l,n-l'} = p$, et que parmi les deux sommes $l + l'$ et $n - l + n - l' = 2n - (l + l')$, il y en a toujours une qui est comprise entre 0 et n, et l'autre entre n et $2n$. Ainsi, dans les produit I et J composés d'expressions de la forme $R_{l,l'}$, lorsque la somme $l + l'$ est comprise entre 0 et n, on pourra substituer à $R_{l,l'}$, l'expression $\dfrac{p}{R_{n-l,n-l'}}$. Les produits I et J pourront donc être mis sous la forme

$$I = -p^f\frac{F}{G}, \quad J = -p^g\frac{G}{F},$$

où f et g sont des nombres entiers tels que $f + g = \frac{N}{2}$ et F et G sont des produits dont les facteurs sont de la forme $R_{l,l'}$, où $n < l + l' < 2n$. Cela permettra ensuite de pouvoir remplacer les $R_{l,l'}$ par des équivalents non nuls modulo p, lorsque la racine primitive ρ de l'équation $x^n = 1$ est remplacée par une racine primitive r de l'équivalence $x^n \equiv 1$

30. Il reprend d'abord les résultats exposés lors de la séance précédente à partir des mêmes notations : on obtient une forme quadratique $4p^\mu = x^2 + ny^2$ lorsque n est de l'une des formes $4x + 3$, $4(4x + 1)$ ou $8(4x + 1)$, $8(4x + 3)$; il précise dans chaque cas comment choisir les nombres h, h', h'', ... Par exemple, si n est de la forme $8(4x + 1)$, les nombres h, h', h'', ..., devront être tels que $\left(\frac{h}{\frac{1}{8}n}\right) = 1$ et $h \equiv 1$ ou $3 \pmod 8$ ou $\left(\frac{h}{\frac{1}{8}n}\right) = -1$ et $h \equiv 5$ ou $7 \pmod 8$.

(mod p) : les combinaisons $-\Pi_{n-l,n-l'}$ où $\Pi_{l,l'} = \dfrac{1.2.3.\ldots.(l+l')\varpi}{(1.2.\ldots.l\varpi)(1.2.\ldots.l'\varpi)}$.

Comme $I + J = A$, on obtient l'équation : $-p^f\dfrac{F}{G} - p^g\dfrac{G}{F} = p^\lambda x$, soit, en multipliant par FG et en divisant par p^m où m est le plus petit des nombres f, g et λ :

$$p^{f-m}F^2 + p^{g-m}G^2 + p^{\lambda-m}FGx = 0.$$

Cauchy traduit alors cette égalité en une équivalence modulo p en substituant à ρ la racine r :

$$p^{f-m}\mathscr{F}^2 + p^{g-m}\mathscr{G}^2 + p^{\lambda-m}\mathscr{F}\mathscr{G}x \equiv 0 \pmod{p},$$

où $\mathscr{F}$ et $\mathscr{G}$ sont les équivalents modulo p de F et G. Ces deux nombres sont premiers à p (d'après ce que l'on a dit précédemment) ; le nombre x est également premier à p (par définition de m).

Il finit par montrer que le nombre μ est toujours « *équivalent à la valeur numérique de la différence entre les deux nombres représentés par f et g* », puis fait le lien entre la différence $f-g$ et la différence $i-j$, où i et j ont été respectivement définis comme le nombre d'entiers inférieurs à $\frac{n}{2}$ et appartenant au groupe h, h', h'', … (respectivement k, k', k'', …). Il obtient $f-g = i-j$ lorsque n est de la forme $8x+7$, $f-g = \dfrac{i-j}{3}$ lorsque n est de la forme $8x+3$ et $f-g = \dfrac{i-j}{2}$ lorsque n est divisible par 4 ou 8. Ces différences ne s'annulent pas dans le cas où $\Delta = -n$, ce qui est bien en accord avec ce qui a été étudié précédemment.

Dans la note du 10 février 1840, intitulée *Discussion des formes quadratiques sous lesquelles se présentent certaines puissances de nombres premiers. Réduction des exposants de ces puissances*, Cauchy rappelle les résultats exposés dans les notes précédentes puis présente une méthode pour réduire encore l'exposant μ, dans le cas où n est un nombre composé. Par exemple, il démontre que si n est un nombre composé de la forme $8x+7$, l'égalité $p^\mu = x^2 + ny^2$ implique l'égalité $p^{\frac{\mu}{2}} = \alpha u^2 + \beta v^2$, où α et β sont tels que $\alpha\beta = n$ et $\left(\frac{\beta}{\alpha}\right) = 1$. Ainsi, si $n = 15$, la théorie de Cauchy donne non seulement la forme quadratique $p^2 = x^2 + 15y^2$, mais également la forme $p = u^2 + 15v^2$. Il obtient des résultats similaires dans les cas où n est composé et de la forme $8x+3$ ou encore divisible par 4 ou 8.

Il termine en annonçant l'intérêt d'utiliser la notion d'indice, introduite par Gauss dans les *Disquisitiones Arithmeticae*, pour déterminer les valeurs des différents nombres intervenant dans sa méthode, h, h', …, k, k', …, i, j, μ, et des équivalents de x et y modulo p. Il cite d'ailleurs la Table d'indices de Jacobi[31].

31. Voir [Jacobi, 1839a]. Ici, Cauchy promet d'ailleurs une explication de son utilisation dans le cadre de sa théorie des les *Exercices d'analyse et de mathématiques*, explication que l'on retrouve dans une des notes du *Mémoire* de 1840.

Dans cette note, Cauchy calcule la valeur de l'exposant μ et montre qu'il est lié avec la différence entre le nombre de résidus et de non-résidus quadratiques du nombre n lorsque celui-ci de la forme $4x+3$, ou du nombre $\frac{1}{4}n$ lorsque n est de la forme $4(4x+1)$ ou encore du nombre $\frac{1}{8}n$ lorsque n est de la forme $8(4x+1)$. Dans le cas où n est de la forme $4x+3$, on retrouve les résultats démontrés par Jacobi dans ses leçons données en 1836-1837. Cauchy va par contre plus loin en considérant d'autres formes du diviseur n.

6 - 16 mars 1840 : sur le nombre de résidus et non-résidus quadratiques

La note du 16 mars 1840 se partage en deux paragraphes : un premier intitulé *Sur les résidus inférieurs à un module donné*, et un deuxième *Sur les résidus et les non-résidus quadratiques inférieurs à la moitié d'un module donné*.

Dans la première partie, Cauchy annonce qu'il va s'appuyer sur des formules indiquées dans [Gauss, 1811]. Cela va lui permettre de démontrer l'égalité utilisée précédemment : $\Delta^2 = (-1)^{\frac{n-1}{2}}n$. À partir de la formule annoncée lors de la séance du 3 février 1840 dans une note intitulée *Sur les fonctions alternées et sur diverses formules d'Analyse*

$$(1-x)(1-x^3)\dots(1-x^{2m-1}) = 1 - \frac{1-x^{2m}}{1-x} + \frac{(1-x^{2m})(1-x^{2m-2})}{(1-x)(1-x^2)}\dots + 1,$$

il déduit, en posant $2m = n-1$ et $x = \rho$ (où ρ est une racine primitive de l'équation $x^n = 1$) :

$$(1-\rho)(1-\rho^3)\dots(1-\rho^{n-2}) = 1 + \rho^{-1} + \rho^{-3} + \dots + \rho^{-\frac{1}{2}n(n-1)},$$

soit en substituant ρ^{-2} à ρ :

$$(1-\rho^{-2})(1-\rho^{-6})\dots(1-\rho^{-2(n-2)}) = 1 + \rho^2 + \rho^6 + \dots + \rho^{n(n-1)}.$$

Puis, en multipliant par $\rho^{\left(\frac{n-1}{2}\right)^2}$, et sachant que $\left(\frac{n-1}{2}\right)^2 = 1+3+5+\dots+(n-2)$ et $m(m-1)+\left(\frac{n-1}{2}\right)^2 \equiv \left(\frac{2m-1\pm n}{2}\right)^2 \pmod n$, on obtient deux expressions de l'expression que Cauchy note habituellement Δ :

$$(\rho-\rho^{-1})(\rho^3-\rho^{-3})\dots(\rho^{n-2}-\rho^{-(n-2)}) = 1 + \rho + \rho^4 + \rho^9 + \dots + \rho^{(n-1)^2}.$$

On a également

$$\Delta = \rho^{\left(\frac{n-1}{2}\right)^2}(1-\rho^4)(1-\rho^8)\dots(1-\rho^{2n-2}),$$

soit, en multipliant les deux égalités précédentes :

$$\Delta^2 = (-1)^{\frac{n-1}{2}}(1-\rho^2)(1-\rho^4)(1-\rho^6)\dots(1-\rho^{2n-4})(1-\rho^{2n-2}).$$

En remarquant que $\rho^{n+k} = \rho^k$, on a :

$$\Delta^2 = (-1)^{\frac{n-1}{2}}(1-\rho)(1-\rho^2)(1-\rho^3)\dots(1-\rho^{n-2})(1-\rho^{n-1}).$$

Cauchy utilise ensuite l'égalité $x^n - 1 = (x-1)(x-\rho)(x-\rho^2)\dots(x-\rho^{n-1})$, pour en déduire, en divisant par $x-1$: $1+x+x^2+\dots+x^{n-1} = (x-\rho)(x-\rho^2)\dots(x-\rho^{n-1})$. En posant $x = 1$, on obtient ainsi une expression pour le nombre n : $n = (1-\rho)(1-\rho^2)\dots(1-\rho^{n-1})$. Finalement, Cauchy conclut :

$$\Delta^2 = (-1)^{\frac{n-1}{2}}.$$

Cauchy utilise ensuite l'expression trigonométrique des racines primitives ρ^k pour en déduire des égalités liées aux sommes trigonométriques. Ainsi, $\rho = e^{m\omega\sqrt{-1}} = \cos m\omega + \sqrt{-1}\sin m\omega$, où $\omega = \dfrac{2\pi}{n}$, et où m est un nombre entier compris entre 0, 1, 2, 3, …, $n-1$. Cauchy rappelle que ρ est une racine primitive lorsque m et n sont premiers entre eux. En considérant $m = 1$, et puisque $\rho - \rho^{-1} = 2\sqrt{-1}\sin\omega$, on obtient :

$$\Delta = (2\sqrt{-1})^{\frac{n-1}{2}}\sin\omega\sin 3\omega\dots\sin(n-2)\omega$$

soit

$$\Delta = 1 + \cos\omega + \cos 4\omega + \dots + \cos(n-1)^2\omega + [\sin\omega + \sin 4\omega + \dots + sin(n-1)^2\omega]\sqrt{-1}.$$

Comme $\omega, 2\omega, \dots, \frac{n-1}{2}\omega$ sont compris entre 0 et π et comme $\sin(2kw) = -\sin[(n-2i)\omega]$, on obtient un produit positif que Cauchy note Ω :

$$\Omega = \sin\omega\sin 2\omega\dots\sin\left(\frac{n-1}{2}\omega\right) = \pm\sin\omega\sin 3\omega\dots\sin(n-2)\omega.$$

Donc, d'après ce qui précède, $2^{n-1}\Omega^2 = n$, soit $2^{\frac{n-1}{2}}\Omega = \sqrt{n}$ puisque Ω est positif.

Finalement, comme

$$\sin\omega\sin 2\omega\dots\sin(n-2)\omega = (-1)^{\frac{(n-1)(n-3)}{8}}\sin\omega\sin 2\omega\dots\sin\left(\frac{n-1}{2}\omega\right),$$

on obtient la valeur suivante pour Δ :

$$\Delta = n^{\frac{1}{2}}(\sqrt{-1})^{(\frac{n-1}{2})^2}.$$

Cette formule permet ainsi de déterminer la valeur exacte de Δ selon la forme de n ($4x+1$ ou $4x+3$).

Cauchy applique ensuite cette formule à des exemples. Par exemple, si $n = 3$, on obtient : $\Delta = 1 + 2\rho = 3^{\frac{1}{2}}\sqrt{-1}$.

Cauchy considère ensuite le cas plus général où $\rho = e^{m\omega\sqrt{-1}}$, où m est premier à n. Il transforme l'expression de Δ pour obtenir une somme alternée en remarquant d'une part que pour $1 \leq l \leq \frac{n}{2}$, $(n-l)^2 \equiv l^2 \pmod{n}$ et donc que

$$\Delta = 1 + 2[\rho + \rho^4 + \ldots + \rho^{\left(\frac{n-1}{2}\right)^2}] = 1 + 2[\rho^h + \rho^{h'} + \rho^{h''} + \ldots],$$

où les h, h', h'', ... désignent les résidus quadratiques modulo n. D'autre part, si on désigne par k, k', k'', ..., les non-résidus quadratiques de n, on a :

$$1 + \rho + \rho^2 + \ldots + \rho^{n-1} = 1 + \rho^h + \rho^{h'} + \ldots + \rho^k + \rho^{k'} + \ldots = 0.$$

On obtient donc :

$$\Delta = \rho^h + \rho^{h'} + \rho^{h''} + \ldots - \rho^k - \rho^{k'} - \rho^{k''} - \ldots.$$

Il remarque enfin que si $\rho = e^{m\omega\sqrt{-1}}$, alors

$$\Delta = \left(\frac{m}{n}\right) n^{\frac{1}{2}} (\sqrt{-1})^{\left(\frac{n-1}{2}\right)^2}.$$

Les formules données ci-dessus sont également valables lorsque n est un nombre composé, de la forme $\nu^a \nu'^b \nu''^c \ldots$, où ν, ν', ν'' sont des nombres premiers. Δ est alors le produit d'expressions du type $1 + \rho + \rho^4 + \rho^9 + \ldots \rho^{(n-1)^2}$ correspondant aux valeurs ν^a, ν'^b, ν''^c et où $\left(\frac{m}{n}\right)$ désigne le symbole de Jacobi :

$$\left(\frac{m}{n}\right) = \left(\frac{m}{\nu}\right)^a \left(\frac{m}{\nu'}\right)^b \left(\frac{m}{\nu''}\right)^c \ldots$$

Lorsque $a = b = c = \ldots = 1$, on a également $\Delta = \rho^h + \rho^{h'} + \rho^{h''} + \ldots - \rho^k - \rho^{k'} - \rho^{k''} - \ldots$, où h, h', ... sont tels que $\left(\frac{h}{n}\right) = \left(\frac{h'}{n}\right) = \ldots = 1$ et $\left(\frac{k}{n}\right) = \left(\frac{k'}{n}\right) = \ldots = -1$.

Pour finir le premier paragraphe, il déduit de son travail des formules trigonométriques, dont par exemple[32] : $S\cos h\omega - S\cos k\omega = \sqrt{n}$, si n est de la forme $4x+1$ et $S\sin h\omega - S\sin k\omega = \sqrt{n}$, si n est de la forme $4x+3$.

Remarquons que lors de ses recherches, Cauchy propose plusieurs méthodes pour déterminer la valeur de Δ ou Δ^2, à partir d'outils différents : calcul intégral, relations trigonométriques, ...

32. Dans ces formules, la lettre S est utilisée pour désigner la somme de toutes les valeurs de h ou de k.

Dans la suite du mémoire, Cauchy considère les résidus et non-résidus quadratiques inférieurs à $\frac{n}{2}$.

Cauchy commence par rappeler certains résultats sur le symbole de Legendre :

- $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$ et $\left(\frac{n-l}{n}\right) = (-1)^{\frac{n-1}{2}}\left(\frac{l}{n}\right)$ donc
- $\left(\frac{n-l}{n}\right) = \left(\frac{l}{n}\right)$ si n est de la forme $4x+1$;
- $\left(\frac{n-l}{n}\right) = -\left(\frac{l}{n}\right)$ si n est de la forme $4x+3$.

À partir de ces remarques, et en utilisant ce qui précède, Cauchy en déduit que

- $S\cos h\omega - S\cos k\omega = \frac{1}{2}\sqrt{n}$ pour $n \equiv 1 \pmod 4$;
- et $S\sin h\omega - S\sin k\omega = \frac{1}{2}\sqrt{n}$ pour $n \equiv 3 \pmod 4$,

si les sommes sont considérées sur les h et k inférieurs à $\frac{n}{2}$ et tels que $\left(\frac{h}{n}\right) = 1$ et $\left(\frac{k}{n}\right) = 1$.

L'objectif est ensuite d'établir des relations entre les sommes de puissances données des résidus et non-résidus quadratiques de n inférieurs à $\frac{n}{2}$.

Pour cela, Cauchy remarque que si n est impair, les nombres inférieurs et premiers à n peuvent être représentés par les formes $2h$, $2k$, $n-2h$, $n-2k$. Il base ensuite la suite de son raisonnement sur le caractère quadratique de 2 : $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$ et distingue donc les quatre formes possibles pour n : $8x+1$, $8x+3$, $8x+5$ et $8x+7$.

Par exemple, si n est de la forme $8x+1$, alors $\left(\frac{2}{n}\right) = \left(\frac{-1}{n}\right) = 1$ et on obtient donc : $\left(\frac{2h}{n}\right) = 1$, $\left(\frac{n-2h}{n}\right) = 1$, $\left(\frac{2k}{n}\right) = -1$ et $\left(\frac{n-2k}{n}\right) = -1$. Ainsi, dans ce cas, l'ensemble des nombres h et $n-h$ correspond à l'ensemble des nombres $2h$ et $n-2h$. Donc si S représente la somme lorsque l'on prend toutes les valeurs possibles de h, on a :$S(h)+S(n-h) = S(2h)+S(n-2h)$ et plus généralement, $Sf(h) + Sf(n-h) = Sf(2h) + Sf(n-2h)$, où f est une fonction quelconque. On peut raisonner de même avec les nombres k et on trouve en particulier :

$$\begin{cases} Sh^m + S(n-h)^m = S(2h)^m + S(n-2h)^m; \\ Sk^m + S(n-k)^m = S(2k)^m + S(n-2k)^m. \end{cases}$$

Après avoir exposé le même type de résultats pour toutes les formes de n, Cauchy pose $Sh^m = s_m$ et $Sk^m = t_m$, avec $i = s_0$ et $j = t_0$, le nombre de valeurs de h et de k inférieurs à $\frac{n}{2}$. Il introduit également les notations S_m et T_m, qui représentent les sommes similaires pour les nombres inférieurs à n. La fin de cette note est un exposé de différentes relations entre les expressions définies précédemment et les expressions $v_m = \left[2^m - \left(\frac{2}{n}\right)\right]\frac{s_m - t_m}{n^m}$. Il obtient notamment que $T_1 - S_1 = n(i-j)$ et $T_2 - S_2 = n^2\frac{i-j}{2}$.

Cauchy conclut en annonçant que Liouville lui a dit avoir obtenu des résultats similaires et en rappelant que Dirichlet a également travaillé sur ce thème [33]. Le fait que Cauchy présente ses recherches sur le nombre de résidus et non-résidus quadratiques est implici-

33. Voir [Dirichlet, 1838].

tement en lien avec ses travaux sur les formes quadratiques de la forme $4p^{\mu} = x^2 + ny^2$; il a en effet démontré dans de précédentes notes que l'exposant μ dépend de la différence qu'il note ici $i - j$.

7 - 6 avril 1840 : Détermination de la valeur de Δ sans calcul intégral et séries infinies

Cette note, présentée à l'Académie le 6 avril 1840, a été reproduite dans le cinquième tome du *Journal de Liouville* en 1840 également. Il introduit son texte en rappelant l'importance de la détermination de la valeur de certaines sommes alternées de racines primitives de l'équation binôme, et tout particulièrement les sommes de Gauss quadratiques : plusieurs savants, depuis plus de trente ans, publient des mémoires sur ces expressions.

Il rappelle que le carré de cette somme, qu'il a noté précédemment Δ^2, a déjà été déterminé par Gauss notamment selon la forme du module. La difficulté principale consiste à déterminer le signe de Δ, question résolue également par Gauss en 1811 dans [Gauss, 1811], puis par Dirichlet à l'aide des intégrales définies dans [Dirichlet, 1838]. Cauchy cite également le mémoire [Lebesgue, 1840b] publié en 1840 dans le *Journal de Liouville*. Il rappelle également ses propres travaux de 1817, sur les fonctions réciproques [34], desquels on peut également déduire la formule en question. Ici, Cauchy veut présenter une nouvelle méthode, n'utilisant pas le calcul intégral, et fait le lien avec les facteurs primitifs du nombre n :

> [...] et ce que les géomètres apprendront sans doute avec plaisir, c'est que, sans recourir ni au Calcul intégral, ni aux séries singulières dont M. Gauss a fait usage, on peut directement, et par une méthode fort simple, transformer en produit une somme alternée, en déterminant le signe qui doit affecter ce même produit. Cette méthode a d'ailleurs l'avantage d'être applicable à d'autres questions du même genre. Ainsi, en particulier, on reconnaîtra sans peine que, si, n étant un nombre premier, $n - 1$ est divisible par 3, ou par 5, etc., un facteur primitif de n, correspondant au diviseur 3, sera proportionnel au produit de $\frac{n-1}{3}$ facteurs trinômes, tandis qu'un facteur primitif de n, correspondant au diviseur 5, sera proportionnel au produit de $\frac{n-1}{5}$ facteurs pentanômes ou composés chacun de cinq termes ; et le rapport du produit en question au facteur primitif de n sera la somme de certaines racines de l'unité respectivement multipliées par des coefficients qui seront équivalents, suivant le module n, à des quantités connues[Cauchy, 1840b, p. 153-154].

34. Cauchy aborde notamment ces fonctions dans le *Bulletin de la Société Philomathique* de 1817. Une fonction réciproque de première espace est de la forme $f(x) = \left(\frac{2}{\Pi}\right)^{\frac{1}{2}} \int_0^{\infty} \varphi(u)\cos(ux)du$, où x est positif et est telle que $\varphi(u) = \left(\frac{2}{\Pi}\right)^{\frac{1}{2}} \int_0^{\infty} f(v)\cos(uv)dv$. Les fonctions réciproques de seconde espèce sont semblables, mais dépendent de la fonction sinus.

Cauchy revient sur ces questions à la fin de sa note.

Cette note contient deux paragraphes : *Valeurs exactes des sommes alternées des racines primitives d'une équation binôme* et *Transformation des sommes alternées en produits.*

Dans le premier paragraphe, Cauchy considère l'expression Δ une somme alternée des racines primitives de $x^n = 1$, « qui soit en même temps une fonction alternée des racines primitives de chacune des équations que l'on peut obtenir en remplaçant n par un diviseur de n » [Cauchy, 1840b], et remarque que si n est un nombre impair composé de facteurs premiers distincts, alors $\Delta = \pm\left(1 + \rho + \rho^4 + \rho^9 + \ldots + \rho^{(n-1)^2}\right)$. Cauchy détermine ensuite à l'aide des fonctions réciproques, définies à partir d'intégrales, la valeur de Δ selon la forme de n : $4x$, $4x+1$, $4x+2$ ou $4x+3$.

Dans le deuxième paragraphe, Cauchy raisonne à partir de l'expression $\Delta = \rho^h + \rho^{h'} + \rho^{h''} - \rho^k - \rho^{k'} - \rho^{k''} - \ldots$, où les nombres h, h', ... représentent les résidus quadratiques de n et où k, k', ... représentent les non-résidus quadratiques de n. Après avoir pris deux exemples, $n = 3$ et $n = 5$, Cauchy annonce que la somme Δ est égale plus généralement au produit $P = (\rho^1 - \rho^{-1})(\rho^3 - \rho^{-3})\ldots(\rho^{n-2} - \rho^{-(n-2)})$, qui est lui-même égal au produit $(\rho^1 - \rho^{n-1})(\rho^2 - \rho^{n-2})\ldots\left(\rho^{\frac{n-1}{2}} - \rho^{\frac{n+1}{2}}\right)$ qui est une fonction alternée des racines primitives considérées [35]. P est donc de l'une des deux formes a ou $a\Delta$, le nombre a étant entier relatif. Cauchy montre alors que P, ne pouvant pas être de la forme a, est nécessairement de la forme $a\Delta$. Ici, Cauchy utilise donc les propriétés des fonctions symétriques et alternées des racines primitives de l'équation $x^n = 1$, abordées dans une des notes précédentes, et démontrées en détails dans le *Mémoire sur la théorie des nombres* de 1840.

En effet, d'après ce qui précède, en multipliant chaque facteur par la puissance qui convient ρ^{-k}, où k est positif, on a :

$$P = \rho^{1+3+5+\ldots+(n-2)}(1-\rho^{-2})(1-\rho^{-6})\ldots(1-\rho^{-2(n-2)}),$$

soit

$$P = \rho^{\left(\frac{n-1}{2}\right)^2}(1-\rho^{n-2})(1-\rho^{n-6})\ldots(1-\rho^4).$$

De même, à partir de la même expression, et en multipliant chaque facteur par la puissance $-\rho^k$, où k est positif, qui convient, on obtient :

$$P = (-1)^{\left(\frac{n-1}{2}\right)}\rho^{-\left(\frac{n-1}{2}\right)^2}(1-\rho^2)(1-\rho^6)\ldots(1-\rho^{n-4}).$$

Finalement, $P^2 = (-1)^{\left(\frac{n-1}{2}\right)}(1-\rho)(1-\rho^2)\ldots(1-\rho^{n-1}) = (-1)^{\left(\frac{n-1}{2}\right)}n$, en considérant l'égalité $(x-\rho)(x-\rho^2)(x-\rho^3)\ldots(x-\rho^{n-1}) = \frac{x^n-1}{x-1} = 1 + x + x^2 + \ldots + x^{n-1}$, avec $x = 1$. P^2 ne peut donc être de la forme a^2 ; on a donc $P^2 = a^2\Delta^2 = (-1)^{\frac{n-1}{2}}n$ et $P = a\Delta$.

35. Cauchy précise en effet que ce produit reste invariable ou change seulement de signe lorsque l'on remplace ρ par ρ^m, où m est premier à n.

De plus, Δ est une fonction symétrique de ρ, ρ^2, ..., donc c'est un nombre entier et n est un nombre premier donc $a^2 = 1$ et $\Delta = (-1)^{\frac{n-1}{2}} n$. Ainsi : $P = \pm\Delta$.

La suite du texte est consacrée à déterminer le signe du second membre $\pm\Delta$. Pour cela, Cauchy remplace une fois de plus les égalités en jeu par des congruences. Ainsi, à la place de $\Delta = \rho^h + \rho^{h'} + \rho^{h''} + \ldots - \rho^k - \rho^{k'} - \rho^{k''} - \ldots$, il remplace les ρ^l par $\left(\frac{l}{n}\right)$ et obtient l'égalité :

$$\left(\frac{h}{n}\right) + \left(\frac{h'}{n}\right) + \ldots - \left(\frac{k}{n}\right) - \left(\frac{k'}{n}\right) - \ldots = n - 1 \equiv -1 \pmod{n}.$$

Cauchy détermine ensuite la valeur de P lorsqu'on y effectue la même substitution. Les termes composant le développement de P, qui est le produit de facteurs de la forme $(\rho^k - \rho^{-k})$, où k est impair, compris entre 1 et $n-2$, sont les expressions de la forme[36] $\rho^{\pm 1 \pm 3 \pm 5 \pm \ldots \pm (n-2)}$, précédés du signe + si l'exposant est composé d'un nombre pair de termes positifs, et du signe − dans le cas contraire. La valeur de P, après remplacement des ρ^k par $\left(\frac{k}{n}\right)$, est égale à la somme des $\pm\left(\frac{\pm 1 \pm 3 \pm 5 \pm \ldots \pm (n-2)}{n}\right) \equiv \pm(\pm 1 + \pm 3 + \pm 5 + \ldots \pm (n-2))^{\frac{n-1}{2}}$ (mod n). Or cette somme est égale à

$$2^m(1.2.3.\ldots.m)1.3.5\ldots(2m-1) = 1.2.3.\ldots.2m = 1.2.3\ldots(n-1) \equiv -1 \pmod{n}.$$

Finalement, en remplaçant les ρ^k par $\left(\frac{k}{n}\right)$, le produit P et la somme Δ sont équivalents à -1 modulo n. On en déduit que $P = \Delta$.

Cauchy donne donc une détermination complète de la valeur de δ sans faire intervenir l'analyse : il utilise principalement des résultats sur les fonctions symétriques et alternées des racines primitives, et une correspondance entre une égalité et une congruence. Comme cela a déjà été vu dans notre première partie, il n'est pas le seul à tenter d'obtenir des démonstrations arithmétiques de résultats prouvés précédemment à l'aide de propriétés de l'analyse. Dans le cas du résultat considéré dans cette note, Kronecker en propose également une fondée sur des arguments élémentaires en 1856 dans le *Journal de Liouville*, en précisant :

> Le problème en question étant résolu par des considérations plus générales dans les deux Mémoires célèbres de Gauss et de M. Dirichlet, j'ai eu en vue seulement de donner une méthode qui puisse s'expliquer facilement dans des leçons sur la théorie des équations binômes. En considérant cette méthode que je viens d'exposer, on voit que j'ai réussi à trouver la valeur exacte de ε en me bornant à déterminer la valeur à laqeuelle ε est congrue suivant le module n [Kronecker, 1856, p. 394].

Kronecker indique également que sa démonstration est proche de celle de Cauchy dans

36. Cauchy précise que la somme des expressions $\pm(\pm a + \pm b \pm \ldots)^m$, où a, b, ... sont m nombres quelconques, ne peut contenir que des termes composés de puissances d'exposant non nul de tous les nombres a, b, ..., car, dans le cas contraire, le coefficient du terme serait nul. Finalement, cette somme, composée de 2^m termes de la forme $m!ab\ldots$ est donc égale à $2^m.1.2.3\ldots.m.ab\ldots$.

le sens où les deux preuves utilisent des arguments de la théorie des nombres, et particulièrement une congruence pour déterminer le signe de Δ. Par contre, pour obtenir la congruence en question, Kronecker ne remplace pas les ρ^h par $\left(\frac{h}{n}\right)$.

Cauchy conclut en indiquant que sa méthode peut être appliqué dans d'autres cas ; il donne quelques précisions concernant le cas cubique. Soit n un nombre premier de la forme $3x+1$, α une racine primitive cubique de l'unité et m une racine primitive de $x^{n-1} \equiv 1 \pmod{n}$. Dans ce cas, le produit P est de la forme

$$P = \left(\rho + \alpha\rho^{m^{\frac{n-1}{3}}} + \alpha^2\rho^{m^{2\frac{n-1}{3}}}\right)\left(\rho^m + \alpha\rho^{m^{1+\frac{n-1}{3}}} + \alpha^2\rho^{m^{1+2\frac{n-1}{3}}}\right)\ldots.$$

Ce produit est alors proportionnel au « facteur primitif de n »[Cauchy, 1840b, p. 165], ce dernier étant $\Theta = \rho + \alpha\rho^m + \alpha^2\rho^{m^2} + \rho^{m^3} + \ldots + \alpha^2\rho^{m^{n-2}}$, ce qui correspond à une somme de Gauss cubique. Puisque P et Θ sont proportionnel, Cauchy observe que le quotient $\frac{P}{\Theta}$ est de la forme $a + b\alpha$, où a et b sont des nombres entiers et peuvent être déterminés par les méthodes exposées précédemment. Ainsi, Cauchy ne le précise pas, mais P et α sont proportionnels dans l'ensemble $\mathbb{Z}[\alpha]$, où α est une racine cubique de l'unité. La prochaine note de Cauchy présentée à l'Académie traite d'ailleurs des sommes de Gauss cubiques.

8 - 13 avril 1840 : sommes de Gauss et résidus cubiques

L'exposé du 13 avril 1840 est intitulé *Sur la sommation de certaines puissances d'une racine primitive d'une équation binôme, et en particulier, des puissances qui offrent pour exposants les résidus cubiques inférieurs au module donné*[37] : Cauchy va développer des résultats similaires à ceux présentés lors de la séance précédente, mais relativement aux résidus cubiques d'un nombre premier p de la forme $3x+1$. Il met d'ailleurs en avant la ressemblance des deux méthodes dans son introduction :

> Supposons que, le module p étant du nombre de ceux qui, divisés par 3, donnent 1 pour reste, on élève une racine primitive aux diverses puissances qui offrent pour exposants les résidus cubiques. La somme de ces puissances, quand on y remplacera la racine primitive donnée par d'autres, pourra successivement acquérir trois valeurs distinctes, et ces trois valeurs seront les trois racines d'une équation connue, à laquelle on parvient à l'aide de la théorie de M. Gauss. D'ailleurs la fonction alternée la plus simple que l'on puisse former avec ces trois valeurs est le produit des trois différences que l'on obtient en les retranchant l'une de l'autre. Or la détermination complète de cette somme est évidemment un problème analogue à celui dont j'ai donné deux solutions nouvelles dans la dernière séance. Seulement ce nouveau problème est d'un ordre plus élevé, attendu que les résidus quadratiques se

37. Cette note est publiée sous le même titre dans le cinquième tome du *Journal de Liouville* en 1840.

> trouvent ici remplacés par des résidus cubiques. Mais, quoique, en raison de cette circonstance, la difficulté semble s'accroître, toutefois je parviens à la surmonter en suivant une marche semblable à celle que j'ai adoptée dans mon dernier Mémoire [Cauchy, 1840c, p. 166-167].

Dans le premier paragraphe, intitulé *Théorèmes divers, relatifs aux modules qui, divisés par 3, donnent l'unité pour reste*, Cauchy introduit les notations habituelles : p est un nombre premier impair, θ est une racine primitive de $x^p = 1$, t est une racine primitive de l'équivalence $x^{p-1} \equiv 1 \pmod{p}$. Les racines primitives de $x^p = 1$ peuvent donc s'écrire θ, θ^2, …, θ^{p-1} ou encore θ, θ^t, θ^{t^2}, …, $\theta^{t^{p-2}}$.

Il pose : $\mathcal{S} = \theta + \theta^t + \theta^{t^2} + \ldots \theta^{t^{p-2}}$ et rappelle que $\mathcal{S} = -1$.

Dans les travaux liés à la somme Δ et aux résidus quadratiques, Cauchy considérait d'une part les racines ρ^h, où h représentait les différents résidus quadratiques et d'autre part les racines ρ^k, où k représentait les différents résidus non-quadratiques. Ici, il considère les trois sommes de puissances de θ. Dans la première, les exposants sont les résidus cubiques t^{3k}, dans la seconde, les exposants sont des non-résidus cubiques de la forme t^{3k+1}, et dans la dernière, les exposants sont des non-résidus cubiques de la forme t^{3k+2} :

$$\begin{cases} \mathcal{S}_0 = \theta + \theta^{t^3} + \theta^{t^6} + \ldots + \theta^{t^{p-4}}, \\ \mathcal{S}_1 = \theta^t + \theta^{t^4} + \theta^{t^7} + \ldots + \theta^{t^{p-3}}, \\ \mathcal{S}_0 = \theta^{t^2} + \theta^{t^5} + \theta^{t^8} + \ldots + \theta^{t^{p-2}}. \end{cases}$$

Les sommes $\mathcal{S}_1$ et $\mathcal{S}_2$ sont respectivement obtenues à partir de $\mathcal{S}_0$ en remplaçant θ par θ^t et θ^{t^2}. De plus, si on remplace θ par une autre racine primitive de l'équation $x^p = 1$, on retrouvera toujours une de ces trois sommes. Remarquons que ces sommes correspondent aux périodes considérées par Gauss dans l'article 358 des *Disquisitiones Arithmeticae*, article dans lequel il démontre également que le quadruple d'un nombre premier de la forme $3k + 1$ peut être mis sous la forme $x^2 + 27y^2$.

Cauchy considère ensuite les sommes S_0, S_1 et S_2 : S_0 est la somme des puissances de θ dont les exposants sont les cubes des nombres entiers de 0 à $p - 1$, S_1 et S_2 sont les sommes obtenus en remplaçant θ respectivement par θ^t et θ^{t^2} dans S_0. Puisque la suite des résidus des puissances $\theta^{t^{3h}}$ est composée de $\frac{p-1}{3}$ termes distincts et est périodiques, il existe une relation entre les sommes $\mathcal{S}_i$ et S_i : $S_i = 1 + 3\mathcal{S}_i$.

D'autre part, soit t^{3m} un terme de la suite 1, t^3, t^6, …, t^{p-4}. Alors, la suite contiendra également un terme équivalent à $-t^{3m} = (-t^m)^3$. Or, $t^{\frac{p-1}{2}} = t^{3\frac{\varpi}{2}} \equiv -1 \pmod{p}$ (puisque t est une racine primitive de $x^{p-1} \equiv 1 \pmod{p}$), donc le terme équivalent à $-t^{3m}$ est $t^{\frac{p-1}{2}+3m} = t^{3\left(m+\frac{\varpi}{2}\right)}$.

Enfin, chacune des sommes $\mathcal{S}_i$ est composée de couples de racines de la forme θ^l et θ^{-l}. Or les sommes de la forme $\theta^l + \theta^l$ sont réelles donc les sommes considérées sont des quantités réelles. Cauchy se propose alors de déterminer les équations du troisième degré dont les sommes $\mathcal{S}_i$ d'une part et les sommes S_i d'autre part sont solutions.

Pour cela, Cauchy élève au carré la somme $\mathcal{S}_0$ et ordonne les termes obtenus de façon à ce que l'on puisse passer d'un terme d'une colonne à un autre de la même colonne en substituant à θ une des racines $\theta^{t^{3m}}$:

$$\left\{\begin{array}{lllll} \mathcal{S}_0^2 & = \theta^{1+1} & +\theta^{1+t^3} & +\theta^{1+t^6} & +\ldots \quad +\theta^{1+t^{p-4}} \\ & = \theta^{t^3+t^3} & +\theta^{t^3+t^6} & +\theta^{t^3+t^9} & +\ldots \quad +\theta^{t^3+1} \\ & & & & \\ & +\ldots & \ldots & \ldots & \ldots \quad \ldots \\ & +\theta^{t^{p-4}+t^{p-4}} & +\theta^{t^{p-4}+1} & +\theta^{p-4+t^3} & +\ldots \quad +\theta^{t^{p-4}+t^{p-7}} \end{array}\right.$$

Finalement, la somme des $\dfrac{p-1}{3}$ termes d'une des colonnes est toujours égale à une des sommes $\mathcal{S}_i$ ou à $\dfrac{p-1}{3}$, lorsque le premier terme est $\theta^{1+t^{\frac{p-1}{2}}} = \theta^0$.

Finalement : $\mathcal{S}_0^2 = \dfrac{p-1}{3} + a\mathcal{S}_0 + b\mathcal{S}_1 + c\mathcal{S}_2$, soit :

$$\left\{\begin{array}{ll} \mathcal{S}_0^2 = \dfrac{p-1}{3}\theta^0 & +a\left(\theta + \theta^{t^3} + \ldots + \theta^{t^{p-4}}\right) \\ & +b\left(\theta^t + \theta^{t^4} + \ldots + \theta^{t^{p-3}}\right) \\ & +c\left(\theta^{t^2} + \theta^{t^5} + \ldots + \theta^{t^{p-2}}\right) \end{array}\right.$$

Pour déterminer les coefficients a, b et c, Cauchy va utiliser une méthode similaire à celle utilisée dans la note précédente : il va remplacer dans les deux expressions données précédemment de $\mathcal{S}_0^2$ les termes θ^l par l^ϖ, où $\varpi = \dfrac{p-1}{3}$ et les considérer modulo p. Cette méthode est bien similaire à celle donnée dans le cas des résidus quadratiques puisque, d'après [Cauchy, 1829a], on a en général : $\left(\frac{k}{p}\right) \equiv k^{\frac{p-1}{n}} \pmod p$.

À partir de ces considérations, il obtient un système de trois équations pour les coefficients a, b et c, en fonction de r, racine primitive de l'équivalence $x^3 \equiv 1 \pmod p$ (donc $r = t^\varpi$) et de $\Pi = \dfrac{(\varpi+1)(\varpi+2)\ldots(2\varpi)}{1.2.3\ldots.\varpi}$:

$$\left.\begin{array}{l} a+b+c \equiv -\dfrac{1}{3} \\ a+br+cr^2 \equiv -\dfrac{2}{3} \\ a+br^2+cr \equiv -\dfrac{2}{3} - \dfrac{\Pi}{3} \end{array}\right\} \pmod p,$$

ainsi qu'une équation sont les $\mathcal{S}_i$ sont les trois solutions :

$$\mathcal{S}^3 + \mathcal{S}^2 + \varpi\mathcal{S} + \frac{\varpi^2 - 3\varpi - 1 - ap}{3} = 0.$$

À partir de cela, Cauchy retrouve notamment que l'équation $4p = A^2 + 27B^2$ est vérifiée pour $A \equiv -\Pi$, $B \equiv \frac{r^2-r}{9}\Pi \pmod{p}$ et rappelle que ce résultat est déjà donné dans [Jacobi, 1827].

La deuxième partie de ce mémoire, très courte, contient quelques réflexions sur les résultats obtenus précédemment. Cauchy conclut finalement :

> Au reste, les formules obtenues dans le premier paragraphe peuvent encore être déduites, comme je le montrerai dans un autre article, de la considération des facteurs primitifs du nombre premier p ; et l'on peut, à l'aide des mêmes méthodes, établir des formules analogues, qui soient relatives, non plus aux résidus cubiques, mais aux résidus des puissances supérieures à la troisième [Cauchy, 1840c, p. 180].

Cauchy n'a pas publié cet article ; cette conclusion confirme néanmoins que Cauchy veut obtenir des résultats sur les sommes de Gauss en utilisant sa notion de facteurs primitifs et en évitant l'utilisation de l'analyse.

9 - Un premier bilan sur les recherches de Cauchy relatives aux formes quadratiques

Dans cette série de notes, Cauchy semble avoir deux objectifs : développer une méthode générale pour obtenir des formes quadratiques de la forme $4p^\mu = x^2 + ny^2$, où n est un diviseur de $p-1$, et déterminer les valeurs de certaines sommes de Gauss en se limitant à des outils et résultats de la théorie des nombres[38]. Dans les deux cas, les travaux de Cauchy sont fondés sur des résultats présentés pour la première fois dans la section VII des *Disquisitiones Arithmeticae* sur les sommes de Gauss. Il utilise les racines primitives de nombres premiers pour obtenir des expressions symétriques et alternées de puissances de racines de l'unité et peut ainsi utiliser les propriétés de ces expressions abordées ici, puis détaillées dans son *Mémoires sur la théorie des nombres* de 1840. Dans la première note, il rappelle le résultat qu'il a énoncé en 1831 en lien avec les nombres de Bernoulli ; il ne se réfère néanmoins plus à ces nombres dans les notes suivantes. Il faut donc attendre la publication de son grand mémoire pour avoir une démonstration du lien existant entre les nombres de Bernoulli et la répartition des résidus et des non-résidus quadratiques.

Nous avons également noté à plusieurs reprises que certaines propriétés obtenues par Cauchy coïncident avec des résultats de Jacobi ou Dirichlet par exemple. Néanmoins, lorsque les deux auteurs allemands développent des réflexions sur les propriétés de certains

38. C'est le cas lorsque Cauchy utilise les congruences. Il donne également des preuves en lien avec les sommes de Gauss en utilisant des outils d'analyse. Par exemple, dans le premier paragraphe de [Cauchy, 1840b], Cauchy présente une méthode pour déterminer la valeur de la somme quadratique de Gauss Δ fondée sur les fonctions réciproques et les intégrales définies. De même, dans une note présentée le 11 mai 1840 à l'Académie des Sciences et intitulée *Sur quelques séries dignes de remarques, qui se présentent dans la théorie des nombres*, Cauchy utilise des intégrales afin d'obtenir des résultats sur les sommes de Gauss.

ensembles d'entiers complexes, comme $\mathbb{Z}[i]$ ou $\mathbb{Z}[\sqrt{-3}]$, Cauchy établit des égalités en lien avec ce qu'il appelle les facteurs primitifs pour obtenir des résultats sur des formes quadratiques faisant intervenir des entiers naturels, ou sur les sommes de Gauss. Nous allons maintenant détailler le contenu du grand *Mémoire sur la théorie des nombres* de Cauchy afin de connaître plus précisément les méthodes utilisées dans le cadre de ses recherches arithmétiques et de montrer que les premières conclusions tirées de l'analyse des premiers articles sont bien confirmées.

CHAPITRE 10

1840 : Le grand « *Mémoire sur la théorie des nombres* »

I Reconstruction de la méthode de Cauchy développée dans son « *Mémoire sur la théorie des nombres* » de 1840 : un exemple

1 - Présentation générale du mémoire

Ce *Mémoire sur la théorie des nombres* est un développement de l'article publié dans le douzième tome du *Bulletin de Férussac* en 1829. Dans son mémoire de 1829, Cauchy indique que ses travaux lui ont permis de découvrir une infinité de lois de réciprocité, thème qu'il ne reprend pas ici, sauf pour détailler la démonstration de la loi de réciprocité quadratique esquissée en 1829. L'objectif principal du mémoire est de résoudre des équations en nombres entiers de la forme $4p^\mu = x^2 + ny^2$ et $p^\mu = x^2 + ny^2$, où p est un nombre premier, et n un diviseur de $p-1$. Les méthodes générales qu'il développe dépendent de la forme du nombre premier p, et de celle du diviseur n. Dans la première partie, Cauchy traite le cas où n est un nombre premier. Il envisage le cas où n est un nombre composé dans les trois autres parties de son mémoire.

Cauchy indique que ce mémoire est celui qu'il a lu le 31 mai 1830. Sa publication a en effet été retardée par son absence de 8 années. Dans la partie principale du *Mémoire*, Cauchy n'expose pas ses intentions au lecteur (travail sur les formes quadratiques ou lois de réciprocité) et *a priori*, ne semble pas développer une méthode générale. Par exemple, il n'introduit à aucun moment la notion de facteurs primitifs, comme il l'a fait dans les *Comptes Rendus* et n'annonce pas explicitement que le procédé utilisé consiste justement à regrouper d'une certaine façon ces expressions. Néanmoins, comme nous allons le voir, c'est bien cette technique qui est utilisée ici. Ce texte ayant été lu pour la première fois en 1830 à l'Académie, cela montre que, même si cette approche a été explicitement utilisée par d'autres mathématiciens dans les années 1830, les courtes publications de Cauchy de 1829 et 1831 se basaient déjà sur celle-ci.

Enfin, Cauchy précise que, par rapport à son travail présenté en 1830 à l'Académie, il a ajouté des notes de bas de page et à la suite du mémoire, et supprimé « une grande partie des numéros placés devant les formules » [Cauchy, 1840a, p. 5]. Cette dernière affirmation est à relativiser. Par exemple, les formules sont numérotées de 1 à 59 dans le premier paragraphe et de 1 à 78 dans le second. D'autre part, comme nous l'avons signalé précédemment, les notes ajoutées au mémoire lu en 1830 à l'Académie nous semblent

réellement nécessaires à la compréhension du texte principal et ne sont pas référencées dans son texte principal. Cela rend la lecture de ce texte de Cauchy assez difficile et pour une meilleure compréhension du contenu de ce travail et un meilleur suivi des différentes démonstrations de Cauchy, nous découpons le mémoire en plusieurs parties et intégrons les notes dans l'exposé principal : nous détaillons dans un premier temps plusieurs notes, pour ensuite pouvoir comprendre le contenu du mémoire principal. Les numérotations des formules que nous utilisons sont par contre reprises du mémoire.

Avant de rentrer dans le texte de Cauchy, nous détaillons ci-dessous un exemple de reconstruction du texte en reproduisant un extrait du mémoire de Cauchy, et en indiquant entre crochets les différents ajouts nécessaires pour obtenir une démonstration complète de son raisonnement, et dans quelles parties du mémoire ces compléments sont donnés. Nous souhaitons en effet montrer la nature du travail qu'il a fallu entreprendre pour donner sens aux recherches de Cauchy (sans en reproduire la totalité, ce qui aurait été très fastidieux). Les formules énoncées par Cauchy dans cet extrait sont ensuite démontrées dans les sections suivantes.

2 - Un exemple de reconstruction

Nous avons reproduit ci-dessous les premières pages du mémoire de Cauchy où celui-ci démontre que, pour tout nombre premier impair p, et tout diviseur premier n de $p-1$ de la forme $4x+3$, on peut toujours trouver des nombres entiers X et Y tels que $4p^{\frac{n-1}{2}} = X^2+nY^2$. Avant cet extrait, Cauchy introduit les notations habituelles (données dans la section sur les préliminaires du chapitre précédent), il rappelle la notion d'indice de Gauss et une version équivalente de la définition généralisée du symbole de Legendre donnée dans [Cauchy, 1829a].

Nous indiquons tout au long du texte dans quelles parties de l'ouvrage de Cauchy sont démontrés les résultats indiqués. Les détails de ces compléments sont donnés dans les sections suivantes, l'objectif étant ici de mettre en avant les difficultés rencontrées à la lecture de ce texte. Nous avons utilisé une taille de police plus petite pour cet extrait et avons indiqué nos annotations entre crochets en caractères linéaux. Rappelons que $p = n\varpi + 1$.

Voici le texte de Cauchy :

Soient maintenant

(8) $$\Theta_h = \theta + \rho^h\theta^t + \rho^{2h}\theta^{t^2} + \ldots + \rho^{(p-2)h}\theta^{t^{p-2}}$$

et

(9) $$\Theta_h\Theta_k = R_{h,k}\Theta_{h+k}.$$

$R_{1,m}$ sera une fonction de ρ de la forme

$$R_{1,m} = a_0 + a_1\rho + a_2\rho^2 + \ldots + a_{n-1}\rho^{n-1};$$

et si l'on pose

$$k \equiv mh \pmod{n},$$

on aura, en supposant m différent de zéro et de $\frac{n}{2}$,

$$R_{h,mh} = a_0 + a_1\rho^h + a_2\rho^{2h} + \ldots + a_{n-1}\rho^{(n-1)h}$$

et

$$R_{h,k} = (-1)^{\varpi(h+k)} \sum \left(\frac{u}{p}\right)^h \left(\frac{v}{p}\right)^k, \tag{10}$$

le signe $\sum$ s'étendant à toutes les valeurs entières de u, v comprises entre les limites 1, $p-1$, et qui vérifieront l'équivalence

$$1 + u + v \equiv 0 \pmod{p}.$$

On aura d'ailleurs, en supposant h différent de zéro,

$$\Theta_h\Theta_{-h} = (-1)^{\varpi h}p, \; R_{h,-h} = -(-1)^{\varpi h}p, \tag{11}$$

et, en supposant h, k, ainsi que $h+k$ non divisibles par n,

$$R_{h,k}R_{-h,-k} = p. \tag{12}$$

On trouvera, au contraire

$$R_{h,0}R_{0,h} = -1. \tag{13}$$

Enfin l'on aura

$$a_0 + a_1 + a_2 + \ldots + a_{n-1} = p - 2 \tag{14}$$

et, en supposant n pair,

$$a_0 - a_1 + a_2 - a_3 + \ldots - a_{n-1} = -(-1)^{\varpi n}2. \tag{15}$$

[Les égalités 9 à 15 sont démontrées dans la note I pour le cas particulier où $\varpi = 1$; elles n'y sont néanmoins pas toujours formulées de la même façon. Par exemple, pour la formule (10), Cauchy n'utilise pas le symbole de Legendre dans la note I. Cauchy revient sur les égalités (14) et (15), et sur d'autres propriétés des coefficients des expressions $R_{h,k}$ dans la note V.]

Par suite, si l'on suppose

$$R_{h,k} = F(\rho), \tag{16}$$

[Le fait que $R_{h,k}$ ne dépend que de ρ est également démontré dans la note I.]

on trouvera

$$F(\rho^m) = R_{mh,mk} \quad \text{et} \quad F(\rho^m)F(\rho^{-m}) = p, \tag{17}$$

[L'égalité (17) est en fait l'égalité (13) de la note I.]

si le nombre m est tel qu'aucune des équations

$$\rho^{mh} = 1, \ \rho^{mk} = 1, \ \rho^{m(h+k)} = 1 \tag{18}$$

[Les égalités (18) sont traduites en termes de divisibilité par le nombre n dans la note I.]

ne soit vérifiée. On aura, au contraire,

$$F(\rho^m) = -(-1)^{\varpi mh - \varpi mk} \tag{19}$$

si une seule des équations (18) est satisfaite, et

$$F(\rho^m) = p - 2 \tag{20}$$

si les trois équations (18) subsistent simultanément.

Soient encore h, k, l trois nombres entiers propres à vérifier la condition

$$h + k + l \equiv 0 \pmod{n}. \tag{21}$$

On aura, en supposant ces nombres tous trois différents de zéro,

$$\Theta_h\Theta_k\Theta_l = (-1)^{\varpi l}\frac{\Theta_h\Theta_k}{\Theta_{h+k}} = (-1)^{\varpi k}\frac{\Theta_h\Theta_l}{\Theta_{h+l}} = (-1)^{\varpi h}\frac{\Theta_k\Theta_l}{\Theta_{k+l}}$$

et, par conséquent,

$$(-1)^{\varpi h}R_{k,l} = (-1)^{\varpi k}R_{l,h} = (-1)^{\varpi l}R_{k,h}. \tag{22}$$

Soit maintenant s une racine primitive de

$$x^{n-1} \equiv 1 \pmod{n}, \tag{23}$$

le nombre n étant supposé premier, et faisons

$$\Theta_1 \Theta_{s^2} \Theta_{s^4} \dots \Theta_{s^{n-3}} = \mathscr{F}(\rho) \tag{24}$$

on aura

$$\Theta_s \Theta_{s^3} \Theta_{s^5} \dots \Theta_{s^{n-2}} = \mathscr{F}(\rho^s) \tag{25}$$

et, de plus,

$$\mathscr{F}(\rho) = \mathscr{F}(\rho^{s^2}) = \mathscr{F}(\rho^{s^4}) = \dots = \mathscr{F}(\rho^{s^{n-3}}),$$

[Cauchy indique en note de bas de page que $1 + s^2 + s^4 + \dots + s^{n-3} \equiv 0 \pmod{n}$: c'est donc pour cette raison que le produit ci-dessus ne dépend que de ρ.]

$$\mathscr{F}(\rho^s) = \mathscr{F}(\rho^{s^3}) = \mathscr{F}(\rho^{s^5}) = \dots = \mathscr{F}(\rho^{s^{n-2}}).$$

Donc $\mathscr{F}(\rho)$ sera de la forme

$$\mathscr{F}(\rho) = c_0 + c_1(\rho + \rho^{s^2} + \rho^{s^4} + \dots + \rho^{s^{n-3}}) + c_2(\rho^s + \rho^{s^3} + \dots + \rho^{s^{n-2}}) \tag{26}$$

[Cauchy démontre que les expressions de la forme $R_{h,k,l\dots}$ sont symétriques par rapport aux puissances ρ^h, ρ^k, ρ^l dans la note III. Les propriétés des fonctions symétriques et alternées des racines primitives d'une équation binôme sont étudiées par Cauchy dans les notes VI et VII. Cela lui permet d'obtenir notamment la formule (26).]

ou

$$\mathscr{F}(\rho) = \frac{2c_0 - c_1 - c_2}{2} + \frac{c_1 - c_2}{2}(\rho - \rho^s + \rho^{s^2} - \rho^{s^3} + \dots + \rho^{s^{n-3}} - \rho^{s^{n-2}})$$

et, comme on aura

$$s^{\frac{n-1}{2}} \equiv -1 \pmod{n},$$

$$\rho + \rho^s + \rho^{s^2} + \dots + \rho^{s^{n-3}} + \rho^{s^{n-2}} = -1,$$

$$(\rho - \rho^s + \rho^{s^2} - \rho^{s^3} + \dots + \rho^{s^{n-3}} - \rho^{s^{n-2}})^2 = (-1)^{\frac{n-1}{2}} n,$$

[Cette dernière égalité correspond à une somme de Gauss quadratique déjà démontrée par Gauss dans [Gauss, 1801, Art. 356] et à la formule (14) obtenue par Cauchy dans la note I.] on trouvera

$$\mathscr{F}(\rho)\mathscr{F}(\rho^s) = \left(\frac{2c_0 - c_1 - c_2}{2}\right)^2 - (-1)^{\frac{n-1}{2}} n \left(\frac{c_1 - c_2}{2}\right)^2,$$

ou, ce qui revient au même,

$$4\mathscr{F}(\rho)\mathscr{F}(\rho^s) = (2c_0 - c_1 - c_2)^2 - (-1)^{\frac{n-1}{2}} n(c_1 - c_2)^2, \tag{27}$$

ou bien encore

$$\mathscr{F}(\rho)\mathscr{F}(\rho^s) = (c_0 - c_1)^2 + (c_0 - c_2)(c_1 - c_2) + \frac{1 - (-1)^{\frac{n-1}{2}} n}{4}(c_1 - c_2)^2. \tag{28}$$

Lorsque n est de la forme $4x + 3$, l'équation (27) ou (28) se réduit à

$$4\mathscr{F}(\rho)\mathscr{F}(\rho^s) = (2c_0 - c_1 - c_2)^2 + n(c_1 - c_2)^2 \tag{29}$$

ou bien à

$$\mathscr{F}(\rho)\mathscr{F}(\rho^s) = (c_0 - c_1)^2 + (c_0 - c_2)(c_1 - c_2) + \frac{n+1}{4}(c_1 - c_2)^2. \tag{30}$$

Au contraire, lorsque n est de la forme $4x + 1$, alors, $\frac{n-1}{2}$ étant pair, la formule (24) donne simplement

$$\mathscr{F}(\rho) = p^{\frac{n-1}{4}}$$

[Cette formule est démontrée dans la note III, dans laquelle Cauchy utilise implicitement des résultats démontrés dans les notes VI et VII.] et ρ disparaît de l'équation (26), qui se trouve réduite à la forme

$$\mathscr{F}(\rho) = c_0.$$

Revenons au cas où n est de la forme $4x + 3$. Comme on aura

$$\mathscr{F}(\rho)\mathscr{F}(\rho^s) = p^{\frac{n-1}{2}},$$

[Cette égalité est démontrée dans la note III, dans laquelle Cauchy utilise implicitement des résultats démontrés dans les notes VI et VII.] l'équation (29) donnera

$$4p^{\frac{n-1}{2}} = (2c_0 - c_1 - c_2)^2 + n(c_1 - c_2)^2.$$

Donc on résoudra l'équation

$$4p^{\frac{n-1}{2}} = X^2 + nY^2 \tag{31}$$

en prenant

$$X = 2c_0 - c_1 - c_2,\ Y = c_1 - c_2.$$

3 - Un résumé de la méthode de Cauchy

En faisant ce travail de reconstruction systématiquement, nous avons pu comprendre l'ensemble de cet article. Nous en détaillons les étapes dans les sections II à VII. Afin de

faciliter (ou de remplacer dans un premier temps) cette lecture, nous présentons ici les principaux points établis dans le mémoire de Cauchy et leur articulation dans le cadre de son travail sur les formes quadratiques.

Comme nous l'avons déjà vu dans les notes de Cauchy insérées dans les *Comptes rendus* de l'Académie des sciences, la méthode est basée sur l'utilisation d'expressions dépendant de racines primitives de l'unité : les sommes $\Theta_h = \theta + \rho^h\theta^t + \rho^{2h}\theta^{t^2} + \ldots + \rho^{(p-2)h}\rho^{t^{p-2}}$, où ρ est une racine primitive de $x^n = 1$ et t une racine primitive du nombre premier p, et les expressions $R_{h,k}$ définies à partir de l'égalité $\Theta_h\Theta_k = R_{h,k}\Theta_{h+k}$, et qui dépendent de ρ. D'une part, Cauchy étudie les propriétés de ces expressions, et plus généralement, les formes des fonctions symétriques et alternées dépendant de racines primitives de l'unité. Il prouve par exemple que toute fonction symétrique des racines n^{e} de l'unité ρ, ρ^2, $\ldots$, ρ^{n-1} (n nombre premier) est de la forme $a_0 + a_1(\rho + \rho^2 + \ldots + \rho^{n-1})$. D'autre part, il démontre des formules fondamentales qui lui permettent d'obtenir des égalités de la forme $4p^\mu = x^2 + ny^2$, où p est un nombre premier et n un diviseur de $p-1$. Parmi celles-ci, on retrouve notamment :

- $\Theta_h\Theta_k = R_{h,k}\Theta_{h+k}$;
- $\Theta_h\Theta_{-h} = (-1)^{h\varpi}p$;
- $(\rho - \rho^s + \rho^{s^2} - \rho^{s^3} + \ldots - \rho^{s^{n-2}})^2 = (-1)^{\frac{n-1}{2}}n$, où s est une racine primitive de n.

Il expose sa méthode sur les formes quadratiques en deux temps : il considère d'abord que le nombre n est premier, puis consacre une grande partie de la partie principale de son mémoire au cas où $n = \omega\nu$, ν premier. Dans ces deux cas, les principes généraux de sa méthode restent les mêmes : il construit des expressions à partir de produits dont les facteurs sont de la forme Θ_h afin d'obtenir l'égalité voulue.

Lorsque n est un nombre premier, il pose ainsi $\mathscr{F}(\rho) = \Theta_1\Theta_{s^2}\Theta_{s^4}\ldots\Theta_{s^{n-3}}$. Cette fonction entière est symétrique par rapport aux racines ρ, ρ^{s^2}, $\ldots$, $\rho^{s^{n-3}}$ d'une part et par rapport aux racines ρ^s, ρ^{s^3}, $\ldots$, $\rho^{s^{n-2}}$ d'autre part. Elle est donc de la forme $\mathscr{F}(\rho) = c_0 + c_1(\rho + \rho^{s^2} + \ldots + \rho^{s^{n-3}}) + c_2(\rho^s + \rho^{s^3} + \ldots + \rho^{s^{n-2}})$. Il prouve ensuite qu'elle peut être mise sous la forme $2\mathscr{F}(\rho) = A + B(\rho - \rho^s + \rho^{s^2} - \rho^{s^3} + \ldots - \rho^{s^{n-2}})$, où A et B sont des nombres entiers. Donc $2\mathscr{F}(\rho^s) = A - B(\rho - \rho^s + \rho^{s^2} - \rho^{s^3} + \ldots - \rho^{s^{n-2}})$. Par conséquent, le produit $4\mathscr{F}(\rho)\mathscr{F}(\rho^s)$ est de la forme $A^2 - (-1)^{\frac{n-1}{2}}nB^2$ et est également égal au quadruple d'une puissance de p d'après la deuxième formule fondamentale rappelée précédemment.

Finalement, lorsque n est de la forme $4k+3$, Cauchy obtient une égalité de la forme $4p^\mu = A^2 + nB^2$, où $\mu = \frac{n-1}{2}$. Il termine l'étude de ce cas en expliquant comment réduire au maximum l'exposant μ, en considérant le nombre de résidus et non-résidus quadratiques inférieurs à $\frac{n}{2}$ et établit le lien entre ces quantités et les nombres de Bernoulli.

Dans le cas où n est un diviseur composé de $p-1$, il pose dans un premier temps

$n = \omega\nu$, où ν est un facteur premier de n. Il introduit alors de nouvelles notations : ς et α sont des racines primitives respectives des équations $x^\nu = 1$ et $x^\omega = 1$ et s et u sont des racines primitives respectives des congruences $x^{nu} \equiv 1 \pmod{p}$ et $x^{\nu-1} \equiv 1 \pmod{\nu}$. Il donne une nouvelle définition pour les expressions Θ_h :

$$\Theta_h = \theta + \alpha^h \varsigma^h \theta^t + \alpha^{2h} \varsigma^{2h} \theta^{t^2} + \ldots + \alpha^{(p-2)h} \varsigma^{(p-2)h} \theta^{t^{p-2}}$$

et, même si les expressions et calculs en jeu sont plus longs, il construit comme précédemment une fonction entière produit de ces expressions, et ayant des propriétés de symétrie par rapport aux différentes racines primitives en jeu. Il obtient ainsi de nouveaux cas d'égalités de la forme $4p^\mu = x^2 + ny^2$, où n est un diviseur de $p - 1$.

II Premières propriétés des sommes Θ_h et $R_{h,k}$ (Note I)

Les notations et les propriétés fondamentales des sommes de Gauss et de Jacobi utilisées dans tout le mémoire sont listées sur trois pages, pratiquement sans aucune justification. Cauchy donne d'ailleurs une définition généralisée du symbole de Legendre, présentée différemment par rapport à son texte de 1829, bien qu'elle soit équivalente. Il rappelle d'abord la définition d'indice, sans se référer à Gauss : Soit k un nombre entier. Alors on note $m = I(k)$ lorsque $k \equiv t^m \pmod{p}$. Cependant, Cauchy ne précise pas que m doit être la plus petite puissance i telle que $k \equiv t^i \pmod{p}$.
Ainsi : $k^\varpi \equiv t^{m\varpi} \equiv r^m \equiv r^{I(k)}$. Il peut ensuite donner sa définition de $\left(\frac{k}{p}\right)$: $\left(\frac{k}{p}\right) = \tau^{m\varpi} = \rho^{I(k)}$.

Il détermine alors la valeur de $\left(\frac{-1}{p}\right)$ en remarquant que $I(-1) = \dfrac{n\varpi}{2}$, puisque t est une racine primitive de $x^{p-1} \equiv 1 \pmod{p}$, et donc [1] :
$\left(\frac{-1}{p}\right) = \rho^{I(-1)} = \rho^{\frac{n\varpi}{2}} = \tau^{\frac{n\varpi}{2}\varpi} = (-1)^\varpi$ car $\tau^{\frac{n\varpi}{2}} = -1$.
Finalement : $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{n}}$.

Il ajoute également que $\left(\frac{h}{p}\right)\left(\frac{k}{p}\right) = \left(\frac{hk}{p}\right)$.

Pour donner une idée des démonstrations de Cauchy en lien avec certaines propriétés des sommes de Gauss et de Jacobi, nous résumons la note I qui est très détaillée, dans laquelle Cauchy développe le cas particulier où $n = p - 1$ et donc $\varpi = 1$. À la fin de la note, il explique rapidement comment obtenir les formules pour le cas général où $p-1 = n\varpi$.

Dans un premier temps, il donne les définitions habituelles, où p est un nombre premier et n un nombre entier quelconque. En particulier, si ρ est une racine primitive de $x^n = 1$,

1. Dans le mémoire, il est indiqué que $\rho^{\frac{n\varpi}{2}} = \tau^{\frac{\varpi}{2}\varpi}$ ce qui me semble être une erreur d'impression.

alors les différentes racines de cette équation peuvent être exprimées sous la forme 1, ρ, ρ^2, …, ρ^{n-1}. De plus, l'équivalence $x^n \equiv 1 \pmod{p}$ admet n racines distinctes si n est un diviseur de $p-1$. Il rappelle ensuite une propriété de la somme des puissances ρ^{im}, où m est un nombre entier et où i est compris entre 0 et $n-1$:

$$1 + \rho^m + \rho^{2m} + \ldots + \rho^{(n-1)m} = \frac{\rho^{nm} - 1}{\rho^m - 1} = \begin{cases} n & \text{si } m \text{ est divisible par } n; \\ 0 & \text{si } m \text{ n'est pas divisible par } n. \end{cases}$$

Puis il donne la propriété équivalente pour la somme des puissances r^{im}, où r est une racine de l'équivalence $x^n \equiv 1 \pmod{p}$:

$$1 + r^m + r^{2m} + \ldots + r^{(n-1)m} = \frac{r^{nm} - 1}{r^m - 1} \equiv \begin{cases} n \pmod{p} & \text{si } m \text{ est divisible par } n; \\ 0 \pmod{p} & \text{si } m \text{ n'est pas divisible par } n. \end{cases}$$

Enfin, il rappelle que, si n est pair, on a $\rho^{\frac{n}{2}} = -1$ et $r^{\frac{n}{2}} \equiv -1 \pmod{p}$.

Ici, comme dans ses premiers mémoires, Cauchy donne parallèlement des propriétés liées à des égalités, puis les propriétés pour les congruences correspondantes, en remplaçant la racine primitive ρ par la racine primitive r. Même s'il ne fait aucune remarque explicite à ce sujet, Cauchy s'appuie donc sur une correspondance entre racines primitives d'équation et de congruence pour obtenir ces résultats.

Il introduit de nouvelles notations, semblables à celles du premier paragraphe, dans le cas où $n = p - 1$:

- p est un nombre premier impair.
- θ est une racine primitive de l'équation $x^p = 1$.
- τ est une racine primitive de l'équation $x^{p-1} = 1$.
- t est une racine primitive de l'équivalence $x^{p-1} \equiv 1 \pmod{p}$.

Les racines de $x^{p-1} \equiv 1 \pmod{p}$ peuvent être représentées par les termes de la progression arithmétique 1, 2, …, $p-1$ ou par les termes de la progression géométrique 1, t, t^2, …, t^{p-2}, donc :

$$1 + \theta + \theta^2 + \ldots + \theta^{p-1} = 0$$

et

$$1 + \theta^t + \theta^{t^2} + \ldots + \theta^{t^{p-2}} = 0. \tag{1}$$

Il applique également les résultats précédents à la racine primitive τ : $\tau^{\frac{p-1}{2}} = -1$ et

$$1+\tau^m+\tau^{2m}+\ldots+\tau^{(p-2)m}=\begin{cases} p-1 \pmod p & \text{si } m \text{ est divisible par } p-1;\\ 0 \pmod p & \text{si } m \text{ n'est pas divisible par } p-1.\end{cases} \qquad (\mathbf{A})$$

Il introduit alors les sommes Θ_h :

$$\Theta_h=\theta+\tau^h\theta^t+\tau^{2h}\theta t^2+\ldots+\tau^{(p-2)h}\theta^{t^{p-2}}$$

et donne trois propriétés[2] de la somme Θ_h : $\Theta_h=\Theta_k$ si $h\equiv k \pmod{p-1}$; $\Theta_0=-1$; et

$$\Theta_h\Theta_k=\sum_{i,j=0}^{p-2}\tau^{ih+jk}\theta^{t^i+t^j} \qquad (2)$$

En effet, seuls les exposants de τ dépendent de h et $\tau^{h+(p-1)k}=\tau^h\times\tau^{(p-1)k}=\tau^h$ puisque τ est une racine primitive de l'équation $x^{p-1}=1$. D'autre part, $\Theta_0=\theta+\theta^t+\theta^{t^2}+\ldots+\theta^{t^{p-2}}=-1$ d'après l'égalité (1). La dernière égalité est une application directe de la définition de Θ_h.

À partir de l'égalité (2), Cauchy détermine les valeurs de i et j rendant l'exposant de θ équivalent à des valeurs données modulo p. L'objectif est de démontrer l'égalité liant les sommes de Gauss avec les sommes de Jacobi : $\Theta_h\Theta_k=R_{h,k}\Theta_{h+k}$.

Dans un premier temps, Cauchy considère les valeurs de i et j telle que $\theta^{t^i+t^j}\equiv 1 \pmod p$: ce sont les valeurs de i et j telles que $t^i+t^j\equiv 0 \pmod p$, soit $t^{i-j}\equiv -1 \pmod p$ ou $t^{j-i}\equiv -1 \pmod p$.
Or, comme t est une racine primitive de $x^{p-1}\equiv 1 \pmod p$, $t^{\pm\frac{p-1}{2}}\equiv -1 \pmod p$. On en déduit donc que $j-i=\pm\dfrac{p-1}{2}$, soit $j=i\pm\dfrac{p-1}{2}$. Le $\pm$ dépend de la valeur de i (si elle est supérieure ou inférieure à $\frac{p-1}{2}$). Donc $\displaystyle\sum_{0\le i,j\le p-2 t^i+t^j\equiv 0 \pmod p}\tau^{ih+jk}\theta^{t^i+t^j}=\sum_{i=0}^{p-2}\tau^{i(h+k)}\tau^{\pm\frac{p-1}{2}k}$.
Finalement, on a $(p-1)$ couples (i,j) qui vérifient cette condition. La somme des termes en θ^0 sera donc égale à, en utilisant l'égalité (A) :

$$\sum_{i=0}^{p-2}\tau^{i(h+k)}\tau^{\pm\frac{p-1}{2}k}=(-1)^k\sum_{i=0}^{p-2}\tau^{i(h+k)}=\begin{cases}(-1)^k(p-1) & \text{si } h+k \text{ est divisible par } p-1;\\ 0 & \text{si } h+k \text{ n'est pas divisible par } p-1.\end{cases}$$

2. Voici comment Cauchy note la troisième égalité dans son mémoire :

$$\Theta_h\Theta_k=S(\tau^{ih+jk}\theta^{t^i+t^j})$$

le signe S s'étendant à toutes les valeurs de i et j comprises dans la suite

$$0,1,2,3,\ldots p-2$$

[Cauchy, 1840a, p. 87].

Il considère[3] ensuite les valeurs de i et j telle que $\theta^{t^i+t^j} \equiv \theta \pmod p$ sont les valeurs de i et j telles que $t^i + t^j \equiv 1 \pmod p$, soit $t^j \equiv 1 - t^i \pmod p$. Or, puisque i est compris entre 0 et $p-2$, seule la valeur $i = 0$ implique $1 - t^i \equiv 0 \pmod p$ donc il existe $(p-2)$ couples (i, j) tels que $t^j \equiv 1 - t^i \pmod p$, avec $1 - t^i \not\equiv 0 \pmod p$.

Cauchy considère pour commencer que $p-1$ ne divise pas $h+k$. Soit $R_{h,k}$ la somme des termes en θ^1 dans (2). Alors

$$R_{h,k} = \sum_{\substack{t^i+t^j \equiv 1 \pmod p \\ 0 \le i,j \le p-2}} \tau^{ih+jk}.$$

Cette somme se compose de $p-2$ termes, égaux à une des puissances τ^l, $0 \le l \le p-2$ donc

$$R_{h,k} = a_0 + a_1\tau + a_2\tau^2 + \ldots + a_{p-2}\tau^{p-2}, \tag{5}$$

où les a_i sont des coefficients entiers tels que

$$a_0 + a_1 + a_2 + \ldots + a_{p-2} = p - 2. \tag{6}$$

Enfin, Cauchy traite le cas général, toujours dans le cas particulier où $p-1$ ne divise pas $h+k$: les valeurs de i et j telle que $\theta^{t^i+t^j} \equiv \theta t^m \pmod p$, où $1 \le m \le p-2$ sont les valeurs de i et j telles que $t^i + t^j \equiv t^m \pmod p$. La somme des termes en θ^{t^m} est

$$\theta^{t^m} \sum_{\substack{t^i+t^j \equiv t^m \pmod p \\ 0 \le i,j \le p-2}} \tau^{ih+jk}$$

et $t^i + t^j \equiv t^m \pmod p$ équivaut à $t^{i-m} + t^{j-m} \equiv 1 \pmod p$.

3. Ici, Cauchy écrit

> Ces systèmes seront ceux pour lesquels l'équivalence
>
> $$t^i + t^j \equiv 1 \pmod p$$
>
> se trouvera vérifiée. Or, cette équivalence, présentée sous la forme
>
> $$t^j = 1 - t^i$$
>
> fournira une seule valeur de j, comprise dans la suite
>
> $$0, 1, 2, 3, \ldots, p-2,$$
>
> pour toute valeur de i, qui étant comprise dans cette même suite, ne rendra pas nulle la différence
>
> $$1 - t^i[\ldots]$$
>
> [Cauchy, 1840a, p. 88].

On remarque donc qu'il transpose sans commentaire une équivalence en équation.

Donc, « en faisant usage de la notation ci-dessus adoptée » [Cauchy, 1840a, p. 90] :

$$R_{h,k} = \sum_{\substack{t^{i-m}+t^{j-m}\equiv 1 \pmod p \\ 0\le i,j\le p-2}} \tau^{(i-m)h+(j-m)k} = \tau^{-m(h+k)} \sum_{\substack{t^{i-m}+t^{j-m}\equiv 1 \pmod p \\ 0\le i,j\le p-2}} \tau^{ih+jk},$$

soit

$$\sum_{\substack{t^{i-m}+t^{j-m}\equiv 1 \pmod p \\ 0\le i,j\le p-2}} \tau^{ih+jk} = R_{h,k}\tau^{m(h+k)}.$$

Finalement, la somme des termes en θ^{t^m} est égale à $R_{h,k}\tau^{m(h+k)}\theta^{t^m}$ et la somme des termes en puissances positives de θ est

$$\underbrace{R_{h,k}\sum_{m=0}^{p-2} \tau^{m(h+k)}\theta^{t^m}}_{\Theta_{h+k}}.$$

Donc, si $h+k$ n'est pas divisible par $p-1$:

$$\Theta_h\Theta_k = R_{h,k}\Theta_{h+k}, \tag{7}$$

où $R_{h,k} = \sum_{\substack{t^i+t^j\equiv 1 \pmod p \\ 0\le i,j\le p-2}} \tau^{ih+jk}$. On a donc :

$$\Theta_h\Theta_k = \Theta_{h+k} \sum_{\substack{t^i+t^j\equiv 1 \pmod p \\ 0\le i,j\le p-2}} \tau^{ih+jk}. \tag{8}$$

Cauchy revient ensuite sur le cas où $p-1$ divise $h+k$. On part de l'égalité précédente sachant que $h+k \equiv 0 \pmod{p-1}$, donc $h \equiv -k \pmod{p-1}$. Cauchy indique ici comment on trouve les valeurs de $R_{h,k}$:

> Donc, si l'on suppose la formule (7) étendue au cas où la somme $h+k$ est divisible par $p-1$, c'est-à-dire si, en choisissant $R_{h,k}$ de manière à vérifier dans tous les cas cette formule, on pose
>
> $$\Theta_{h,-h} = R_{h,-h}\Theta_0 \tag{9}$$
>
> [Cauchy, 1840a, p. 91].

On aura, puisque $h+k$ est divisible par $p-1$, et d'après la valeur calculée plus haut pour la somme des termes en θ^0 :

$$R_{h,-h} = \sum_{\substack{t^i+t^j\equiv 1 \pmod p \\ 0\le i,j\le p-2}} \tau^{(i-j)h} - (-1)^h(p-1).$$

$t^i + t^j \equiv 1 \pmod p$ entraîne $t^{i-j} \equiv t^{-j} - 1 \pmod{p-1}$. Comme t est une racine primitive de $x^{p-1} \equiv 1 \pmod p$, $t^{\frac{p-1}{2}} \equiv -1 \pmod p$ donc les valeurs de $i-j$ considérées dans la somme précédente sont telles que $i - j \neq \dfrac{p-1}{2}$. Or, la somme $S\tau^{(i-j)h}$ est nulle si elle contient toutes les valeurs de $i-j$ comprises entre 0 et $p-2$. Donc, si l'on considère cette même somme en éliminant la valeur correspondant à $i - j = \frac{p-1}{2}$, on obtient $-\tau^{\frac{p-1}{2}h} = -(-1)^h$.

Donc $R_{h,-h} = \sum_{\substack{t^i+t^j \equiv 1 \pmod p \\ 0 \leq i,j \leq p-2}} \tau^{(i-j)h} - (-1)^h(p-1) = -(-1)^h - (-1)^h(p-1) = -(-1)^h p.$

Finalement : si $p-1$ ne divise pas h, et puisque $\Theta_h\Theta_{-h} = R_{h,-h}\Theta_0$:

$$\Theta_h\Theta_{-h} = (-1)^h p \tag{11}$$

Comme nous l'avons vu dans le chapitre précédent, cette égalité est fondamentale pour ce qui va suivre sur les formes quadratiques ; les expressions θ_h et θ_{-h} sont ce que Cauchy appelle les facteurs primitifs dans ses notes publiées aux *Comptes Rendus* des séances de l'Académie des Sciences en 1840.

Si $p-1$ divise h, alors h est pair, et $(-1)^h = 1$ et $\tau^h = 1$ donc [4] :

$R_{h,-h} = \sum_{\substack{t^i+t^j \equiv 1 \pmod p \\ 0 \leq i,j \leq p-2}} \tau^{(i-j)h} - (-1)^h(p-1) = (p-2) - (p-1) = -1.$

Enfin, Cauchy donne encore des propriétés de $R_{h,k}$:

> Au reste, on peut conclure immédiatement de la formule (7) : 1° que la valeur de $R_{h,k}$ ne varie pas lorsqu'on fait croître ou décroître h ou k d'un multiple de $p-1$; 2° que $R_{h,k}$ se réduit à -1 dès que l'une des quantités h, k est divisible par $p-1$ [Cauchy, 1840a, p. 92].

Toujours d'après la formule (7), on a $\Theta_h\Theta_k = R_{h,k}\Theta_{h+k}$ et $\Theta_{-h}\Theta_{-k} = R_{-h,-k}\Theta_{-h-k}$. En multipliant ces deux égalités, on obtient :

$$\Theta_h\Theta_{-h}\Theta_k\Theta_{-k} = R_{h,k}\Theta_{h+k}R_{-h,-k}\Theta_{-h-k}.$$

Donc, d'après (11) :

$$(-1)^h p(-1)^k p = R_{h,k}R_{-h,-k}(-1)^{h+k}p$$

soit, lorsque h, k et $h+k$ ne sont pas divisibles par $p-1$:

$$R_{h,k}R_{-h,-k} = p. \tag{13}$$

4. Les deux égalités précédentes sont représentées comme des équivalences dans le texte de Cauchy : $(-1)^h \equiv 1$ et $\tau^h \equiv 1$.

Cette formule, fondamentale pour la suite, donne une décomposition du nombre premier p en deux nombres complexes, mais Cauchy ne fait aucune remarque à ce sujet.

Pour finir, Cauchy indique que pour obtenir les formules du premier paragraphe de son mémoire, il suffit de remplacer h par ϖh, k par ϖk, ...

Il remarque également que, dans (11), si $h = \frac{p-1}{2}$, et comme $\Theta_{-\frac{p-1}{2}}\Theta_{\frac{p-1}{2}} = \Theta^2_{\frac{p-1}{2}}$ puisque $-\frac{p-1}{2} \equiv \frac{p-1}{2} \pmod{p-1}$, on obtient :

$$\Theta^2_{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} p \tag{14}$$

soit

$$(\theta - \theta^t + \theta^{t^2} + \ldots + \theta^{t^{p-3}} - \theta^{t^{p-1}})^2 = (-1)^{\frac{p-1}{2}} p, \tag{14}$$

ce qui « fournit un théorème, très remarquable, de M. Gauss » [Cauchy, 1840a, p. 94]. C'est l'expression qu'il note habituellement Δ. Là encore, c'est une égalité qu'il utilise à de nombreuses reprises dans la partie principale de son mémoire et dans les quatorze notes qui le complètent.

III Racines primitives d'une équation binôme, fonctions symétriques et alternées de ces racines

Ce sujet a été rencontré à plusieurs reprises dans les notes insérées aux *Comptes Rendus*. Ici, Cauchy donne des propriétés des fonctions symétriques et alternées des puissances de racines primitives, des exposants de ces puissances et reproduit des raisonnements pratiquement identiques à ce que l'on peut retrouver dans les *Comptes Rendus*.

1 - Propriétés des fonctions symétriques des racines primitives (Note VI)

Dans la sixième note, intitulée *Sur la somme des racines primitives d'une équation binôme, et sur les fonctions symétriques de ces racines*, Cauchy démontre notamment que toute fonction f symétrique des racines primitives de l'équation $x^n = 1$, lorsque n est un nombre premier, est de la forme $f(\rho) = a_0 + a_1(\rho + \rho^2 + \ldots + \rho^{n-1})$.

Cauchy commence par énoncer des théorèmes sur les racines primitives d'équations binômes de la forme $x^n = 1$ où n est un nombre composé puis il montre que les fonctions symétriques de la forme $f(\rho) = \sum_{i=0}^{n-1} a_i \rho^i$ sont des fonctions linéaires de la somme $\sum_{i=0}^{n-1} \rho^i$.

Soient m et n, des nombres entiers et ω, leur plus grand diviseur commun. Cauchy rappelle alors qu'il existe des quantités u et v telles que $mu - nv = \omega$. Donc, une racine commune des équations $x^m = 1$ et $x^n = 1$ est également racine de l'équation $x^\omega = 1$. De plus, si x est une racine primitive de $x^n = 1$, alors x est racine de $x^m = 1$ seulement si m est divisible par n.

Soit n un nombre entier quelconque. ρ est une racine primitive de l'équation

$$x^n = 1, \tag{1}$$

et on désigne par h, k, l les nombres entiers inférieurs à n et premiers à n. Cauchy rappelle pourquoi [5] les nombres ρ^h, ρ^k, ρ^l représentent les différentes racines primitives de l'équation $x^n = 1$. De plus, si m est premier à n, les nombres ρ^{mh}, ρ^{mk}, ρ^{ml}, ... représentent également les racines primitives de $x^n = 1$. Finalement :

> Donc, si m devient premier à n, les diverses racines primitives de l'équation (1) pourront être représentées, soit par les termes de la suite
>
> $$\rho^h, \rho^k, \rho^l, \dots,$$
>
> soit par les termes de la suite
>
> $$\rho^{mh}, \rho^{mk}, \rho^{ml}, \dots,$$
>
> qui coïncideront avec les termes de la première, rangés dans un ordre différent[Cauchy, 1840a, p. 224-225].

Cauchy expose ensuite comment déterminer les racines primitives de l'équation (1) lorsque le nombre n est composé de plusieurs facteurs. Par exemple, si $n = \varphi\chi$, où φ et χ sont premiers entre eux, et si ξ et η sont des racines primitives respectives des équations $x^\varphi = 1$ et $x^\chi = 1$. Le produit $(\xi\eta)^m$ est égal à 1 si m est divisible par φ et par χ, c'est-à-dire si m est divisible par n. Donc $x = \xi\eta$ est racine de l'équation $x^n = 1$. Réciproquement, si m est tel que $(\xi\eta)^m$, alors $(\eta\xi)^{m\varphi} = 1$ et $\eta^{m\varphi} = 1$, soit $m\varphi \equiv 0 \pmod{\chi}$, d'où $m \equiv 0 \pmod{\chi}$. De même, $m \equiv 0 \pmod{\varphi}$. Donc pour que $(\xi\eta)^m = 1$, m doit être divisible par φ et χ, et donc par $\varphi\chi = n$ puisque φ et χ sont premiers entre eux. On en déduit que n est la plus petite puissance de $(\eta\xi)$ vérifiant (1) : $\eta\xi$ est donc une racine primitive de l'équation (1). Enfin, « chaque racine primitive ρ de l'équation (1) ne pourra être formée que d'une seule manière par la multiplication de deux racines primitives propres à vérifier les équations » [Cauchy, 1840a, p. 226] $x^\varphi = 1$ et $x^\chi = 1$. En effet, si ξ et ξ_1 sont des racines primitives de

5. En effet, d'après ce qui précède, ρ est racine de l'équation $x^{mh} = 1$, si m est divisible par n, et on en déduit que ρ^{nh} est la plus petite puissance de ρ^h égale à 1.

$x^\varphi = 1$ et η, η_1 sont des racines primitives de $x^\chi = 1$, et si $\xi\eta = \xi_1\eta_1$, alors $(\xi\eta)^\varphi = (\xi_1\eta_1)^\varphi$, soit $\eta^\varphi = \eta_1^\varphi$. Donc $\left(\frac{\eta_1}{\eta}\right)^\varphi = 1$ et $\left(\frac{\eta_1}{\eta}\right)^\chi = 1$. $\frac{\eta_1}{\eta}$ est donc une racine commune des équations $x^\varphi = 1$ et $x^\chi = 1$. Donc $\frac{\eta_1}{\eta}$ est également racine de l'équation $x^{\mathrm{PGCD}(\varphi,\chi)} = 1$, soit $x = 1$ puisque χ et φ sont premiers entre eux. Finalement : $\frac{\eta_1}{\eta} = 1$, soit $\eta_1 = \eta$. De même, on trouve $\xi_1 = \xi$. Finalement, Cauchy énonce le premier théorème de cette note :

> **Théorème I.** - *Si le nombre entier n est le produit de deux facteurs φ, χ premiers entre eux, on obtiendra les diverses racines primitives de l'équation*
>
> $$x^n = 1$$
>
> *et on les obtiendra chacune d'une seule manière, en multipliant successivement les diverses racines primitives de l'équation*
>
> $$x^\varphi = 1$$
>
> *par chacune des racines primitives de l'équation*
>
> $$x^\chi = 1.$$

Cauchy obtient alors deux théorèmes. avec les mêmes notations que précédemment, si $x^n = 1$ admet N racines primitives ρ, ρ_1, ρ_2, …, $x^\varphi = 1$ admet ϕ racines primitives ξ, ξ_1, ξ_2, …et $x^\chi = 1$ admet X racines primitives η, η_1, η_2, …, alors

- $\rho + \rho_1 + \rho_2 + \ldots = (\xi + \xi_1 + \xi_2 + \ldots)(\eta + \eta_1 + \eta_2 + \ldots)$;
- $N = \phi X$.

Cauchy en déduit des résultats similaires dans le cas où le nombre n est le produit d'un nombre quelconque de facteurs premiers entre eux, ce qui vaut pour n'importe quel nombre n : il suffit de considérer sa décomposition en facteurs premiers.

Cauchy applique ensuite ces théorèmes aux divers cas possibles. On désigne par $\mathscr{S}$ la somme des racines primitives de l'équation $x^n = 1$ et N le nombre de racines primitives de cette équation.

- Si $n = 2$, $x^2 = 1$ admet une seule racine primitive : -1. Donc $\mathscr{S} = -1$ et $N = 1$.

- Si n est un nombre premier impair, les racines primitives de $x^n = 1$ sont les puissances de ρ, dont l'exposant est inférieur et premier à n, soit : ρ, ρ^2, …, ρ^{n-1}. Donc $\mathscr{S} = \sum_{i=1}^{n-1} \rho^i = \frac{\rho^n - \rho}{\rho - 1} = \frac{1 - \rho}{\rho - 1}$.
  Donc $\mathscr{S} = -1$ et $N = n - 1$.

- Si n est une puissance de 2, les racines primitives de $x^n = 1$ sont les puissances de ρ dont l'exposant est impair et inférieur à n donc

$\mathscr{S} = \rho + \rho^3 + \ldots + \rho^{n-1} = \dfrac{\rho^{n+1} - \rho}{\rho^2 - \rho} = 0$

Donc $= 0$ et $N = \frac{n}{2}$.

Cauchy remarque également que $\rho^{\frac{n}{2}} = -1$, et que $\rho^{\frac{n}{2}+h} = -\rho^h$ donc les racines primitives de $x^n = 1$ seront égales à $\pm\rho$ et leur somme sera bien nulle.

- Si $n = \nu^a$, où ν est un nombre premier impair, les racines primitives de $x^n = 1$ sont les ρ^i, $0 \leq i \leq n-1$, sauf celles dont l'exposant i n'est pas premier à $n = \nu^a$ soit

$$\rho^0, \rho^\nu, \rho^{2\nu}, \ldots \rho^{n-\nu} = \rho^{(\frac{n}{\nu}-1)\nu}.$$

Ces $\frac{n}{\nu}$ racines sont les racines de l'équations $x^{\frac{n}{\nu}} = 1$ et leur somme est nulle, comme la somme des racines de l'équation $x^n = 1$. Finalement : la somme des racines primitives de $x^n = 1$ est égale à la différence de la somme des racines de $x^n = 1$ avec la somme des racines de $x^{\frac{n}{\nu}} = 1$: elle est donc nulle également.

Finalement : $\mathscr{S} = 0$ et $N = n - \frac{n}{\nu} = n\left(1 - \frac{1}{\nu}\right) = \nu^{a-1}\left(1 - \frac{1}{\nu}\right)$.

- Si n est un nombre quelconque dont la décomposition en facteurs premiers est : $n = \nu^a \nu'^b \nu''^c \ldots$, alors N et $\mathscr{S}$ se déduisent des résultats précédents. À l'aide des notations précédentes, si l'on pose $\varphi = \nu^a$, $\chi = \nu'^b$, $\ldots$, alors $\phi = \nu^a\left(1 - \frac{1}{\nu}\right)$, $X = \nu'^b\left(1 - \frac{1}{\nu'}\right)$, $\ldots$, soit

$$N = n\left(1 - \frac{1}{\nu}\right)\left(1 - \frac{1}{\nu'}\right)\left(1 - \frac{1}{\nu''}\right)\ldots \tag{16}$$

D'autre part, $\mathscr{S}$ sera égal au produit des sommes des racines primitives des équations $x^{\nu^a} = 1$, $x^{\nu'^b} = 1$, $\ldots$ donc deux cas sont possibles :

– Si n est composé d'au moins deux facteurs égaux entre eux, alors $\mathscr{S} = 0$.

– Si n est un nombre premier et composé de facteurs premiers tous distincts, alors $\mathscr{S} = 1$ si le nombre de facteurs est pair, et $\mathscr{S} = -1$ si le nombre de facteurs est impair.

On considère maintenant une fonction entière d'une racine primitive ρ de $x^n = 1$, notée $f(\rho)$. Puisque $\rho^n = 1$, $f(\rho)$ est de la forme

$$f(\rho) = a_0 + a_1\rho + a_2\rho^2 + \ldots + a_{n-1}\rho^{n-1}, \tag{22}$$

où les a_i sont des *coefficients indépendant de* ρ. Cauchy ajoute une propriété supplémentaire à la fonction f :

> Supposons d'ailleurs que, dans la fonction $f(\rho)$, les différents termes se trans-

forment les uns dans les autres, quand on y remplace la racine primitive ρ par une autre racine primitive ρ^m. Alors $f(\rho)$ sera ce qu'on peut nommer une *fonction symétrique* des racines primitives de l'équation (1), ou, ce qui revient au même, une fonction symétrique des puissances ρ^h, ρ^k, ρ^l, ..., h, k, l, ..., étant les entiers inférieurs à n et premiers à n [Cauchy, 1840a, p. 235].

Cela signifie que les coefficients des ρ^h, ρ^k, ρ^l, ..., seront les mêmes. De même, si n n'est pas un nombre premier et i un nombre entier positif, les coefficients des termes en ρ^{ih}, ρ^{ik}, ρ^{il}, ..., (soit les racines primitives d'une équation de la forme $x^\omega = 1$, où ω divise n) seront également les mêmes. Finalement :

> [...] une telle fonction se réduira toujours à une fonction linéaire des diverses valeurs que peut acquérir la somme des racines primitives de l'équation $[x^\omega = 1]$, quand on prend successivement pour ω chacun des diviseurs du nombre n, y compris ce nombre lui-même [Cauchy, 1840a, p. 236].

Par exemple, si le nombre n est premier, alors la fonction $f(\rho)$ est de la forme

$$f(\rho) = a_0 + a_1(\rho + \rho^2 + \ldots + \rho^{n-1}). \tag{24}$$

Ce résultat est important car il permet à Cauchy d'obtenir des résultats dans la partie principale du mémoire.

Cauchy termine cette note en expliquant pourquoi, si n est premier, $h < n$ et s une racine primitive de $x^{n-1} \equiv 1 \pmod{n}$, les trois suites

$$\rho, \rho^2, \rho^3, \ldots, \rho^{n-1};$$

$$\rho, \rho^s, \rho^{s^2}, \ldots, \rho^{s^{n-2}}$$

$$\rho^h, \rho^{sh}, \rho^{s^2 h}, \ldots, \rho^{s^{n-2} h}$$

contiennent chacune toutes les racines primitives de $x^n = 1$.

2 - Propriétés des fonctions alternées des racines primitives (Note VII)

Dans la note suivante, Cauchy étudie les propriétés d'expressions contenant des sommes alternées de racines primitives. Dans cette note, *Sur les sommes alternées des racines primitives des équations binômes et sur les fonctions alternées de ces racines*, Cauchy entreprend le même travail que dans la note précédente à partir de fonctions alternées des racines primitives de $x^n = 1$. Il distingue les cas où n est un produit de facteurs premiers tous distincts ou non. Il commence par déterminer la valeur de la somme alternée des racines primitives de l'équation $x^n = 1$ en fonction de la forme de n, puis en

déduit des résultats sur les fonctions alternées des racines primitives de la même équation.

On utilise les mêmes notations que dans la note précédente. Cauchy va démontrer que l'on peut partager les entiers h, k, l, ..., en deux groupes h, h', h'', ... et k, k', k'', ... et donc partager les racines primitives de l'équation $x^n = 1$ en deux groupes : ρ^h, $\rho^{h'}$, $\rho^{h''}$, ... et ρ^k, $\rho^{k'}$, $\rho^{k''}$, ..., « de telle sorte qu'après la substitution de ρ^m à ρ, les deux derniers groupes se trouvent encore composés chacun des mêmes racines, ou transformés l'un dans l'autre » [Cauchy, 1840a, p. 240]. Cauchy illustre ce partage des racines primitives avec le cas particulier où $n = 5$. Pour pouvoir partager les racines primitives de $x^n = 1$ en deux groupes répondant aux conditions exposées précédemment, le nombre N de ces racines primitives doit être pair pour que les deux groupes contiennent chacun le même nombre $\frac{n}{2}$ de racines.

(a) Calcul de la somme alternée des racines primitives de $x^n = 1$

Cauchy introduit alors la somme alternée

$$\mathcal{S} = \rho^h + \rho^{h'} + \rho^{h''} + \ldots - \rho^k - \rho^{k'} - \rho^{k''} - \ldots, \tag{2}$$

qui est invariable ou qui change seulement de signe lorsque l'on remplace la racine primitive ρ par une autre racine primitive ρ^m.

Si la substitution de ρ^m à ρ laisse invariable la somme $\mathcal{S}$, alors les termes ρ^l, ρ^{ml}, $\rho^{m^2 l}$, ..., $\rho^{m^{\iota-1} l}$, où ι est l'indice[6] de m modulo n, sont affectés du même signe. Par contre, si le signe de $\mathcal{S}$ est modifié après substitution de ρ^m à ρ, alors les termes $\rho^{m^i l}$ et $\rho^{m^{i+1} l}$ sont affectés de signes contraires. Ainsi, ρ^l et $\rho^{m^i l}$ seront affectés du même signe si i est pair, et de signes contraires si i est impair. En particulier, ρ^l et $\rho^{m^2 l}$ sont affectés du même signe. On suppose pour la suite que l'exposant 1 fait partie du groupe h, h', h'', ..., donc, pour tout nombre m premier à n, ρ et ρ^{m^2} sont affectés du même signe. On en déduit que le groupe h, h', h'', ..., contient tous les exposants équivalents à des carrés modulo n, soit les résidus quadratiques relatifs modulo n.

Cauchy va maintenant déterminer la valeur de $\mathcal{S}$ en fonction de la valeur de n.

n est un nombre premier impair ou une puissance d'un nombre premier impair

6. c'est-à-dire la plus petite puissance de m équivalente à l'unité modulo n.

Dans ce cas, les entiers $h, k, l, \ldots$, sont racines de $x^N \equiv 1 \pmod{n}$. Parmi ces nombres, $\frac{N}{2}$ sont des résidus quadratiques et vérifient $x^{\frac{N}{2}} \equiv 1 \pmod{n}$, $\frac{N}{2}$ sont des non-résidus quadratiques et vérifient $x^{\frac{N}{2}} \equiv -1 \pmod{n}$. D'après ce qui précède, on peut dire que h, h', h'', ... sont les $\frac{N}{2}$ résidus quadratiques et k, k', k'', ..., sont $\frac{N}{2}$ non-résidus quadratiques. Si s est une racine primitive de $x^N \equiv 1 \pmod{n}$, alors h, h', h'', ... sont représentés par les nombres 1, s^2, s^4, ..., s^{N-2} et on obtient donc la somme alternée

$$\mathcal{S} = \rho - \rho^s + \rho^{s^2} - \rho^{s^3} + \ldots - \rho^{s^{N-1}}. \tag{8}$$

Si n est un nombre premier impair, alors $N = n - 1$, et (8) devient

$$\mathcal{S} = \rho - \rho^s + \rho^{s^2} - \rho^{s^3} + \ldots - \rho^{s^{n-2}}, \tag{9}$$

où s est une racine primitive de $x^{n-1} \equiv 1 \pmod{n}$.

D'après la formule (14) de la note I, on a

$$(\rho - \rho^s + \rho^{s^2} - \rho^{s^3} + \ldots - \rho^{s^{n-2}})^2 = (-1)^{\frac{n-1}{2}} n, \tag{11}$$

soit

$$\mathcal{S}^2 = (-1)^{\frac{n-1}{2}} n. \tag{12}$$

Le nombre n étant premier impair, on en déduit :

- $\mathcal{S}^2 = n$ et $\mathcal{S} = \pm\sqrt{n}$ si $n = 4x + 1$;
- $\mathcal{S}^2 = -n$ et $\mathcal{S} = \pm n^{\frac{1}{2}}\sqrt{-1}$ si $n = 4x + 3$.

Le signe dépend de la racine primitive choisie au départ.

Si n est une puissance d'un nombre premier impair : $n = \nu^a$, où $a > 1$. D'après ce qui précède, ρ^l et $\rho^{l'}$ sont affectés du même signe dans $\mathcal{S}$ s'il existe un m tel que $l' \equiv m^2 l \pmod{n}$, c'est-à-dire si $\frac{l}{l'}$ est un résidu quadratique modulo n. $\frac{l}{l'}$ doit donc être racine de l'équivalence $x^{\frac{N}{2}} \equiv 1 \pmod{n}$. Cauchy montre que c'est le cas[7] si $l' \equiv l \pmod{\nu}$. Donc, si $n = \nu^a$, $a > 1$, les termes en ρ^l, $\rho^{l+\nu}$, $\rho^{l+2\nu}$, ..., $\rho^{l+n-\nu} = \rho^{l+\nu(\frac{n}{\nu}-1)}$ sont affectés du même signe dans la somme $\mathcal{S}$. Or :

7. En effet, si $l' \equiv l \pmod{\nu}$, alors $l'^{\nu} \equiv l^{\nu} \pmod{\nu^2}$, $l'^{\nu^2} \equiv l^{\nu^2} \pmod{\nu^3}$, ..., $l'^{\nu^{a-1}} \equiv l^{\nu^{a-1}} \pmod{\nu^a}$. Donc $\left(\frac{l'}{l}\right)^{\nu^{a-1}} \equiv 1 \pmod{n}$. Il suffit alors d'élever cette égalité à la puissance $\frac{\nu-1}{2}$: $\nu^{a-1}\frac{\nu-1}{2} = \frac{N}{2}$, et on obtient l'égalité voulue.

$\rho^l + \rho^{l+\nu} + \rho^{l+2\nu} + \ldots + \rho^{l+n-\nu} = \rho^l \dfrac{1-\rho^n}{1-\rho^\nu} = 0$. Finalement : $\mathcal{S} = 0$ lorsque $n = \nu^a$, $a > 1$, ν nombre premier impair.

n est une puissance de 2

Si $n = 2$, il n'y a qu'une seule racine primitive : -1. C'est le seul cas où N n'est pas pair.

Considérons le cas où n est une puissance de 2. Cauchy distingue trois cas différents.

Tout d'abord, on suppose que $n = 4$: $h = 1$, $k = 3$ et $\mathcal{S} = \rho - \rho^3$ est une somme alternée des racines primitives de l'équation $x^4 = 1$. On a également [8] : $\mathcal{S} = 2\rho = \pm 2\sqrt{-1}$, donc $\mathcal{S}^2 = -4$.

Si $n = 8$, on distingue trois cas :

- $h = 1$, $h' = 3$, $k = 5$, $k' = 7$, et $\mathcal{S} = \rho + \rho^3 - \rho^5 - \rho^7$, ce qui donne $\mathcal{S} = -8$. En effet, d'après la note précédente : $\rho + \rho^3 + \rho^5 + \rho^7 = 0$, soit $\rho + \rho^3 = -\rho^5 - \rho^7$, donc $\mathcal{S} = 2\rho + 2\rho^3$. Donc $\mathcal{S}^2 = 4(\rho^2 + \rho^6) + 8\rho^4$. Toujours d'après la note précédente, $\rho^2 + \rho^6 = 0$ et $\rho^4 = -8$. Finalement : $\mathcal{S}^2 = -8$.
- $h = 1$, $h' = 5$, $k = 3$, $k' = 7$, et $\mathcal{S} = \rho + \rho^5 - \rho^3 - \rho^7 = 2\rho + 2\rho^5 = 0$.
- $h = 1$, $h' = 7$, $k = 3$, $k' = 5$ et $\mathcal{S} = \rho + \rho^7 - \rho 3 - \rho 5 = 2\rho + 2\rho^7$, soit $\mathcal{S}^2 = 4\rho^6 + 4\rho + 8\rho^8 = 8$.

Si n est une puissance de 2, supérieure à la troisième. On pose $l' = l + \frac{n}{2}$ et on choisit d tel que $ld \equiv 1 \pmod{n}$, soit $\frac{1}{l} \equiv d \pmod{n}$. Alors $\frac{l'}{l} \equiv 1 + \frac{n}{2}d \pmod{n}$, ce qui revient à [9] $\frac{l'}{l} \equiv \left(1 + \frac{n}{4}d\right)^2 \pmod{n}$. Donc l' est équivalent au produit $m^2 l$, où m est premier à n, c'est-à-dire impair. Donc ρ et $\rho^{l'}$ sont affectés de signes contraires dans une somme alternée $\mathcal{S}$. D'autre part, comme ρ est une racine primitive de $x^n = 1$, alors $\rho^{\frac{n}{2}} = -1$ et $\rho^{l'} = -\rho^l$, soit $\rho^l + \rho^{l'} = 0$. Comme ρ^l et $\rho^{l'}$ sont affectés du même signe, la somme $\mathcal{S}$ est composée de sommes partielles nulles, donc $\mathcal{S} = 0$.

Cas général

Cauchy résume les résultats obtenus pour les cas particuliers précédents avant de passer au cas général. On considère un nombre n entier quelconque donc la décomposition en facteurs premiers est $n = \nu^a \nu'^b \nu''^c \ldots$. Une racine primitive ρ de l'équation $x^n = 1$ est

8. Cauchy ne précise pas s'il obtient cela en utilisant les valeurs des racines primitives de $x^4 = 1$, ou s'il utilise ce qu'il a démontré dans la note précédente : la somme des racines primitives de $x^n = 1$ est nulle si n admet plusieurs facteurs égaux.

9. En effet, $\left(1 + \frac{n}{4}d\right)^2 = 1 + \dfrac{n}{2}d + \dfrac{n^2}{16}$, où $\dfrac{n^2}{16}$ est un multiple de n puisque n est une puissance de 2 au moins égale à 16.

le produit de racines primitives ξ, η, ζ, ... des équations $x^{\nu^a} = 1$, $x^{\nu'^b} = 1$, $x^{\nu''^c} = 1$, ... Plus généralement, les différentes racines primitives de $x^n = 1$ seront des nombres de la forme $\xi^l \eta^{l'} \zeta^{l''} \ldots$, où l est premier à ν, l' est premier à ν', l'' est premier à ν'', ... La somme alternée $\mathcal{S}$ est une fonction entière de ρ, et donc également de ξ, de η, ... Cauchy montre alors que $\mathcal{S}$ est nécessairement proportionnelle à la somme des racines primitives de $x^{\nu^a} = 1$ et à une somme alternée de ces racines. Il en est de même pour les autres racines primitives. Donc $\mathcal{S}$ est proportionnelle au produit de facteurs dont chaque facteur est la somme ou une somme alternée des racines primitives d'une équation $x^{nu^a} = 1$, ... Réciproquement, il montre que le produit de sommes symétriques ou de sommes alternées de ce type est nécessairement une fonction alternée des racines primitives de $x^n = 1$. D'après ce qui précède, pour l'équation $x^{\nu^a} = 1$, la somme de ses racines primitives est égale à -1, et a pour carré l'unité, et la somme alternée de ses racines primitives est nulle ou a pour carré $\pm\nu^a$. Ainsi, pour l'équation $x^n = 1$, $\mathcal{S}$ est nulle ou $\mathcal{S}^2 = \pm n$ ou $\mathcal{S} = \pm\omega$, où ω est un diviseur de n. Si chaque produit formant la somme $\mathcal{S}$ est une somme alternée, alors $\mathcal{S} = 0$ ou $\mathcal{S} = \pm n$. En particulier, pour que $\mathcal{S}^2 = \pm n$, la somme devra être composée de sommes alternées seulement, les facteurs impairs de n devront être tous distincts et le facteur pair devra être 4 ou 8.

(b) Détermination des fonctions alternées des racines primitives de $x^n = 1$

Cauchy considère une fonction entière de la racine primitive ρ, que l'on peut écrire sous la forme $f(\rho) = a_0 + a_1\rho + a_2\rho^2 + \ldots + a_{n-1}\rho^{n-1}$, et qui répond aux conditions suivantes :

> Supposons d'ailleurs que, dans le cas où l'on remplace la racine primitive ρ de l'équation (1) par une autre racine primitive ρ^m de la même équation, les différents termes contenus dans $f(\rho)$ se transforment, au signe près, les uns dans les autres, et que deux termes, qui se déduisent ainsi l'un de l'autre, se trouvent toujours affectés du même signe pour certaines valeurs h, h', h'', ..., du nombre m, mais affectés de signes contraires pour d'autres valeurs k, k', k'', ... du même nombre... [Cauchy, 1840a, p. 257].

Pour satisfaire ces conditions, on doit avoir $a_0 = 0$ et $f(\rho)$ est une fonction linéaire de sommes alternées des racines primitives de $x^n = 1$ ou de $x^\omega = 1$, où ω est un diviseur de n. Cauchy appelle une telle fonction *fonction alternée*. L'objectif est de déterminer les formes de ces fonctions dans des cas particuliers.

Si $n = \nu^a$, où ν est un nombre premier impair et a un entier positif non nul, les diviseurs de n sont de la forme ν^i, $1 \leq i \leq a$ et les sommes alternées des racines primitives de l'équation $x^{\nu^i} = 1$ sont nulles sauf si $i = 1$ d'après ce qui précède. Cauchy note cette somme alternée non nulle Δ et on a donc

$$f(\rho) = a\Delta,$$

où a est un coefficient indépendant de ρ.

Si $n = 2^a$, où a est un entier positif non nul, on doit avoir $a > 1$ pour avoir plus d'une racine primitive et ainsi former une somme alternée des racines primitives de $x^n = 1$. Comme précédemment, la somme des racines primitives de $x^\omega = 1$, où ω est un diviseur de n sera nulle sauf dans les cas où $\omega = 4$ ou $\omega = 8$. $f(\rho)$ sera donc composée d'au plus deux termes.
Si $n = 4$, alors $f(\rho) = a\Delta$ où $\Delta = \pm 2\sqrt{-1}$.
Si $n = 8$, il y a trois cas à considérer en fonction de la somme alternée des racines primitives de $x^8 = 1$ choisie :

$$\rho + \rho^3 - \rho^5 - \rho^7, \quad \rho + \rho^5 - \rho^3 - \rho^7 = 0, \quad \rho + \rho^7 - \rho^3 - \rho^5.$$

Or, on sait que $f(\rho)$ est une fonction linéaire des différentes sommes $\rho^{ih} + \rho^{ih'} + \rho^{ih''} + \ldots + \rho^{ik} - \rho^{ik'} - \rho^{ik''} - \ldots$. Or, si on prend pour la somme $\rho^h + \rho^{h'} + \rho^{h''} + \ldots + \rho^k - \rho^{k'} - \rho^{k''} - \ldots$ chacune des trois sommes précédentes, les sommes $\rho^{2h} + \rho^{2h'} + \rho^{2h''} + \ldots + \rho^{2k} - \rho^{2k'} - \rho^{2k''} - \ldots$ correspondantes sont égales à :

$$0, \quad \rho^2 - \rho^6 = \pm 2\sqrt{-1}, \quad 0.$$

Finalement, $f(\rho) = a\Delta$, où Δ est une somme alternée des racines primitives de $x^4 = 1$ ou de $x^8 = 1$.
Pour $n = 2^a > 8$, on arrive aux mêmes conclusions puisque les sommes alternées des racines primitives de $x^\omega = 1$ sont nulles sauf dans les cas où $\omega = 4, 8$.

Puis Cauchy considère le cas général : $n = \nu^a \nu'^b \nu''^c \ldots$.

Ici, Cauchy traite uniquement le cas où $f(\rho)$ est formée uniquement de fonctions alternées des racines primitives des équations $x^\omega = 1$, où ω divise n. Dans ce cas, n doit être impair ou divisible plusieurs fois par 2. Alors $f(\rho)$ sera nulle ou proportionnelle à plusieurs sommes alternées Δ, Δ', Δ'', ...de racines primitives des équations $x^\nu = 1$, $x^{\nu'} = 1$, $x^{\nu''} = 1$, ...si ν, ν', ν'' sont tous impairs. $f(\rho)$ sera donc proportionnelle au produit $\Delta\Delta'\Delta''$, qui est une somme alternée des racines primitives de l'équation $x^\omega = 1$, où $\omega = \nu\nu'\nu'' \ldots$. Donc $f(\rho)$ sera de la forme

$$f(\rho) = a\Delta\Delta'\Delta'' \ldots.$$

Si $\nu = 2$, alors on obtient le même résultat avec $\omega = 4\nu\nu'\nu'' \ldots$ ou $\omega = 8\nu\nu'\nu'' \ldots$.

Si n est impair, alors d'après la formule (12), $\Delta^2 = (-1)^{\frac{\nu-1}{2}}$, ..., et donc $\Delta^2\Delta'^2\Delta''^2 = (-1)^{\frac{\nu-1}{2} + \frac{\nu'-1}{2} + \frac{\nu''-1}{2} + \cdots} \nu\nu'\nu'' \ldots = (-1)^{\frac{\omega-1}{2}} \omega = \pm\omega$, où $\omega = \nu\nu'\nu''$. On obtient d'ailleurs le même

résultat si n est divisible par 4 ou par 8.

Finalement : $[f(\rho)]^2 = \pm\omega a^2$. On remarque que $\omega = n$ si n est composé de facteurs impairs inégaux, et éventuellement du facteur 4 ou 8. Cauchy conclut en détaillant les cas où $f(\rho) = na^2$ et $f(\rho) = -na^2$ en utilisant les résultats précédents sur les sommes alternées.

3 - Sur les exposants des puissances de racines primitives (Note VIII)

L'objectif de cette note est d'étudier certaines propriétés des nombres h, k, l, ... Cauchy reprend les mêmes notations que dans la note VII. Dans un premier temps, il démontre des théorèmes sur les sommes $h + h' + h'' + \ldots$ et $k + k' + k'' + \ldots$ selon la forme du nombre n, puis il expose une technique pour savoir si deux racines primitives données ρ et ρ^l sont précédées du même signe ou non dans la somme $\mathcal{S}$, toujours selon la forme de n.

Si le nombre n est premier, les nombres h, h', h'', ..., désignent les résidus quadratiques de n et k, k', k'', ... désignent les non-résidus quadratiques de n. En remarquant que les exposants h, h', h'', ... représentent toutes les racines de l'équivalence $x^{\frac{n-1}{2}} \equiv 1 \pmod{n}$, on en déduit que leur somme est équivalente à zéro modulo n, lorsque $\frac{n-1}{2} > 1$. Il en est de même pour les nombres k, k', k'', ... Le théorème I affirme donc que, si n est un nombre premier supérieur à 3, les sommes $h + h' + h'' + \ldots$ et $k + k' + k'' + \ldots$ sont divisibles par n. Cauchy donne une autre démonstration de ce théorème en remplaçant les exposants h, h', h'', ... par 1, s^2, s^4, ..., s^{n-3} où s est une racine primitive de $x^{n-1} \equiv 1 \pmod{n}$, et en calculant la somme des termes de la progression géométrique $1 + s^2 + s^4 + \ldots + s^{n-3}$ modulo n. Il fait de même avec s, s^3, ..., s^{n-2}.

Dans le cas où $n = \nu^a$, où ν est un nombre premier impair, les nombres h, h', h'', ..., désignent toujours les résidus quadratiques, les nombres k, k', k'', ... les non-résidus quadratiques. Cauchy démontre que les sommes $h + h' + h'' + \ldots$ et $k + k' + k'' + \ldots$ sont divisibles par $\nu^{a-1} = \frac{n}{\nu}$: c'est l'objet du théorème II. Là encore, il donne une deuxième démonstration basée sur la considération des suites géométriques 1, s^2, s^4, ..., s^{n-3} d'une part et s, s^3, s^5, ..., s^{n-2} d'autre part. Dans la théorème III, Cauchy étudie le cas où ν est de la forme $4x + 1$: dans ce cas, il démontre que les deux sommes $h + h' + h'' + \ldots$ et $k + k' + k'' + \ldots$ sont divisibles par n.

Dans le théorème IV, Cauchy considère un nombre n entier supérieur à 2 et la somme $h + k + l + \ldots$. Il démontre que $h + k + l + \ldots \equiv 0 \pmod{n}$. Cauchy, dans ces théorèmes, alterne les utilisations du vocabulaire "divisible par n" et "équivalente à zéro modulo n".

Après ces quatre résultats, Cauchy développe une « observation importante » :

> si, dans la somme alternée $\mathcal{S}$, on remplace ρ par ρ^l, alors, suivant que l sera

équivalent à l'un des nombres

$$h, h', h'', \ldots$$

ou à l'un des nombres

$$k, k', k'', \ldots$$

cette même somme se trouvera multipliée par +1 ou par −1, c'est-à-dire que les termes précédés du signe + s'y trouveront échangés ou non contre les termes précédés du signe −, cette espèce de multiplication ou d'échange ayant lieu dans le cas même où n renfermerait des facteurs égaux, et où, par suite, en vertu des propriétés de la racine ρ, la somme alternée $\mathcal{S}$ s'évanouirait [Cauchy, 1840a, p. 273].

Dans le cas où n est un nombre premier ou la puissance d'un nombre premier, les nombres h, h', h'', ... désignant les résidus quadratiques, et les nombres k, k', k'', ... désignant les non-résidus quadratiques, remplacer ρ par ρ^l dans la somme alternée $\mathcal{S}$ revient en fait à multiplier celle-ci par $\left[\frac{l}{n}\right]$. Dans la suite, Cauchy étudie les effets de cette substitution de ρ à ρ^l dans la somme $\mathcal{S}$ en fonction de la forme de n.

Il considère le cas où n est un nombre impair quelconque, dont la décomposition en facteurs premiers est $n = \nu^a \nu'^b \nu''^c \ldots$. Il démontre le théorème suivant :

Théorème V. - Soit n un nombre premier impair ; ν, ν', ν'', ... ses facteurs premiers ; a, b, c, ... les exposants de ces facteurs dans le nombre n ; l un des entiers inférieurs à n mais premiers à n ; et ρ une des racines primitives de l'équation (1)$[x^n = 1]$. Si une somme alternée $\mathcal{S}$ de ces racines est en même temps une fonction alternée des racines primitives de chacune des équations (14) $[x^{\nu^a} = 1, x^{\nu'^b} = 1, \ldots]$, les deux termes

$$\rho, \rho^l$$

seront, dans la somme alternée $\mathcal{S}$, affectés du même signe ou de signes contraires suivant qu'on aura

$$(19) \qquad \left[\frac{l}{n}\right] = 1 \text{ ou } \left[\frac{l}{n}\right] = -1.$$

Il en résulte encore que, dans le cas où, comme nous l'avons supposé, le groupe des nombres

$$h, h', h'', \ldots$$

renferme l'unité, l fait partie ou non de ce même groupe suivant que la première ou la seconde des formules (19) se vérifie [Cauchy, 1840a, p. 276].

Cauchy étudie ensuite le cas où n est une puissance de 2, puis le cas où n est un nombre pair contenant au moins un facteur impair. Cauchy en déduit les théorèmes VI à IX selon que n est divisible par une puissance de 2 en général, puis par 4 ou par 8 (ce qui correspond à des cas particuliers pour la somme $\mathcal{S}$, comme on l'a vu dans la note précédente). Il conclut cette note par le théorème plus général suivant :

THÉORÈME XI. - Lorsque la somme alternée $\mathcal{S}[\dots]$, vérifie l'équation (17), savoir

$$\mathcal{S}^2 = \pm n,$$

les deux groupes d'exposants

$$h, h', h'', \dots,$$

$$k, k', k'', \dots$$

vérifient la condition (7), savoir

$$h + h' + h'' + \dots \equiv k + k' + k'' + \dots \equiv 0 \pmod{n},$$

à moins toutefois que le module n ne se réduise à l'un des trois nombres

$$3, 4, 8$$

[CAUCHY, 1840a, p. 292].

Il remarque que cette équivalence est même vérifiée pour une valeur de $\mathcal{S}$ dans le cas où $n = 8$. Rappelons que pour que $\mathcal{S}^2 = \pm n$, n doit être un produit de facteurs premiers impairs distincts et d'un facteur pair éventuel égal à 4 ou 8 et que la somme $\mathcal{S}$ ne doit être composée que de sommes alternées seulement.

4 - D'autres théorèmes sur les exposants (Note IX)

Dans cette note, Cauchy reprend les mêmes notations que précédemment. L'objectif est notamment de déterminer pour quels nombres n les exposants l et $-l$ ou l et $2l$ sont dans le même groupe. Cela revient à déterminer si -1 et 2 sont résidus quadratiques de n.

Cauchy commence par remarquer que si m est un nombre premier à n et inférieur à n, alors

- Si m fait partie du premier groupe, alors mh, $m'h'$, ... appartiennent au groupe h, h', ... et mk, mk', ..., appartiennent au groupe k, k', ... ;
- Par contre, si m appartient au deuxième groupe, mh, mh', ... appartiennent au second groupe tandis que mk, mk', ..., appartiennent au premier groupe.

Cauchy traduit cette observation en termes de groupes de racines :

> Des principes que nous venons de rappeler, il résulte encore que, si l'on remplace ρ par ρ^m, les deux groupes des racines primitives ρ^h, $\rho^{h'}$, $\rho^{h''}$, ... et ρ^k, $\rho^{k'}$, $\rho^{k''}$, ... resteront composés chacun des mêmes racines, ou se transformeront l'un dans l'autre, suivant que m sera équivalent, suivant le module n, à l'un des nombres h, h', h'', ... ou à l'un des nombres k, k', k'', ... [CAUCHY, 1840a, p. 295].

Il introduit alors une fonction $I = f(\rho^h, \rho^{h'}, \rho^{h''}, \dots)$, qui est symétrique des racines ρ,

ρ^h, $\rho^{h''}$, … et pose $J = f(\rho^k, \rho^{k'}, \rho^{k''}, \ldots)$. Alors, la somme $I+J$ est une fonction symétrique et $I-J$ est une fonction alternée des racines primitives de $x^n = 1$.

Il considère n tel que $\mathcal{S} = \pm n$, c'est-à-dire que le nombre n est de la forme $\nu\nu'\nu''\ldots$ ou $4\nu\nu'\nu''\ldots$ ou $8\nu\nu'\nu''\ldots$ où ν, ν', ν'', … sont des facteurs premiers impairs distincts. Il rappelle les égalités démontrées dans la note précédente : la valeur de $\left[\frac{h}{n}\right]$ lorsque n est impair, $\left[\frac{h}{\frac{1}{4}n}\right]$ lorsque le facteur pair de n est égal à 4 et $\left[\frac{h}{\frac{1}{8}n}\right]$ lorsque le facteur pair de n est égal à 8. Il démontre que, dans le cas où n est impair composé de facteurs premiers distincts, on a toujours les formules

$$\left[\tfrac{-1}{n}\right] = (-1)^{\frac{n-1}{2}} \text{ et } \left[\tfrac{2}{n}\right] = (-1)^{\frac{n^2-1}{8}},$$

où $\left[\frac{-1}{n}\right] = \left[\frac{-1}{\nu}\right]\left[\frac{-1}{\nu'}\right]\left[\frac{-1}{\nu''}\right]\ldots$.

Dans le cas où $n = 4\nu\nu'\nu''\ldots$, la formule relative au caractère quadratique de -1 se traduit par $\left[\frac{-1}{\frac{1}{4}n}\right] = (-1)^{\frac{\frac{n}{4}-1}{2}}$. On en déduit une égalité semblable dans le cas où le facteur pair de n est 8. Cauchy distingue alors deux cas :

- lorsque $\mathcal{S}^2 = n$, alors 1 et -1 appartiennent au même groupe car, comme il l'a démontré précédemment, le nombre n est alors de l'une trois formes $4x+1$, $4(4x+3)$, $8(2x+1)$;
- lorsque $\mathcal{S}^2 = -n$, alors 1 et -1 appartiennent à des groupes différents, car n est alors de l'une des trois formes $4x+3$, $4(4x+1)$ et $8(2x+1)$.

Il en déduit des résultats similaires pour les nombres 1 et 2, et plus généralement, l, et $2l$, puis il montre que si n est pair tel que $\mathcal{S}^2 = n$, alors chacun des groupes d'exposants h, h', h'', … et k, k', k'', … contiennent chacun autant de termes inférieurs à $\frac{n}{2}$ que de termes supérieurs à $\frac{n}{2}$.

Cauchy conclut cette note en rappelant la signification du symbole de Jacobi : si n est de la forme ν^a, où ν est un nombre premier, la notation $\left[\frac{l}{n}\right]$ désigne la puissance $\left[\frac{l}{\nu}\right]^a$ et « on pourrait étendre à des nombres impairs quelconques la loi de réciprocité qui existe entre deux nombres premiers impairs » [Cauchy, 1840a, p. 307].

IV Les formes quadratiques $p^\mu = x^2 + ny^2$, où n est un diviseur premier de $p-1$

Nous résumons ici le début de la partie principale du mémoire de Cauchy. Comme nous l'avons annoncé précédemment, Cauchy ne met pas en avant dans ce texte les clés de sa méthode basée sur l'utilisation des facteurs primitifs. D'autre part, il utilise librement et sans référence les divers résultats démontrés dans les notes que nous avons étudiées précédemment.

Dans ce paragraphe, le diviseur n de $p-1$ est supposé premier et impair.

1 - Multiplication des facteurs primitifs

Cauchy donne l'expression générale de $R_{h,k}$ pour des valeurs particulières de h et k :

> $R_{1,m}$ sera une fonction de ρ de la forme
>
> $$R_{1,m} = a_0 + a_1\rho + a_2\rho^2 + \ldots + a_{n-1}\rho^{n-1};$$
>
> et, si l'on pose
>
> $$k \equiv mh \pmod{n},$$
>
> on aura, en supposant m différent de zéro et de $\frac{n}{2}$,
>
> $$R_{h,mh} = a_0 + a_1\rho^h + a_2\rho^{2h} + \ldots + a_{n-1}\rho^{(n-1)h}$$
>
> et
>
> $$R_{h,k} = (-1)^{\varpi(h+k)} \sum \left(\frac{u}{p}\right)^h \left(\frac{v}{p}\right)^k,$$
>
> le signe $\sum$ s'étendant à toutes les valeurs entières de u, v, comprises entre les limites 1, $p-1$, et qui vérifieront l'équivalence
>
> $$1 + u + v \equiv 0 \pmod{p}$$
>
> [Cauchy, 1840a, p. 7-8] [10].

Cauchy énonce des formules [11] qu'il démontre dans le cas particulier où $\varpi = 1$ dans la note I :

- si h n'est pas divisible par $p-1$,

$$\Theta_h\Theta_{-h} = (-1)^{\varpi h}p \text{ et } R_{h,-h} = -(-1)^{\varpi h}p; \tag{11}$$

- Si h, k, et $h+k$ ne sont pas divisibles par n,

$$R_{h,k}R_{-h,-k} = p; \tag{12}$$

-

$$R_{h,0} = R_{0,h} = -1; \tag{13}$$

10. Cette formule correspond à la formule (8) de la Note I, en utilisant la notation $\left(\frac{u}{p}\right)$.

11. On a l'égalité (14) car l'expression $R_{h,k}$ est composée de $p-2$ termes de la forme ρ^k. La formule (15) est équivalente à la formule (11) pour $h = \frac{n}{2}$, car $\rho^n = 1$ et $\rho^{\frac{n}{2}} = -1$. Par contre, une erreur s'est glissée dans le texte : on devrait obtenir : $-(-1)^{\frac{\varpi n}{2}}p$.

•

$$a_0 + a_1 + a_2 + \ldots + a_{n-1} = p - 2; \tag{14}$$

•

$$a_0 - a_1 + a_2 - a_3 + \ldots - a_{n-1} = -(-1)^{\frac{\varpi n}{2}} \tag{15}$$

Ensuite, comme $R_{h,k}$ est une expression dépendant de ρ, Cauchy pose : $R_{h,k} = F(\rho)$, puis il traduit certaines propriétés de l'expression $R_{h,k}$ en fonction de F :

- si m est tel qu'aucune des équations suivantes n'est vérifiée [12] :

$$\rho^{mh} = 1,\ \rho^{mk} = 1,\ \rho^{m(h+k)} = 1, \tag{18}$$

alors

$$F(\rho^m) = R_{mh,mk} \text{ et } F(\rho^m)F(\rho^{-m})) = p; \tag{17}$$

- Si une seule des équations (18) est vérifiée, alors :

$$F(\rho^m) = -(-1)^{\varpi mh - \varpi mk}; \tag{19}$$

- Si les trois équations sont satisfaites, alors :

$$F(\rho^m) = p - 2 \tag{20}$$

Il considère ensuite trois nombres entiers non nuls h, k, l tels que $h+k+l \equiv 0 \pmod{n}$. Alors :

$$\Theta_h\Theta_k\Theta_l = (-1)^{\varpi l}\frac{\Theta_h\Theta_k}{\Theta_{h+k}} = (-1)^{\varpi k}\frac{\Theta_h\Theta_l}{\Theta_{h+l}} = (-1)^{\varpi h}\frac{\Theta_l\Theta_k}{\Theta_{l+k}},$$

c'est-à-dire :

$$(-1)^{\varpi h}R_{k,l} = (-1)^{\varpi k}R_{l,h} = (-1)^{\varpi l}R_{k,h}. \tag{22}$$

12. La deuxième égalité de (17) correspond en fait à la formule (13) de la note I. Ces trois équations suivantes sont équivalentes au critère de divisibilité suivant : mh, mk et $m(h+k)$ ne doivent pas être divisibles par n (et donc également par $p-1$, ce qui correspond aux cas particuliers étudiés dans la Note I).

En effet, comme $\rho^n = 1$ par définition : $R_{h,k} = R_{h+in,k+jn}$ et $\Theta_h = \Theta_{h+in}$ pour tous nombres entiers i et j. Or, $h + k + l \equiv 0 \pmod{n}$ donc $l \equiv -h - k \pmod{n}$ et $\Theta_l = \Theta_{-h-k}$. Finalement :

$$\Theta_h\Theta_k\Theta_l = \Theta_h\Theta_k\Theta_{-h-k} = R_{h,k}\Theta_{h+k}\Theta_{-h-k} = (-1)^{\varpi(h+k)}pR_{h,k}.$$

En réitérant le même procédé avec $h + l$ et $k + l$, et en simplifiant par p, on obtient l'égalité (22).

Dans la suite de cette partie, n représente un nombre premier. Soit s, une racine primitive de $x^{n-1} \equiv 1 \pmod{n}$. Alors : $1 + s^2 + s^4 + \ldots + s^{n-3} = \dfrac{s^{n-1} - 1}{s^2 - 1} \equiv 0 \pmod{n}$, donc $\Theta_{1+s^2+s^4+\ldots+s^{n-3}} = \Theta_0 = -1$ donc, d'après les propriétés des expressions $R_{h,k}$, on peut poser :

$$\Theta_1\Theta_{s^2}\Theta_{s^4}\ldots\Theta_{s^{n-3}} = \mathscr{F}(\rho), \tag{24}$$

et

$$\Theta_s\Theta_{s^3}\Theta_{s^5}\ldots\Theta_{s^{n-2}} = \mathscr{F}(\rho^s). \tag{25}$$

Cauchy ne le précise pas, mais $\mathscr{F}$ désigne une expression algébrique dépendant de ρ. Ici, $\mathscr{F}(\rho)$ et $\mathscr{F}(\rho^s)$ correspondent en fait aux deux produits de facteurs primitifs que Cauchy utilise explicitement dans ses notes aux *Comptes Rendus* publiées en 1840 : en effet, s étant une racine primitive, cette racine ne peut être un résidu quadratique, et les nombres 1, s^2, s^4, $\ldots s^{n-3}$ correspondent bien aux résidus quadratiques de n, notés h, h', h'', …en 1840 et les nombres s, s^3, s^5, …, s^{n-2} sont les non-résidus quadratiques de n. On a de plus : $\mathscr{F}(\rho) = \mathscr{F}(\rho^{s^2}) = \ldots = \mathscr{F}(\rho^{s^{n-3}})$ et $\mathscr{F}(\rho^s) = \mathscr{F}(\rho^{s^3}) = \ldots = \mathscr{F}(\rho^{s^{n-2}})$. Autrement dit, et c'est comme cela que Cauchy l'exprimera dans ses notes, la fonction $\mathscr{F}$ est symétrique de ρ, ρ^{s^2}, …, $\rho^{s^{n-3}}$, et donc de la somme $1 + \rho^{s^2} + \rho^{s^4} + \rho^{s^{n-3}}$ d'une part et symétrique de ρ^s, ρ^{s^3}, …, $\rho^{s^{n-2}}$ et de la somme de ces racines d'autre part. $\mathscr{F}(\rho)$ peut donc être mise sous la forme :

$$\mathscr{F}(\rho) = c_0 + c_1(\rho + \rho^{s^2} + \rho^{s^4} + \ldots + \rho^{s^{n-3}}) + c_2(\rho^s + \rho^{s^3} + \ldots + \rho^{s^{n-2}}). \tag{26}$$

En utilisant la propriété $\sum_{i=0}^{n-2} \rho^{s^i} = 0$, on obtient :

$$\mathscr{F}(\rho) = \frac{2c_0 - c_1 - c_2}{2} + \frac{c_1 - c_2}{2}(\rho - \rho^s + \rho^{s^2} - \rho^{s^3} + \ldots - \rho^{s^{n-2}}).$$

On voit ainsi apparaître une somme alternée de racines primitives. De plus, à plusieurs reprises dans ses notes (cela correspond notamment à la formule (14) de la Note I), Cauchy a démontré que $(\rho - \rho^s + \rho^{s^2} - \rho^{s^3} + \ldots - \rho^{s^{n-2}})^2 = (-1)^{\frac{n-1}{2}} n$. On obtient donc :

$$\mathscr{F}(\rho)\mathscr{F}(\rho^s) = \left(\frac{2c_0 - c_1 - c_2}{2}\right)^2 - (-1)^{\frac{n-1}{2}} n \left(\frac{c_1 - c_2}{2}\right)^2,$$

soit

$$4\mathscr{F}(\rho)\mathscr{F}(\rho^s) = (2c_0 - c_1 - c_2)^2 - (-1)^{\frac{n-1}{2}} n(c_1 - c_2)^2. \tag{27}$$

Donc, si n est de la forme $4x + 3$, alors (27) devient :

$$4\mathscr{F}(\rho)\mathscr{F}(\rho^s) = (2c_0 - c_1 - c_2)^2 + n(c_1 - c_2)^2. \tag{29}$$

Par contre, si n est de la forme $4x + 1$, alors $\dfrac{n-1}{2}$ est pair et $\mathscr{F}(\rho) = p^{\frac{n-1}{4}} = c_0$. Cauchy précise que cela se déduit *simplement* de la formule (24). Cette formule est également démontrée dans la note III, dont nous donnons un aperçu dans le cas où n est premier ci-dessous.

Cauchy revient plus en détail sur le cas où n est de la forme $4x+3$. On a $\mathscr{F}(\rho)\mathscr{F}(\rho^s) = p^{\frac{n-1}{2}}$. Là encore, Cauchy ne donne pas de référence ; cette égalité est également démontrée dans la Note III. On a donc : $4p^{\frac{n-1}{2}} = (2c_0 - c_1 - c_2)^2 + n(c_1 - c_2)^2$, ce qui donne l'équation

$$4p^{\frac{n-1}{2}} = X^2 + nY^2,$$

où $X = 2c_0 - c_1 - c_2$ et $Y = c_1 - c_2$.

Ainsi, comme en 1840, Cauchy obtient bien une égalité de la forme $4p^\mu = x^2 + ny^2$, avec une méthode similaire. La seule différence est qu'il ne met pas en avant les outils des facteurs primitifs comme il le fait en 1840.

Dans l'égalité obtenue, les nombres X et Y peuvent être divisibles par p. La suite de la première partie du mémoire est consacrée à déterminer le plus grand exposant λ tel que p^λ divise simultanément X et Y et à ainsi obtenir le plus petit μ tel que $4p^\mu = x^2 + ny^2$. Avant d'étudier ce passage, nous résumons la note III, qui contient des résultats sur certains produits des sommes Θ_h et les démonstrations de quelques égalités utilisées ci-dessus.

2 - Multiplication des sommes de Gauss (Note III)

Il rappelle les propriétés de θ_h démontrées dans la note I notamment :

- $\Theta_{h+i(p-1)} = \Theta_h$ pour tout i nombre entier relatif ;
- Si h est divisible par $p-1$: $\Theta_h = \Theta_0 = -1$;
- Si h n'est pas divisible par $p-1$: $\Theta_h\Theta_{-h} = (-1)^h p$;

Si[13] n divise $p-1$, on pose $\varpi = \frac{p-1}{n}$, $\rho = \tau^{\varpi}$ ($p = n\varpi + 1$ et ρ est ainsi une racine primitive de $x^n = 1$) et

$$\Theta_h = \theta + \rho^h\theta^t + \rho^{2h}\theta^{t^2} + \ldots + \rho^{(p-2)h}\theta^{t^{p-2}}. \tag{1}$$

Dans ce cas, Θ_h est une fonction de θ et ρ et $\Theta_{h+in} = \Theta_h$ pour tout i nombre entier relatif. Comme précédemment :

$$\Theta_h = \Theta_0 = -1. \tag{2}$$

Si h n'est pas divisible par n

$$\Theta_h\Theta_{-h} = (-1)^{\varpi h} p = \Theta_h\Theta_{n-h}. \tag{3}$$

Il rappelle que :

$$\Theta_h\Theta_k = R_{h,k}\Theta_{h+k}, \tag{4}$$

où $R_{h,k}$ est une fonction de ρ seulement. De plus, si $h+k$ n'est pas divisible par n :

$$R_{h,k} = \sum_{\substack{0\le i,j,\le p-2 \\ t^i+t^j\equiv 1 \pmod p}} \rho^{ih+jk}. \tag{5}$$

Soient h, k, l, des nombres entiers quelconques. En appliquant plusieurs fois (4), on trouve :

$$\Theta_h\Theta_k\Theta_l \ldots = R_{h,k,l,\ldots}\Theta_{h+k+l+\ldots}, \tag{7}$$

où $R_{h,k,l\ldots}$ est une fonction de ρ telle que $R_{h,k,l,\ldots} = R_{h,k}R_{h+k,l}\ldots$.

Cauchy ajoute, sans le justifier, que si $h+k+l$ n'est pas divisible par n, alors

13. Dans le texte, il est écrit « en nommant h un diviseur de $p-1$ » mais cela ne semble pas avoir de sens.

(8) $$R_{h,k,l,\ldots} = \sum_{\substack{0\le i,i',i'',\ldots\le p-2 \\ t^i+t^{i'}+t^{i''}+\ldots\equiv 1 \pmod p}} \rho^{ih+i'k+i''l+\ldots}.$$

Enfin, Cauchy rappelle que comme le produit $\Theta_h\Theta_k\Theta_l\ldots$ et l'expression $\Theta_{h+k+l+\ldots}$ sont des fonctions symétriques et entières de ρ^h, ρ^k, ρ^l, ... et donc des fonctions linéaires à coefficients entiers des sommes

$$\begin{array}{llll} \rho^h & +\rho^k & +\rho^l & +\ldots, \\ \rho^{2h} & +\rho^{2k} & +\rho^{2l} & +\ldots, \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots, \\ \rho^{(n-1)h} & +\rho^{(n-1)k} & +\rho^{(n-1)l} & +\ldots, \end{array}$$

on peut en déduire qu'il en est de même pour $R_{h,k,l,\ldots} = \dfrac{\Theta_h\Theta_k\Theta_l\ldots}{\Theta_{h+k+l+\ldots}}$.

Les résultats contenus dans la partie principale du mémoire permettent d'exprimer un nombre premier p, ou $4p$ ou $4p^\mu$ en une expression de la forme $x^2 + ny^2$ où n est un diviseur de $p-1$.

Cauchy va maintenant distinguer les différents cas selon la forme du nombre n.

Si $n = 2$, alors $\rho = -1$, $\varpi = \frac{p-1}{2}$ et, d'après la formule (3), $\Theta_1^2 = (-1)^{\frac{p-1}{2}}p$, soit

(10) $$(\theta - \theta^t + \theta^{t^2} - \ldots - \theta^{t^{p-2}})^2 = (-1)^{\frac{p-1}{2}}p.$$

Si n est un nombre premier impair, alors les racines primitives de $x^n = 1$ sont les ρ^i, avec $1 \le i \le n-1$. D'après l'équation (3) :

$$\Theta_1\Theta_{n-1} = \Theta_2\Theta_{n-2} = \ldots = \Theta_{\frac{n-1}{2}}\Theta_{\frac{n+1}{2}} = (-1)^{\frac{p-1}{n}h}p = p,$$

puisque $\frac{p-1}{n}$ est pair. On en déduit :

(12) $$\Theta_1\Theta_2\Theta_3\ldots\Theta_{n-1} = p^{\frac{n-1}{2}}.$$

Si s est une racine primitive de l'équivalence $x^{n-1} \equiv 1 \pmod n$, alors les puissances 1, s, s^2, ..., s^{n-2} représentent modulo n tous les entiers compris entre 1 et $n-1$. On peut donc écrire (12) sous la forme

(14) $$\Theta_1\Theta_s\Theta_{s^2}\ldots\Theta_{s^{n-2}} = p^{\frac{n-1}{2}}.$$

Cauchy utilise ensuite le fait que les racines 1, s^2, s^4, …, s^{n-3} sont également racines de l'équivalence $x^{\frac{n-1}{2}} \equiv 1 \pmod n$ et que s, s^3, …, s^{n-2} sont racines de $x^{\frac{n-1}{2}} \equiv -1 \pmod n$. Il décompose le produit $\Theta_1\Theta_s\Theta_{s^2}\ldots\Theta_{s^{n-2}}$ en deux produits : $\Theta_1\Theta_{s^2}\ldots\Theta_{s^{n-3}} = R_{1,s^2,\ldots,s^{n-3}}\Theta_{1+s^2+\ldots+s^{n-3}}$ et $\Theta_s\Theta_{s^3}\ldots\Theta_{s^{n-2}} = R_{s,s^3,\ldots,s^{n-2}}\Theta_{s+s^3+\ldots+s^{n-2}}$.
Or :
$1+s^2+s^4+\ldots+s^{n-3} = \dfrac{s^{n-1}-1}{s^2-1} \equiv 0 \pmod n$ et $s+s^3+s^5+\ldots+s^{n-2} = s\dfrac{s^{n-1}-1}{s^2-1} \equiv 0 \pmod n$.

Comme $\Theta_0 = -1$, les égalités précédentes deviennent : $\Theta_1\Theta_{s^2}\ldots\Theta_{s^{n-3}} = -R_{1,s^2,\ldots,s^{n-3}}$ et $\Theta_s\Theta_{s^3}\ldots\Theta_{s^{n-2}} = -R_{s,s^3,\ldots,s^{n-2}}$. Finalement, $\Theta_1\Theta_{s^2}\ldots\Theta_{s^{n-3}}$ et $R_{1,s^2,\ldots,s^{n-3}}$ sont des fonctions entières et symétriques de ρ, ρ^{s^2}, …, $\rho^{s^{n-3}}$ et $\Theta_s\Theta_{s^3}\ldots\Theta_{s^{n-2}}$ et $R_{s,s^3,\ldots,s^{n-2}}$ sont des fonctions entières et symétriques de ρ^s, ρ^{s^3}, …, $\rho^{s^{n-2}}$.

De plus, une fonction entière et symétrique de ρ, ρ^{s^2}, …, $\rho^{s^{n-3}}$ est une fonction linéaire des sommes $\rho^m + \rho^{ms^2} + \ldots + \rho^{ms^{n-3}}$, $m \le n$. Ces sommes sont toujours égales à $\rho + \rho^{s^2} + \ldots + \rho^{s^{n-3}}$ ou $\rho^s + \rho^{s^3} + \ldots + \rho^{s^{n-2}}$. Donc :
$\Theta_1\Theta_{s^2}\ldots\Theta_{s^{n-3}} = c_0 + c_1(\rho + \rho^{s^2} + \ldots + \rho^{s^{n-3}}) + c_2(\rho^s + \rho^{s^3} + \ldots + \rho^{s^{n-2}})$,
et, en remplaçant ρ par ρ^s :
$\Theta_s\Theta_{s^3}\ldots\Theta_{s^{n-2}} = c_0 + c_1(\rho^s + \rho^{s^3} + \ldots + \rho^{s^{n-2}}) + c_2(\rho + \rho^{s^2} + \ldots + \rho^{s^{n-3}})$.

On a $\rho + \rho^s + \rho^{s^2} + \ldots + \rho^{s^{n-2}} = -1$ et si on remplace p par n, θ par ρ et t par s, et si on pose $\rho - \rho^s + \rho^{s^2} - \ldots - \rho^{s^{n-2}} = \Delta$, la formule (10) devient :

(15) $$\Delta^2 = (-1)^{\frac{n-1}{2}} n.$$

On en déduit : $\rho + \rho^{s^2} + \ldots + \rho^{s^{n-3}} = -\dfrac{1-\Delta}{2}$ et $\rho^s + \rho^{s^3} + \ldots + \rho^{s^{n-2}} = -\dfrac{1+\Delta}{2}$, soit :

(16) $$\begin{cases} 2\Theta_1\Theta_{s^2}\Theta_{s^4}\ldots\Theta_{s^{n-3}} = A + B\Delta, \\ 2\Theta_s\Theta_{s^3}\Theta_{s^5}\ldots\Theta_{s^{n-2}} = A - B\Delta, \end{cases}$$

où $A = 2c_0 - c_1 - c_2$, $B = c_1 - c_2$ sont *de même espèce* c'est-à-dire soit simultanément pairs, soit simultanément impairs. Les égalités (16) permettent d'obtenir des expressions des deux produits de facteurs primitifs qui, multipliées entre elles, sont bien égales à une forme $x^2 \pm ny^2$.

Enfin, d'après les égalités (14), (15) et (16), on a :

(18) $$4p^{\frac{n-1}{2}} = A^2 - (-1)^{\frac{n-1}{2}} nB^2.$$

De plus, comme $s^{\frac{n-1}{2}} \equiv -1 \pmod{n}$, $\Theta_{s^m}\Theta_{s^{m\pm\frac{n-1}{2}}} \equiv \Theta_{s^m}\Theta_{-s^m} \pmod{n}$, donc [14]

$$\Theta_{s^m}\Theta_{s^{m\pm\frac{n-1}{2}}} = p. \tag{19}$$

On choisit le signe qui est affecté à $\frac{n-1}{2}$ de façon à ce que $m \pm \frac{n-1}{2}$ soit compris entre 0 et n-2. De plus, m et $m \pm \frac{n-1}{2}$ sont de la même parité si $n = 4x+1$ et de parités inverses si $n = 4x+3$. On distingue donc ces deux cas.

Si $n = 4x+1$, alors les deux produits $\Theta_1\Theta_{s^2}\ldots\Theta_{s^{n-3}}$ et $\Theta_s\Theta_{s^3}\ldots\Theta_{s^{n-2}}$ sont formés de $\frac{p-1}{2}$ produits de deux facteurs de la forme $\Theta_{s^m}\Theta_{s^{m\pm\frac{n-1}{2}}}$ égaux à p et ils seront donc égaux à $p^{\frac{n-1}{2}}$. On en déduit que $A = 2p^{\frac{n-1}{2}}$ et $B = 0$.

Si $n = 4x+3$, $\frac{n-1}{2}$ est impair, et l'égalité (18) devient :

$$4p^{\frac{n-1}{2}} = A^2 + nB^2. \tag{20}$$

Soit p^λ, la plus grande puissance de p divisant A et B. On pose $A = p^\lambda x$, $B = p^\lambda y$ et $\mu = \frac{n-1}{2} - 2\lambda$ et on obtient

$$4p^\mu = x^2 + ny^2. \tag{21}$$

Cauchy ne fait alors aucun commentaire à ce sujet mais on reconnaît ici la forme d'équation qu'il résout dans des cas particuliers à plusieurs reprises dans ce mémoire.

Cauchy introduit ici deux nouvelles notations, avant de les utiliser pour traduire certaines des égalités précédentes :

- $[1] = \Theta_1\Theta_{s^2}\Theta_{s^4}\ldots\Theta_{s^{n-3}}$, produit composé des facteurs Θ_h tels que $h^{\frac{n-1}{2}} \equiv 1 \pmod{n}$.
- $[-1] = \Theta_s\Theta_{s^3}\Theta_{s^5}\ldots\Theta_{s^{n-2}}$, produit composé des facteurs Θ_h tels que $h^{\frac{n-1}{2}} \equiv -1 \pmod{n}$.

Il traduit ainsi les égalités obtenues précédemment par :

$$p^{\frac{n-1}{2}} = [1][-1]$$

$$2[1] = A + B\Delta, \qquad 2[-1] = A - B\Delta.$$

La suite de la note est consacrée à l'étude de cas où n est un nombre composé : nous y reviendrons plus loin.

14. Dans le texte, cette égalité est indiquée sous forme d'une équivalence modulo n.

Grâce à ces démonstrations, Cauchy obtient bien une égalité de la forme

$$4p^{\frac{n-1}{2}} = X^2 + nY^2.$$

La suite de son texte est donc consacré à la détermination de plus grand nombre λ tel que p^λ divise X^2 et Y^2, c'est-à-dire au plus petit μ tel que $4p^\mu = x^2 + ny^2$.

V Détermination de l'exposant μ et des sommes $R_{h,k}$

1 - Détermination de l'exposant μ

Soit v tel que $v^{\frac{n-1}{2}} \equiv 1 \pmod n$ et $(1+v)^{\frac{n-1}{2}} \equiv 1 \pmod n$. v et $1+v$ sont donc des résidus quadratiques de n. Utiliser ces nombres va permettre à Cauchy de travailler avec les sommes de Jacobi $R_{h,k}$. En effet :

$$\Theta_1\Theta_{s^2}\dots\Theta_{s^{n-3}} = \Theta_v\Theta_{vs^2}\dots\Theta_{vs^{n-3}} = \Theta_{1+v}\Theta_{(1+v)s^2}\dots\Theta_{(1+v)s^{n-3}} = \mathscr{F}(\rho),$$

donc, comme $R_{h,k} = \dfrac{\Theta_h\Theta_k}{\Theta_{h+k}}$ on obtient :

$$\mathscr{F}(\rho) = \frac{\Theta_1\Theta_v}{\Theta_{1+v}}\frac{\Theta_{s^2}\Theta_{vs^2}}{\Theta_{(1+v)s^2}}\dots\frac{\Theta_{s^{n-3}}\Theta_{vs^{n-3}}}{\Theta_{(1+v)s^{n-3}}} = R_{1,v}R_{s^2,vs^2}\dots R_{s^{n-3},vs^{n-3}}, \tag{32}$$

$$\mathscr{F}(\rho^s) = R_{s,vs}R_{s^3,vs^3}\dots R_{s^{n-2},vs^{n-2}}. \tag{33}$$

Si n est un nombre de la forme $4x+3$, alors il est de la forme $8x+7$ ou de la forme $8x+3$. Si n est de la forme $8x+7$, alors 2 est un résidu quadratique modulo n soit $2^{\frac{n-1}{2}} \equiv 1 \pmod n$ donc on peut prendre $v = 1$ et on a

$$\begin{cases} \mathscr{F}(\rho) = R_{1,1}R_{s^2,s^2}\dots R_{s^{n-3},s^{n-3}} \\ \mathscr{F}(\rho^s) = R_{s,s}R_{s^3,s^3}\dots R_{s^{n-2},s^{n-2}}, \end{cases} \tag{34}$$

soit, à partir de la formule (26) [15] :

15. L'expression de Y est ici erronée : en effet, on obtient la dernière partie de l'égalité en multipliant au numérateur et au dénominateur par la somme alternée $\rho - \rho^s + \dots - \rho^{s^{n-2}}$ et en utilisant l'égalité $(\rho-\rho^s+\dots-\rho^{s^{n-2}}) = (-1)^{\frac{n-1}{2}}n$. On doit donc avoir $Y = c_1 - c_2 = \dfrac{(-1)^{\frac{n-1}{2}}}{n}(\rho-\rho^s+\dots-\rho^{s^{n-2}})[\mathscr{F}(\rho)-\mathscr{F}(\rho^s)]$. La suite du raisonnement de Cauchy est néanmoins valide malgré cette erreur.

$$(35)\qquad \begin{cases} X = 2c_0 - c_1 - c_2 & = \mathscr{F}(\rho) + \mathscr{F}(\rho^s) \\ Y = c_1 - c_2 & = \dfrac{\mathscr{F}(\rho) - \mathscr{F}(\rho^s)}{\rho - \rho^s + \ldots - \rho^{s^{n-2}}} \\ & = (-1)^{\frac{n-1}{2}} n(\rho - \rho^s + \ldots - \rho^{s^{n-2}})[\mathscr{F}(\rho) - \mathscr{F}(\rho^s)]. \end{cases}$$

Cauchy introduit la notation $\Pi_{h,k}$ qui correspond à ce que l'on appelle aujourd'hui les combinaisons :

$$(36)\qquad \Pi_{h,k} = \frac{1.2.3.[(h+k)\varpi]}{(1.2.3.\ldots h\varpi)(1.2.3\ldots k\varpi)},$$

où $0 \leq h, k \leq n$. Si $n < h + k \leq 2n$ alors $\Pi_{h,k} \equiv 0 \pmod p$ et si $0 \leq h + k \leq n$, alors $\Pi_{h,k}$ n'est pas divisible par p.

Dans le cas où $h + k < n$, Cauchy pose $l = n - h - k$ (soit $h + k + l = n$). D'une part, on a [16] :

$$\begin{aligned} 1.2.3.\ldots(n-1) &\equiv [1.2.3\ldots(h+k)\varpi][(-1)(-2)\ldots(-l\varpi)] \pmod n \\ &\equiv [1.2.3.\ldots(h+k)\varpi](-1)^{l\varpi}(1.2.3.\ldots l\varpi) \pmod n. \end{aligned}$$

D'autre part : $1.2.3.\ldots(n-1) \equiv -1 \pmod n$, ce qui correspond à l'application du théorème de Wilson puisqu'on considère que n est premier. Cauchy en déduit donc [17] :

$$1.2.3.\ldots(h+k)\varpi \equiv (-1)^{l\varpi+1}\frac{1}{1.2.3\ldots l\varpi} \pmod n.$$

Finalement [18] :

$$(38)\qquad \Pi_{h,k} = \frac{(-1)^{l\varpi+1}}{(1.2.3\ldots h\varpi)(1.2.3\ldots k\varpi)(1.2.3\ldots l\varpi)}.$$

En posant $R_{h,k} = F(\rho)$, on a : $F(r) = -\Pi_{n-h,n-k}$. Cauchy ne donne ici aucune idée de la démonstration de ce résultat. On reconnaît ici un passage d'une égalité exprimée en fonction de ρ, racine de l'équation $x^n = 1$ à une égalité exprimée en fonction de r, racine de l'équivalence $x^n \equiv 1 \pmod p$. Comme précédemment, il utilise dans les deux

16. En effet : $-l\varpi = -(n-h-k) \times \frac{p-1}{n} = (h+k)\varpi - (p-1) \equiv (h+k)\varpi + 1 \pmod n$. Néanmoins, Cauchy ne précise pas quel module est considéré dans ces équivalences.

17. Dans le mémoire, la formule est écrite comme une égalité et non comme une équivalence ; nous supposons que c'est une erreur de frappe.

18. Il semble qu'ici, Cauchy considère toujours des équivalences qu'il note comme des égalités.

cas des égalités. Ici, Cauchy s'appuie donc sur la correspondance entre les égalités et les équivalences. Une démonstration de cette égalité est donnée dans la note V du mémoire. Nous la détaillons plus loin.

Cauchy reprend alors son raisonnement afin de déterminer le nombre λ :

$$(40)\qquad \begin{cases} \dfrac{X}{p^\lambda} = \dfrac{\mathscr{F}(\rho)}{p^\lambda} + \dfrac{\mathscr{F}(\rho^s)}{p^\lambda} \\ \dfrac{Y}{p^\lambda} = \dfrac{(-1)^{\frac{n-1}{2}}}{n}(\rho - \rho^s + \ldots - \rho^{s^{n-2}})[\dfrac{\mathscr{F}(\rho)}{p^\lambda} - \dfrac{\mathscr{F}(\rho^s)}{p^\lambda}] \\ = \dfrac{(-1)^{\frac{n-1}{2}}}{n}(\rho - \rho^s + \ldots - \rho^{s^{n-2}})[\mathscr{F}(\rho) - \mathscr{F}(\rho^s)] \end{cases}$$

Cauchy raisonne alors en considérant ces égalités modulo p :

> [...] et, comme les seconds membres des formules (40) seront des fonctions symétriques de ρ, ρ^2, ..., ρ^{n-1}, ils devront rester équivalents, suivant le module p, à $\dfrac{X}{p^\lambda}$ et à $\dfrac{Y}{p^\lambda}$, quand on y remplacera ρ par r. Donc, alors, l'un et l'autre seront entiers, et l'un d'eux au moins sera non divisible par p [Cauchy, 1840a, p. 13].

Pour $1 \leq h \leq \dfrac{n-1}{2}$, on peut remplacer[19] $R_{h,h}$ par $\dfrac{p}{R_{-h,-h}}$ dans (34) ce qui donne

$$\begin{cases} \mathscr{F}(\rho) = p^{\nu'}\varphi(\rho), \\ \mathscr{F}(\rho^s) = p^{\frac{n-1}{2}-\nu'}\chi(\rho) = p^{\nu''}\chi(\rho), \end{cases}$$

où ν' est le nombre d'exposants 1, s^2, s^4, ..., s^{n-3} qui sont équivalents à un nombre entier compris entre 1 et $\frac{n-1}{2}$, où $\nu'' = \frac{n-1}{2} - \nu'$, et où $\varphi(r)$ et $\chi(r)$ « ne seront équivalents ni à zéro ni à $\frac{1}{0}$ suivant le module p » [Cauchy, 1840a, p. 13]. Il suffit alors de poser $\lambda = \min(\nu', \nu'')$. En posant $X = p^\lambda x$ et $Y = p^\lambda y$, on aura

$$(44)\qquad 4p^\mu = x^2 + ny^2,$$

où $\mu = \pm\left(\dfrac{4\nu' - n + 1}{2}\right)$.

Cauchy résume alors la première partie de la note IV - où l'on obtient le nombre noté ici ν' - pour en déduire que $\mu = \pm 2\mathscr{A}_{\frac{n+1}{4}}$, où $\mathscr{A}_{\frac{n+1}{4}}$ désigne un nombre de Bernoulli. Cela montre bien que Cauchy, en 1830, avait bien une démonstration de l'existence de ce lien. Nous résumons ci-après la note IV, où la démonstration de Cauchy est plus détaillée que dans la partie principale du mémoire. Cauchy conclut ce premier paragraphe en appliquant les résultats précédents à trois exemples et en déduit que les équations $p = x^2 + 7y^2$,

19. En effet, selon la formule (12), $R_{h,h}R_{-h,-h} = p$ si h et $2h$ ne sont pas divisibles par n.

$4p^2 = x^2 + 11y^2$ et $p^2 = x^2 + 163y^2$ sont résolubles en nombres entiers, lorsque p est de la forme $nx + 1$ pour $n = 8$, $n = 11$ et $n = 163$ respectivement.

2 - Lien avec les nombres de Bernoulli (Note IV)

Ce résultat est important : en effet, c'est apparemment la première fois que les nombres de Bernoulli sont mis en lien avec les résidus quadratiques. Ils seront notamment utilisés par Kummer dans sa démonstration de certains cas du dernier théorème de Fermat. Nous reviendrons sur ce point dans la conclusion de cette partie.

Cauchy démontre dans la note IV des résultats liant la différence du nombre de résidus et de non résidus quadratiques avec les nombres de Bernoulli. Il donne les principales étapes de cette démonstration dans la partie principale du mémoire ; nous allons ici résumer ce qu'il fait dans la note IV, où il utilise le calcul intégral et le calcul différentiel. Ici, les nombres de Bernoulli interviennent lors de résultats sur le développement en série entière de $tanz$.

Cauchy commence par rappeler des propriétés sur les résidus et non-résidus quadratiques d'un nombre premier p, avec notamment l'égalité :

$$\left[\frac{1}{p}\right] + \left[\frac{2}{p}\right] + \left[\frac{3}{p}\right] + \ldots + \left[\frac{p-1}{p}\right] = 0. \tag{10}$$

Il se place ensuite dans un cas plus général, où il considère un ensemble fini de nombres premiers à p ; l'objectif est ici de déterminer la valeur de la différence entre le nombre de résidus et non-résidus quadratiques contenus dans cet ensemble de nombres.

Soient a, b, c, $\ldots$, l, un ensemble de n nombres premiers à p. Soit n', le nombre de résidus quadratiques contenus dans cet ensemble, et n'' le nombre de non-résidus quadratiques. Alors $n' + n'' = n$ et $n' - n'' = \left[\frac{1}{p}\right] + \left[\frac{2}{p}\right] + \left[\frac{3}{p}\right] + \ldots + \left[\frac{p-1}{p}\right]$ ce qui donne l'égalité

$$n' - n'' = a^{\frac{p-1}{2}} + b^{\frac{p-1}{2}} + c^{\frac{p-1}{2}} + \ldots + l^{\frac{p-1}{2}} \pmod{p}, \tag{13}$$

que Cauchy réécrit en utilisant le calcul différentiel :

$$n' - n'' \equiv \frac{d^{\frac{p-1}{2}}\left(e^{az} + e^{bz} + e^{cz} + \ldots + e^{lz}\right)}{dz^{\frac{p-1}{2}}} \pmod{p}, \tag{14}$$

où l'on pose $z = 0$ après la différenciation. Selon Cauchy, utiliser l'outil du calcul différentiel permet d'obtenir facilement la valeur de la différence $n' - n''$, et d'en déduire les valeurs de n' et n'', dans le cas où $n < p$ et où les nombres a, b, c, $\ldots l$, peuvent être mis sous la forme d'une progression arithmétique h, $h + k$, $h + 2k$, $\ldots$, $h + (n-1)k$. Dans

ce cas :
$e^{az} + e^{bz} + e^{cz} + \ldots + e^{lz} = \sum_{i=0}^{n-1} e^{(h+ikz)} = e^{hz} \sum_{i=0}^{n-1} e^{ikz} = e^{hz} \frac{e^{nkz-1}}{e^{kz-1}}$. Donc (14) devient :

$$n' - n'' = \frac{d^{\frac{p-1}{2}}}{dz^{\frac{p-1}{2}}} \left[e^{hz} \frac{e^{nkz-1}}{e^{kz-1}} \right]. \tag{15}$$

Cauchy développe alors un exemple « pour fixer les idées » : le cas où l'on cherche le nombre de résidus quadratiques et de non-résidus quadratiques inférieurs à $\frac{p}{2}$. On considère donc la progression arithmétique 1, 2, 3, …, $\frac{p-1}{2}$, soit $n = \frac{p-1}{2}$, $h = 1$, $k = 1$ et

$$n' - n'' = \frac{d^{\frac{p-1}{2}}}{dz^{\frac{p-1}{2}}} \left(\frac{e^{\frac{p+1}{2}z} - e^z}{e^{z-1}} \right). \tag{16}$$

Il détermine ensuite la différence entre le rapport $\frac{e^{\frac{p+1}{2}z} - e^z}{e^{z-1}}$ et ce même rapport lorsque $p = 0$:
$\frac{e^{\frac{p+1}{2}z} - e^z}{e^z - 1} - \frac{e^{\frac{1}{2}z} - e^z}{e^z - 1} = \frac{e^{\frac{p+1}{2}z} - e^{\frac{1}{2}z}}{e^z - 1} = \left(e^{\frac{p+1}{2}z} - e^{\frac{1}{2}z} \right) (e^z - 1)^{-1}$. Cauchy en déduit que la dérivée d'ordre $\frac{p-1}{2}$ de cette expression est composée de termes proportionnels à $e^{\frac{p+1}{2}z} - e^{\frac{1}{2}z}$ ou à une de ses dérivées. Comme $e^{\frac{p+1}{2}z} - e^{\frac{1}{2}z}$ et ses dérivées s'annulent lorsque l'on prend $z = 0$ et $p = 0$, et comme $\frac{e^{\frac{1}{2}z} - e^z}{e^z - 1} = -\frac{1}{2} \left(1 + \frac{e^{\frac{1}{4}z} - e^{-\frac{1}{4}z}}{e^{\frac{1}{4}z} + e^{-\frac{1}{4}z}} \right)$, on obtient, pour $z = 0$:

$$\frac{d^{\frac{p-1}{2}}}{dz^{\frac{p-1}{2}}} \left(\frac{e^{\frac{p+1}{2}z} - e^z}{e^z - 1} - \frac{e^{\frac{1}{2}z} - e^z}{e^z - 1} \right) \equiv 0 \pmod{p}.$$

On obtient donc, d'après (16) ainsi que l'équivalence et l'égalité précédentes :

$$n' - n'' \equiv -\frac{1}{2} \frac{d^{\frac{p-1}{2}}}{dz^{\frac{p-1}{2}}} \left(\frac{e^{\frac{1}{4}z} - e^{-\frac{1}{4}z}}{e^{\frac{1}{4}z} + e^{-\frac{1}{4}z}} \right) \pmod{p}. \tag{18}$$

Comme après les différenciations, on pose $z = 0$, on peut remplacer z par $z\sqrt{-1}$, ce qui permet d'introduire la fonction tangente, et ainsi les nombres de Bernoulli :

$$n' - n'' \equiv (-1)^{1-\frac{p-1}{4}} \frac{1}{2} \frac{d^{\frac{p-1}{2}} \tan \frac{z}{4}}{dz^{\frac{p-1}{2}}}. \tag{19}$$

Enfin, Cauchy rappelle le développement de $\tan z$:

$$\tan\frac{z}{4} = 2\left(\frac{1}{6}\,\frac{2^2-1}{2}\,\frac{z}{1.2} + \frac{1}{30}\,\frac{2^4-1}{2^3}\,\frac{z^3}{1.2.3.4} + \frac{1}{42}\,\frac{2^4-1}{2^4}\,\frac{z^4}{1.2.3.4.5.6} + \dots\right), \tag{20}$$

où $\frac{1}{6}$, $\frac{1}{30}$, $\frac{1}{42}$, ... représentent les nombres de Bernoulli [20], notés $\mathscr{A}_1$, $\mathscr{A}_2$, $\mathscr{A}_3$, ...

L'introduction des nombres de Bernoulli peut paraître étonnante voire artificielle ici : en effet, Cauchy travaille initialement avec une somme de puissances de nombres entiers, et passe par des manipulations liées à l'analyse pour finalement obtenir une expression dépendant de $\tan z$, et ainsi utiliser son développement avec les nombres de Bernoulli. Rappelons néanmoins que les nombres de Bernoulli ont d'abord été introduits par Jacques Bernoulli lors de son étude de sommes de puissances semblables, de la forme $1^k+2^k+\ldots+x^k$. Cela est d'ailleurs indiqué dans un des ouvrages de Lacroix intitulé *Traité des différences et des séries, faisant suite au traité du calcul différentiel et du calcul intégral*, publié en 1800. D'autre part, les nombres de Bernoulli apparaissent dans les séries de Taylor des fonctions trigonométriques : dans son traité, Lacroix indique d'ailleurs le développement de la cotangente en fonction des nombres de Bernoulli [21]. Ces développements trigonométriques sont donc présents dans certains traités d'analyse.

Cauchy va maintenant considérer deux cas, selon que p est de la forme $4x+1$, et donc $\frac{p-1}{2}$ pair, ou p est de la forme $4x+3$, soit $\frac{p-1}{2}$ impair.

Si p est de la forme $4x+1$, alors $n'-n'' \equiv 0 \pmod p$ (car d'après le développement de $\tan z$, la dérivée $k^{\text{ème}}$ de $\tan z$ est nulle pour $z=0$ si k est pair). Dans ce cas, $n' \equiv n'' \equiv \dfrac{p-1}{4} \pmod p$, soit $n' = n'' = \dfrac{p-1}{4}$.

Si p est de la forme $4x+3$, alors on utilise les formules précédentes ainsi que l'équivalence $2^{p-1} \equiv 1 \pmod p$ et on obtient :

$$n'-n'' \equiv (-1)^{\frac{p+1}{2}} 2\left(2-2^{\frac{p-1}{2}}\right)\mathscr{A}_{\frac{p+1}{4}} \pmod p. \tag{22}$$

Cauchy utilise ensuite des résultats qu'il ne démontrera que plus loin :

- Si p est de la forme $8x+3$, alors $2^{\frac{p-1}{2}} \equiv -1 \pmod p$ et donc $n'-n'' \equiv -6\mathscr{A}_{\frac{p+1}{4}}$.

  On en déduit donc, puisque $n'+n'' = \frac{p-1}{2}$: $n' \equiv \dfrac{p-1}{4} - 3\mathscr{A}_{\frac{p+1}{4}}$ et $n'' \equiv \dfrac{p-1}{4} + 3\mathscr{A}_{\frac{p+1}{4}}$
- Si p est de la forme $8x+7$, alors $2^{\frac{p-1}{2}} \equiv 1 \pmod p$ et donc $n'-n'' \equiv 2\mathscr{A}_{\frac{p+1}{4}}$.

20. Nous renvoyons à la note de la page 294 pour un commentaire sur la notation de ces nombres par Cauchy.

21. Voir [Lacroix, 1800, p. 427].

On en déduit donc : $n' \equiv \dfrac{p-1}{4} + \mathscr{A}_{\frac{p+1}{4}}$ et $n'' \equiv \dfrac{p-1}{4} - \mathscr{A}_{\frac{p+1}{4}}$.

Cauchy rappelle qu'il a déjà présenté ces résultats en 1830, et publié un extrait en 1831 dans le *Bulletin de Férussac*.

Signalons également que dans la partie principale de son mémoire, après avoir résumé la preuve détaillée ici, Cauchy reprend les exemples $n = 7$ et $n = 11$ qu'il avait déjà donné dans [Cauchy, 1831]. Il développe également l'exemple $n = 163$, mais sans utiliser les nombres de Bernoulli : à partir de la liste des puissances successives d'une racine primitive, il détermine directement les valeurs de nombres n' et n''. Cela vient du fait que seuls les premiers nombres de Bernoulli sont connus, mais il est remarquable que Cauchy ne fasse aucun commentaire à ce sujet [22]. D'autre part, comme en 1831, Cauchy ne justifie pas l'existence de l'inverse des dénominateurs des nombres de Bernoulli dans les équivalences considérées.

3 - Déterminer un équivalent des expressions $R_{h,k}$ modulo p (Note V)

Dans cette note, Cauchy démontre la proposition fondamentale utilisée également par Jacobi : transposer une équation en équivalence afin de déterminer un équivalent des expressions $R_{h,k}$.

Cette note est intitulée *Détermination des fonctions $R_{h,k}$, ... et des coefficients qu'elles renferment* et contient une quarantaine de pages.

Cauchy utilise à nouveau des notations semblables aux notes précédentes et rappelle des résultats justifiés précédemment, dont :

Si $h + k$ n'est pas divisible par $p - 1$,

(8) $$R_{h,k} = \sum_{\substack{1 \le i \le p-2 \\ t^i + t^j \equiv 1 \pmod p}} (\tau^{ih+jk}).$$

On a également :

(10 et 12) $$R_{h,k} = \sum_{\substack{1 \le i \le p-2 \\ t^i + t^j \equiv 1 \pmod p}} (\tau^{ih+jk}) = \sum_{i=0}^{p-2} a_i \tau^i,$$

où les a_i sont des nombres entiers et tels que

22. Rappelons que Lebesgue, dans [Lebesgue, 1842], note d'ailleurs que la méthode de Cauchy n'est pas praticable pour cette raison : voir p. 101.

(11) $$\sum_{i=1}^{p-2} a_i = p-2.$$

Si on remplace τ par τ^m

- Si $m(h+k)$ n'est pas divisible par $p-1$, on obtient :

(13) $$S(\tau^{imh+jmk}) = \sum_{i=0}^{p-2} a_i \tau^{im},$$

soit

(14) $$R_{mh,mk} = \sum_{i=0}^{p-2} a_i \tau^{im}.$$

- Si $m(h+k)$ est divisible par $p-1$:

  1. si mh et mk ne sont pas divisibles par $p-1$, alors

(16) $$R_{mh,mk} = \sum_{i=0}^{p-2} a_i \tau^{im} = -1.$$

  2. Si mh et mk sont divisibles par $p-1$:

(18) $$R_{mh,mk} = \sum_{i=0}^{p-2} a_i \tau^{im} = p-2.$$

Cauchy donne une méthode pour déterminer les coefficients a_i pour t, h et k donnés. Il faut résoudre l'*équation* $t^i + t^j \equiv 1 \pmod{p}$ pour j et en déduire la valeur de j correspondant à chaque valeur de i.
Par exemple, $p = 5$. Alors $\tau = \pm\sqrt{-1}$ est une racine primitive de $x^4 = 1$. t est une racine primitive de $x^4 \equiv 1 \pmod{5}$: on peut donc prendre $t = 2$. Pour $i = 1, 2, 3$, on a respectivement : $j = 2, 1, 3$.
Ainsi : $S(\tau^{ih+jk}) = \tau^{h+2k} + \tau^{2h+k} + \tau^{3(h+k)}$. On peut alors en déduire les a_i en fonction des valeurs de h et k, et en utilisant les formules (8) et (10).

Cauchy donne ensuite des formules permettant de déterminer les a_i en fonction des sommes $S(\tau^{imh+jmk})$. En effet, à partir de la formule (13) :

$$(19)\qquad \begin{cases} a_0 + a_1 + a_2 + \ldots + a_{p-2} = p-2 \\ a_0 + a_1\tau + a_2\tau^2 + \ldots + a_{p-2}\tau^{p-2} = S\big(\tau^{ih+jk}\big) \\ a_0 + a_1\tau^2 + a_2\tau^4 + \ldots + a_{p-2}\tau^{2(p-2)} = S\big(\tau^{2(ih+jk)}\big) \\ \ldots \\ a_0 + a_1\tau^{p-2} + a_2\tau^{2(p-2)} + \ldots + a_{p-2}\tau^{(p-2)^2} = S\big(\tau^{(p-2)(ih+jk)}\big) \end{cases}$$

Pour déterminer le coefficient a_m, on multiplie respectivement les égalités de (19) par 1, τ^{-m}, τ^{-2m}, $\ldots$, $\tau^{-(p-2)m}$. On obtient donc :

$$\begin{cases} \sum_{i=0}^{p-2} a_i = p-2 \\ \sum_{i=0}^{p-2} a_i\tau^{i-m} = \tau^{-m}S\big(\tau^{ih+jk}\big) \\ \sum_{i=0}^{p-2} a_i\tau^{2(i-m)} = \tau^{-2m}S\big(\tau^{2(ih+jk)}\big) \\ \ldots \\ \sum_{i=0}^{p-2} a_i\tau^{(p-2)(i-m)} = \tau^{-(p-2)m}S\big(\tau^{(p-2)(ih+jk)}\big) \end{cases}$$

En additionnant ces différentes égalités, le membre de gauche est égal à :

$$\sum_{i=0}^{p-2} a_i \sum_{j=0}^{p-2} \tau^{j(i-m)} = \sum_{\substack{0\le i\le p-2 \\ i\neq m}} a_i \sum_{j=0}^{p-2} \tau^{j(i-m)} + (p-1)a_m.$$

Or, Cauchy rappelle que :

- Si h n'est pas divisible par $p-1$:

$$(20)\qquad 1 + \tau^h + \tau^{2h} + \ldots + \tau^{(p-2)h} = 0.$$

- Si h est divisible par $p-1$:

$$(21)\qquad 1 + \tau^h + \tau^{2h} + \ldots + \tau^{(p-2)h} = p-1.$$

Donc, si $i \neq m$, alors $i-m$ n'est pas divisible par $p-1$, donc $\sum_{j=0}^{p-2} \tau^{j(i-m)} = 0$.

On en déduit donc le membre de gauche est égal à $(p-1)a_m$.

Finalement, on obtient :

$$(22) \qquad (p-1)a_m = p-2+\sum_{s=1}^{p-2}\tau^{-sm}S(\tau^{s(ih+jk)}),$$

soit

$$(23) \quad (p-1)a_m = p-2+\tau^{(p-2)m}S(\tau^{ih+jk})+\tau^{(p-3)m}S(\tau^{2(ih+jk)})+\ldots+\tau^{m}S(\tau^{(p-2)(ih+jk)}).$$

Cauchy traduit ensuite des égalités en équivalences : si on prend i, j tels que $t^i+t^j\equiv 1 \pmod p$, on considère l tel que $ih+jk\equiv l \pmod{p-1}$, où $0\le l\le p-2$, alors $\tau^{ih+ik}=\tau^l$ et $t^{ih+ik}\equiv t^l \pmod p$. Finalement, à partir de la formule (10), on obtient :

$$(24) \qquad S(t^{ih+jk})\equiv\sum_{s=0}^{p-2}a_s t^s \pmod p$$

et à partir de la formule (13) :

$$(25) \qquad S(t^{imh+jmk})\equiv\sum_{s=0}^{p-2}a_s t^{ms} \pmod p.$$

En reproduisant le même raisonnement que ci-dessus, appliqué aux équivalences, on obtient :

$$(29) \qquad (p-1)a_m\equiv p-2+\sum_{s=1}^{p-2}t^{-sm}S(t^{s(ih+jk)}) \pmod p,$$

soit

$$(30) \qquad a_m\equiv 2-t^{(p-2)m}S(t^{ih+jk})-t^{(p-3)m}S(t^{2(ih+jk)})-\ldots-t^{m}S(t^{(p-2)(ih+jk)}) \pmod p.$$

D'après (11), on doit avoir $a_m\le p-2$. Ces quantités a_m pourront être trouvées à partir des formules précédentes si on trouve des équivalents modulo p aux sommes $S(t^{s(ih+jk)})$. La suite de la note est donc consacrée à déterminer les valeurs de ces sommes modulo p en fonction des valeurs de h et k.

On suppose que les nombres h et k sont compris entre 0 et $p-2$. En effet, on peut toujours se ramener à ce cas puisque t est une racine de $x^{p-1}\equiv 1 \pmod p$.

- Si $h+k=0$, soit $h=k=0$, alors

(32) $$S(t^{ih+jk}) = p-2.$$

soit

(33) $$S(t^{ih+jk}) \equiv -2 \pmod{p}.$$

- Si $h+k = p-1$, alors $ih+jk = i(p-1-k)+jk = i(p-1)+(j-i)k$. Comme τ est une racine de $x^{p-1} = 1$, alors

(35) $$S(\tau^{ij+jk}) = S(\tau^{(j-i)k}) = \tau + \tau^2 + \ldots + \tau^{p-2} = -1.$$

Finalement :

(36) $$S(t^{ij+jk}) \equiv -1 \pmod{p}.$$

- Si $0 < h+k < p-1$: comme $t^i + t^j \equiv 1 \pmod{p}$, on a :

(38) $$S(t^{ij+jk}) \equiv S(t^{ih}(1-t^i)k) \pmod{p},$$

où la somme est faite pour les valeurs de i comprise entre 0 et $p-2$.
De plus, comme $0 < h+k < p-1$ et comme $\sum_{s=0}^{p-2} t^{sh} \equiv 0 \pmod{p}$, on a : $\sum_{i=0}^{p-2} t^{i(h+j)} \equiv 0 \pmod{p}$ pour tout j compris entre 0 et k. Donc les termes du second membre de (38) sont équivalents à 0 modulo p. Ainsi, dans le cas où $0 < h+k < p-1$:

(39) $$S(t^{ij+jk}) \equiv 0 \pmod{p}.$$

- Si $h+k > p-1$, alors $p-1 < h+k < 2(p-1)$. Dans ce cas, en posant $H = (p-1)-h$ et $K = (p-1)-k$, $0 < H+K = 2(p-1)-(h+k) < p-1$.
On a : $S(t^{ih+jk}) \equiv S(t^{-iH-jK}) \pmod{p}$. Cauchy pose $j-i \equiv \iota \pmod{p}$, soit $ih+jk \equiv ih+(i+\iota)k \pmod{p}$ et obtient $S(t^{ih+jk}) \equiv S(t^{-\iota k}t^{-i(h+k)}) \pmod{p}$. De plus, $t^i+t^j \equiv 1 \pmod{p}$, donc $t^{-i} \equiv 1+t^{\iota} \pmod{p}$. Il obtient alors

(45) $$S(t^{ih+jk}) \equiv S[t^{\iota K}(1+t^{\iota})^{H+K}] \pmod{p}.$$

En sommant sur les valeurs de ι telles que $t^{-i} \equiv 1+t^{\iota} \pmod p$, c'est-à-dire les valeurs comprises entre 0 et $p-2$ différentes de $\frac{p-1}{2}$ (car dans ce cas, on aurait $t^{\iota} \equiv 1+t^{\frac{p-1}{2}} \equiv 0$.).
On peut prendre toutes les valeurs de ι comprises entre 0 et $p-2$.
Ensuite, en considérant le développement de $(1+t^{\iota})^{H+K}$ selon les puissances croissantes de t^{ι} et avec (27), (28) et (45), il obtient :

$$S(t^{ih+jk}) \equiv (p-1)\frac{1.2.3\ldots(H+K)}{(1.2.3.\ldots.H)(1.2.3.\ldots.K)} \equiv -\Pi_{H,K} \pmod p. \tag{46}$$

Cette formule est également valable pour $h+k<p-1$ (car dans ce cas $H+K>p-1$ et $\Pi_{H,K} \equiv 0 \pmod p$). La formule (46) est équivalente à :

$$S(t^{ih+jk}) \equiv -\Pi_{p-1-h,p-1-k} \pmod p. \tag{50}$$

Lorsque h et k sont des nombres entiers relatifs quelconques, la notation $\Pi_{h,k}$ désignera le quotient $\frac{1.2.3....(H+K)}{(1.2....H)(1.2....K)}$, où $0 \leq H, K \leq p-1$ sont les résidus de h et k. Finalement, pour des nombres entiers quelconques h et k tels que $h+k$ n'est pas divisible par $p-1$:

$$S(t^{ih+jk}) \equiv -\Pi_{h,k} \pmod p. \tag{51}$$

Dans le cas où $p-1$ divise $h+k$, on aura les formules (33) et (36).

On suppose maintenant que l'on remplace, dans les formules (33), (36) et (51), les nombres h et k par mh et mk, où $0 \leq m \leq p-2$. Cauchy donne alors dans ce cas les formules correspondant aux formules (33), (36), (51) et (30). On a notamment :

$$a_m \equiv 2 + \Pi_{h,k}t^m + \Pi_{2h,2k}t^{2m} + \ldots + \Pi_{(p-2)h,(p-2)k}t^{(p-2)m} \pmod p. \tag{56}$$

Cauchy illustre sa méthode pour déterminer les coefficients $R_{h,k}$ pour $p=5$, avec $t=2$. D'après (56), on a :
$a_m \equiv 2 + \Pi_{h,k}2^m + \Pi_{2h,2k}2^{2m} + \Pi_{3h,3k}2^{2m} \pmod 5$.
Avec $h=k=1$, on a :
$\Pi_{1,1} = \frac{1.2}{1.1} = 2$, $\Pi_{2,2} = \frac{1.2.3.4}{1.2.1.2} = 6 \equiv 1 \pmod 5$ et $\Pi_{3,3} = \frac{6!}{3!3!} = 20 \equiv 0 \pmod 5$ (car $3h+3k > p-1$).
Donc $a_m \equiv 2 + 2^{m+1} + 2^{2m} \equiv 2 + 2^{m+1} + (-1)^m \pmod 5$.
Finalement, il trouve : $a_0 \equiv 0$, $a_1 \equiv 5 \equiv 0$, $a_2 \equiv 1$, $a_3 \equiv 2 \pmod 5$.

Or, les coefficients a_i sont des nombres positifs compris entre 0 et $p-2=3$ donc, d'après

la formule (12) :
$R_{1,1} = \tau^2 + 2\tau^3$. Cette égalité avait déjà été trouvée en utilisant (8).

Cauchy revient ensuite au cas général, pour en déduire :

> Une conséquence importante à laquelle on se trouve immédiatement conduit par la seule inspection des formules (8) et (51), c'est que, dans le cas où la somme $h + k$ n'est pas divisible par $p - 1$, l'expression
>
> $$\Pi_{-h,-k}$$
>
> équivaut, au signe près, à ce que devient la fonction entière de τ représentée par
>
> $$R_{h,k},$$
>
> quand on y remplace une racine primitive τ de l'équation
>
> $$x^{p-1} = 1$$
>
> par une racine primitive t de l'équivalence
>
> $$x^{p-1} \equiv 1 \pmod{p}.$$

Cauchy insiste, comme Jacobi [23] en 1837, sur l'importance de cette correspondance. Rappelons qu'il en fait usage dès sa publication de 1831.

Cauchy conclut en rappelant la difficulté principale de sa méthode :

> Lorsqu'on veut appliquer à des cas particuliers les formules ci-dessus établies, toute la difficulté se réduit à trouver, pour des valeurs de h et k positives, mais inférieures au module p, des quantités équivalentes aux expressions de la forme
>
> $$\Pi_{h,k} = \frac{1.2.3\ldots(h+k)}{(1.2.\ldots.h)(1.2.\ldots.k)},$$
>
> c'est-à-dire aux coefficients numériques que renferme le développement de la puissance
>
> $$(1+t)^{h+k}$$
>
> du binôme $1 + t$. Le calcul direct de ces coefficients devient assez pénible lorsque le nombre t acquiert une valeur considérable. Mais alors même des quantités équivalentes à ces coefficients, suivant le module p, peuvent être assez facilement obtenues par l'une des méthodes que nous allons indiquer [Cauchy, 1840a, p. 196-197].

Pour cela, Cauchy va utiliser la notion d'*indice* qui permet de réduire l'opération de

23. Voir p. 299.

multiplication modulo p à une opération d'addition [24]. En 1839, dans son *Canon Arithmeticus* [Jacobi, 1839a], Jacobi donne une table d'indices pour tous les nombres premiers inférieurs à 1000. Cauchy va d'ailleurs s'y référer à plusieurs reprises :

> D'abord, si, en désignant par t une racine primitive de l'équivalence
>
> $$t^{p-1} \equiv 1 \pmod{p},$$
>
> on nomme *indices* des nombres entiers
>
> $$1, 2, 3, 4, \ldots$$
>
> les diverses valeurs de l'exposant i, pour lesquelles la puissance t^i deviendra successivement équivalente à ces nombres entiers suivant le module p, il est clair, d'une part, que deux nombres seront équivalents, suivant le module p, quand leurs indices seront, ou égaux, ou équivalents suivant le modulo $p-1$, d'autre part, que l'indice d'un produit sera équivalent à la somme des indices de ses facteurs et l'indice d'un rapport à la différence des indices de ses deux termes. Cela posé, si, en se bornant à considérer des nombres entiers et des indices plus petits que la limite p, on construit deux Tables qui offrent le nombre correspondant à chaque indice et l'indice correspondant à chaque nombre, l'addition successive des indices placés à la suite les uns des autres dans la seconde Table fournira les indices des produits
>
> $$1.2, 1.2.3, 1.2.3.4, \ldots$$
>
> et dès lors il deviendra facile de calculer l'indice du rapport
>
> $$\Pi_{h,k} = \frac{1.2.3.\ldots.(h+k)}{(1.2.\ldots.h)(1.2.\ldots.k)},$$
>
> par conséquent une quantité qui soit équivalente à ce rapport suivant le module p. M. Jacobi ayant effectivement construit les Tables dont nous venons de parler pour toute valeur de p inférieure à 1000, il en résulte que, pour une semblable valeur, on obtiendra sans peine un nombre équivalent à $\Pi_{h,k}$ suivant le module p [Cauchy, 1840a, p. 197-198].

Cauchy donne alors quelques exemples relatifs au nombre $p = 17$ et indique également comment déterminer les équivalents de $\Pi_{h,k}$ rapidement, sans utiliser les tables d'indices :

24. Rappelons que c'est Gauss qui introduit la notion d'indice dans la troisième section des *Disquisitiones Arithmeticae*. Gauss indique d'ailleurs, lorsqu'il met en avant le fait que les diverses puissances d'une racine primitive d'un nombre premier p sont congrues modulo p aux nombres entiers compris entre 1 et $p-1$: « Cette propriété remarquable est d'une bien grande utilité, et peut considérablement abréger les opérations arithmétiques relatives aux congruences, à peu près de la même manière que l'introduction des logarithmes dans l'arithmétique ordinaire en abrège les opérations » [Gauss, 1801, art. 57]. Il ajoute un peu plus loin : « Les théorèmes qui regardent les indices sont absolument analogues à ceux qui regardent les logarithmes » [Gauss, 1801, art. 58].

on peut utiliser le « *triangle arithmétique* de Pascal et *les propriétés bien connues de ces nombres* »[25]. Il utilise donc les relations suivantes :

$$\Pi_{h,k} = \Pi_{h-1,k} + \Pi_{h,k-1}, \tag{58}$$

$$\Pi_{h,k} = \Pi_{k,h}, \tag{59}$$

$$\Pi_{h,1} = h + 1,\ \Pi_{1,k} = k + 1. \tag{60}$$

Cauchy donne ensuite quelques exemples de Tables construites à l'aide de sa méthode, et indique dans quelle mesure les valeurs obtenues pour $R_{h,k}$ varient en fonction de la racine primitive choisie.

Enfin, Cauchy conclut en traduisant les formules obtenues dans cette note puis en développant un exemple dans le cas où l'on suppose $p-1 = n\varpi$ et où l'on considère $\Theta_h = \sum_{i=0}^{p-2} \rho^{ih}\theta^{t^i}$, où ρ est une racine primitive de l'équation $x^n = 1$.

VI Les formes quadratiques $p^\mu = x^2 + ny^2$, où n est un diviseur composé de $p-1$

Dans la partie principale de son mémoire, les paragraphes II, III et IV sont consacrés à des cas où le nombre n n'est plus un nombre premier. Nous allons détailler ce que Cauchy expose dans le deuxième paragraphe, dans lequel on voit bien le principe de sa méthode générale.

1 - Un exemple : $n = \omega\nu$, où ν est un nombre premier

Dans le deuxième paragraphe de la partie principale du mémoire, le nombre n, diviseur de $p-1$ est composé. Il pose $n = \omega\nu$, où ν est un facteur premier de n. Cauchy pose également : $\omega\varpi = \psi$. Donc $p-1 = n\varpi = \nu\psi$. Cauchy ne le précise pas mais on a $p = \nu\psi+1$, où ν est un nombre premier : on va donc pouvoir utiliser des résultats de la partie précédente, pour obtenir des formes quadratiques du type $p^\mu = x^2 + ny^2$. Il introduit des racines primitives relatives aux facteurs ν et ω :

- ς une racine primitive de $x^\nu = 1$;

25. Cauchy se réfère à la formule : $\binom{i}{j} = \binom{i-1}{j-1} + \binom{i-1}{j}$, équivalente à $\Pi_{h,k} = \Pi_{h,k-1} + \Pi_{h-1,k}$.

- α est une racine primitive de $x^\omega = 1$; on pourra donc prendre : $\rho = \varsigma\alpha$;
- s est une racine primitive de $x^\nu \equiv 1 \pmod p$;
- u est une racine primitive de $x^{\nu-1} \equiv 1 \pmod \nu$.

Par rapport au premier paragraphe, s joue le rôle de r, qui était une racine primitive de $x^n \equiv 1 \pmod p$, et u joue le rôle de s, qui était une racine primitive de $x^{n-1} \equiv 1 \pmod n$.

Puisque n est un multiple de ν et $n = \omega\nu$, on peut représenter les nombres compris entre 1 et $n-1$ à l'aide de la racine primitive ν par la suite [26] :

$$1, u, \ldots, u^{\nu-2}, \nu+1, \nu+u, \ldots, \nu+u^{\nu-2}, \ldots, (\omega-1)\nu+1, (\omega-1)\nu+u, \ldots, (\omega-1)\nu+u^{\nu-2}.$$

En utilisant les notations précédentes, on a :

$$\Theta_h = \theta + \alpha^h\varsigma^h\theta^t + \alpha^{2h}\varsigma^{2h}\theta^{t^2} + \ldots + \alpha^{(p-2)h}\varsigma^{(p-2)h}\theta^{t^{p-2}}.$$

On suppose que ν et ω sont premiers entre eux, et on pose $\upsilon = \dfrac{1}{\nu} \pmod\omega$, pour obtenir :

- $\alpha^{u^m+\upsilon\nu(1-u^m)} = \alpha$, car $\alpha^\omega = 1$ par définition et $\upsilon\nu \equiv 1 \pmod\omega$;
- $\varsigma^{u^m+\upsilon\nu(1-u^m)} = \varsigma^{u^m}$, car $\varsigma^\nu = 1$ par définition ;
- $\Theta_{u^m+\upsilon\nu(1-u^m)} = \theta + \alpha\varsigma^{u^m}\theta^t + \alpha^2\varsigma^{2u^m}\theta^{t^2} + \ldots + \alpha^{p-2}\varsigma^{(p-2)u^m}\theta^{t^{p-2}}$.
-

$$(2) \qquad \Theta_{u^m+\upsilon\nu(h+u^m)} = \Theta_{u^m+\omega k\upsilon\nu(h+u^m)} = \theta + \alpha^h\varsigma^{u^m}\theta^t + \ldots + \alpha^{(p-2)h}\varsigma^{(p-2)u^m}\theta^{t^{p-2}}$$

On pose, en s'appuyant sur les mêmes définitions et principes que précédemment et en remarquant que $1 + u^2 + \ldots + u^{\nu-3} + \upsilon\nu\left[\frac{\nu-1}{3} - \left(u^2 + \ldots + u^{\nu-3}\right)\right] \equiv \upsilon\nu\frac{\nu-1}{2} \pmod\nu$:

$$(1) \qquad \Theta_1\Theta_{u^2+\upsilon\nu(1-u^2)} \ldots \Theta_{u^{\nu-3}+\upsilon\nu(1-u^{\nu-3})} = \mathscr{F}(\alpha,\varsigma)\Theta_{\upsilon\nu\frac{\nu-1}{2}}.$$

Dans la première partie du mémoire, on avait $\mathscr{F}(\rho) = \Theta_1\Theta_{s^2}\Theta_{s^4} \ldots \Theta_{s^{n-3}}$. On observe donc que $\mathscr{F}(\alpha,\varsigma)$ correspond au produit $\mathscr{F}(\rho)$, en remplaçant s^{2k} par $u^{2k} + \upsilon\nu(1-u^{2k})$. Comme précédemment, on a :

$$(3) \qquad \mathscr{F}(\alpha,\varsigma) = \mathscr{F}(\alpha,\varsigma^{u^2}) = \mathscr{F}(\alpha,\varsigma^{u^4}) = \ldots = \mathscr{F}(\alpha,\varsigma^{u^{\nu-3}}).$$

Cauchy donne ensuite deux autres produits possibles des Θ_h, qui permettent d'obtenir des égalités du même type.

26. Il manque tous les multiples de ν. Ce sont donc tous les nombres compris entre 1 et $n-1$, sauf les multiples de ν.

D'une part, si h est impair

$$\Theta_{1+\upsilon\nu(h-1)}\Theta_{u^2+\upsilon\nu(h-u^2)}\dots\Theta_{u^{\nu-3}+\upsilon\nu(h-u^{\nu-3})} = \mathscr{F}(\alpha^h,\varsigma)\Theta_{\upsilon\nu\frac{\nu-1}{2}h} \tag{4}$$

et

$$\mathscr{F}(\alpha^h,\varsigma) = \mathscr{F}(\alpha^h,\varsigma^{u^2}) = \mathscr{F}(\alpha^h,\varsigma^{u^4}) = \dots = \mathscr{F}(\alpha^h,\varsigma^{u^{\nu-3}}). \tag{5}$$

D'autre part, toujours en supposant h impair :

$$\Theta_{-1-\upsilon\nu(h-1)}\Theta_{-u^2-\upsilon\nu(h-u^2)}\dots\Theta_{-u^{\nu-3}-\upsilon\nu(h-u^{\nu-3})} = \mathscr{F}(\alpha^{-h},\varsigma^{-1})\Theta_{-\upsilon\nu\frac{\nu-1}{2}h} \tag{6}$$

et

$$\mathscr{F}(\alpha^{-h},\varsigma^{-1}) = \mathscr{F}(\alpha^{-h},\varsigma^{-u^2}) = \mathscr{F}(\alpha^{-h},\varsigma^{-u^4}) = \dots = \mathscr{F}(\alpha^{-h},\varsigma^{-u^{\nu-3}}). \tag{7}$$

Finalement, on obtient :

$$\mathscr{F}(\alpha^h,\varsigma)\mathscr{F}(\alpha^{-h}\varsigma^{-1}) = \frac{\theta_{1+\upsilon\nu(h-1)}\theta_{-1-\upsilon\nu(h-1)}\dots\Theta_{u^{\nu-3}+\upsilon\nu(h-u^{\nu-3})}\Theta_{-u^{\nu-3}-\upsilon\nu(h-u^{\nu-3})}}{\Theta_{\upsilon\nu\frac{\nu-1}{2}h}\Theta_{-\upsilon\nu\frac{\nu-1}{2}h}} \tag{8}$$

En utilisant la propriété $\Theta_h\Theta_{-h} = (-1)^{\varpi h}p$, on obtient finalement que [27] $\mathscr{F}(\alpha^h,\varsigma)\mathscr{F}(\alpha^{-h},\varsigma^{-1})$ est égal à $\pm p^{\frac{n-1}{2}}$ ou $\pm p^{\frac{n-1}{3}}$. Cauchy utilise donc toujours la même méthode pour obtenir les formes quadratiques voulues : il cherche à déterminer un produit composé de deux facteurs de la forme $\mathscr{F}(\alpha^a,\varsigma^b)$ tel qu'il soit égal à une puissance de p.

Comme il le fait régulièrement dans la suite de ce mémoire, Cauchy étudie un cas particulier « pour fixer les idées » [Cauchy, 1840a, p. 23], avec $\omega = 4$ et considère que ν est impair et de la forme $4x+1$. On peut donc poser $\upsilon = 1$: dans ce cas $\upsilon\nu = 4x+1 \equiv 1 \pmod{\omega}$, ce qui correspond à la définition de υ.

27. Le numérateur est composé de $\frac{\nu-1}{2}$ facteurs de la forme $\Theta_h\Theta_{-h}$ donc le numérateur est égal à $\pm p^{\frac{n-1}{2}}$. D'autre part, le dénominateur est égal à $(-1)^{\varpi\upsilon\nu\frac{\nu-1}{2}h}p = \pm p$ lorsque $\varpi\upsilon\nu\frac{\nu-1}{2}h$ ne divise pas $p-1$ et est égal à 1 lorsque $\varpi\upsilon\nu\frac{\nu-1}{2}h$ divise $p-1$. Cela dépend donc de la valeur de υ.

Il suppose également que h et $\frac{\nu-1}{4}$ sont impairs (ν est donc de la forme $8x+3$) et détermine la valeur [28] des différents produits de la forme $\Theta_k\Theta_{-k}$:

$$\begin{cases} \Theta_{1+\nu(h-1)}\Theta_{-1-\nu(h-1)} = (-1)^{\varpi\nu h}p = (-1)^{\varpi}p, \\ \Theta_{u^2+\nu(h-u^2)}\Theta_{-u^2-\nu(h-u^2)} = (-1)^{\varpi\nu h}p = (-1)^{\varpi}p, \\ \dots \\ \Theta_{\nu\frac{\nu-1}{2}h}\Theta_{-\nu\frac{\nu-1}{2}h} = (-1)^{\varpi\frac{\nu-1}{2}} = 1 \end{cases}$$

On trouve donc $\mathscr{F}(\alpha^h,\varsigma)\mathscr{F}(\alpha^{-h},\varsigma^{-1}) = p^{\frac{\nu-3}{2}}$.

Cauchy développe ensuite le cas particulier où $h=1$:

$$\mathscr{F}(\alpha,\varsigma)\mathscr{F}(\alpha,\varsigma^{-1}) = p^{\frac{\nu-3}{2}}.$$

Comme α est ici une racine primitive de $x^4=1$, Cauchy pose $\alpha=\sqrt{-1}$, et développe le cas particulier où $\omega=4$, $\nu=5$, soit $n=20$, ce qui correspond à un des cas traités par Jacobi.

On obtient alors $\mathscr{F}(\alpha,\varsigma)\mathscr{F}(\alpha^{-1},\varsigma^{-1}) = p$ et $\mathscr{F}(\alpha,\varsigma) = \dfrac{\Theta_1\Theta_{u^2+5(1-u^2)}}{\Theta_{10}}$, où u est une racine primitive de $x^4 \equiv 1 \pmod 5$. Comme $u^2 \equiv -1 \pmod 5$, il peut aller plus loin :

$\mathscr{F}(\alpha,\varsigma) = \dfrac{\Theta_1\Theta_{-11}}{\Theta_{10}} = \dfrac{\Theta_1\Theta_9}{\Theta_{10}} = R_{1,9}$ et $\mathscr{F}(\alpha^{-1},\varsigma^{-1}) = R_{-1,-9} = R_{19,11}$, soit

$$R_{1,9}R_{19,11} = p.$$

Avec des calculs semblables, et en considérant le produit $p = \mathscr{F}(\alpha,\varsigma^3)\mathscr{F}(\alpha^{-1},\varsigma^3)$, Cauchy obtient :

$$R_{3,7}R_{17,13} = p.$$

Il pose alors [29] :

$$2\mathscr{F}(\alpha,\varsigma) = \lambda' + \mu'\sqrt{-1} + (\lambda'' + \mu''\sqrt{-1})(\varsigma - \varsigma^2 - \varsigma^3 + \varsigma^4)$$

et donc

$$2\mathscr{F}(\alpha,\varsigma^3) = \lambda' + \mu'\sqrt{-1} - (\lambda'' + \mu''\sqrt{-1})(\varsigma - \varsigma^2 - \varsigma^3 + \varsigma^4)$$

28. On utilise la formule $\Theta_h\Theta_{-h} = (-1)^{\varpi h}$, qui est valable lorsque $p-1$ ne divise pas h. Ici, on a donc : $\Theta_{u^{2k}+\nu(h-u^{2k})} = (-1)^{\varpi(u^{2k}+\nu(h-u^{2k}))} = (-1)^{\varpi(u^{2k}(1-\nu)+\nu h)} = (-1)^{\varpi\nu h}$ car $(1-\nu)$ est un nombre pair. Néanmoins, h et ν sont impair donc leur produit l'est également : on devrait donc avoir $(-1)^{\varpi\nu h}p = -(-1)^{\varpi}p\dots$

29. Dans le texte, la somme alternée de la première égalité est $\varsigma - \varsigma^2 + \varsigma^3 - \varsigma^4$: c'est vraisemblablement une erreur de frappe.

$$2\mathscr{F}(\alpha^{-1},\varsigma) = \lambda' - \mu'\sqrt{-1} + (\lambda'' - \mu''\sqrt{-1})(\varsigma - \varsigma^2 - \varsigma^3 + \varsigma^4)$$

$$2\mathscr{F}(\alpha^{-1},\varsigma^3) = \lambda' - \mu'\sqrt{-1} - (\lambda'' - \mu''\sqrt{-1})(\varsigma - \varsigma^2 - \varsigma^3 + \varsigma^4)$$

Il ne justifie pas ces égalités. Néanmoins, la première est semblable à celle utilisée dans le premier paragraphe : en effet, Cauchy a démontré que les propriétés de $\mathscr{F}(\rho)$ implique que cette expression est de la forme $a + b(\rho - \rho^s + \rho^{s^2} - \rho^{s^3} + \ldots - \rho^{s^{n-2}})$, où a et b sont des nombres entiers. Or, ici, Cauchy pose également $\mathscr{F}(\alpha,\varsigma) = \lambda' + \mu'\sqrt{-1} + (\lambda'' + \mu''\sqrt{-1})(\varsigma - \varsigma^2 + \varsigma^4 - \varsigma^3)$, où la somme alternée considérée correspond bien aux sommes considérées précédemment. Cauchy utilise donc toujours une expression de la forme $a + b(\rho - \rho^s + \rho^{s^2} - \rho^{s^3} + \ldots - \rho^{s^{n-2}})$, mais ici, les nombres a et b sont des nombres de l'anneau $\mathbb{Z}[i]$. Cauchy ne commente absolument pas le fait qu'il utilise dans ce cas des nombres entiers complexes : il semble simplement transposer ses raisonnements précédents.

Les trois égalités suivantes s'obtiennent facilement : en effet, $\alpha^{-1} = -\sqrt{-1}$ et en remplaçant ς par ς^3 dans la somme alternée $\varsigma - \varsigma^2 - \varsigma^3 + \varsigma^4$, on obtient l'opposé $-(\varsigma - \varsigma^2 - \varsigma^3 + \varsigma^4)$.

Cauchy en déduit, à partir des égalités $4p = 4\mathscr{F}(\alpha,\varsigma)\mathscr{F}(\alpha^{-1},\varsigma) = 4\mathscr{F}(\alpha,\varsigma^3)\mathscr{F}(\alpha^{-1},\varsigma^3)$, et en distinguant les termes multiples de $\sqrt{-1}$:

$$4p = [\lambda' + \lambda''(\varsigma - \varsigma^2 - \varsigma^3 + \varsigma^4)]^2 + [\mu' + \mu''(\varsigma - \varsigma^2 - \varsigma^3 + \varsigma^4)]^2$$

$$4p = [\lambda' - \lambda''(\varsigma - \varsigma^2 - \varsigma^3 + \varsigma^4)]^2 + [\mu' - \mu''(\varsigma - \varsigma^2 - \varsigma^3 + \varsigma^4)]^2$$

Ainsi, puisque $(\varsigma - \varsigma^2 - \varsigma^3 + \varsigma^4)^2 = 5$, et en posant $S = \varsigma - \varsigma^2 - \varsigma^3 + \varsigma^4)$ on obtient l'égalité :

$$\lambda'^2 + 2\lambda'\lambda''S + 5\lambda''^2 + \mu'^2 + 2\mu'\mu''S + 5\mu''^2 = \lambda'^2 - 2\lambda'\lambda''S + \lambda''^2 + \mu'^2 - 2\mu'\mu''S + 5\mu''^2.$$

Finalement, on a :

$$4p = \lambda'^2 + \mu'^2 + 5(\lambda''^2 + \mu''^2) \text{ et } \lambda'\lambda'' = -\mu'\mu''.$$

Cauchy explique ensuite comment obtenir les valeurs de λ', λ'', μ' et μ'' en utilisant une correspondance équation - équivalence à l'aide de la correspondance $R_{h,k} \equiv -\Pi - h, -k \pmod p$. Soit s une racine primitive de $x^5 \equiv 1 \pmod p$ et a une racine primitive de $x^4 \equiv 1 \pmod p$; on va donc considérer des équivalences à partir d'égalités obtenues en remplaçant $\alpha = \sqrt{-1}$ par a et ς par s. Ainsi, par exemple, $\mathscr{F}(\alpha,\varsigma) = R_{1,9}$, donc :

$$\lambda' + \mu' a + (\lambda'' + \mu'' a)(s - s^2 - s^3 + s^4) \equiv 2\mathscr{F}(a,s) \equiv -2\Pi_{19,11} \equiv 0 \pmod p.$$

On obtient ainsi un système d'équations permettant de déduire facilement les valeurs des coefficients recherchés.

Après avoir développé le cas particulier où $p = 41$, Cauchy reprend le cas où $\omega = 4$ et où ν est un nombre impair de la forme $4x + 1$. Il aboutit notamment au résultat suivant, où on considère $\nu = 5$:

> Donc, tout nombre premier de la forme $20x + 1$ est en même temps de la forme $\beta^2 + 5\gamma^2$, en sorte qu'on peut satisfaire, par des valeurs entières de x, y à l'équation
>
> $$p = x^2 + 5y^2$$
>
> [Cauchy, 1840a, p. 37].

D'après les informations dont nous disposons dans les leçons données par Jacobi [30], ce dernier traite exactement le même cas. Il applique également les résultats obtenus au cas où $\nu = 13$.

Les deux derniers paragraphes traitent d'autres cas où le nombre n est composé, en supposant par exemple que le nombre ω est un nombre premier.

2 - Multiplications des sommes de Gauss dans le cas où n est un nombre composé (suite de la note III)

Dans la seconde partie de la troisième note, Cauchy reprend le raisonnement de la première partie en considérant que le nombre n est composé. Rappelons, qu'à cette occasion, Cauchy introduit une nouvelle notation pour désigner les deux produits de facteurs primitifs considérés. Ainsi ; $[1] = \Theta_1\Theta_{s^2}\Theta_{s^4}\ldots\Theta_{s^{n-3}}$ est le produit des Θ_{s^k}, où l'exposant k est un nombre pair et $[-1] = \Theta_s\Theta_{s^3}\Theta_{s^5}\ldots\Theta_{s^{n-2}}$. Cela permet d'exprimer les égalités obtenues de manière plus simple. Cauchy généralise ici sa notation dans le cas où n n'est plus premier.

Dans un premier temps, Cauchy considère le cas où $n = \nu\omega$, ν et ω étant des nombres premiers entre eux. Un de ces deux facteurs, ν par exemple, est impair. Soit ς, une racine primitive de l'équation $x^\nu = 1$ et α, une racine primitive de l'équation $x^\omega = 1$. Alors, $\rho = \varsigma\alpha$ est bien une racine primitive de $x^n = 1$, et on aura $\rho^h = \varsigma^i\alpha^j$, où $h \equiv i \pmod{\nu}$ et $h \equiv j \pmod{\omega}$.

Ainsi, Θ_h, que Cauchy note également $\Theta_{i,j}$ ici, peut être exprimé en fonction des indices i et j :

$$\Theta_h = \theta + \varsigma^i\alpha^j\theta^t + \varsigma^{2i}\alpha^{2j}\theta^{t^2} + \ldots + \varsigma^{(p-2)i}\alpha^{(p-2)j}\theta^{t^{p-2}} = \Theta_{i,j}. \tag{22}$$

30. Voir leçon 31 de [Jacobi, 2007].

Cauchy donne ensuite des propriétés de $\Theta_{i,j}$:

- $\Theta_{i,j} = \Theta_{i+k\nu,j+k'\omega}$;
- Si $\Theta_h = \Theta_{i,j}$, alors $\Theta_{-h} = \Theta_{-i,-j}$;
- h et i sont de même parité si $\varpi = \frac{p-1}{\nu\omega}$ est impair ;
- Si i est divisible par ν et j est divisible par ω, alors $\Theta_{i,j} = \Theta_{0,0} = -1$;
- Dans le cas contraire, $\Theta_{i,j}\Theta_{-i,-j} = (-1)^{\varpi j} p = \Theta_{i,j}\Theta_{\nu-i,\omega-j}$.

Enfin, puisque $p-1 = \nu\omega\varpi$, si ν et ω sont impairs, alors ϖ est pair, et donc la dernière égalité devient :

$$\Theta_{i,j}\Theta_{-i,-j} = p. \tag{25}$$

Cauchy étudie ensuite plusieurs cas, en fonction de la décomposition en facteurs premiers du nombre n .

(a) Premier cas étudié : $n = \nu\omega$ est le produit de deux nombres premiers impairs.

Soit u une racine primitive de $x^{\nu-1} \equiv 1 \pmod{\nu}$ et a une racine primitive de $x^{\omega-1} \pmod{\omega}$. À partir des propriétés des racines primitives et de la définition de $\Theta_{i,j}$ donnée précédemment, toutes les valeurs de Θ_h, où h est premier à n, sont donc représentées par :

$$\left\{\begin{array}{lllll} \Theta_{1,1} & \Theta_{u,1} & \Theta_{u^2,1} & \dots & \Theta_{u^{\nu-2},1} \\ \Theta_{1,a} & \Theta_{u,a} & \Theta_{u^2,a} & \dots & \Theta_{u^{\nu-2},a} \\ \Theta_{1,a^2} & \Theta_{u,a^2} & \Theta_{u^2,a^2} & \dots & \Theta_{u^{\nu-2},a^2} \\ \dots & \dots & \dots & \dots & \dots \\ \Theta_{1,a^{\omega-2}} & \Theta_{u,a^{\omega-2}} & \Theta_{u^2,a^{\omega-2}} & \dots & \Theta_{u^{\nu-2},a^{\omega-2}} \end{array}\right. \tag{28}$$

Ces différentes valeurs sont au nombre de $N = (\nu-1)(\omega-1)$. N est aussi égal au nombre de termes compris entre 1 et $n-1$, premiers à $n = \nu\omega$.

Cauchy applique les principes précédents au cas où $n = \nu\omega$. On cherche à obtenir $\Theta_{h+k+l+\dots} = -1$ pour avoir $\Theta_h\Theta_k\Theta_l \dots = -R_{h,k,l,\dots}$ comme précédemment et ainsi pouvoir utiliser les propriétés des fonctions symétriques. Pour cela, la somme $h+k+l+\dots$ doit être divisible par $n = \omega\nu$. C'est le cas si on prend toutes les valeurs Θ_h de la forme $\theta_{u^{2i},a^{2j}}$. Dans ce cas, $h+k+l+\dots$ est équivalente modulo ν à la somme des premiers indices dans $\Theta_{i,j}$, soit : $\frac{\omega-1}{2}(1+u^2+\dots+u^{\nu-3}) = \frac{\omega-1}{2}\frac{u^{\nu-1}-1}{u^2-1} \equiv 0 \pmod{\nu}$. D'autre part, $h+k+l+\dots$ est équivalente modulo ω à la somme des seconds indices dans $\Theta_{i,j}$, soit : $\frac{\nu-1}{2}(1+a^2+\dots+a^{\omega-3}) = \frac{\nu-1}{2}\frac{u^{\omega-1}-1}{u^2-1} \equiv 0 \pmod{\omega}$.
De plus, si $\Theta_h = \Theta_{i,j}$, alors $\varsigma^h = \varsigma^i$ et $\alpha^h = \alpha^j$, donc le produit

$$(\Theta_{1,1}\Theta_{u^2,1}\dots\Theta_{u^{\nu-3},1})(\Theta_{1,a^2}\Theta_{u^2,a^2}\dots\Theta_{u^{\nu-3},a^2})\dots(\Theta_{1,a^{\omega-3}}\Theta_{u^2,\omega-3}\dots\Theta_{u^{\nu-3},\omega-3})$$

est une fonction symétrique de ς, ς^{u^2}, …, $\varsigma^{u^{\nu-3}}$ et de α, α^{a^2},…, $\alpha^{a^{\omega-3}}$.

Cauchy introduit une notation similaire à [1] pour simplifier les raisonnements : $[1,1] = (\Theta_{1,1}\Theta_{u^2,1}\dots\Theta_{u^{\nu-3},1})(\Theta_{1,a^2}\Theta_{u^2,a^2}\dots\Theta_{u^{\nu-3},a^2})\dots(\Theta_{1,a^{\omega-3}}\Theta_{u^2,\omega-3}\dots\Theta_{u^{\nu-3},\omega-3})$, ce qui correspond au produit des Θ_h tel que h est premier à n et vérifie les équivalences $x^{\frac{\nu-1}{2}} \equiv 1 \pmod{\nu}$ et $x^{\frac{\omega-1}{2}} \equiv 1 \pmod{\omega}$. De même, $[1,-1]$ désigne le produit des Θ_h tel que h est premier à n et vérifie les équivalences $x^{\frac{\nu-1}{2}} \equiv 1 \pmod{\nu}$ et $x^{\frac{\omega-1}{2}} \equiv -1 \pmod{\omega}$, et ainsi de suite. On a donc :

(33)
$$[1,1] = (\Theta_{1,1}\Theta_{u^2,1}\dots\Theta_{u^{\nu-3},1})(\Theta_{1,a^2}\Theta_{u^2,a^2}\dots\Theta_{u^{\nu-3},a^2})\dots(\Theta_{1,a^{\omega-3}}\Theta_{u^2,a^{\omega-3}}\dots\Theta_{u^{\nu-3},a^{\omega-3}}),$$

(34)
$$[1,-1] = (\Theta_{1,a}\Theta_{u^2,a}\dots\Theta_{u^{\nu-3},a})(\Theta_{1,a^3}\Theta_{u^2,a^3}\dots\Theta_{u^{\nu-3},a^3})\dots(\Theta_{1,a^{\omega-2}}\Theta_{u^2,a^{\omega-2}}\dots\Theta_{u^{\nu-3},a^{\omega-2}}),$$

(35)
$$[-1,1] = (\Theta_{u,1}\Theta_{u^3,1}\dots\Theta_{u^{\nu-2},1})(\Theta_{u,a^2}\Theta_{u^3,a^2}\dots\Theta_{u^{\nu-2},a^2})\dots(\Theta_{u,a^{\omega-3}}\Theta_{u^3,a^{\omega-3}}\dots\Theta_{u^{\nu-2},a^{\omega-3}}),$$

(36)
$$[-1,-1] = (\Theta_{u,a}\Theta_{u^3,a}\dots\Theta_{u^{\nu-2},a})(\Theta_{u,a^3}\Theta_{u^3,a^3}\dots\Theta_{u^{\nu-2},a^3})\dots(\Theta_{u,a^{\omega-2}}\Theta_{u^3,a^{\omega-2}}\dots\Theta_{u^{\nu-2},a^{\omega-2}}).$$

De manière similaire, le produit $[1,-1]$ est une fonction symétrique de ς, ς^{u^2}, …, $\varsigma^{u^{\nu-3}}$ et de α^a, α^{a^3},…, $\alpha^{a^{\omega-2}}$, et ainsi de suite.

De plus, $u^{\frac{\nu-1}{2}} \equiv -1 \pmod{\nu}$ et $a^{\frac{\omega-1}{2}} \equiv -1 \pmod{\omega}$, donc (25) devient :

(37)
$$\Theta_{u^m,a^{m'}}\Theta_{a^{m\pm\frac{\nu-1}{2}},u^{m'\pm\frac{\omega-1}{2}}} = \Theta_{u^m,a^{m'}}\Theta_{-u^m,-a^{m'}} = p.$$

D'après cette dernière propriété, on peut déterminer la valeur des expressions $[\pm1,\pm1]$ ou au moins la valeur de leurs produits en fonction de la parité des nombres $\frac{\nu-1}{2}$ et $\frac{\omega-1}{2}$, et donc de la forme des facteurs ν et ω.

En effet, si ν est de la forme $4x+1$, alors les indices m et $m \pm \frac{\nu-1}{2}$ sont de même « espèce » (c'est-à-dire de même parité). Il en est de même pour ω. Ainsi, dans le cas où ν et ω sont tous deux de la forme $4x+1$, chacun des produits $[\pm1,\pm1]$ sont formés de $\frac{N}{4}$ produits de la forme correspondant à la formule (37). Ainsi, $[\pm1,\pm1] = p^{\frac{N}{8}}$. Finalement :

$$p^{\frac{N}{2}} = [1,1][1,-1][-1,1][-1,-1].$$

Si ν et ω sont de la forme $4x+1$, alors $[1,1]$, $[1,-1]$, $[-1,1]$, et $[-1,-1]$ sont des produits composés de $\frac{N}{4}$ facteurs, soit $\frac{N}{8}$ produits de la forme $\Theta_{u^m,a^{m'}}\Theta_{a^{m\pm\frac{\nu-1}{2}},u^{m'\pm\frac{\omega-1}{2}}}$. Donc, d'après (37), $[1,1]=[1,-1]=[-1,1]=[-1,-1]=p^{\frac{N}{8}}$ et finalement :

((38)) $$p^{\frac{N}{2}}=[1,1][1,-1][-1,1][-1,-1].$$

Si ν et ω sont de la forme $4x+3$, il faut obtenir des produits $\Theta_{i,j}\Theta_{i',j'}$ tels que d'une part i et i' et d'autre part j et j' ne soient pas de la même parité afin de pouvoir appliquer la formule (37). On obtient ainsi deux produits de $\frac{N}{4}$ facteurs : $[1,1][-1,-1]=p^{\frac{N}{4}}$ et $[-1,1][1,-1]=p^{\frac{N}{4}}$. On obtient ainsi la formule (38).

Dans le cas où ν et ω ne sont pas de la même forme, on obtient également la formule (38), toujours en multipliant les expressions $[\pm1,\pm1]$ de manière à pouvoir appliquer la formule (37).

Cauchy continue sa démonstration dans le cas où ν et ω sont des nombres de la forme $4x+3$. Alors, d'après ce qui précède, le produit $[1,1][1,-1]$ sera une fonction symétrique de ς, ςu^2, ς^{u^4}, …, $\varsigma^{u^{\nu-3}}$ et donc une fonction linéaire des sommes $\varsigma+\varsigma^{u^2}+\varsigma^{u^4}+\ldots+\varsigma^{u^{\nu-3}}$ et $\varsigma^u+\varsigma^{u^3}+\varsigma^{u^5}+\ldots+\varsigma^{u^{\nu-2}}$. Ce produit sera également une fonction symétrique de α, α^a, α^{a^2}, …, $\alpha^{a^{\omega-2}}$, et donc de leur somme, qui est égale à -1. Finalement, on a :

$$[1,1][1,-1]=c_0+c_1(\varsigma+\varsigma^{u^2}+\varsigma^{u^4}+\ldots+\varsigma^{u^{\nu-3}})+c_2(\varsigma^u+\varsigma^{u^3}+\varsigma^{u^5}+\ldots+\varsigma^{u^{\nu-2}}).$$

On obtient une expression similaire du produit $[-1,1][-1,-1]$ en substituant ς^u à ς :

$$[-1,1][-1,-1]=c_0+c_1(\varsigma^u+\varsigma^{u^3}+\varsigma^{u^5}+\ldots+\varsigma^{u^{\nu-2}})+c_2(\varsigma+\varsigma^{u^2}+\varsigma^{u^4}+\ldots+\varsigma^{u^{\nu-3}}).$$

En reprenant des notations similaires à la première de la note, on pose $\varsigma-\varsigma^u+\varsigma^{u^2}-\varsigma^{u^3}+\ldots-\varsigma^{u^{\nu-2}}=\Delta$. On a lors : $\Delta^2=(-1)^{\frac{\nu-1}{2}}\nu$. De plus : $\varsigma+\varsigma^u+\varsigma^{u^2}+\varsigma^{u^3}+\ldots+\varsigma^{u^{\nu-2}}=-1$. On a donc $[1,1][1,-1]=\frac{1}{2}(A+B\Delta)$ et $[-1,1][-1,-1]=\frac{1}{2}(A-B\Delta)$, où $A=2c_0-c_1-c_2$ et $B=c_1-c_2$. On obtient ainsi la forme quadratique

$$4p^{\frac{N}{2}}=A^2+\nu B^2.$$

En multipliant les facteurs primitifs dans un autre ordre, soit en considérant les produits $[1,1][-1,1]$ et $[1,-1][-1,-1]$, on obtient l'égalité

$$4p^{\frac{N}{2}}=A^2+\omega B^2.$$

Dans le cas où ν est de la forme $4x+3$ et ω de la forme $4x+1$, on considère les

deux produits $[1,1][-1,-1]$ et $[1,-1][-1,1]$. Le premier produit est une fonction entière et symétrique des racines ς, ς^{u^2}, ..., $\varsigma^{u^{\nu-3}}$ et ς^u, ς^{u^3}, ..., $\varsigma^{u^{\nu-2}}$ d'une part et de α, α^{a^2}, ..., $\alpha^{a^{\omega-3}}$ et de α^a, α^{a^3}, ..., $\alpha^{a^{\omega-2}}$ d'autre part. C'est donc une fonction linéaire des sommes $\varsigma + \varsigma^u + \ldots + \ldots + \varsigma^{u^{\nu-2}}$ et $\alpha + \alpha^u + \ldots + \varsigma^{\alpha^{\omega-2}}$, expressions qui sont toutes deux égales à -1. Le produit $[1,1][-1,-1]$ sera également une fonction symétrique des sommes $(\alpha + \alpha^{a^2} + \ldots + \alpha^{a^{\omega-3}})(\varsigma + \varsigma^{u^2} + \ldots + \alpha^{u^{\nu-3}}) + (\alpha^a + \alpha^{a^3} + \ldots + \alpha^{a^{\omega-2}})(\varsigma^u + \varsigma^{u^3} + \ldots + \alpha^{u^{\nu-2}})$ et $(\alpha^a + \alpha^{a^3} + \ldots + \alpha^{a^{\omega-2}})(\varsigma + \varsigma^{u^2} + \ldots + \alpha^{u^{\nu-3}}) + (\alpha + \alpha^{a^2} + \ldots + \alpha^{a^{\omega-3}})(\varsigma^u + \varsigma^{u^3} + \ldots + \alpha^{u^{\nu-2}})$.

Cauchy pose, de manière similaire à ce qui précède : $\varsigma - \varsigma^u + \varsigma^{u^2} - \ldots - \varsigma^{\nu-2} = \Delta$ et $\alpha - \alpha^a + \alpha^{a^2} - \ldots - \alpha^{a^{\omega-2}} = \Delta'$ et démontre que les sommes précédentes sont alors égales à $\dfrac{1 \pm \Delta\Delta'}{2}$. On conclut alors de même : $4p^{\frac{N}{2}} = A^2 - B^2\Delta^2\Delta'^2$. Or, $\Delta^2 = (-1)^{\frac{\nu-1}{2}}\nu$ et $\Delta'^2 = (-1)^{\frac{\omega-1}{2}}\omega$. Finalement, lorsque ν est de la forme $4x+1$ et ω de la forme $4x+3$, et comme $\nu\omega = n$, on obtient la forme quadratique :

$$4p^{\frac{N}{2}} = A^2 + nB^2.$$

Bien sûr, dans chacun des cas analysés, on peut parfois abaisser la valeur de l'exposant de la puissance de p.

Cauchy remarque que ces formules coïncident bien avec ce qui a été obtenu dans les première, troisième et quatrième parties du mémoire, et qu'elles peuvent être généralisées. Il considère par exemple le nombre n comme produit de trois facteurs premiers.

(b) Deuxième cas étudié : $n = \nu\nu'\nu''$ est le produit de trois nombres premiers impairs.

Dans le cas où le nombre n est composé de trois facteurs, Cauchy définit les produits $[\pm1, \pm1, \pm1]$ de la même manière que précédemment. Soient u, u', u'', les racines primitives respectives des équations $x^{\nu-1} \equiv 1 \pmod{\nu}$, $x^{\nu'-1} \equiv 1 \pmod{\nu'}$, $x^{\nu''-1} \equiv 1 \pmod{\nu''}$. De même, soient ς, ς', ς'', les racines primitives respectives des équations $x^\nu = 1$, $x^{\nu'} = 1$, $x^{\nu'} = 1$. Enfin, $\Delta = \varsigma - \varsigma^u + \varsigma^{u^2} - \ldots - \varsigma^{u^{\nu-2}}$, Δ', Δ'' étant les expressions correspondantes pour les racines ς' et ς''.

Cauchy réitère alors les raisonnements développés précédemment. Il détermine en particulier, en fonction de la forme des trois facteurs ν,ν', ν'' dans quels cas , les expressions Θ_h et Θ_{-h} sont dans la même expression de la forme $[\pm1, \pm1 \pm 1]$ ou dans deux expressions différentes afin de pouvoir utiliser la formule (37). Il démontre notamment que, dans le cas où il y a un ou trois des facteurs qui sont de la forme $4x+3$ - c'est-à-dire quand le nombre n est de la forme $4x+3$ - on obtient une forme quadratique de la forme $p^{\frac{N}{2}} = A^2 + nB^2$. Cauchy conclut que l'on peut généraliser sa démonstration au cas où le nombre n est composé de plusieurs facteurs premiers impairs : on obtient une forme quadratique $p^{\frac{N}{2}} = A^2 + nB^2$ dans le cas où n est de la forme $4x+3$.

(c) Troisième cas étudié : n est un nombre pair.

Cauchy commence par étudier le cas où le nombre n est de la forme $n = 2^k\nu$, où ν est un nombre premier impair, Il indique que lorsque le facteur pair est égal à 2, on obtient des formules équivalentes à celles du cas $n = \nu$.

On pose $n = 4\nu$. Soient α, ς et ρ les racines primitives respectives des équations $x^4 = 1$, $x^\nu = 1$ et $x^n = 1$ et on a $\rho = \alpha\varsigma$. Cauchy définit la notation $\Theta_{i,j}$ comme précédemment. Les différentes expressions de Θ_h, où h est premier à n, sont donc :

$$\Theta_{1,1}, \Theta_{u,1}, \Theta_{u^2,1}, \ldots, \Theta_{u^{\nu-2},1}$$

$$\Theta_{1,3}, \Theta_{u,3}, \Theta_{u^2,3}, \ldots, \Theta_{u^{\nu-2},3},$$

où u est une racine primitive de la congruence $x^{\nu-1} \equiv 1 \pmod{\nu}$.

Cauchy réintroduit ensuite les expressions $[\pm 1, \pm 1]$, et, à l'aide de la méthode précédente, si ν est de la forme $8x + 1$ ou $8x + 5$, alors on obtient la forme quadratique $p^{\nu-1} = A^2 + \nu B^2$. Il montre également que dans le cas particulier où $n = 4$, et donc p est de la forme $4x + 1$, on obtient $p = x^2 + y^2$. Ce théorème avait déjà été démontré par Euler en particulier.

Comme précédemment, Cauchy considère le cas plus général où $n = 4\nu\nu' \ldots$. Il l'illustre par $n = 4\nu\nu'$ et reprend les notations introduites dans le cas où n est composé de trois facteurs premiers impairs. Dans le cas où les facteurs impairs sont de la même forme - et donc dans le cas où n est de la forme $4(4x+1)$ - on obtient la forme quadratique $p^{\frac{N}{2}} = A^2 + \frac{n}{4}B^2$.

Il conclut cette note en résumant sa méthode dans le cas où n est de la forme $8\nu\nu' \ldots$, où ν, ν', $\ldots$, sont des nombres premiers impairs.

VII Retour sur la démonstration de la loi de réciprocité quadratique amorcée en 1829

Contrairement à [Cauchy, 1829a], Cauchy ne fait aucune référence aux lois de réciprocité dans la partie principale de ce texte, qui correspond au travail qu'il a présenté à l'Académie en 1830. Il insère néanmoins dans la quatrième note de son mémoire une démonstration de la loi de réciprocité quadratique, qui permet de compléter le schéma de preuve donné dans [Cauchy, 1829a]. Cauchy commence par exposer une méthode pour déterminer le caractère quadratique de 2, puis la généralise pour obtenir la loi de réciprocité.

1 - Recherche de la valeur de $\left[\frac{2}{p}\right]$ où p est un nombre premier impair

Soit p, un nombre premier impair. Cauchy veut déterminer $\left[\frac{2}{p}\right]$, c'est-à-dire le reste de la division de $2^{\frac{p-1}{2}}$ par p. Cauchy utilise alors une méthode qui, selon lui, est connue :

> Pour y parvenir, il suffira, comme on sait, d'élever à la puissance du degré p l'un quelconque des facteurs imaginaires dans lesquels peut se décomposer le nombre 2 [Cauchy, 1840a, p. 173].

On a $2 = (1+\sqrt{-1})(1-\sqrt{-1}) = (1+\alpha)(1-\alpha)$, où α représente une des racines primitives de l'équation $x^4 = 1$.

D'après la formule (1) : $(1+\alpha)^p = 1 + \alpha^p + pP$, P désigne une fonction entière de α à coefficients numériques entiers.
D'autre part, $\alpha^2 = -1$ et $(1+\alpha)^2 = 2\alpha$ donc
$(1+\alpha)^p = (1+\alpha)^{p-1}(1+\alpha) = 2^{\frac{p-1}{2}}\alpha^{\frac{p-1}{2}}(1+\alpha)$.
Finalement, on a : $2^{\frac{p-1}{2}}\alpha^{\frac{p-1}{2}}(1+\alpha) = 1 + \alpha^p + pP$, soit

$$2^{\frac{p-1}{2}} = \frac{1+\alpha^p}{\alpha^{\frac{p-1}{2}}(1+\alpha)} + p\frac{P}{\alpha^{\frac{p-1}{2}}(1+\alpha)}. \tag{28}$$

Or, si p est de la forme $4x+1$, alors $1+\alpha^p = 1+\alpha$ et [31] :

$$\frac{1+\alpha^p}{\alpha^{\frac{p-1}{2}}(1+\alpha)} = \frac{1}{\alpha^{\frac{p-1}{2}}} = \alpha^{\frac{p-1}{2}} = (\alpha^2)^{\frac{p-1}{4}} = (-1)^{\frac{p-1}{4}} = (-1)^{\frac{p+1}{2}\frac{p-1}{4}}.$$

Si p est de la forme $4x+3$, alors $1+\alpha = \alpha(1+\alpha^3) = \alpha(1+\alpha^p)$ et $\alpha^{p+1} = 1$ donc [32] :

$$\frac{1+\alpha^p}{\alpha^{\frac{p-1}{2}}(1+\alpha)} = \frac{1}{\alpha^{\frac{p+1}{2}}} = \alpha^{p+1}2 = (-1)^{\frac{p+1}{4}} = (-1)^{\frac{p-1}{2}\frac{p+1}{4}}.$$

Dans tous les cas : $\dfrac{1+\alpha^p}{\alpha^{\frac{p-1}{2}}(1+\alpha)} = (-1)^{\frac{(p-1)(p+1)}{8}}$. On a donc :

$$2^{\frac{p-1}{2}} = (-1)^{\frac{(p-1)(p+1)}{8}}\left(1 + p\frac{P}{1+\alpha^p}\right). \tag{29}$$

31. Dans la formule ci-dessous, si on pose $p = 4x+1$, alors $\frac{p-1}{4} = x$ et $\frac{p+1}{2} = 2x+1$ donc $(-1)^{\frac{p-1}{4}} \neq (-1)^{\frac{p+1}{2}\frac{p-1}{4}}$. La démonstration de Cauchy comporte donc une erreur. La méthode présentée ici a néanmoins l'intérêt de pouvoir être appliquée correctement dans le cas de la loi de réciprocité quadratique.

32. Là encore, nous retrouvons une erreur similaire.

De plus, le produit $p\dfrac{P}{1+\alpha^p} = \dfrac{pP(1-\alpha^p)}{2}$ sera égal à $\pm\left(2^{\frac{p-1}{2}} \pm 1\right)$. Comme $P(1-\alpha)^p$ est une fonction entière de α à coefficients entiers et comme sa moitié est égale à une quantité entière, on en déduit que $\dfrac{pP(1-\alpha^p)}{2}$ est un multiple de p et donc :

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{1}{2}\frac{p-1}{2}\frac{q-1}{2}}.$$

Cauchy détaille ensuite, selon la forme de p, ce que l'on obtient à partir de la formule précédente :

- 2 est résidu quadratique modulo p si p est de la forme $8x \pm 1$;
- 2 'est non-résidu quadratique modulo p si p est de la forme $8x \pm 3$.

Relation existant entre $\left[\frac{q}{p}\right]$ et $\left[\frac{p}{q}\right]$, où p et q sont des nombres premiers impairs

Cauchy indique qu'il va utiliser une méthode similaire à la précédente pour démontrer la loi de réciprocité quadratique :

> Une méthode semblable à celle que nous venons de rappeler et par laquelle on obtient la valeur de $\left[\frac{2}{p}\right]$ peut servir à trouver généralement la relation qui existe entre les deux expressions $\left[\frac{q}{p}\right]$ et $\left[\frac{p}{q}\right]$ ou, ce qui revient au même, entre les restes de la division de 2^{q-1} par p et de 2^{p-1} par q, p et q désignant deux nombres premiers impairs [33]. Effectivement, pour obtenir une transformation de l'expression $\left[\frac{q}{p}\right] \equiv p^{q-1}$,il suffit d'élever à la puissance p l'une des racines carrées imaginaires de $\pm p$ [Cauchy, 1840a, p. 177].

Cauchy utilise pour cela un résultat obtenu dans la Note I :

$$\Delta^2 = (-1)^{\frac{p-1}{2}} p, \tag{36}$$

où $\Delta = \theta - \theta^t + \theta^{t^2} + \ldots - \theta^{t^{p-2}}$ représente une racine carrée complexe de $\pm p$, θ est une racine primitive de $x^{p-1} = 1$ et t est une racine primitive de $x^{p-1} \equiv 1 \pmod{p}$.

De plus, la formule donne :

$$\Delta^q = \theta^q - \theta^{qt} + \theta^{qt^2} - \ldots - \theta^{qt^{p-2}} + qQ, \tag{37}$$

où qQ est une fonction entière de θ à coefficients numériques entiers et multiples de q. De plus, comme t est une racine primitive de $x^{p-1} \equiv 1 \pmod{p}$:
$\theta^q - \theta^{qt} + \theta^{qt^2} - \ldots - \theta^{qt^{p-2}} = \pm\left(\theta - \theta^t + \theta^{t^2} - \ldots - \theta^{t^{p-2}}\right) = \pm\Delta$, le signe $\pm$ dépendant du caractère quadratique de q modulo p, donc :

33. Ici, Cauchy considère en fait des restes de $p^{\frac{q-1}{2}}$ et $q^{\frac{p-1}{2}}$... De plus, on a $\left(\frac{p}{q}\right) = p^{\frac{q-1}{2}}$, en élevant à la puissance q une racine carrée de $\pm p$. C'est ce qu'il fait ensuite en calculant Δ^q.

(38) $$\Delta^q = \left[\frac{q}{p}\right]\Delta + qQ.$$

Enfin, $\Delta^q = (\theta - \theta^t + \theta^{t^2} - \ldots - \theta^{t^{p-2}})^q$ est une fonction entière et symétrique de θ, θ^{t^2}, θ^{t^4}, …, $\theta^{t^{p-3}}$ d'une part, et de θ^t, θ^{t^3}, θ^{t^5}, …, $\theta^{t^{p-2}}$ d'autre part ; Δ^q est donc une fonction entière et linéaire des sommes $\theta+\theta^{t^2}+\theta^{t^4}+\ldots+\theta^{t^{p-3}}$ d'une part, et de $\theta^t+\theta^{t^3}+\theta^{t^5}+\ldots+\theta^{t^{p-2}}$ et elle change de signe lorsqu'on substitue θ^t à θ : Δ^q est donc proportionnelle à la différence de ces deux sommes, c'est-à-dire qu'elle est proportionnelle à Δ. On en déduit donc que, dans l'égalité (38), qQ est aussi proportionnel à Δ. En divisant (38) par Δ, on obtient donc

$$\Delta^{q-1} \equiv \left[\frac{q}{p}\right] \pmod{q},$$

et, comme $\Delta^2 = (-1)^{\frac{p-1}{2}}p$, $\Delta^{q-1} = \left[(-1)^{\frac{p-1}{2}}p\right]^{\frac{q-1}{2}}$ et donc :

$$\left[\frac{q}{p}\right] \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}} p^{\frac{q-1}{2}} \pmod{q},$$

soit la loi de réciprocité de Legendre :

$$\left[\frac{q}{p}\right] = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left[\frac{p}{q}\right].$$

Cauchy rappelle qu'il a déjà donné une démonstration semblable dès 1829, dans le *Bulletin de Férussac*[34], et qu'elle est « plus rigoureuse que celle qu'avait obtenue M. Legendre et plus courte que celles auxquelles M. Gauss était d'abord parvenu » [Cauchy, 1840a, p. 179]. Notons néanmoins qu'elle est certes plus courte que les démonstrations de la loi de réciprocité quadratique données par Gauss, mais qu'elle s'appuie notamment sur des propriétés des expressions Θ_h et Δ qui ont été démontrées précédemment. Gauss, dans sa sixième démonstration, travaille également sur l'expression que Cauchy note Δ, pour une indéterminée x (et non pour une racine primitive de $x^{p-1} = 1$), et raisonne à l'aide de divisions par $1 - x^p$. Il calcule séparément les puissances Δ^{q-1} et Δ^q comme Cauchy, mais le fait qu'il n'utilise que des raisonnements s'appuyant sur des divisions de polynômes rend la démonstration moins claire. Cauchy fait également référence à la dernière démonstration de cette loi publiée par Legendre en 1830 dans sa troisième édition de la *Théorie des nombres*, attribuée par ce dernier à Jacobi, et très semblable à celle présentée dans ce mémoire. Jacobi décrit en effet succinctement sa démonstration de la loi de réciprocité quadratique dans une lettre à Legendre datée du 5 août 1827 sur une dizaine de lignes[35]. Sa méthode s'appuie également sur la fonction Δ, qu'il élève à la puissance

34. On retrouve effectivement dans ce mémoire une démonstration semblable sur le fond de la loi de réciprocité quadratique.

35. C'est la première lettre échangée entre les deux hommes et présentée dans

q. La convergence des méthodes de Jacobi et Cauchy, à la même époque, est une fois de plus remarquable.

VIII Cauchy et les formes quadratiques : méthodes et outils

Entre 1829 et 1840, Cauchy publie deux types de textes en lien avec les congruences. Comme nous l'avons vu dans la première partie, ses articles de 1830 notamment contiennent des propriétés générales des congruences, que Cauchy démontre en transposant des preuves déjà connues de la théorie des équations à la théorie des congruences, en utilisant explicitement l'analogie existant entre les équations et les congruences. Le deuxième type de publications concerne les formes quadratiques $p^\mu = x^2 + ny^2$ et $4p^\mu = x^2 + ny^2$, où n est un diviseur de $p - 1$. Comme nous l'avons vu dans son mémoire de 1829 publié dans le *Bulletin de Férussac*, Cauchy annonce alors des résultats très généraux sur les résidus et les lois de réciprocité. Il obtient d'ailleurs des formules générales en lien avec sa version généralisée du symbole de Legendre. Néanmoins, dès 1831, ses recherches sont clairement axées sur les formes quadratiques citées précédemment. Cauchy n'aborde à aucun moment la théorie des formes quadratiques exposée par Gauss dans la section V des *Disquisitiones Arithmeticae* : ses raisonnements sont en effet tous fondés sur la considération des expressions nommées aujourd'hui les sommes de Gauss et de Jacobi, dont les premières sont introduites dans la section VII des *Disquisitiones Arithmeticae*. La ressemblance entre les méthodes développées par Cauchy et Jacobi à la même période et vraisemblablement de manière indépendante s'explique par la source commune des deux mathématiciens : leur étude de la septième section du traité de Gauss les a poussés à travailler de manière plus générale sur les sommes de Gauss, et à obtenir des résultats en lien avec celles-ci.

Les congruences et les résidus interviennent donc dans les recherches de Cauchy comme outils de démonstration : le fait d'utiliser des racines primitives de nombres premiers lui permet d'obtenir des expressions qui sont symétriques ou alternées par rapport aux racines primitives de l'équation $x^n = 1$. Dans le grand mémoire de 1840, Cauchy consacre plusieurs notes à démontrer les propriétés de ces fonctions symétriques et alternées, et à déterminer leur forme : cela lui permet ensuite d'établir une méthode générale pour obtenir les formes quadratiques considérées. Cette méthode est fondée sur ce que Cauchy appelle en 1840 les facteurs primitifs. Multiplier ces facteurs primitifs dans un certain ordre lui permet d'obtenir les formes quadratiques citées précédemment et Cauchy peut ainsi énoncer des

[Legendre et Jacobi, 1875]. La théorie des nombres ne sera presque plus abordée par la suite dans cette correspondance, dont la partie mathématique est essentiellement consacrée à la théorie des fonctions elliptiques. Legendre déconseille d'ailleurs à Jacobi, dans sa lettre du 9 février 1828, de passer trop de temps à travailler sur la théorie des nombres car les recherches associées sont « très difficiles et ne mènent souvent à aucun résultat »[Legendre et Jacobi, 1875, p. 226].

résultats généraux, en fonction de la forme du nombre n diviseur de $p-1$. Sur ce thème, il va bien plus loin que Jacobi par exemple, en considérant plus de cas différents. D'autre part, il utilise également à plusieurs reprises une correspondance équation-congruence pour lever une ambiguïté sur le signe d'un des membres de l'égalité ou pour déterminer la valeur de certains coefficients. Il utilise cette correspondance de la même manière que Jacobi, en substituant à une racine p^{e} de l'unité une racine primitive du nombre p, afin d'obtenir des équivalents modulo p des expression $R_{h,k}$. Il emploie donc un procédé inverse à ce que l'on peut retrouver dans ses articles généraux sur les congruences publiés en 1830 : dans ces derniers, il utilise la théorie des équations pour démontrer des théorèmes de la théorie des congruences tandis qu'ici, il emploie le processus inverse.

Nous avons signalé à plusieurs reprises les ressemblances existant entre les recherches de Cauchy et de Jacobi, tant du point de vue des méthodes développés que de certains résultats obtenus. Il existe néanmoins des différences remarquables entre les travaux des deux mathématiciens : Jacobi applique la théorie de la cyclotomie aux formes quadratiques considérées ici, mais il consacre également ses recherches aux lois de réciprocité [36] et aux résidus d'ordre supérieur. Par exemple, dans [Jacobi, 1839b], il considère les résidus de cinquième, huitième et douzième puissance et montre, à partir de la considération de sommes de Gauss, des résultats sur la décomposition en facteurs premiers complexes des nombres premiers de la forme $5n+1$, $8n+1$ et $12n+1$. Cauchy, de son côté, ne considère pas les résidus d'ordre supérieur dans ses publications postérieures à 1829 et se consacre uniquement aux formes quadratiques. Il ne fait également aucune remarque explicite sur son utilisation des nombres complexes dans ses travaux de théorie des nombres. Il ne commente par exemple pas son appellation "facteurs primitifs".

Il est également remarquable que Cauchy ait introduit les nombres de Bernoulli dans le cadre de ses recherches sur les formes quadratiques. Ces nombres sont effectivement fondamentaux dans les recherches de Kummer sur le dernier théorème de Fermat. Nous commenterons également l'introduction apparemment surprenante de ces nombres dans les recherches arithmétiques des deux mathématiciens dans la conclusion de cette partie. Cette utilisation des nombres de Bernoulli par Cauchy s'accompagne également d'une utilisation importante d'outils de l'analyse. En effet, afin de montrer le lien entre les nombres de Bernoulli et le nombre de résidus et non-résidus quadratiques, Cauchy traduit une égalité en nombres entiers en égalité entre des fonctions trigonométriques, puis utilise des différenciations pour faire apparaître la fonction tangente et introduire ainsi les nombres de Bernoulli à l'aide du développement en série de cette fonction. Comme nous l'avons indiqué, Cauchy emploie également dans d'autres mémoires de théorie des nombres des outils de l'analyse, comme le calcul intégral et ses fonctions réciproques, afin de déterminer la valeur de la somme de Gauss notée Δ. Les mémoires de Cauchy en

36. Rappelons que, dans son cours donné entre 1836 et 1837, Jacobi obtient à partir de la théorie de la cyclotomie des démonstrations des lois de réciprocité cubique et biquadratique.

question entrent donc dans le domaine de l'analyse algébrique arithmétique défini dans [Goldstein et Schappacher, 2007a] : Cauchy y met en relation des résultats de différente nature. Dans d'autres mémoires, Cauchy obtient également une détermination de Δ basée sur des considérations arithmétiques et insiste sur l'importance de construire également ce type de démonstration.

Finalement, comme nous l'avons souligné dans notre première partie, les recherches arithmétiques de Cauchy analysées dans ce chapitre et celui qui précède sont fondées sur une correspondance entre équations et congruences, utilisées dans les deux sens par Cauchy. De plus, même si, dans son premier mémoire de 1829, Cauchy insiste particulièrement sur l'importance des résidus et des lois de réciprocité dans la théorie des nombres, il n'y fait pratiquement plus allusion par la suite et se focalise sur l'étude de certaines formes quadratiques. Pour cela, il se base sur la section VII de l'ouvrage de Gauss et utilise les propriétés particulières de symétrie des sommes de Gauss et de Jacobi. Pour obtenir ses résultats, Cauchy manipule de nombreuses identités algébriques, ce qui renvoie aux pratiques déjà rencontrées chez Lagrange dans notre deuxième partie. En ce sens, comme Poinsot, Cauchy appartient à la "filiation" de Lagrange et Legendre indiquée dans notre première partie : il utilise les congruences en analogie avec les équations, et a pour principal objectif l'étude de formes quadratiques, qui sont finalement des équations indéterminées. Pourtant ses recherches, publiées pendant la même période que les Jacobi, Dirichlet, Kummer, ..., répondent à celles de ces mathématiciens allemands ; nous verrons dans quelle mesure dans la conclusion de cette partie.

CHAPITRE 11

1847 : une nouvelle définition des nombres complexes

I Cauchy et les nombres complexes : un bref aperçu

Dans la première moitié du XIX^{e} siècle, de nombreux travaux abordent la question des nombres complexes. Nous avons indiqué le questionnement d'Abel sur la forme des racines imaginaires des équations. D'autre part, Gauss, Dirichlet, Jacobi, Lebesgue, Poinsot, Galois, ..., publient des mémoires où ils considèrent, voire étudient, les nombres complexes en théorie des nombres, soit du point de vue des racines imaginaires des congruences, soit du point de vue de nombres entiers complexes, comme les entiers de Gauss par exemple. Plus généralement, plusieurs mémoires et traités ont pour objet, au moins en partie, les nombres complexes et leur représentation. Deux courants principaux coexistent alors[1] :

- Le réalisme géométrique, notamment pour Argand ou Mourey, doit donner un certain substrat intuitif, conférer une existence légitime et un statut admissible à ces êtres, dépourvus de sens, que sont jusque-là les nombres imaginaires ;
- Le formalisme de l'algèbre symbolique, pour Servois, s'apparente à la position des algébristes de l'École de Cambridge, qui défend une *pureté* de la science algébrique, science des symboles et de leur combinaison, indépendante de toute formulation géométrique. Dans cette conception, toutes les opérations sur les symboles sont jugées possibles *a priori*, la seule contrainte étant que les lois de combinaison de ces symboles coïncident avec les lois de l'arithmétique quand les symboles représentent aux mêmes des quantités arithmétiques [Dahan Dalmedico, 1997, p. 30].

Jusque dans les années 1830, Cauchy ne fait aucune remarque relative à une représentation géométrique des nombres complexes. D'autre part, son point de vue est également différent de celui de l'école algébrique anglaise, puisqu'il ne suppose pas la validité des opérations et autres propriétés *a priori* mais justifie le passage des réels aux imaginaires, en particulier dans son cours d'*Analyse algébrique*, publié en 1821. Il ne considère pas les nombres complexes comme des nombres ou des quantités, mais comme des expressions symboliques, c'est-à-dire des « expressions qui n'ont aucune signification en elles-mêmes, mais qu'il faut ensuite considérer comme deux égalités entre nombres réels » [Dahan Dalmedico, 1997, p. 29]. Le symbole $\sqrt{-1}$ est donc vu par Cauchy comme un outil de calcul commode, et non comme un objet mathématique. Il nomme donc les

1. Nous nous appuyons ici sur les analyses de [Dahan Dalmedico, 1979], [Dahan Dalmedico, 1997] et [Flament, 2003]. Nous renvoyons à ces ouvrages pour un exposé détaillé de ces courants.

nombres complexes des *expressions imaginaires*. À partir des années 1830, il considère dans certains de ces travaux une représentation des expressions imaginaires par des points du plan par « nécessité topologique » [Dahan Dalmedico, 1997, p. 29].

En 1847, il donne deux méthodes pour remplacer ces expressions imaginaires par des quantités réelles : une méthode géométrique et une méthode basée sur ce qu'il nomme les *équivalences algébriques*[2]. Dans cette section, nous allons étudier les trois textes de Cauchy sur sa théorie des équivalences algébriques, dont l'objectif principal est de faire en sorte que i soit une quantité réelle et que l'usage du symbole $\sqrt{-1}$ devienne ainsi inutile[3].

Deux mémoires de Cauchy sur ce thème sont publiés dans les *Comptes Rendus* des séances de l'Académie des Sciences entre juin et juillet 1847. Sa théorie des équivalences algébriques est ensuite reprise dans un texte publié dans ses *Exercices d'analyse et de physique mathématique*. Remarquons que la période de publication de ces travaux se situe à la fin de l'époque de ses notes sur le dernier théorème de Fermat. Il semble d'ailleurs vouloir tenter de l'appliquer à la théorie des nombres, mais ne poursuit pas les recherches à ce sujet. Il est donc vraisemblable que cette nouvelle théorie des imaginaires ait été conçue après ses réflexions sur les nombres complexes qu'il nomme polynômes radicaux, et donc après sa lecture des travaux de Kummer sur le même thème. Dans [Cauchy, 1847d], Cauchy se réfère en effet à un article publié en 1846 dans le trentième tome *Journal de Crelle* par Kummer[4], lorsqu'il introduit des congruences, dont le module n'est plus un nombre mais un polynôme irréductible : or, dans [Kummer, 1846], l'auteur n'utilise que des nombres entiers pour modules. Par contre, dans [Kummer, 1844], qui est inséré dans le *Journal de Liouville* en 1847, Kummer emploie des congruences dont les modules sont des expressions $f(\alpha)$, où f est une fonction entière et α une racine complexe de l'unité. Ainsi, Kummer considère des congruences dont le module est un nombre complexe, et non plus un nombre entier. Néanmoins, une différence fondamentale avec les équivalences données ici par Cauchy est que les modules considérés par Kummer restent des nombres, tandis que ceux introduits par Cauchy sont des polynômes.

2. Voir notamment [Dahan Dalmedico, 1997] pour des commentaires sur la cohérence de ces deux points de vue.

3. Ces travaux de Cauchy sont notamment étudiés dans [Dahan Dalmedico, 1979], [Dahan Dalmedico, 1997] et [Flament, 2003]. Notre objectif principal n'est pas ici de commenter l'évolution de la vision des nombres complexes par Cauchy, mais de mettre en avant une autre application des congruences par cet auteur.

4. Voir [Kummer, 1846].

II La théorie symbolique des imaginaires de Cauchy présentée dans les *Comptes Rendus* des séances de l'Académie des Sciences

Cauchy publie deux articles sur une *nouvelle théorie des imaginaires* dans les *Comptes Rendus* des séances de l'Académie, datés du 28 juin et du 26 juillet 1847, et rattachés respectivement à l'Analyse algébrique et à l'Analyse mathématique. En effet, dans le premier mémoire, Cauchy commence par établir une théorie des équivalences algébriques, dans lequel il utilise des équivalences dont le module est un polynôme, et non plus un nombre et le second mémoire est intitulé *Mémoire sur l'application de la nouvelle théorie des imaginaires aux diverses branches des mathématiques*. Cauchy y donne des applications en algèbre, trigonométrie et géométrie.

1 - Une première présentation : *Mémoire sur une nouvelle théorie des imaginaires, et sur les racines symboliques des équations et des équivalences* (séance du 28 juin 1847)

Avant de présenter sa *nouvelle théorie des imaginaires*, Cauchy revient sur son cours d'*Analyse algébrique* de 1821 et rappelle :

> [...] j'avais considéré les équations imaginaires comme des formules symboliques, c'est-à-dire comme des formules qui, prises à la lettre et interprétées d'après les conventions généralement établies, sont inexactes et n'ont pas de sens, mais desquelles on peut déduire des résultats exacts en modifiant et altérant, selon des règles fixes, ou ces formules, ou les symboles qu'elles renferment [Cauchy, 1847d, p. 1121].

Ici, Cauchy souhaite donner un statut autre qu'"outil" ou "instrument de calcul" à ces imaginaires :

> Mais il est évident que la théorie des imaginaires deviendrait beaucoup plus claire encore et beaucoup plus facile à saisir, qu'elle pourrait être mise à la portée de toutes les intelligences, si l'on parvenait à réduire les expressions imaginaires et la lettre i elle-même, à n'être que des quantités réelles[Cauchy, 1847d, p. 1121].

C'est l'objet de cette note de dix pages : construire une nouvelle théorie symbolique des imaginaires qui permet de ne plus recourir à des symboles, tels $\sqrt{-1}$, n'ayant aucune signification réelle.

(a) Généralités sur les équivalences algébriques

Cauchy commence par rappeler la notion de *nombres équivalents*, et de *polynômes équivalents*. Deux polynômes $\varphi(x)$ et $\chi(x)$ sont équivalents suivant le module $\varpi(x)$ lors-

qu'ils donnent le même reste après division par $\varpi(x)$; ils peuvent être désignés à l'aide de la notation de Gauss :

$$\varphi(x) \equiv \chi(x) \pmod{\varpi(x)}.$$

Cauchy remarque d'ailleurs que cette notation a déjà été utilisée par Kummer [5]. Il ajoute également que cette équivalence peut être remplacée par l'équation $R\varphi(x) = R\chi(x)$, si *la lettre caractéristique* R placée devant une fonction $f(x)$ désigne le reste de $f(x)$ après division par $\varpi(x)$. Ainsi, si $f(x)$ est divisible par $\varpi(x)$, on a : $Rf(x) = 0$. Il indique encore une autre notation, impliquant la lettre i (mais sans lien avec les nombres complexes pour l'instant) :

> Au lieu de placer une lettre caractéristique R devant une fonction entière $\varphi(x)$, pour indiquer le reste qu'on obtient quand on divise cette fonction par $\varpi(x)$, on pourrait convenir que l'on se servira, pour cette indication, d'une *lettre symbolique* substituée à la variable x, dans la fonction elle-même. Soit i cette lettre symbolique. La seule présence de la lettre i, substituée à x dans une fonction entière $\varphi(x)$, indiquera qu'avant de poser dans cette fonction $x = i$, on doit la réduire au reste de sa division par $\varpi(x)$... [Cauchy, 1847d, p. 1122].

Les égalités données précédemment s'écrivent alors $\varphi(i) = \chi(i)$ et $f(i) = 0$. De même, si $\varpi(x)$ ne divise pas $f(x)$, alors on effectue la division euclidienne de $f(x)$ par $\varpi(x)$: $f(x) = \Pi(x)\varpi(x) + \psi(x)$. Et on a $f(i) = \Pi(i)\varpi(i) + \psi(i) = \psi(i)$.

Quelques remarques sur le statut de cette nouvelle notation :

> Mais il importe d'observer que, si l'équation (9) $[f(i) = \Pi(i)\varpi(i) + \psi(i)]$ se réduit à la formule symbolique (10) $[f(i) = \psi(i)]$, cela tient uniquement à la convention adoptée, suivant laquelle on doit, dans le second membre de l'équation (9), effacer le terme qui renferme $\varpi(x)$, dès que l'on substitue i à x. Si, après cette substitution, $\varpi(i)$ se réduit à zéro, c'est en vertu de la convention dont il s'agit, i pouvant d'ailleurs être numériquement égal à une quantité réelle quelconque, qui, prise pour valeur de x, pourra fournir pour $\varpi(x)$ une valeur très différente de zéro.
>
> Pour nous rapprocher, autant que possible, du langage algébrique, généralement admis dans la théorie des imaginaires, nous dirons que i est une *racine symbolique* de l'équation *caractéristique* $\varpi(x) = 0$, et même de l'équation $f(x) = 0$ quand $f(x)$ sera divisible par $\varpi(x)$: mais au mot *racine symbolique* nous n'attacherons pas l'idée d'une valeur de x pour laquelle $\varpi(x)$ ou $f(x)$ devienne numériquement égal à zéro ; et tandis que les racines réelles d'une équation algébrique en x, par exemple de l'équation (12) $[f(x) = 0]$, devront annuler le premier membre $f(x)$, une racine symbolique i de la même équation devra faire évanouir, non pas $f(x)$, mais le reste de la division de $f(x)$ par un certain diviseur $\varpi(x)$, et même faire évanouir ce reste, quel que soit x [Cauchy, 1847d, p. 1123].

5. À ce sujet, nous renvoyons à notre commentaire plus haut.

Cauchy insiste ici particulièrement sur la nature *symbolique* des équations et des racines considérées. Enfin, Cauchy remarque que si le diviseur $\varpi(x)$ est de degré n alors le reste $\psi(x)$ est de degré $n-1$ au maximum et est donc de la forme $\psi(x) = a_0 + a_1x + a_2x^2 + \ldots a_{n-1}x^{n-1}$, où les a_i sont des constantes. Cauchy conclut que $\psi(x)$ est nul lorsque les a_i sont tous nuls.

(b) Application de la théorie des équivalences algébriques aux imaginaires

Après cette introduction où Cauchy considère un diviseur $\varpi(x)$ quelconque, il indique comment appliquer cette théorie aux imaginaires :

> Une théorie nouvelle et rigoureuse des formules et des équations imaginaires se déduit immédiatement des principes généraux que nous venons d'exposer. Pour obtenir cette nouvelle théorie, il suffit de réduire le diviseur $\varpi(x)$ au facteur binôme x^2+1, et, par conséquent, de prendre pour point de départ cette convention fondamentale, que la *lettre symbolique* i, substituée à la lettre x dans une fonction entière $f(x)$, indiquera la valeur que reçoit non pas cette fonction $f(x)$, mais le reste de la division algébrique de $f(x)$ par x^2+1, quand on attribue à x la valeur particulière i [Cauchy, 1847d, p. 1124].

Cauchy rappelle alors la signification de i en tant que racine symbolique : i est racine symbolique de $f(x)$ lorsque le reste de $f(x)$ après division par x^2+1 est nul. Ainsi : $i^2+1 = 0$.

Cauchy démontre alors quelques propriétés de ces équations symboliques, qui sont en fait équivalentes aux propriétés habituelles de nombres complexes.

Ainsi, considérons $\varphi(x)$ et $\chi(x)$, des fonctions entières de x donnant le même reste après division par x^2+1. Alors, on note $\varphi(i) = \chi(i)$. Si, après division par x^2+1, $\varphi(x)$ (respectivement $\chi(x)$) donne pour reste $ax+b$ (respectivement $cx+d$), alors on a $a+bi = c+di$. Or, puisqu'après division par x^2+1, i peut être remplacé par n'importe quelle valeur, les polynômes $ax+b$ et $cx+d$ doivent donc être égaux pour n'importe quel x et on déduit ainsi $a=c$ et $b=d$. Cauchy déduit d'autres propriétés, notamment la formule de Moivre : $(\cos\alpha + i\sin\alpha)^n = \cos n\alpha + i\sin n\alpha$.

(c) Application à la théorie des nombres

Ici, Cauchy propose d'appliquer sa théorie des équivalences algébriques non plus aux équations, mais aux équivalences. Ainsi, l'*équation caractéristique* doit être à coefficients entiers, et la *racine symbolique* i peut prendre une valeur quelconque, mais entière. De plus :

> S'il s'agit d'équivalences relatives à un module premier p, le coefficient de la plus haute puissance de x dans la formule caractéristique pourra toujours être supposé réduit à l'unité [Cauchy, 1847d, p. 1128].

En effet, un nombre non nul admet toujours un inverse dans $\mathbb{Z}/p\mathbb{Z}$, lorsque p est un nombre premier. Ici, Cauchy considère donc simultanément deux formes d'équivalences : d'une part, les équivalences habituelles dont le module est un nombre premier p, et d'autre part, les équivalences algébriques où l'on considère le reste de l'expression considérée par un polynôme $\varpi(x)$.

2 - Applications de la nouvelle théorie des imaginaires (séance du 26 juillet 1847)

Dans cette note de quatre pages, Cauchy donne un aperçu des applications de sa nouvelle théorie des racines symboliques dans quatre domaines : l'algèbre, la trigonométrie, la théorie des nombres (avec la théorie de la cyclotomie) et la géométrie.

Il commence par donner une traduction du théorème fondamental de l'algèbre - une équation de degré n a toujours n racines réelles ou imaginaires - en termes de division par i^2+1 :

> *$f(x)$ étant une fonction entière de x, si l'on pose $x = a + bi$, a, b, i étant des quantités réelles, on pourra toujours choisir a et b de manière que le reste de la division de $f(a+bi)$ par i^2+1 s'évanouisse, quelle que soit la valeur réelle de i. Si d'ailleurs la fonction $f(x)$ est du degré n, le nombre des systèmes de valeurs de a et de b, qui rempliront la condition indiquée, sera précisément égal à n* [Cauchy, 1847e, p. 129].

Il fait de même avec le théorème de Moivre :

> *Si l'on divise la $n^{ième}$ puissance de $\cos\alpha + i\sin\alpha$ par i^2+1, le reste de la division sera $\cos n\alpha + i\sin\alpha$* [Cauchy, 1847e, p. 130].

De même, dans la théorie des nombres, et plus particulièrement dans l'étude des polynômes radicaux, les racines de l'unité ρ et θ deviennent des indéterminées[6], et il faut considérer les membres des égalités obtenues dans ce domaine comme les restes après division par $\rho^n - 1$ et $\theta^p - 1$.

Enfin, Cauchy donne également un exemple d'application de sa nouvelle théorie aux problèmes de géométrie, où sont considérés des points et des lignes imaginaires.

Cauchy, ici, applique sa nouvelle théorie des imaginaires aux différents domaines où sont habituellement considérés des nombres complexes, et traduit quelques propriétés en termes d'équivalences algébriques.

6. Rappelons que, dans tous les travaux en théorie des nombres de Cauchy, ρ désigne une racine n^e de l'unité, et θ désigne une racine p^e de l'unité.

III Le « *Mémoire sur la théorie des équivalences algébriques substituée à la théorie des imaginaires* »

Enfin, Cauchy insère dans ses *Exercices d'analyse et de physique mathématique* un *Mémoire sur la théorie des équivalences algébriques substituée à la théorie des imaginaires*, qui constitue une sorte de synthèse sur cette méthode construite par Cauchy à partir de la notion d'équivalence algébrique. Cauchy reproduit dans les *Préliminaires* l'introduction de sa note du 28 juin 1847.

(a) Équivalences arithmétiques et algébriques

La première partie de ce mémoire est intitulée *Sur les équivalences arithmétiques et algébriques* ; Cauchy commence par y rappeler, comme dans sa note du 28 juin 1847, les notions de nombres équivalents et polynômes équivalents. Un seul terme est nouveau : le *module* $\varpi(x)$ peut également être nommé le *diviseur*.

Cauchy distingue deux types d'équivalences : les équivalences *arithmétiques*, en lien avec les divisions arithmétiques et les équivalences *algébriques*, en lien avec les divisions algébriques. Cauchy ne le précise pas mais les premières, qu'il attribue à Gauss, concernent donc les divisions par des nombres et les deuxièmes, pour lesquelles il se réfère à Kummer, se rapportent aux divisions par les polynômes. Afin de ne pas confondre les deux, Cauchy introduit de nouvelles notations pour les équivalences algébriques : le signe = ne sera plus remplacé par le symbole ≡, mais par [7] ≍ dans le cas général et ≃ dans le cas où le diviseur est x^2+1, c'est-à-dire dans le cadre de la théorie des imaginaires. Il justifie également sa préférence pour le mot *diviseur* : « pour éviter toute méprise, et attendu que le mot *module* a reçu dans la langue analytique un grand nombre d'acceptations diverses, je donnerai la préférence au mot *diviseur*, quand il s'agira de nommer le polynôme par lequel on doit effectivement diviser les deux membres d'une équivalence algébrique » [Cauchy, 1847a, p. 95]. Il applique donc ces nouvelles notations et définitions à un exemple, en indiquant sa signification en termes d'égalités :

> Cela posé, la formule
>
> $$\varphi(x) \asymp \chi(x) \pmod{\operatorname{div} \varpi(x)}$$
>
> exprimera que les deux polynômes $\varphi(x)$ et $\chi(x)$ sont équivalents entre eux, suivant le diviseur $\varpi(x)$, ou, en d'autres termes, que les deux polynômes, divisés algébriquement par $\varpi(x)$, fournissent le même reste. Cette équivalence pourra donc toujours être remplacée par une équation de la forme
>
> $$\varphi(x) = \chi(x) + u\varpi(x),$$

7. La partie supérieure de ce symbole est en fait un crochet trapézoïdal.

u désignant une fonction entière de x [Cauchy, 1847a, p. 96].

Ce principe est fondamental pour la suite de la nouvelle théorie de Cauchy car il lui permet de démontrer plusieurs propriétés des équivalences algébriques. Ici, il traduit donc les équivalences algébriques en termes d'équations et nous retrouvons cette correspondance équivalence-équation utilisée très souvent par Cauchy. D'autre part, il observe également des analogies entre les équivalences algébriques et arithmétiques : ainsi, les « équivalences algébriques, quand elles sont toutes relatives au même diviseur, peuvent être, aussi bien que des équivalences arithmétiques, combinées entre elles par voie d'addition, de soustraction et de multiplication » [Cauchy, 1847a, p. 96]. Il démontre cette propriété en utilisant le principe énoncé précédemment. En termes modernes, il montre que l'ensemble des équivalences algébriques, relatives à un diviseur donné, est un anneau. Il en déduit également qu'une équivalence algébrique peut également être élevée à une puissance entière quelconque.

Cauchy démontre également le résultat suivant :

> Lorsque que le diviseur $\varpi(x)$ est une fonction entière du degré n, une équivalence relative à ce diviseur entraîne avec elle n équations, qu'on obtient en divisant le premier membre par $\varpi(x)$, après avoir fait passer tous les termes dans ce premier membre, et en égalant ensuite à zéro les coefficients des diverses puissances de x comprises dans le reste de la division effectuée [Cauchy, 1847a, p. 98].

Ce résultat avait déjà été donné dans les notes précédentes. Une équivalence peut effectivement toujours être ramenée à la forme $f(x) \asymp 0 \pmod{\text{div } \varpi(x)}$, c'est-à-dire $c_0 + c_1 x + c_2 x^2 + \ldots + c_{n-1} x^{n-1} = 0$, pour tout x. Ainsi, pour $x = 0$, on obtient $c_0 = 0$, et ainsi de suite.

Cauchy présente une application : le cas où $\varpi(x) = x^n - 1$. Comme $x^n - 1$ divise tout binôme de la forme $x^{mn} - 1$, on a : $x^{mn} - 1 \asymp 0 \pmod{\text{div} x^n - 1}$, soit $x^{mn} \asymp 1$. Donc pour tous l et m entiers, on a : $x^{mn+l} \asymp x^l$. Cauchy remarque donc que l'on peut ainsi connaître le reste d'une fonction $f(x) = \sum_{k=0}^{\cdots} a_k x^k$. On aura en effet :

$$f(x) \asymp a_0 + a_n + a_{2n} + \ldots + (a_1 + a_{n+1} + a_{2n+1} + \ldots)x + \ldots + (a_{n-1} + a_{2n-1} + \ldots)x^{n-1} \pmod{\text{div } x^n - 1}.$$

Il remarque que ce résultat est également valable dans le cas d'une série, où l'on obtiendrait « la somme d'une série convergente ordonnée suivant les puissances entières et ascendantes de la variable x ». Cauchy prolonge ainsi sa théorie aux séries, sans poser la question de la convergence de chacune des séries considérées.

Avant d'exposer sa théorie dans le cas des nombres complexes, il reprend le même raisonnement dans le cas où $\varpi(x) = x^n + 1$.

(b) Application aux imaginaires

Dans la deuxième partie de son mémoire, *Substitution des équivalences algébriques aux équations imaginaires*, Cauchy commence par renier totalement le symbole $\sqrt{-1}$:

> Dans la théorie des équivalences algébriques substituée à la théorie des imaginaires, la lettre i cessera de représenter le signe symbolique $\sqrt{-1}$ que nous répudierons complètement, et que nous pouvons abandonner sans regret, puisqu'on ne saurait dire ce que signifie ce prétendu signe, ni quel sens on doit lui attribuer. Au contraire, nous représenterons par la lettre i une quantité réelle, mais indéterminée ; et, en substituant le signe $\preceq$ au signe $=$, nous transformerons ce qu'on appelait une *équation imaginaire* en une équivalence algébrique, relative à la variable i et au diviseur i^2+1 [Cauchy, 1847a, p. 101].

Comme cela est remarqué dans [Dahan Dalmedico, 1979] et [Flament, 2003], les expressions "équation symbolique" et "racine symbolique" ont disparu pour laisser place à une *quantité réelle mais indéterminée* pour désigner la lettre i ; Cauchy ramène donc ainsi la théorie des imaginaires à la considération de quantités réelles seulement.

Enfin, Cauchy ajoute qu'il ne sera plus nécessaire de préciser le diviseur à partir du moment où on utilise le symbole $\preceq$. Il commence ensuite à démontrer quelques propriétés de ces équivalences algébriques particulières.

Ainsi, comme i^2+1 divise les binômes de la forme $i^{2m}-(-1)^m$, alors $i^{2m} \preceq (-1)^m$ et $i^{2m+1} \preceq (-1)^m i$. Ainsi : $i^{4m} \preceq 1$, $i^{4m+1} \preceq i$, $i^{4m+2} \preceq -1$, $i^{4m+3} \preceq -i$ et une fonction entière $f(i) = \sum_k = 0^{\cdots} a_k i^k$ vérifiera toujours l'équivalence

$$f(i) \preceq a_0 - a^2 + a_4 - a_6 + \ldots + (a_1 - a_3 + a_5 - \ldots)i.$$

Cauchy considère ensuite des produit de facteurs linéaires pour aboutir à la démonstration d'un théorème élémentaire de théorie des nombres : le produit de deux sommes de deux carrés est également une somme de deux carrés.

Ainsi, il remarque :

$$(\alpha+\beta i)(\gamma+\delta i) = \alpha\gamma + (\alpha\delta+\beta\gamma)i + \beta\delta i.$$

Donc, d'après ce qui précède, on obtient l'équivalence :

$$(\alpha+\beta i)(\gamma+\delta i) \preceq \alpha\gamma - \beta\delta + (\alpha\delta+\beta\gamma)i. \tag{8}$$

De même :

$$(\alpha-\beta i)(\gamma-\delta i) \preceq \alpha\gamma - \beta\delta - (\alpha\delta+\beta\gamma)i.$$

Ainsi, en multipliant ces deux équivalences, on obtient :

$$(\alpha^2+\beta^2)(\gamma^2+\delta^2) \asymp (\alpha\gamma-\beta\delta)^2+(\alpha\delta+\beta\gamma)^2.$$

Comme l'indéterminée i n'apparaît pas dans cette dernière équivalence, on en déduit l'égalité correspondante :

$$(\alpha^2+\beta^2)(\gamma^2+\delta^2) = (\alpha\gamma-\beta\delta)^2+(\alpha\delta+\beta\gamma)^2,$$

ce qui correspond au résultat annoncé plus haut.

Cauchy remarque d'ailleurs : « *si les deux membres de l'équivalence se réduisent à des fonctions linéaires de i, on pourra remplacer encore le signe $\asymp$ par le signe $=$, et réduire ainsi l'équivalence proposée à une équation véritable* » [Cauchy, 1847a, p. 103]. Là encore, Cauchy va utiliser son principe à plusieurs reprises afin de démontrer les propriétés habituelles des fonctions trigonométriques.

Enfin, Cauchy montre que les équivalences relatives à la théorie des imaginaires pourront toujours être ramenées à un couple d'équations réelles : « les deux équations réelles dont il s'agit sont précisément celles que l'on considérait comme pouvant être symboliquement représentées par l'équation imaginaire à laquelle nous avons substitué l'équivalence $[f(i) \asymp 0]$ » [Cauchy, 1847a, p. 104].

(c) Applications

Les trois dernières parties du mémoire sont consacrées aux applications possibles de cette nouvelle théorie des imaginaires.

Cauchy commence par revenir sur les applications possibles à la trigonométrie. À partir de la formule (8), Cauchy démontre le théorème de Moivre. En effet, si on pose $\alpha+\beta i = \cos x + i\sin x$, $\gamma+\delta i = \cos y + i\sin y$, et ainsi de suite, on obtient[8] : $(\cos x + i\sin x)(\cos y + i\sin y)\ldots \asymp \cos(x+y+\ldots)+i\sin(x+y+\ldots)$. Ainsi, en posant $x=y=\ldots$, on a :

$$(\cos x + i\sin x)^n \asymp \cos nx + i\sin nx.$$

Cauchy énonce ce résultat en termes de divisibilité : « *Si l'on divise la $n^{ième}$ puissance du binôme $\cos x + i\sin x$ par i^2+1, le reste de la division sera $\cos nx + i\sin nx$* » [Cauchy, 1847a, p. 105].

Il s'intéresse ensuite au résultat d'Euler lié aux exponentielles :

> Voyons maintenant quelle est l'équivalence algébrique qui doit être substituée à

8. Il suffit d'appliquer les formules trigonométriques : $\cos(x+y) = \cos x\cos y + \sin x\sin y$ et $\sin(x+y) = \sin x\cos y + \cos x\sin y$.

la relation découverte par Euler, entre les sinus et les cosinus et les exponentielles imaginaires [Cauchy, 1847a, p. 106].

Pour cela, Cauchy rappelle que $e^x = 1 + \frac{x}{1} + \frac{x^2}{1.2} + \frac{x^3}{1.2.3} \ldots$ et applique cette égalité à ix. À partir des séries associées à $\cos x$ et $\sin x$, il déduit l'équivalence :

$$e^{ix} \simeq \cos x + i \sin x.$$

Cauchy conclut cette partie en remarquant qu'à partir des équivalences algébriques obtenues, on peut déduire les égalités utilisées habituellement dans ce domaine. En effet, lorsque l'on a une équivalence dont les deux membres sont des expressions linéaires de i, alors ils représentent les restes après divisions par $i^2 + 1$ et sont donc égaux.

Il traduit ensuite des résultats en lien avec les modules et les arguments à l'aide de ses nouvelles notations, puis termine son mémoire par un cinquième paragraphe intitulé *Sur la substitution des racines des équivalences algébriques aux racines imaginaires des équations.*

Cauchy considère à nouveau un polynôme entier de degré n : $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$, où les a_k sont des nombres réels. Il rappelle que cette équation admet au plus n racines réelles, et peut même ne pas en avoir. Par contre, en posant $x = \alpha + \beta i$, on a l'équivalence $f(x) \simeq 0$, qui admet toujours n racines. Ainsi : « on pourra toujours trouver des systèmes de valeurs réelles des quantités α et β, pour lesquels se vérifie la condition $f(\alpha + \beta i) \simeq 0$ » [Cauchy, 1847a, p. 117]. Il énonce ensuite trois théorèmes que l'on retrouve classiquement dans la théorie des équations :

- l'équivalence $f(x) \simeq 0$ admet exactement n racines ;
- si $x_1, x_2, \ldots, x_n$ sont les n racines alors $f(x) \simeq (x - x_1)(x - x_2) \ldots (x - x_n)$;
- Cauchy indique enfin la propriété des relations entre coefficients et racines d'une équation polynomiale.

Il ne démontre rien ici, renvoyant le lecteur à une méthode de démonstration déjà utilisée des années plus tôt pour démontrer certaines propriétés des équivalences arithmétiques :

> On pourra aisément démontrer ces diverses propositions, et même les étendre au cas où chacun des coefficients compris dans la fonction entière $f(x)$ serait remplacé par un binôme de la forme $\alpha + \beta i$, si l'on part des principes établis dans le paragraphe précédent, surtout dans le paragraphe IV, et si l'on suit d'ailleurs la démarche que j'ai adoptée, dans le IV^e volume des *Exercices de Mathématiques*, en démontrant les propositions correspondantes de la théorie des équations. Pour que les démonstrations données alors deviennent applicables, il n'y a presque autre chose à faire que de remplacer le signe = par le signe $\simeq$, et les mots *équations*, *égal*, etc., par les mots *équivalence*, *équivalent*, etc [Cauchy, 1847a, p. 117-118].

Ainsi, Cauchy reprend exactement les mêmes arguments que pour les résultats qu'il énonce en 1830 sur les équivalences (arithmétiques) : il suffit de transposer les démonstrations connues pour les équations aux équivalences algébriques, et particulièrement à la théorie des imaginaires, en changeant le signe =.

Enfin, Cauchy conclut son mémoire avec cette idée fondamentale : avec sa théorie des équivalences algébriques, les racines imaginaires des équations deviennent des racines réelles des équivalences algébriques. Lorsque ces dernières sont indépendantes de i, elles sont en même temps des racines réelles de l'équation considérée.

Finalement, dans sa nouvelle théorie des imaginaires basée sur ce qu'il nomme les équivalences algébriques, Cauchy utilise une nouvelle application des congruences, en considérant des modules qui sont des polynômes et construisant les nombres complexes comme des éléments de ce que nous appellerions maintenant $\mathbb{R}[X]/(X^2+1)$. Cela lui permet de construire une théorie des imaginaires en considérant uniquement des quantités réelles. Nous avons également pu voir à plusieurs reprises que Cauchy démontre les premiers principes de cette théorie en se basant sur la correspondance équation - équivalence algébrique. Cauchy ne reprend pas ensuite cette théorie et ne l'applique pas à ses recherches en théorie des nombres ou en analyse par exemple. Néanmoins, cette utilisation des congruences par Cauchy est particulièrement intéressante puisqu'elle permet de redéfinir les nombres complexes à partir de fondements algébriques. Cette nouvelle définition fait passer les imaginaires du statut de symboles à celui de racines réelles d'équivalences. Le fait de pouvoir ramener la théorie des imaginaires à la considération d'objets réels seulement et d'en déduire les principales propriétés de cette théorie permet de légitimer les opérations usuelles faites sur les nombres complexes.

CHAPITRE 12

Cauchy, la théorie des nombres et les autres

Nous avons commenté dans les chapitres précédents les différentes utilisations des congruences par Cauchy. Nous avons également donné un aperçu des travaux de Jacobi sur le même thème et dans notre première partie, nous avons abordé les thèmes traités par Dirichlet et Kummer sur la période de publication de Cauchy. L'origine commune des différents travaux de ces mathématiciens en théorie des nombres est l'ouvrage de Gauss. Dans une histoire centrée sur les résidus d'ordre supérieur et les lois de réciprocité associées, les résultats obtenus par Cauchy semblent effectivement, comme le remarque Lemmermeyer à plusieurs reprises, dispersés et peu convaincants par rapport à ceux de ses collègues allemands, dont l'un des thèmes principaux est justement l'étude des résidus d'ordre supérieur, et des lois de réciprocité associées. Par contre, si on lit les travaux de Cauchy à la lumière des résultats obtenus dans la section VII de Gauss, les recherches de Cauchy sur les formes quadratiques $4p^{\mu} = x^2 + ny^2$ sont dans la continuité des propriétés abordées par Gauss [1]. Ces mathématiciens n'aboutissent donc pas aux mêmes conclusions en partie parce que leurs perspectives ne semblent pas être les mêmes. Ici, nous voulons montrer que, malgré ces différences, les travaux de Cauchy d'une part, et ceux de Jacobi, Dirichlet, Kummer, et Kronecker d'autre part se répondent dans une certaine mesure, à partir d'un exemple : les utilisations des nombres de Bernoulli par Cauchy et Kummer.

Retraçons de manière chronologique les différents résultats liant l'utilisation des nombres de Bernoulli par Cauchy dans ses travaux sur les formes quadratiques et par Kummer dans sa démonstration du dernier théorème de Fermat pour les nombres qu'il qualifie de réguliers. En 1831, Cauchy publie dans le *Bulletin de Férussac* une courte note dans laquelle il énonce un théorème sur certaines formes quadratiques : soit p un nombre premier, n un diviseur de $p-1$ de la forme $4k+3$, alors l'équation $4p^m = x^2 + ny^2$ est résoluble en nombres entiers, quand $m \equiv \pm 2A_{\frac{n+1}{4}} \pmod{n}$, où $A_{\frac{n+1}{4}}$ est un nombre de Bernoulli. De plus, si n' représente le nombre de résidus quadratiques de n inférieurs à $\frac{n-1}{2}$, $m = \frac{|n-1-4n'|}{2}$ ou $m = \frac{|n-1-4n'|}{6}$ selon que n est de la forme $8k+7$ ou $8k+3$. Le nombre m correspond [2] de plus à la différence entre le nombre de résidus et de non-résidus quadratiques de n inférieurs à $\frac{n-1}{2}$. Cauchy démontre ce résultat, entre autres, dans son grand mémoire de 1840, dont la partie principale a été présentée en 1830 à l'Académie des Sciences. Ici, Cauchy fait donc le lien entre l'exposant de la puissance de p de la forme quadratique obtenue, le nombre de résidus et de non-résidus quadratiques compris entre certaines limites et les

1. Rappelons que Gauss, dans l'article 358, montre à partir de ses sommes que les nombres premiers p de la forme $3x+1$ sont tels qu'il existe des nombres entiers a et b vérifiant l'égalité $4p = a^2 + 27b^2$.

2. En effet, le nombre de non-résidus quadratiques inférieurs à $\frac{n-1}{2}$ est égal à $\frac{n-1}{2} - n'$.

nombres de Bernoulli.

Nous avons également vu que Jacobi obtient le même type de résultat dans ses leçons données en 1836 et 1837 à Königsberg, sans utiliser les nombres de Bernoulli : il fait le lien entre l'exposant m de la forme quadratique et la différence entre le nombre de résidus et de non-résidus quadratiques inférieurs à $\frac{n}{2}$.

Dans son mémoire publié en 1838 dans le *Journal de Crelle* sous le titre *Sur l'usage des séries infinies dans la théorie des nombres*, Dirichlet utilise les séries pour déterminer le nombre de classes de formes quadratiques de déterminant négatif. Il prouve [3] notamment que si q est un nombre premier de la forme $4k+3$, alors le nombre de classes de formes quadratiques de déterminant $-q$ est égal à la différence entre le nombre de résidus et de non-résidus quadratiques de q inférieurs à $\frac{1}{2}q$.

Dans ce mémoire, Dirichlet démontre sa formule du nombre de classes de certaines formes quadratiques : si p est un nombre premier de la forme $4k+3$, alors le nombre de classes des formes quadratiques de déterminant $-p$ est égal à la différence entre le nombre de résidus et de non-résidus quadratiques de p inférieurs à $\frac{p}{2}$.

Ainsi, si l'on confronte les travaux des trois savants, il est clair que le nombre de classes de formes quadratiques de déterminant négatif $-p$ où p est de la forme $4k+3$, le nombre de résidus et non-résidus quadratiques de p inférieurs à $\frac{p}{2}$ et les nombres de Bernoulli sont liés, ces derniers étant en lien avec les deux premiers sous la forme d'une congruence donnée par Cauchy dès 1831. Il est d'ailleurs intéressant de voir que Lebesgue commente ces trois résultats dans [Lebesgue, 1842], en indiquant que la méthode de Cauchy pour déterminer le nombre de résidus et non-résidus quadratiques inférieurs à $\frac{p}{2}$ n'a qu'une valeur théorique puisque le calcul des nombres de Bernoulli est ardu. Remarquons enfin que, même s'il est indiqué dans [Lemmermeyer, 2000, p. 394] que Cauchy obtient des résultats sur le nombre de classes de formes quadratiques, ce dernier ne fait aucune allusion dans ses travaux à la théorie des formes quadratiques présentée par Gauss dans la section V de son ouvrage, et donc au nombre de classes de formes quadratiques.

Enfin, Kummer, à partir de 1844, développe sa théorie des nombres idéaux. Dans [Kummer, 1847], il met en avant l'analogie qui existe entre des cas particuliers de sa théorie des nombres idéaux et la théorie des formes quadratiques de Gauss [4]. Il indique

3. Voir [Dirichlet, 1838, p. 265].

4. Nous reprenons ici l'analyse de [Edwards, 1977]. Kummer observe, en définissant des nombres complexes idéaux équivalents :

> Ich gehe in einige nähere Entwickelungen dieser beiden Sätze ein. Zwei ideale complexe Zahlen, welche, mit einer und derselben idealen Zahl multiplicirt, beide zu wirklichen complexen Zahlen machen, nenne ich *äquivalent* oder derselben Classe angehörig, weil dise Untersuchung über die wirklichen und die idealen complexen Zahlen vollständig identisch ist mit der Classification gewisser zusammengehöriger Formen vom $\lambda-1$ten Grade mit $\lambda-1$ Variabeln, über welche *Dirichlet* die Hauptresultate gefunden, aber noch nicht veröffentlicht hat, so dass ich nicht genau weiss, ob sein princip der classification mit diesem, aus der Theorie der complexen Zahlen

notamment [5] que la théorie des formes quadratiques binaires est semblable à celle des nombres complexes de la forme $x + y\sqrt{D}$; en particulier la notion d'équivalence qu'il définit sur les nombres complexes idéaux pour les nombres complexes de la forme $x+y\sqrt{D}$ coïncide avec celle définie par Gauss pour les formes quadratiques. Ainsi, le nombre de classes des nombres idéaux complexes et le nombre de classes de formes quadratiques sont égaux dans ce cas. Kummer fait d'ailleurs référence à plusieurs reprises aux travaux de Dirichlet sur ce thème. Or, en 1847, Kummer propose une démonstration du dernier théorème de Fermat pour les nombres premiers qu'il qualifie de *réguliers*. Ces nombres *réguliers* p sont tels qu'en considérant les nombres cyclotomiques formés à partir des racines p^{e} de l'unité, ils ne divisent pas le nombre de classes de nombres idéaux complexes associés. Kummer montre qu'il est plus simple de ramener cette condition à la suivante [6] : p ne doit pas diviser les numérateurs des nombres de Bernoulli B_2, B_4, ..., B_{p-3}. Ainsi, en regroupant les différents résultats obtenus par Cauchy, Jacobi, Dirichlet et Kummer entre 1831 et 1847, on voit apparaître un lien entre l'utilisation des nombres de Bernoulli par Cauchy et Kummer dans des cadres différents. Kummer, dans une lettre à Kronecker datée du 2 janvier 1852 où il discute de l'équation de Fermat $x^\lambda+y^\lambda = z^\lambda$, indique d'ailleurs explicitement qu'il connaît les travaux de Cauchy en lien avec les nombres de Bernoulli :

> Meine Voraussetzung daß λ nicht eine Ausnahmzahl sei, daß B_n nicht $\equiv 0 \pmod{\lambda}$ sei für einen der Werthe $n = 1, 2, 3, \ldots, \frac{\lambda-3}{2}$, ist von CAUCHY schon dahin zurückgeführt, daß die Summe $1^{\lambda-4}+2^{\lambda-4}+\ldots+\left(\frac{\lambda-1}{2}\right)^{\lambda-4}$ nicht durch λ theilbar sei, welches darauf hinauslaüft, daß nur B_n nicht $\equiv 0 \pmod{\lambda}$ sein muß, ohne diese Voraussetzung aber geht es nicht [KUMMER, 1975, p. 91].

Même si Cauchy, Jacobi, Dirichlet et Kummer n'abordent pas leurs recherches dans la même perspective, cette reconstitution met en évidence une circulation des résultats et méthodes de Cauchy parmi les mathématiciens allemands. Réciproquement, comme nous l'avons signalé lors de notre analyse des mémoires de Cauchy sur sa théorie symbolique des imaginaires, Cauchy utilise les méthodes développées par Kummer dans ses recherches pour introduire ses équivalences algébriques.

Cette théorie symbolique des imaginaires n'est pas reprise ensuite par Cauchy. Mais est présentée par Grunert dans son journal *Archiv der Mathematik und Physik* en 1865 et 1866 [7]. Grunert y reprend de manière très détaillée les différentes propriétés démontrées par Cauchy dans ses mémoires. On retrouve également une généralisation des congruences dans la troisième édition du *Cours d'algèbre supérieure* de Serret, publiée en 1866, dans

sich ergebenden genau überinstimmt [KUMMER, 1847, p. 324].

5. « Die ganze Theorie der Formen vom zweiten Grade, mit zwei Variabeln, kann nämlich als Theorie der complexen Zahlen von der Form $x + y\sqrt{D}$ aufgefasst werden, und führt dann nothwendig zu idealen complexen Zahlen derselben Art »[KUMMER, 1847, p. 325].

6. À ce sujet, voir par exemple [EDWARDS, 1977].

7. Voir [GRUNERT, 1865] et [GRUNERT, 1866].

laquelle il consacre quelques paragraphes à l'étude de congruences suivant un nombre premier et une fonction entière irréductible[8].

Enfin et surtout, cette utilisation des congruences est très semblable à celle choisie par Kronecker dans sa théorie arithmétique des grandeurs algébriques. Jacqueline Boniface montre que « la généralisation de l'arithmétique[9] selon Kronecker est fondée sur une *réduction* du concept de nombre » [Boniface, 2002]. L'objectif de Kronecker est donc de réduire le concept de nombre aux nombres entiers seulement, en définissant ensuite à partir des congruences les fractions et les rationnels comme des *grandeurs*. La ressemblance entre les théories de Cauchy et Kronecker ressortent particulièrement bien à partir de la définition des nombres négatifs par Kronecker par exemple :

> Kronecker took up Cauchy's method precisely in order to avoid the concepts of negative number and of fractional number. Thus, to avoid the introduction of the concept of negative number, he replaces equality by a congruence and the "minus" sign by an indeterminate :
>
> > The concept of negative number can be avoided by replacing, in the formulas, the -1 factor by an indeterminate x and the equality by Gauss's congruence sign modulo $(x+1)$. Thus the equality : $7-9=3-5$ changes into the congruence $7+9x \equiv 3+5x \pmod{x+1}$ [Kronecker, 1887, p. 345] .
>
> Thus there seems to exist a filiation from Gauss to Kronecker through Cauchy, in which operative concepts and the use of indeterminates are transmitted, whose goal is to avoid the introduction of new symbolical signs (Cauchy) or new objects (Kronecker) [Boniface, 2007, 339-340].

Une fois encore, nous voyons donc que, bien que dans ses travaux, Cauchy n'ait pas les mêmes objectifs que Jacobi ou Kummer, ses recherches sur cette nouvelle théorie des imaginaires s'appuient néanmoins sur des outils et objets développés par Gauss et Kummer, et des raisonnements de la même forme sont ensuite travaillés par Kronecker dans le cadre de son programme d'arithmétisation.

8. Voir le troisième chapitre de la section *Les propriétés des nombres entiers*.

9. L'auteur indique que l'arithmétique au sens de Kronecker est une *arithmétique générale* qui contient également l'algèbre et l'analyse : voir [Boniface, 2002, p. 141-152].

Conclusion Générale

À travers cette étude, nous nous sommes proposés de clarifier la mise en place des congruences sur la scène mathématique française entre 1801 et 1850, et plus particulièrement de comprendre pourquoi Poinsot et Cauchy, qui semblent participer activement à leur diffusion ont disparu des histoires de ce domaine publiées au XX^{e} siècle.

Notre hypothèse de départ était que l'historiographie fondée sur une conception des résidus et des congruences telle qu'elle opère dans la théorie algébrique des nombres identifiait rétrospectivement les résultats à considérer (en particulier les différentes versions des lois de réciprocité) au lieu d'examiner l'ensemble des pratiques et des recherches où interviennent ces notions entre 1801 et 1850. Nous avons donc d'abord construit un corpus de textes liés à ces notions : il constitue de fait ce que nous avons appelé la scène française. La lecture globale de cet ensemble d'écrits a montré que congruences et résidus n'y ont pas connu un développement autonome en général, mais ont été considérés dans un lien très fort avec les équations. Libri, et Lebesgue lui-même, prouvent des théorèmes sur le nombre des racines entières des congruences qui répondent aux travaux de Sturm sur le nombre de racines réelles des équations. D'autres auteurs transposent directement des énoncés de théorèmes ou des démonstrations de la théorie des équations vers la théorie des congruences. Ces travaux autour des congruences semblent avoir des racines communes avec ceux de Lagrange et Legendre qui associent théorie des nombres et équations indéterminées, même s'ils y intégrent les outils et méthodes des *Disquisitiones Arithmeticae* de Gauss, et tout particulièrement de la section VII. Ils sont donc bien ancrés dans un rapprochement entre algèbre et théorie des nombres. Mais c'est l'algèbre comme théorie des équations (et non comme théorie des structures) qui est visée ici et il ne s'agit jamais de développer un nouveau type de concept mixte arithmético-algébrique comme celui de corps fini.

Néanmoins, ce point commun retrouvé dans les textes composant notre corpus ne doit certainement pas amener à imaginer une école française autour des congruences, dans le sens d'un regroupement autour d'un ou de quelques chefs de file. D'une part, il n'est pas spécifique aux auteurs de cette scène française [10] et d'autre part, il n'est pas le reflet d'une pratique mathématique unifiée autour des congruences. Ainsi, Libri développe une théorie des congruences, qui pour lui est incluse dans la théorie des équations indéterminées, elle-même contenue dans l'analyse et il suggère une théorie des nombres fondée sur la considération des fonctions circulaires. Un lien entre théorie des nombres, algèbre et analyse apparaît également dans les travaux de Cauchy et dans ceux de Galois, et de ce point de vue, les travaux de ces trois savants appartiennent au courant de recherche de l'*analyse algébrique arithmétique*. Celui-ci n'est bien sûr pas limité à la scène française, et il est notable qu'il se décline différemment chez ces auteurs. Mais par ailleurs, Poinsot n'ap-

10. Nous renvoyons par exemple à [Stern, 1834], dans lequel l'auteur obtient les racines d'une congruence en s'appuyant sur l'expression des racines de l'équation correspondante : voir page 61 de notre première partie.

plique à aucun moment des outils d'analyse dans ses mémoires et le rapprochement qu'il souhaite mettre en place lie la théorie des nombres, l'algèbre et la géométrie. A proximité de Gauss et de Poinsot, Sophie Germain qui met en avant l'utilité des congruences et des résidus dans les recherches sur le dernier théorème de Fermat ne s'inscrit pourtant pas nécessairement dans une de ces configurations disciplinaires.

Même si les congruences ne font pas l'objet d'une mise en discipline à proprement parler, elles alimentent sur la scène française comme ailleurs une réflexion multiforme sur les objets mathématiques, leurs pratiques de fonctionnement, les transferts possibles d'un type de problématiques à un autre, et bien sûr les relations entre algèbre et arithmétique. Les analogies mises en avant entre les théories des équations et des congruences induisent en effet des problématiques et des pratiques spécifiques. Ainsi, comme nous venons de le rappeler, le fait de voir la théorie des congruences comme incluse dans (Libri) ou analogue à (Poinsot par exemple) celles des équations fait naître des questionnements déjà utilisés dans la théorie des équations comme celui relatif au nombre de racines entières des congruences, que l'on retrouve chez Libri et Lebesgue. Cela amène également Libri à réfléchir sur la nature de ces racines, et à exprimer analytiquement le fait qu'un nombre soit entier. De même, comme pour les équations et le travail autour de racines qui ne sont pas réelles, certains auteurs sont amenés à considérer des solutions de congruences qui ne sont pas entières : on retrouve des recherches sur ces solutions, alors qualifiées d'imaginaires, chez différents auteurs (Poinsot, Lebesgue, Galois, ...). Prendre en compte ces racines imaginaires amènent d'ailleurs à considérer des espèces de nombres nouveaux — tout comme ceux étudiés par Gauss ou Jacobi dans le cadre de leurs recherches sur les lois de réciprocité, même s'ils sont évidemment tout à fait différents. Ainsi, ce lien fort entre théories des équations et des congruences implique donc des pratiques, forgées à partir de ces dernières, tant du point de vue des objets considérés (racines - entières ou imaginaires - de congruences, dont l'expression peut être directement déterminée à partir de l'expression des racines des équations correspondantes) que des démonstrations (transfert direct des énoncés et démonstrations de certains théorèmes de la théorie des équations vers celle des congruences notamment, souvent sans justification supplémentaire de ce transfert ou des opérations sur les congruences).

Les écrits de Cauchy et de Poinsot nous donnent également deux exemples importants de travaux sur les congruences participant à la recherche de fondements du savoir mathématique. D'une part, le fait de considérer une généralisation des congruences en prenant en compte non pas des nombres entiers mais des polynômes pour module permet à Cauchy de définir les nombres complexes en évitant le recours à de purs symboles (comme l'est pour lui $\sqrt{-1}$), et de baser cette construction algébrique sur des concepts arithmétiques. Kronecker reprendra d'ailleurs un peu plus tard cette approche pour aller plus loin dans ce sens. D'autre part, en pensant les congruences comme un analogue des équations et en

mettant en avant les propriétés fondamentales des racines primitives, Poinsot insiste sur l'importance des relations entre objets et propose la théorie de l'ordre comme approche commune pour l'algèbre, la théorie des nombres et la géométrie.

C'est l'étude approfondie des textes retenus de Poinsot et Cauchy, identifiés comme deux auteurs clés, qui nous a permis de caractériser plus finement les pratiques autour des congruences par ces deux savants. Les formulations utilisées par Poinsot sont par exemple fondamentales pour comprendre la mise au point progressive de ce qu'il appelle la théorie de l'ordre. Par exemple, nous avons observé une évolution sensible de sa définition de l'algèbre [11] entre ses publications de 1808 et 1820. De même, seule une lecture de l'ensemble de ses textes d'algèbre et de théorie des nombres permet de saisir le sens réel des mots *groupe* et *ordre* par exemple. Puisqu'il n'en donne à aucun moment des définitions formelles, le lecteur doit décider si ces termes sont utilisés dans un sens courant, ou si Poinsot place une idée précise derrière ce vocabulaire. Or, il use de ces formules de manière récurrente, dans le cadre de situations qu'il qualifie d'analogues. Notamment Poinsot introduit sa notion d'ordre sans la définir précisément comme un fondement de l'algèbre, de la théorie des nombres et de la géométrie dans son *Extrait de quelques recherches nouvelles sur l'algèbre et la théorie des nombres* de 1818. C'est en 1820 qu'il définit l'ordre comme la « disposition mutuelle que l'on peut observer actuellement entre plusieurs objets » [Poinsot, 1820, p. 402]. Cette définition très générale n'est en fait mise en œuvre par Poinsot que pour des ensembles d'objets (permutations ou racines) qui peuvent être engendrés par un seul élément. Mais le fait que Poinsot applique le même vocabulaire à des objets d'algèbre et de théorie des nombres (groupes de permutations, groupes de racines par exemple) confirme le lien qu'il établit fortement entre ces deux domaines. Nous remarquons toutefois qu'il s'agit pour lui de détecter un principe d'organisation commun, décliné ensuite sur des types d'objets (dont les résidus) qui restent distincts. Nous avons retrouvé cette utilisation d'adjectifs similaires en algèbre et en théorie des nombres chez Cauchy et les racines primitives, substitutions primitives, facteurs primitifs [12]. De même, à plusieurs reprises, Cauchy présente parallèlement des résultats, des formules sur les équations et leurs homologues pour les congruences. Le choix de ses notations n'est pas non plus anodin : lorsqu'il désigne par ρ une racine d'une équation, il utilise la lettre r pour désigner une racine de la congruence associée. Tous ces détails liés à la forme des textes renforcent ce que notre première lecture a mis en avant : le lien intime existant pour nos auteurs entre la théorie des équations et des congruences se manifeste ainsi tout au long de leurs textes.

Par exemple, dans le cas du *Mémoire sur l'application de l'algèbre à la théorie des nombres* de 1820, le théorème énoncé par Poinsot a pour objet la résolution des congruences

11. Voir page 263.
12. Voir page 306.

binômes. Un relevé des résultats contenus dans ce mémoire indiquerait donc que le travail de Poinsot a ici pour objectif la résolution explicite d'une classe de congruences. Néanmoins, la lecture de ce texte de Poinsot montre que son travail constitue moins une recherche sur l'objet des congruences qu'une mise en avant des analogies existant entre les expressions des racines des équations et des congruences. De même, en ce qui concerne Cauchy, comme nous l'avons souligné dans la quatrième partie, seul un long travail de reconstruction de la méthode de Cauchy à partir à la fois des notes publiées dans les *Comptes Rendus* des séances de l'Académie, de la partie principale du *Mémoire sur la théorie des nombres* publiés en 1840 et des diverses notes qui y ont été ajoutées nous a permis de dégager les outils utilisés et les principes généraux de la méthode qu'il emploie pour travailler sur les formes quadratiques de la forme $4p^m = x^2 + ny^2$, où p est premier et n un diviseur de $p-1$. Ainsi, une lecture superficielle de la partie principale de son *Mémoire* permet de repérer les résultats obtenus sur les formes quadratiques, mais ne laisse pas transparaître l'importance des fonctions symétriques et alternées des racines primitives, dont les propriétés sont démontrées dans des notes.

Seule l'étude détaillée des textes de nos auteurs permet de détecter certains non-dits essentiels pour comprendre ces transferts, et qui n'apparaissent pas nécessairement lors d'une première lecture. Nous avons indiqué que Poinsot et Cauchy transposent très régulièrement des égalités vers des égalités modulo un nombre premier p en observant qu'il suffit d'ajouter des multiples bien choisis de p. Cette pratique est particulièrement frappante lorsque Poinsot donne des exemples dans lesquels il obtient l'expression des racines d'une congruence à partir de l'expression des racines d'une équation, sans commenter la validité de ce transfert, ni le choix des cas particuliers considérés. Les deux auteurs illustrent en effet leurs résultats par des exemples dont ils n'explicitent pas les particularités qui les rendent justement exemplaires. Par exemple, dans son mémoire de 1831, Cauchy applique son théorème sur les formes quadratiques $p^m = x^2 + ny^2$, où n est un nombre premier de la forme $4k+3$ et diviseur de $p-1$ à deux cas particuliers. Or, cela implique de déterminer l'équivalent d'un nombre de Bernoulli, qui est fractionnaire, modulo un nombre premier. Cauchy ne commente pas le fait que le dénominateur du nombre de Bernoulli en question admet toujours un inverse, sauf dans le cas où il est un multiple du module considéré. Ces non-dits suggèrent que Poinsot et Cauchy appréhendent résidus et congruences par transposition directe des manipulations algébriques utilisées habituellement pour travailler avec les équations dans ces cas d'égalités modulo p sans que ne soit alors explicitée la validité de ce transfert.

Ces différentes conclusions nous poussent à reposer la question de la révolution des mathématiques du XIX$^{\text{e}}$ siècle, évoquée par Jeremy Gray. D'après notre deuxième partie, le lien fort entre la théorie des nombres et la résolution d'équations est en continuité avec les pratiques arithmétiques de Lagrange, puis celle de Legendre, centrées autour

de la résolution des équations indéterminées. À ces pratiques s'ajoute l'introduction par Gauss des congruences, nouvel objet de la théorie des nombres, dont la définition et les propriétés fondamentales sont données dès le début des *Disquisitiones Arithmeticae*, dans lesquelles sont ensuite développés des thèmes de recherche où cet objet occupe une place centrale. Avec l'étude de notre corpus, nous avons été témoin d'approches variées résultant de combinaisons à différents niveaux des deux pratiques que nous venons de mentionner, et induisant des effets différents. Ainsi, par exemple, Legendre refuse l'utilisation des congruences, lorsque Sophie Germain, dans le premier quart du XIX^{e} siècle également, intègre rapidement les différentes notions développées dans le traité de Gauss et Victor-Amédée Lebesgue publie, plus tard, des mémoires sur les résidus d'ordre supérieur, suivant ainsi les thèmes amorcés par Gauss... On ne peut donc pas conclure de manière globale sur la question des ruptures et des continuités au XIX^{e} siècle : on ne retrouve en aucun cas une ligne directrice découlant exclusivement de Lagrange ou de Gauss, ou une rupture radicale avec leurs démarches, mais on assiste plutôt une ramification complexe de pratiques autour des congruences pouvant être analysée à plusieurs niveaux. Par exemple, du point de vue des raisonnements et de la rigueur, nous avons indiqué l'utilisation régulière de transferts entre équations et congruences : ainsi, Cauchy passe des équations aux congruences (en 1830), puis des congruences aux équations (en 1840), sans justifier ni commenter la légitimité de ce transfert ; cela contraste bien évidemment avec les définitions soigneuses et les justifications détaillées qui apparaissent dans certains de ses travaux d'analyse. Sur la période considérée, nous n'avons pas assisté à une rupture radicale des pratiques ou des approches, mais, *a posteriori*, des actes fondateurs ont vu le jour dans cette première moitié du XIX^{e} siècle : nous avons ainsi rappelé plus haut la construction des nombres complexes sur des concepts arithmétiques de Cauchy, découlant de ses réflexions sur la nature de ces nombres et de sa pratique des congruences en particulier et de la théorie des nombres plus généralement, ainsi que la proposition de la notion d'ordre comme fondement de l'algèbre, la théorie des nombres et la géométrie par Poinsot, à partir de ses différents travaux dans ces trois domaines. Ces actes fondateurs ne sont bien sûr pas le résultat des recherches d'un seul savant, de la même façon que la théorie de Galois ne repose pas seulement sur les épaules d'Évariste. Par exemple, même si, toujours *a posteriori*, la théorie de l'ordre de Poinsot peut faire penser aux travaux de Galois, et plus généralement à la théorie des groupes, nous avons également montré que les recherches de Poinsot ne contiennent pas d'avancées techniques par rapport à l'ouvrage de Gauss, et la considération des relations dans les mathématiques n'est pas non plus inédite dans le premier quart du XIX^{e} siècle ; Poinsot fait par contre particulièrement ressortir les principes fondamentaux de la méthode de Gauss et fonde ses réflexions sur ces principes, en occultant l'aspect technique de certains résultats (il n'aborde par exemple pas la question de la résolubilité des équations intermédiaires obtenues par Gauss). C'est finalement le dernier contexte pris en compte - les différentes références à Poinsot par les

savants de la deuxième moitié du XIX^{e} siècle - qui permet d'appréhender les effets des travaux de Poinsot autour de la théorie de l'ordre sur la communauté mathématique.

En plus d'une lecture globale des textes de notre corpus, et d'une étude approfondie de certains écrits de Poinsot et Cauchy, nous avons également utilisé des contextes supplémentaires afin d'évaluer la circulation des idées et des résultats de nos deux mathématiciens dans la communauté savante du XIX^{e} siècle. Des informations sur ce point sont données par la recherche des références à ces deux auteurs dans les travaux du XIX^{e} siècle et, dans le cas de Cauchy surtout, par la confrontation de ses écrits avec ceux des savants ayant produit des recherches sur des thèmes proches.

Dans le cas de Poinsot, ce ne sont pas les résultats qui sont repris, mais les idées générales qu'il a développées autour de ses travaux sur les congruences binômes notamment et qu'il résume sous le nom de *théorie de l'ordre*. Nous avons ainsi retrouvé plusieurs références, implicites ou explicites, à sa théorie de l'ordre. Ainsi, Jordan s'appuie par exemple sur la théorie de l'ordre (et donc la section VII de Gauss vue par Poinsot) pour interpréter les travaux de Galois [13]. De plus, les références à Poinsot retrouvées chez Peacock en 1833, chez Jacobi dans son cours de 1836-1837 et chez Bachmann à la fin du siècle montrent également que les écrits de Poinsot sont également lus en dehors de la scène française. À partir de notre ensemble de références, nous avons également constaté que la théorie de l'ordre, et Poinsot par la même occasion, sont à plusieurs reprises placés au cœur de l'évolution de l'algèbre dans des ouvrages de la seconde moitié du XIX^{e} siècle.

Le cas de Cauchy est différent, puisqu'on ne retrouve que très peu de références à ses travaux sur les formes quadratiques notamment. Par contre, grâce à l'analyse de notre corpus, nous avons mis en évidence des similarités frappantes entre les outils et les résultats obtenus par Jacobi et Cauchy dans leurs travaux publiés à la fin des années 1820. En relevant les résultats et méthodes développés dans un ensemble de textes dont les auteurs sont Jacobi, Dirichlet, Kummer et Cauchy, nous avons vu les nombres de Bernoulli apparaître dans les recherches de Cauchy en lien avec la répartition des résidus quadratiques, pour ensuite revenir chez Kummer en relation avec le nombre de classes de nombres idéaux. Si Kummer ne cite pas Cauchy dans ses publications, il connaît le contenu de ses travaux, comme nous l'avons vu à travers sa correspondance. De même, lorsque Cauchy définit en 1847 les équivalences algébriques, qui sont en fait des congruences dont le module est un polynôme, il se réfère à des travaux de Kummer publiés dans le *Journal de Crelle*, mais non reproduits dans les publications françaises.

Leurs cas témoignent une fois de plus de l'inadéquation de la notion de précurseur,

13. Nous renvoyons à [Brechenmacher, 2011], dont l'auteur a également montré que cette approche par la théorie de l'ordre semble également avoir été appliquée dans d'autres domaines, comme la mécanique et la cristallographie par exemple.

dans la mesure où celle-ci ne prendrait sens qu'en sélectionnant a priori une ligne de développement spécifique. Poinsot et Cauchy participent à différents niveaux aux changements que nous avons évoqués dans l'introduction générale, en particulier en donnant à voir le fonctionnement de certaines constructions sur d'autres objets, sans pour autant adhérer au projet d'une arithmétique généralisée comme modèle des mathématiques : en ce qui concerne les travaux de Cauchy, ce sont d'une part des résultats précis (sur les nombres de Bernoulli par exemple) qui semblent avoir leur place dans un ensemble de résultats mathématiques techniques et d'autre part, une nouvelle construction d'un objet mathématique connu, les nombres complexes, *via* l'introduction de congruences généralisées. L'influence des travaux arithmétiques de Poinsot se situe à un autre niveau, avec la proposition d'une nouvelle approche pour l'algèbre et la théorie des nombres, fondée sur la notion d'ordre, qui semble guider tout un ensemble de savants de la deuxième moitié du XIX^{e} siècle.

Ces différents travaux incitent finalement à reconsidérer les recherches publiées dans la première moitié du XIX^{e} siècle afin de mieux saisir leurs différentes ramifications, en l'occurrence de comprendre quelles alternatives se sont offertes dans la formation et la reconfiguration disciplinaires, l'approche des mathématiques, et d'appréhender la manière dont les auteurs de cette période ont conçu « ce rapprochement curieux de l'algèbre et de la théorie des nombres »[Poinsot, 1820, p.402].

Bibliographie

Bibliographie

[Abel, 1824] Abel Niels Henrik, 1824, «Mémoire sur les équations algébriques, où l'on démontre l'impossibilité de la résolution de l'équation générale du cinquième degré». Christiania. Repr. in *Œuvres complètes*, éd. L. Sylow, S. Lie, t. 1, Christiania : Grøndahl, p.28-33.

[Abria et Houël, 1876] Abria Joseph-Benoît et Houël Jules, 1876, «Notice sur la vie et les travaux de Victor-Amédée Lebesgue». *Bulletino di bibliografia e di storia delle scienze matematiche e fisiche*, vol. 9, p. 554–582.

[Alfonsi, 2005] Alfonsi Liliane, 2005, *Étienne Bézout (1730-1783) : mathématicien, académicien et professeur au siècle des Lumières*. Thèse de doctorat, Université Paris 6, Paris.

[Archibald, 2002] Archibald Thomas, 2002, «Charles Hermite and German Mathematics in France». Dans Parshall Karen Hunger et Rice Adrian C. (eds), *Mathematics Unbound. The Evolution of an International Mathematical Research Community (1800-1945)*, Providence : American Mathematical Society, p. 123–137.

[Aubry, 1907] Aubry Auguste, 1907, «Le lemme fondamental de la théorie des nombres». *L'Enseignement mathématique*, vol. 9, p. 286–305.

[Aubry, 1909a] Aubry Auguste, 1909a, «L'œuvre arithmétique d'Euler». *L'Enseignement mathématique*, vol. 11, p. 329–356.

[Aubry, 1909b] Aubry Auguste, 1909b, «Sur les travaux arithmétiques de Lagrange, de Legendre et de Gauss». *L'Enseignement mathématique*, vol. 11, p. 430–450.

[Ausejo et Hormigón, 1993] Ausejo Elena et Hormigón Mariano (eds), 1993, *Messengers of Mathematics : European Mathematical Journals (1800-1946)*. Madrid : Siglo XXI.

[Auvinet, 2011] Auvinet Jérôme, 2011, *Charles-Ange Laisant. Itinéraires et engagements d'un mathématicien, d'un siècle à l'autre (1841-1920)*. Thèse de doctorat, Université de Nantes, Nantes.

[Bachmann, 1892] Bachmann Paul, 1892, *Die Elemente der Zahlentheorie*. Leipzig : Teubner.

[Barlow, 1811] Barlow Peter, 1811, *An Elementary Investigation of the Theory of Numbers : with its Application to the Indeterminate and Diophantine Analysis, the Analytical and Geometrical Division of the Circle, and Several Other Curious Algebraical and Arithmetical Problems*. London : Johnson.

[Belhoste, 1982] Belhoste Bruno, 1982, *Augustin-Louis Cauchy et la pratique des sciences exactes en France au XIX^e siècle*. Thèse de 3ème cycle, Université Paris 1, Paris.

[Belhoste, 1985] Belhoste Bruno, 1985, *Cauchy, un mathématicien légitimiste au XIX^e siècle*. Paris : Belin.

[Belhoste, 1989] Belhoste Bruno, 1989, «Les caractères généraux de l'enseignement secondaire scientifique de la fin de l'Ancien Régime à la Première Guerre Mondiale». *Histoire de l'éducation*, vol. 41, p. 3–45.

[Belhoste, 1991] Belhoste Bruno, 1991, *Augustin-Louis Cauchy*. New York : Springer-Verlag.

[Belhoste, 1995] Belhoste Bruno, 1995, *Les sciences dans l'enseignement secondaire français. Textes officiels. Tome 1 : 1789-1914*. Paris : INRP.

[Belhoste, 1998] Belhoste Bruno, 1998, «Pour une réévaluation du rôle de l'enseignement dans l'histoire des mathématiques». *Revue d'histoire des mathématiques*, vol. 4, p. 289–304.

[Belhoste et Lützen, 1984] Belhoste Bruno et Lützen Jesper, 1984, «Joseph Liouville et le Collège de France». *Revue d'histoire des sciences*, vol. 37 (3-4), p. 255–304.

[Bertrand, 1890] Bertrand Joseph, 1890, *Éloge historique de Louis Poinsot*. Paris : Institut de France.

[Binet, 1831] Binet Jacques Philippe Marie, 1831, «Mémoire sur la résolution des équations indéterminées du premier degré en nombres entiers». *Journal de l'École polytechnique*, vol. 13, p. 289–296.

[Binet, 1841a] Binet Jacques Philippe Marie, 1841a, «Note sur une nouvelle méthode pour trouver le plus grand commun diviseur des nombres entiers, ou des polynômes algébriques, et sur l'application de cette méthode aux congruences du premier degré». *Comptes rendus hebdomadaires des séances de l'Académie des sciences*, vol. 13, p. 349–353.

[Binet, 1841b] Binet Jacques Philippe Marie, 1841b, «Note sur une propriété des nombres premiers, et sur la détermination des nombres associés d'Euler». *Comptes rendus hebdomadaires des séances de l'Académie des sciences*, vol. 13, p. 210–213.

[Binet, 1849] Binet Jacques Philippe Marie, 1849, «Théorie des nombres». *Comptes rendus hebdomadaires des séances de l'Académie des sciences*, vol. 28, p. 686–687.

[Boniface, 2002] Boniface Jacqueline, 2002, *Les constructions des nombres réels dans le mouvement d'arithmétisation de l'analyse*. Paris : Ellipses.

[Boniface, 2007] Boniface Jacqueline, 2007, «The Concept of Number from Gauss to Kronecker». Dans Goldstein Catherine, Schappacher Norbert et Schwermer

Joachim (eds), *The Shaping of Arithmetic after C. F. Gauss's Disquisitiones Arithmeticae*, Berlin : Springer, p. 314–342.

[Bottazzini, 1986] Bottazzini Umberto, 1986, *The Higher Calculus : A History of Real and Complex Analysis from Euler to Weierstrass*. New York, Berlin, Heidelberg : Springer-Verlag.

[Boucard, 2006] Boucard Jenny, 2006, *Euler, Lagrange et le théorème des quatre carrés*. Master d'histoire des sciences et des techniques, Centre François Viète, Université de Nantes.

[Bouniakowsky, 1831] Bouniakowsky Victor, 1831, «Sur les congruences du second degré». *Mémoires de l'Académie impériale des sciences de Saint-Pétersbourg*, vol. 1, p. 563–582.

[Bourbaki, 1984] Bourbaki Nicolas, 1984, *Éléments d'histoire des mathématiques*. Masson. Repr. Berlin, Paris : Springer, 2007.

[Bourdon, 1828] Bourdon Pierre Louis Marie, 1828, *Élémens d'arithmétique*. Paris : Bachelier, 6^{e} édition.

[Bradley et Sandifer, 2007] Bradley Robert E. et Sandifer C. Edwards (eds), 2007, *Leonhard Euler : Life, Work and Legacy*. Amsterdam : Elsevier.

[Brechenmacher, 2010] Brechenmacher Frédéric, 2010, «Une histoire de l'universalité des matrices mathématiques». *Revue de synthèse*, vol. 131 (4), p. 569–603.

[Brechenmacher, 2011] Brechenmacher Frédéric, 2011, «Self-Portraits with Évariste Galois, (and the Shadow of Camille Jordan)». *Revue d'histoire des mathématiques*, vol. 17 (2), p. 271–369.

[Brian et Demeulenaere Douyère, 1996] Brian Éric et Demeulenaere Douyère Christiane (eds), 1996, *Histoire et mémoire de l'Académie des sciences. Guide de recherches*. Paris : Lavoisier.

[Bru et Martin, 2005] Bru Bernard et Martin Thierry, 2005, «Le baron de Férussac, la couleur de la statistique et la topologie des sciences». *Journal électronique d'histoire des probabilités et de la statistique*, vol. 1 (2), p. 1–43.

[Bucciarelli, 1980] Bucciarelli Louis L., 1980, *Sophie Germain : An Essay in the History of the Theory of Elasticity*. Boston : Reidel.

[Bullynck, 2006] Bullynck Maarten, 2006, *Vom Zeitalter der Formalen Wissenschaften. Anleitung zur Verarbeitung von Erkenntnissen anno 1800, vermittelst einer parallelen Geschichte*. Thèse de doctorat, Universiteit Ghent, Ghent.

[Bullynck, 2009] Bullynck Maarten, 2009, «Modular Arithmetic before C. F. Gauss : Systematizations and Discussions on Remainder Problems in 18th-Century Germany». *Historia Mathematica*, vol. 36, p. 48–72.

[Buraux-Bourgeois, 1993] Buraux-Bourgeois, 1993, «L'analyse diophantienne chez Lagrange». *Cahier du séminaire d'histoire des mathématiques*, vol. 3, p. 13–23.

[Burckhardt, 1983] Burckhardt Johann Jakob, 1983, «Leonhard Euler, 1707-1783». *Mathematics Magazine*, 2ème série, vol. 56 (5), p. 273–277.

[Bussotti, 2006] Bussotti Paolo, 2006, *From Fermat to Gauss : Indefinite Descent and Methods of Reduction in Number Theory*. Augsburg : Erwin Rauner Verlag.

[Bézout, 1764] Bézout Étienne, 1764, «Recherches sur le degré des équations résultantes de l'évanouissement des inconnues et sur les moyens qu'on doit employer pour trouver ces équations». *Histoire de l'Académie royale des sciences, avec les Mémoires de mathématiques et de physique, Année 1764*, p. 288–338.

[Bézout, 1765] Bézout Étienne, 1765, «Sur la résolution générale des équations de tous les degrés». *Histoire de l'Académie royale des sciences, avec les Mémoires de mathématiques et de physique, Année 1765*, p. 533–552.

[Calinger, 1996] Calinger Ronald, 1996, «Leonhard Euler : The First St. Petersburg Years (1727 - 1741)». *Historia Mathematica*, vol. 23, p. 121–166.

[Caplat, 1986] Caplat Guy (ed.), 1986, *Les inspecteurs généraux de l'instruction publique*. Paris : INRP / CNRS.

[Cassinet, 1988] Cassinet Jean, 1988, «Paolo Ruffini (1765 - 1822) : la résolution algébrique des équations et les groupes de permutations». *Bollettino di Storia delle scienze satematiche*, vol. VIII(1), p. 21–69.

[Catalan, 1842] Catalan Eugène-Charles, 1842, «Sur les fractions décimales périodiques». *Nouvelles annales de mathématiques*, vol. 1, p. 457–470.

[Cauchy, 1813] Cauchy Augustin-Louis, 1813, «Recherches sur les nombres». *Journal de l'École polytechnique*, 16ème cahier, vol. 9, p. 99–123. Repr. in *Œuvres complètes*, éd. Académie des sciences, 2ème sér., t. 1, Paris : Gauthier-Villars, 1882-1974, p. 39-63.

[Cauchy, 1815a] Cauchy A. L., 1815a, «Mémoire sur le nombre de valeurs qu'une fonction peut acquérir lorsqu'on y permute de toutes les manières possibles les quantités qu'elles renferment». *Journal de l'École polytechnique*, 17ème cahier, vol. 10, p. 1–28. Repr. in *Œuvres complètes*, éd. Académie des sciences, 2ème sér., t. 1, Paris : Gauthier-Villars, 1882-1974, p. 64-90.

[Cauchy, 1815b] Cauchy A. L., 1815b, «Mémoire sur les fonctions qui ne peuvent obtenir que deux valeurs égales et de signes contraires par suite des transpositions opérées entre les variables qu'elles renferment». *Journal de l'École polytechnique*, 17ème cahier, vol. 10, p. 29–97. Repr. in *Œuvres complètes*, éd. Académie des sciences, 2ème sér., t. 1, Paris : Gauthier-Villars, 1882-1974, p. 91-169.

[Cauchy, 1818] Cauchy Augustin-Louis, 1818, «Démonstration du théorème général de Fermat sur les nombres polygones». *Mémoires de la classe des sciences mathématiques et physiques de l'Institut de France*, vol. 14, p. 177–220. Repr. in *Œuvres complètes*, éd. Académie des sciences, 2ème sér., t. 6, Paris : Gauthier-Villars, 1882-1974, p. 320-353.

[Cauchy, 1829a] Cauchy Augustin-Louis, 1829a, «Mémoire sur la théorie des nombres». *Bulletin des sciences mathématiques, physiques et chimiques*, vol. 12, p. 205–221. Repr. in *Œuvres complètes*, éd. Académie des sciences, 2ème sér., t. 2, Paris : Gauthier-Villars, 1882-1974, p. 88-107.

[Cauchy, 1829b] Cauchy Augustin-Louis, 1829b, «Sur diverses propositions relatives à l'algèbre et à la théorie des nombres». *Exercices de mathématiques*, vol. 4, p. 217–252. Repr. in *Œuvres complètes*, éd. Académie des sciences, 2ème sér., t. 9, Paris : Gauthier-Villars, 1882-1974, p. 259-297.

[Cauchy, 1829c] Cauchy Augustin-Louis, 1829c, «Sur la résolution des équivalences dont les modules se réduisent à des nombres premiers». *Exercices de mathématiques*, vol. 4, p. 253–292. Repr. in *Œuvres complètes*, éd. Académie des sciences, 2ème sér., t. 9, Paris : Gauthier-Villars, 1882-1974, p. 298-341.

[Cauchy, 1831] Cauchy Augustin-Louis, 1831, «Mémoire sur la théorie des nombres». *Bulletin des sciences mathématiques, physiques et chimiques*, vol. 15, p. 137–139.

[Cauchy, 1839] Cauchy Augustin-Louis, 1839, «Sur la théorie des nombres, et en particulier sur les formes quadratiques des puissances d'un nombre premier ou du quadruple de ces puissances». *Comptes rendus hebdomadaires des séances de l'Académie des sciences*, vol. 9, p. 519–525. Repr. in *Œuvres complètes*, éd. Académie des sciences, 1ère sér., t. 4, Paris : Gauthier-Villars, 1882-1974, p. 506-513.

[Cauchy, 1840a] Cauchy Augustin-Louis, 1840a, «Mémoire sur la théorie des nombres». *Mémoires de l'Académie royale des sciences de l'Institut de France.*, vol. 17, p. 249–768. Repr. in *Œuvres complètes*, éd. Académie des sciences, 1ère sér., t. 3, Paris : Gauthier-Villars, 1882-1974, p. 5-450.

[Cauchy, 1840b] Cauchy Augustin-Louis, 1840b, «Méthode simple et nouvelle pour la détermination complète des sommes alternées, formées avec les racines primitives des équations binômes». *Comptes rendus hebdomadaires des séances de l'Académie des sciences*, vol. 10, p. 560–572. Repr. in *Œuvres complètes*, éd. Académie des sciences, 1ère sér., t. 5, Paris : Gauthier-Villars, 1882-1974, p. 152-166.

[Cauchy, 1840c] Cauchy Augustin-Louis, 1840c, «Sur la sommation de certaines puissances d'une racine primitive d'une équation binôme, et en particulier, des puissances qui offrent pour exposants les résidus cubiques inférieurs au module donné». *Comptes rendus hebdomadaires des séances de l'Académie des sciences*, vol. 10, p.

594–606. Repr. in *Œuvres complètes*, éd. Académie des sciences, 1ère sér., t. 5, Paris : Gauthier-Villars, 1882-1974, p. 166-180.

[Cauchy, 1840d] Cauchy Augustin-Louis, 1840d, «Théorèmes relatifs aux formes quadratiques des nombres premiers et de leurs puissances». *Comptes rendus hebdomadaires des séances de l'Académie des sciences*, vol. 10, p. 51–61. Repr. in *Œuvres complètes*, éd. Académie des sciences, 1ère sér., t. 5, Paris : Gauthier-Villars, 1882-1974, p. 52-64.

[Cauchy, 1841] Cauchy Augustin-Louis, 1841, «Mémoire sur diverses formules relatives à l'Algèbre et à la théorie des nombres». *Comptes rendus hebdomadaires des séances de l'Académie des sciences*, vol. 12, p. 698–711, 813–847. Repr. in *Œuvres complètes*, éd. Académie des sciences, 1ère sér., t. 6, Paris : Gauthier-Villars, 1882-1974, p. 99-146.

[Cauchy, 1846] Cauchy Augustin-Louis, 1846, «Mémoire sur les arrangements que l'on peut former avec des lettres données et sur les permutations ou substitutions à l'aide desquelles on passe d'un arrangement à un autre». *Exercices d'analyse et de physique mathématique*, vol. 3, p. 151–252. Repr. in *Œuvres complètes*, éd. Académie des sciences, 2ème sér., t. 13, Paris : Gauthier-Villars, 1882-1974, p. 171-282.

[Cauchy, 1847a] Cauchy Augustin-Louis, 1847a, «Mémoire sur la théorie des équivalences algébriques substituée à la théorie des imaginaires». *Exercices d'analyse et de physique mathématique*, vol. 4, p. 87–110. Repr. in *Œuvres complètes*, éd. Académie des sciences, 2ème sér., t. 14, Paris : Gauthier-Villars, 1882-1974, p. 93-120.

[Cauchy, 1847b] Cauchy Augustin-Louis, 1847b, «Mémoire sur les racines des équations algébriques à coefficients entiers, et sur les polynômes radicaux». *Comptes rendus hebdomadaires des séances de l'Académie des sciences*, vol. 24, p. 407–414.

[Cauchy, 1847c] Cauchy Augustin-Louis, 1847c, «Mémoire sur les racines des équivalences correspondantes à des modules quelconques premiers ou non premiers, et sur l'avantage que présente l'emploi de ces racines dans la théorie des nombres». *Comptes rendus hebdomadaires des séances de l'Académie des sciences*, vol. 25, p. 37–46.

[Cauchy, 1847d] Cauchy Augustin-Louis, 1847d, «Mémoire sur une nouvelle théorie des imaginaires, et sur les racines symboliques des équations et des équivalences». *Comptes rendus hebdomadaires des séances de l'Académie des sciences*, vol. 24, p. 1120–1130.

[Cauchy, 1847e] Cauchy Augustin-Louis, 1847e, «Sur l'application de la nouvelle théorie des imaginaires aux diverses branches des sciences mathématiques». *Comptes rendus hebdomadaires des séances de l'Académie des sciences*, vol. 25, p. 129–132.

[Choquet et Mayer, 1836] Choquet Charles et Mayer Mathias, 1836, *Traité élémentaire d'algèbre*. Paris : Bachelier, 2e édition.

[Cooper, 1926] Cooper Albert Everett, 1926, *A Topical History of the Theory of Quadratic Residues*. Non publié, University of Chicago. University of Chicago Archives.

[Cournot, 1825] Cournot Antoine Augustin, 1825, «Mémoire sur l'application de l'algèbre à la théorie des nombres ; par M. Poinsot». *Bulletin des sciences mathématiques, astronomiques, physiques et chimiques*, vol. 3, p. 144–145.

[Cournot, 1827] Cournot Antoine Augustin, 1827, «Des résidus cubiques ; par le Dr. Jacobi». *Bulletin des sciences mathématiques, astronomiques, physiques et chimiques*, vol. 8, p. 302.

[Cournot, 1847] Cournot Antoine Augustin, 1847, *De l'origine et des limites de la correspondance entre l'algèbre et la géométrie*. Paris : Hachette.

[Cournot, 1913] Cournot Antoine Augustin, 1913, *Souvenirs (1760 - 1860)*. Paris : Hachette.

[Couturat, 1898] Couturat Louis, 1898, «Sur les rapports du nombre et de la grandeur». *Revue de métaphysique et de morale*, vol. VI, p. 422–447.

[Cox, 1989] Cox David A., 1989, *Primes of the form $x^2 + ny^2$*. New York : Wiley.

[Crosland, 1992] Crosland Maurice, 1992, *Science under Control - The French Academy of Sciences, 1795 - 1914*. Cambridge : Cambridge University Press.

[Dahan Dalmedico, 1979] Dahan Dalmedico Amy, 1979, *Les recherches algébriques de Cauchy*. Thèse de 3ème cycle, Université Paris 13, Paris.

[Dahan Dalmedico, 1980] Dahan Dalmedico Amy, 1980, «Les travaux de Cauchy sur les substitutions. Étude de son approche du concept de groupe». *Archive for History of Exact Sciences*, vol. 23 (4), p. 279–319.

[Dahan Dalmedico, 1982] Dahan Dalmedico Amy, 1982, «Résolubilité des équations par radicaux et premier mémoire d'Évariste Galois». Dans *Présence d'Évariste Galois*, vol. 48, APMEP, p. 43–53.

[Dahan Dalmedico, 1997] Dahan Dalmedico Amy, 1997, «L'étoile « imaginaire » a-t-elle immuablement brillé ? Le nombre complexes et ses différentes interprétations dans l'œuvre de Cauchy». Dans Flament Dominique (ed.), *Le nombre, une hydre à n visages*, Paris : Maison des Sciences de l'Homme, p. 29–50.

[De Comberousse, 1890] De Comberousse Charles, 1890, *Cours de mathématiques à l'usage des candidats à l'École polytechnique, à l'École normale supérieure, à École centrale des arts et manufactures. Tome quatrième. Algèbre supérieure. Seconde partie*. Paris : Gauthier-Villars.

[Del Centina, 2005] Del Centina Andrea, 2005, «Letters of Sophie Germain Preserved in Florence». *Historia Mathematica*, vol. 32, p. 60–75.

[Del Centina, 2008] Del Centina Andrea, 2008, «Unpublished Manuscripts of Sophie Germain and a Reevaluation of her Work on Fermat's Last Theorem». *Archive for History of Exact Sciences*, vol. 62, p. 349–392.

[Delambre, 1810] Delambre Jean-Baptiste Joseph, 1810, *Rapport historique sur les progrès des sciences mathématiques depuis 1789, et sur leur état actuel*. Paris : Imprimerie Impériale.

[Descartes, 1701] Descartes René, 1701, «Regulae ad directionem ingenii». Dans *Opuscula posthuma, physica et mathematica*, Amsterdam : Blaeu. Repr. in *Œuvres de Descartes, publiées par Victor Cousin*, t. 11, Paris : Levrault, 1826, p. 216-329.

[Desmarest, 1852] Desmarest Eugène, 1852, *Théorie des nombres - Traité de l'analyse indéterminée du second degré à deux inconnues suivi de l'application de cette analyse à la recherche des racines primitives, avec une table de ces racines pour tous les nombres premiers compris entre 1 et 10000*. Paris : Hachette.

[Despeyrous, 1861] Despeyrous Théodore, 1861, «Mémoire sur la théorie générale des permutations». *Journal de mathématiques pures et appliquées*, 2ème sér., vol. 6, p. 417–439.

[Despeyrous, 1865a] Despeyrous Théodore, 1865a, «Classifications des permutations d'un nombre quelconque de lettres en groupes de permutations inséparables». *Journal de mathématiques pures et appliquées*, 2ème sér., vol. 10, p. 177–202.

[Despeyrous, 1865b] Despeyrous Théodore, 1865b, «Sur la détermination des nombres de valeurs que prennent les fonctions par les permutations des lettres qu'elles renferment». *Journal de mathématiques pures et appliquées*, 2ème sér., vol. 10, p. 54–64.

[Despeyrous, 1884] Despeyrous Théodore, 1884, *Cours de mécanique par M. Despeyrous, avec des Notes par M. G. Darboux, Tome Premier*. Paris : Hermann.

[Dhombres, 1985] Dhombres Jean, 1985, «French Mathematical Textbooks from Bézout to Cauchy». *Historia Scientiarum*, vol. 28, p. 91–137.

[Dhombres, 1994] Dhombres Jean, 1994, «Le journal professionnel au XIXe siècle : enjeux généraux d'une enquête en cours». *Rivista di Storia della Scienza*, vol. 2 (2), p. 99–136.

[Dhombres et Gilain, 1992] Dhombres Jean et Gilain Christian, 1992, «Bibliographie concernant Cauchy (1974 à aujourd'hui)». *Revue d'histoire des sciences*, vol. 45 (1), p. 129–134.

[Dickson, 1919-1923] Dickson Leonard Eugene, 1919-1923, *History of the Theory of Numbers*. Washington : Carnegie Institue of Washington. Repr. Mineola : Dover Publications, 2005.

[Dirichlet, 1828a] Dirichlet Johann Peter Gustav Lejeune-, 1828a, «Démonstrations nouvelles de quelques théorèmes relatifs aux nombres». *Journal für die reine und angewandte Mathematik*, vol. 3, p. 390–393.

[Dirichlet, 1828b] Dirichlet Johann Peter Gustav Lejeune-, 1828b, «Mémoire sur l'impossibilité de quelques équations indéterminées du 5^{e} degré». *Journal für die reine und angewandte Mathematik*, vol. 3, p. 354–375.

[Dirichlet, 1828c] Dirichlet Johann Peter Gustav Lejeune-, 1828c, «Recherches sur les diviseurs premiers d'une classe de formules du quatrième degré». *Journal für die reine und angewandte Mathematik*, vol. 3, p. 35–69.

[Dirichlet, 1832] Dirichlet Johann Peter Gustav Lejeune-, 1832, «Démonstration d'une propriété analogue à la loi de réciprocité qui existe entre deux nombres premiers quelconques». *Journal für die reine und angewandte Mathematik*, vol. 9, p. 379–389.

[Dirichlet, 1837] Dirichlet Johann Peter Gustav Lejeune-, 1837, «Sur la manière de résoudre l'équation $t^2 - pu^2 = 1$ au moyen des fonctions circulaires». *Journal für die reine und angewandte Mathematik*, vol. 17, p. 286–290.

[Dirichlet, 1838] Dirichlet Johann Peter Gustav Lejeune-, 1838, «Sur l'usage des séries infinies dans la théorie des nombres». *Journal für die reine und angewandte Mathematik*, vol. 18, p. 259–274.

[Dirichlet, 1839a] Dirichlet Johann Peter Gustav Lejeune-, 1839a, «Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres.» *Journal für die reine und angewandte Mathematik*, vol. 19, p. 324–369.

[Dirichlet, 1839b] Dirichlet Johann Peter Gustav Lejeune-, 1839b, «Ueber den Satz : dass jede arithmetische Progression, deren erstes Glied und Differenz keinen gemeinschaftlichen Factor haben, unendlich viel Primzahlen enthält». *Abhandlungen der Königlichen Preußischen Akademie der Wissenschaften zu Berlin. Mathematische Abhandlungen (1837)*, p. 45–81. Traduction française par M. Terquem, Démonstration de cette proposition : toute progression arithmétique dont le premier terme et la raison sont des entiers sans diviseur commun, contient une inifnité de nombres premiers, *Journal de mathématiques pures et appliquées*, 1$^{\text{ère}}$ série, tome 4, 1839, p. 393-422.

[Dirichlet, 1840] Dirichlet Johann Peter Gustav Lejeune-, 1840, «Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres (suite).» *Journal für die reine und angewandte Mathematik*, vol. 21, p. 1–12, 134–155.

[Dirichlet, 1842] Dirichlet Johann Peter Gustav Lejeune-, 1842, «Recherches sur les formes quadratiques à coefficients et à indéterminées complexes». *Journal für die reine und angewandte Mathematik*, vol. 24, p. 291–371.

[Dirichlet, 1843] Dirichlet Johann Peter Gustav Lejeune-, 1843, «Untersuchungen über der Theorie der complexen Zahlen». *Abhandlungen der Königlichen Preußischen Akademie der Wissenschaften zu Berlin. Mathematische Abhandlungen (1841)*, p. 141–161. Traduction française par M. Faye, Recherches sur la théorie des nombres complexes, *Journal de mathématiques pures et appliquées* , tome 9, 1844, p. 245-269.

[Drot, 1845] Drot, 1845, «Note sur les chiffres qui peuvent terminer les puissances quelconques des nombres entiers». *Nouvelles annales de mathématiques*, vol. 4, p. 637–644.

[Durand-Richard, 1990] Durand-Richard Marie-José, 1990, «Genèse de l'algèbre symbolique en Angleterre : une influence possible de John Locke». *Revue d'histoire des sciences*, vol. 43 (2-3), p. 129–180.

[Durand-Richard, 1996] Durand-Richard Marie-José, 1996, «L'Ecole algébrique anglaise : les conditions conceptuelles et institutionnelles d'un calcul symbolique comme fondement de la connaissance». Dans Goldstein Catherine, Gray Jeremy et Ritter Jim (eds), *L'Europe mathématique - Mythes, histoires, identités*, Paris : Maison des sciences de l'homme, p. 445–478.

[Durand-Richard, 2008] Durand-Richard Marie-José (ed.), 2008, *L'analogie dans la démarche scientifique*. Paris : Harmattan.

[Décaillot, 1998] Décaillot Anne-Marie, 1998, «L'arithméticien Édouard Lucas (1842-1891)». *Revue d'histoire des mathématiques*, vol. 4, p. 191–236.

[Edwards, 1975-1977] Edwards Harold M., 1975-1977, «The Background of Kummer's Proof of Fermat's Last Theorem for Regular Primes». *Archive for History of Exact Sciences*, vol. 14, p. 219–236. Postcript to the "Background of Kummer's Proof...", *Archive for History of Exact Sciences*, vol. 17, p. 381-394.

[Edwards, 1977] Edwards Harold M., 1977, *Fermat's Last Theorem. A Genetic Introduction to Algebraic Number Theory*, vol. 50. New York : Springer-Verlag.

[Edwards, 1980] Edwards Harold M., 1980, «The Genesis of Ideal Theory». *Archive for History of Exact Sciences*, vol. 23, p. 321–378.

[Edwards, 1983] Edwards Harold M., 1983, «Euler and Quadratic Reciprocity». *Mathematics Magazine*, vol. 56 (5), p. 285–291.

[Ehrhardt, 2007] Ehrhardt Caroline, 2007, *Évariste Galois et la théorie des groupes. Fortune et réélaborations (1811-1910)*. Thèse de doctorat, EHESS, Paris.

[Ehrhardt, 2010] Ehrhardt Caroline, 2010, «La naissance posthume d'Évariste Galois (1811-1832)». *Revue de synthèse*, 6ème sér., vol. 131 (4), p. 543–568.

[Ehrhardt, 2011] Ehrhardt Caroline, 2011, «A Quarrel between Joseph Liouville and Guillaume Libri at the French Academy of Sciences in the Middle of the Nineteenth Century». *Historia Mathematica*, vol. 38 (3), p. 389–414.

[Eisenstein, 1844a] Eisenstein Gotthold, 1844a, «Einfacher Algorithmuis zur Bestimmung des Werthes von $\left(\frac{a}{b}\right)$». *Journal für die reine und angewandte Mathematik*, vol. 27, p. 317–318.

[Eisenstein, 1844b] Eisenstein Gotthold, 1844b, «Einfacher Beweis und Verallgemeinerung des Fundamentaltheorems für die Formen dritten Grades mit drei Variabeln, welche der Kreistheilung ihre Entstehung verdanken». *Journal für die reine und angewandte Mathematik*, vol. 28, p. 223–248.

[Eisenstein, 1844c] Eisenstein Gotthold, 1844c, «Geometrischer Beweis und Verallgemeinerung des Fundamentaltheorems für die quadratischen Reste». *Journal für die reine und angewandte Mathematik*, vol. 28, p. 246–248.

[Eisenstein, 1844d] Eisenstein Gotthold, 1844d, «Neuer und elementarer Beweis des Legendreschen Reciprocitäts-Gesetzes». *Journal für die reine und angewandte Mathematik*, vol. 27, p. 322–329.

[Euler, 1738] Euler Leonhard, 1738, «Observationes de theoremate quodam Fermatiano aliisque ad numeros primos spectantibus». *Commentarii academiae scientiarum Petropolitanae*, vol. 6, p. 103–107.

[Euler, 1741a] Euler Leonhard, 1741a, «Solutio problematis ad geometriam situs pertinentis». *Commentarii academiae scientiarum Petropolitanae*, vol. 8, p. 128–140.

[Euler, 1741b] Euler Leonhard, 1741b, «Theorematum quorundam ad numeros primos spectantium demonstratio». *Commentarii academiae scientiarum Petropolitanae*, vol. 8, p. 141–146.

[Euler, 1750] Euler Leonhard, 1750, «Theoremata circa divisores numerorum». *Novi Commentarii academiae scientiarum Petropolitanae*, vol. 1, p. 20–48.

[Euler, 1751] Euler Leonhard, 1751, «Theoremata circa divisores numerorum in hac forma $paa \pm qbb$ contentorum». *Commentarii academiae scientiarum Petropolitanae*, vol. 14, p. 151–181.

[Euler, 1755] Euler Leonhard, 1755, *Institutiones calculi differentialis cum eius usu in analysi finitorum ac doctrina serierum*. Saint-Pétersbourg : Acad. Imperialis.

[Euler, 1758] Euler Leonhard, 1758, «De numeris, qui sunt aggregata duorum quadratorum». *Novi Commentarii academiae scientiarum Petropolitanae*, vol. 4, p. 3–40.

[Euler, 1760a] Euler Leonhard, 1760a, «Demonstratio theorematis Fermatiani omnem numerum primum formae 4n+1 esse summam duorum quadratorum». *Novi Commentarii academiae scientiarum Petropolitanae*, vol. 5, p. 3–13.

[Euler, 1760b] Euler Leonhard, 1760b, «Demonstratio theorematis Fermatiani omnem numerum sive integrum sive fractum esse summam quatuor pauciorumve quadratorum». *Novi Commentarii academiae scientiarum Petropolitanae*, vol. 5, p. 13–58.

[Euler, 1761a] Euler Leonhard, 1761a, «Specimen de usu observationum in mathesi pura». *Novi Commentarii academiae scientiarum Petropolitanae*, vol. 6, p. 185–230.

[Euler, 1761b] Euler Leonhard, 1761b, «Theoremata circa residua ex divisione potestatum relicta». *Novi Commentarii academiae scientiarum Petropolitanae*, vol. 7, p. 49–82.

[Euler, 1763] Euler Leonhard, 1763, «Theoremata arithmetica nova methodo demonstrata». *Novi Commentarii academiae scientiarum Petropolitanae*, vol. 8, p. 74–104.

[Euler, 1774] Euler Leonhard, 1774, «Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia». *Novi Commentarii academiae scientiarum Petropolitanae*, vol. 18, p. 85–135.

[Euler, 1780] Euler Leonhard, 1780, «Novae demonstrationes circa resolutionem numerorum in quadrata». *Nova Acta Eruditorum*, vol. 2, p. 48–69.

[Euler, 1783a] Euler Leonhard, 1783a, «De quibusdam eximiis proprietatibus circa divisores potestatum occurrentibus». Dans *Opuscula Analytica*, vol. 1, Saint-Pétersbourg : Acad. Imperialis, p. 242–295.

[Euler, 1783b] Euler Leonhard, 1783b, «Disquitio accuratior circa residua ex divisione quadratorum altiorumque potestatum per numeros primos relicta». Dans *Opuscula Analytica*, vol. 1, Saint-Pétersbourg : Acad. Imperialis, p. 121–156.

[Euler, 1783c] Euler Leonhard, 1783c, «Miscellanea analytica». Dans *Opuscula Analytica*, vol. 1, Saint-Pétersbourg : Acad. Imperialis, p. 329–344.

[Euler, 1783d] Euler Leonhard, 1783d, «Observationes circa divisionem quadratorum per numeros primos». Dans *Opuscula Analytica*, vol. 1, Saint-Pétersbourg : Acad. Imperialis, p. 64–84.

[Euler, 1787] Euler Leonhard, 1787, «Novae demonstrationes circa divisores numerorum formae $xx + nyy$». *Nova Acta Academiae Scientarum Imperialis Petropolitinae*, vol. 1, p. 47–74.

[Euler, 1849] Euler Leonhard, 1849, «Tractatus de numerorum doctrina capita sedecim, quae supersunt». Dans Rudio Ferdinand (ed.), *Commentationes arithmeticae*, vol. 2, Berlin : Teubner, p. 503 – 575.

[Fenster, 1999] Fenster Della, 1999, «Why Dickson Left Quadratic Reciprocity Out of his *History of the Theory of Numbers*». *The American Mathematical Monthly*, vol. 106 (7), p. 618–627.

[Fenster, 2007] Fenster Della, 2007, «Gauss Goes West : The Reception of the *Disquisitiones Arithmeticae* in the USA». Dans Goldstein Catherine, Schappacher Norbert et Schwermer Joachim (eds), *The Shaping of Arithmetic after C. F. Gauss's Disquisitiones Arithmeticae*, Berlin : Springer, p. 463–479.

[Ferreirós, 2007] Ferreirós José, 2007, «The Rise of Pure Mathematics as Arithmetic with Gauss». Dans Goldstein Catherine, Schappacher Norbert et Schwermer Joachim (eds), *The Shaping of Arithmetic after C. F. Gauss's Disquisitiones Arithmeticae*, Berlin : Springer, p. 234–268.

[Flament, 2003] Flament Dominique, 2003, *Histoire des nombres complexes. Entre algèbre et géométrie.* Paris : CNRS.

[Lefebure de Fourcy, 1833] Lefebure de Fourcy Louis-Étienne, 1833, *Leçons d'algèbre.* Paris : Bachelier.

[Francoeur, 1838] Francoeur Louis-Benjamin, 1838, *Algèbre supérieure.* Bruxelles : Meline, Cans.

[Frei, 2007] Frei Günther, 2007, «The Unpublished Section Eight : On the Way to Function Fields over a Finite Field». Dans Goldstein Catherine, Schappacher Norbert et Schwermer Joachim (eds), *The Shaping of Arithmetic after C. F. Gauss's Disquisitiones Arithmeticae*, Berlin : Springer, p. 159–198.

[Galois, 1830] Galois Évariste, 1830, «Sur la théorie des nombres». *Bulletin des sciences mathématiques, physiques et chimiques*, vol. 13, p. 428–435.

[Galois, 1908] Galois Évariste, 1908, *Manuscrits de Evariste Galois, publiés par Jules Tannery.* Paris : Gauthier-Villars.

[Gauss, 1801] Gauss Carl Friedrich, 1801, *Disquisitiones Arithmeticae.* Leipzig : Fleischer. Traduction française par A. C. M. Poullet-Delisle, *Recherches arithmétiques*, Paris : Courcier, 1807.

[Gauss, 1808] Gauss Carl Friedrich, 1808, «Theorematis arithmetici demonstratio nova». *Commentationes Societatis Regiae Scientiarum Gottingensis recentiores (Commentationes mathematicae)*, vol. 16, p. 69–74. Repr. in *Werke*, vol. II, *Höhere Arithmetik*, ed. Königliche Gesellschaft der Wissenschaften zu Göttingen, Göttingen : Universitäts-Druckerei, 1863, p. 3-8.

[Gauss, 1811] Gauss Carl Friedrich, 1811, «Summatio quarundam serierum singularium». *Commentationes societatis regiae scientiarum Gottingensis recentiores*, vol. 1. Repr. in *Werke*, vol. II, *Höhere Arithmetik*, ed. Königliche Gesellschaft der Wissenschaften zu Göttingen, Göttingen : Universitäts-Druckerei, 1863, p. 11-45.

[Gauss, 1818] Gauss Carl Friedrich, 1818, «Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et ampliationes novae». *Commentationes societatis regiae scientiarum Gottingensis recentiores*, vol. 4, p. 3–20. Repr. in *Werke*, vol. II, *Höhere Arithmetik*, ed. Königliche Gesellschaft der Wissenschaften zu Göttingen, Göttingen : Universitäts-Druckerei, 1863, p. 49-64.

[Gauss, 1828] Gauss Carl Friedrich, 1828, «Theoria residuorum biquadraticorum, Commentatio prima». *Commentationes societatis regiae scientiarum Gottingensis recentiores*, vol. 6, p. 27–56. Repr. in *Werke*, vol. II, *Höhere Arithmetik*, ed. Königliche

Gesellschaft der Wissenschaften zu Göttingen, Göttingen : Universitäts-Druckerei, 1863, p. 65-92.

[Gauss, 1832] Gauss Carl Friedrich, 1832, «Theoria residuorum biquadraticorum, Comentatio secunda». *Commentationes societatis regiae scientiarum Gottingensis recentiores*, vol. 7, p. 89–148. Repr. in *Werke*, vol. II, *Höhere Arithmetik*, ed. Königliche Gesellschaft der Wissenschaften zu Göttingen, Göttingen : Universitäts-Druckerei, 1863, p. 93-150.

[Gauss, 1863] Gauss Carl Friedrich, 1863, *Werke*, vol. II, *Höhere Arithmetik*, ed. Königliche Gesellschaft der Wissenschaften zu Göttingen, Göttingen : Universitäts-Druckerei.

[Gauthier, 2007] Gauthier Sébastien, 2007, *La Géométrie des nombres comme discipline (1890-1945)*. Thèse de doctorat, Université Paris 6, Paris.

[Germain, 1831] Germain Sophie, 1831, «Note sur la manière dont se décomposent les valeurs de y et z dans l'équation $\frac{4(x^p-1)}{x-1} = y^2 \pm pz^2$, et celles de Y' et Z' dans l'équation $\frac{4(x^{p^2}-1)}{x-1} = Y'^2 \pm pZ'^2$». *Journal für die reine und angewandte Mathematik*, vol. 27, p. 201–204.

[Gilain, 1989] Gilain Christian, 1989, «Cauchy et le cours d'analyse de l'École polytechnique». *Bulletin de la Société des amis de la bibliothèque de l'École polytechnique*, vol. 5, p. 3–46.

[Gilain, 1991] Gilain Christian, 1991, «Sur l'histoire du théorème fondamental de l'algèbre : théorie des équations et calcul intégral». *Archive for History of Exact Sciences*, vol. 42, p. 91–136.

[Gispert, 1991] Gispert Hélène, 1991, *La France mathématique. La Société mathématique de France*. Paris : SFHST et SMF.

[Gispert, 2001] Gispert Hélène, 2001, «Les journaux scientifiques en Europe». Dans *L'Europe des Sciences*, Paris : Seuil, p. 391–404.

[Goldstein, 1989] Goldstein Catherine, 1989, «Le métier des nombres aux XVII^{e} et XIX^{e} siècles». Dans Serres Michel (ed.), *Éléments d'histoire des sciences*, Paris : Bordas, p. 274–295.

[Goldstein, 1995] Goldstein Catherine, 1995, *Un théorème de Fermat et ses lecteurs*. Saint-Denis : Presses Universitaires de Vincennes.

[Goldstein, 1999] Goldstein Catherine, 1999, «Sur la question des méthodes quantitatives en histoire des mathématiques : le cas de la théorie des nombres en France (1870-1914)». *Acta historiae rerum naturalium nec non technicarum*, 3ème sér., vol. 28, p. 187–214.

[Goldstein, 2005] Goldstein Catherine, 2005, «Johann Peter Gustav Lejeune-Dirichlet, Vorlesungen über Zahlentheorie, First edition (1863)». Dans Grattan-Guinness Ivor (ed.), *Landmark Writings in Western Mathematics*, Amsterdam : Elsevier, p. 480–490.

[Goldstein, 2007] Goldstein Catherine, 2007, «The Hermitian Form of Reading the *Disquisitiones*». Dans Goldstein Catherine, Schappacher Norbert et Schwermer Joachim (eds), *The Shaping of Arithmetic after C. F. Gauss's Disquisitiones Arithmeticae*, Berlin : Springer, p. 377–410.

[Goldstein, 2011] Goldstein Catherine, 2011, «Un arithméticien contre l'arithmétisation : les principes de Charles Hermite». Dans Flament Dominique et Nabonnand Philippe (eds), *La Justification en mathématiques*, Paris : Maison des sciences de l'homme.

[Goldstein, 2009] Goldstein Catherine, 2009, «Gabriel Lamé et la théorie des nombres : « une passion malheureuse » ?» *Bulletin de la SABIX*, vol. 44, p. 131–139.

[Goldstein et Schappacher, 2007a] Goldstein Catherine et Schappacher Norbert, 2007a, «A Book in Search of a Discipline (1801 - 1860)». Dans Goldstein Catherine, Schappacher Norbert et Schwermer Joachim (eds), *The Shaping of Arithmetic after C. F. Gauss's Disquisitiones Arithmeticae*, Berlin : Springer, p. 3–65.

[Goldstein et Schappacher, 2007b] Goldstein Catherine et Schappacher Norbert, 2007b, «Several Disciplines and a Book (1860 - 1901)». Dans Goldstein Catherine, Schappacher Norbert et Schwermer Joachim (eds), *The Shaping of Arithmetic after C. F. Gauss's Disquisitiones Arithmeticae*, Berlin : Springer, p. 67–103.

[Goldstein et al., 2007] Goldstein Catherine, Schappacher Norbert et Schwermer Joachim (eds), 2007, *The Shaping of Arithmetic after C. F. Gauss's Disquisitiones Arithmeticae*. Berlin : Springer.

[Gouhier, 1997] Gouhier Henri, 1997, *La vie d'Auguste Comte*. Paris : Vrin, 2e édition.

[Grabiner, 1981] Grabiner Judith V., 1981, *The Origins of Cauchy's Rigorous Calculus*. Cambridge : MIT Press.

[Grattan-Guinness, 1980] Grattan-Guinness Ivor (ed.), 1980, *From the Calculus to Set Theory 1630-1910. An Introduction History*. London : Dickworth.

[Gray, 1992] Gray Jeremy, 1992, «The Nineteenth-Century Revolution in Mathematical Ontology». Dans Gillies Donald (ed.), *Revolutions in Mathematics*, Oxford : Clarendon Press, p. 226–248.

[Grunert, 1846] Grunert Johann August, 1846, «Ueber zwei Sätze aus der Algebra und aus der Zahlenlehre». *Archiv der Mathematik und Physik*, vol. 7, p. 367–386.

[Grunert, 1865] Grunert Johann August, 1865, «Theorie der Aequivalenzen». *Archiv der Mathematik und Physik*, vol. 44, p. 443–477.

[Grunert, 1866] Grunert Johann August, 1866, «Allgemeine Theorie der Wurzeln der Aequivalenzen, mit besonderer Rücksicht auf die Theorie der Gleichungen». *Archiv der Mathematik und Physik*, vol. 45, p. 454–492.

[Guimarães, 1900] Guimarães Rodolphe, 1900, *Les mathématiques en Portugal*. Coìmbre : Imprimerie de l'Université.

[Guisti, 2000] Guisti Enrico, 2000, *La naissance des objets mathématiques*. Paris : Ellipses.

[Guntau et Laitko, 1987] Guntau Martin et Laitko Hubert (eds), 1987, *Der Ursprung der modernen Wissenschaften. Studien zur Entstehung wissenschaftlicher Disziplinen*. Berlin : Akademie-Verlag.

[Gérini, 2002] Gérini Christian, 2002, *Les « Annales » de Gergonne : apport scientifique et épistémologique dans l'histoire des mathématiques*. Villeneuve d'Ascq : Septentrion.

[Hamburg, 1976/77] Hamburg Robin Rider, 1976/77, «The Theory of Equations in the 18th Century : the Work of Joseph Lagrange». *Archive for History of Exact Sciences*, vol. 16 (1), p. 17–36.

[Hermite, 1849] Hermite Charles, 1849, «Démonstration élémentaire d'une proposition relative aux diviseurs de $x^2 + Ay^2$». *Journal de mathématiques pures et appliquées*, vol. 14, p. 451–452.

[Hill, 1995] Hill Amy Marie, 1995, *Sophie Germain : a Mathematical Biography*. Thèse de doctorat, Department of Mathematics and Honors College of the University of Oregon, Eugene.

[Houzel, 2002] Houzel Christian, 2002, *La géométrie algébrique. Recherches historiques*. Paris : Blanchard.

[Houzel, 2007] Houzel Christian, 2007, «Elliptic Functions and Arithmetic». Dans Goldstein Catherine, Schappacher Norbert et Schwermer Joachim (eds), *The Shaping of Arithmetic after C. F. Gauss's Disquisitiones Arithmeticae*, Berlin : Springer, p. 291–312.

[Ireland et Rosen, 1990] Ireland Kenneth et Rosen Michael, 1990, *A Classical Introduction to Modern Number Theory*. New York : Springer-Verlag, 2e édition.

[Itard, 1969] Itard Jean, 1969, *Les nombres premiers*. Paris : Presses Universitaires de France.

[Jacobi, 1827] Jacobi Carl Gustav Jacob, 1827, «De residuis cubiscis commentatio numerosa». *Journal für die reine und angewandte Mathematik*, vol. 2, p. 66 – 69.

[Jacobi, 1832] Jacobi Carl Gustav Jacob, 1832, «Observatio arithmetica de numero classium divisorum quadraticorum formae $yy + Azz$ designante A numerum primum formae $4n+3$». *Journal für die reine und angewandte Mathematik*, vol. 9, p. 189–192.

[Jacobi, 1837] Jacobi Carl Gustav Jakob, 1837, «Über die Kreistheilung und ihre Anwendung auf die Zahlentheorie». *Monatsbericht der Akademie der Wissenschaften zu Berlin*, p. 127–136. Traduction française par E. Laguerre-Werly, Sur la division du cercle et son application à la théorie des nombres, *Nouvelles annales de mathématiques*, 1ère série, tome 15, 1856, p. 337-352.

[Jacobi, 1839a] Jacobi Carl Gustav Jacob, 1839a, *Canon arithmeticus sive tabulae quibus exhibentur pro singulis numeris primis vel primorum potestatibus infra 1000 numeri an datos indices et indices ad datos numerus pertinentes*. Berlin : Typis Academicis.

[Jacobi, 1839b] Jacobi Carl Gustav Jacob, 1839b, «Ueber die complexen Primzahlen, welche in der Theorie der Reste der 5ten, 8ten und 12ten Potenzen zu betrachten sind». *Journal für die reine und angewandte Mathematik*, vol. 19, p. 314–318. Traduction française par M. Faye, Sur les nombres premiers complexes que l'on doit considérer dans la théorie des résidus de cinquième, huitième et douzième puissance, *Journal de mathématiques pures et appliquées*, 1ère série, tome 8, 1843, p. 268-272.

[Jacobi, 1881-1891] Jacobi C.-G.-J., 1881-1891, «Briefe Jacobi's an Gauss». Dans *Gesammelte Werke*, vol. 7, Berlin : Reimer, p. 389–406.

[Jacobi, 2007] Jacobi Carl Gustav Jacob, 2007, *Vorlesungen über Zahlentheorie—Wintersemester 1836/37, Königsberg*. Augsburg : Dr. Erwin Rauner Verlag.

[Jahnke et Otte, 1981] Jahnke Hans Niels et Otte Michael, 1981, «Origins of the Program of "Arithmetization of Mathematics"». Dans Mehrtens Herbert, Bos Henk J. M. et Schneider Ivo (eds), *Social History of Nineteenth Century Mathematics*, Boston, Basel, Stuttgart : Birkhäuser, p. 21–50.

[Jordan, 1861] Jordan Camille, 1861, «Mémoire sur le nombre des valeurs d'une fonction». *Journal de l'École polytechnique*, vol. 22, p. 113–194.

[Jordan, 1881] Jordan Camille, 1881, *Notice sur les travaux de M. Camille Jordan, ingénieur des Mines, professeur à l'École polytechnique, à l'appui de sa candidature à l'Académie des sciences (section de géométrie)*. Paris : Gauthier-Villars.

[Julia, 1942 - 1950] Julia Gaston, 1942 - 1950, «La vie et l'œuvre de J. - L. Lagrange». *L'Enseignement mathématique*, vol. 39, p. 9–21.

[Klein, 1926-1927] Klein Felix, 1926-1927, *Vorlesungen über die Entwicklung der Mathematik im 19. Jahrhundert*. Berlin : Springer.

[Kline, 1972] Kline Morris, 1972, *Mathematical Thought from Ancient to Modern Times*. New York : Oxford University Press.

[Knobloch, 1991] Knobloch Eberhard, 1991, «L'analogie et la pensée mathématique». Dans Rashed Roshdi (ed.), *Mathématiques et philosophie de l'Antiquité à l'âge classique*, Paris : CNRS, p. 217–237.

[Kronecker, 1856] Kronecker Leopold, 1856, «Sur une formule de Gauss». *Journal de mathématiques pures et appliquées*, vol. 1, p. 392–395.

[Kronecker, 1887] Kronecker Leopold, 1887, «Über den Zahlbegriff». *Journal für die reine und angewandte Mathematik*, vol. 101, p. 337–355.

[Kummer, 1844] Kummer Ernst Eduard, 1844, «De numeris complexis, qui radicibus unitatis et numeris integris realibus constant». Gratulationschrift der Univ. Breslau zur Jubelfeier der Univ. Königsberg, Breslau. Repr. in *Journal de mathématiques pures et appliquées*, t. 12, 1847, p. 185-212.

[Kummer, 1846] Kummer Ernst Eduard, 1846, «Über die Divisoren gewisser Formen der Zahlen, welche aus der Theorie der Kreistheilung entstehen». *Journal für die reine und angewandte Mathematik*, vol. 30, p. 107–116.

[Kummer, 1847] Kummer Ernst Eduard, 1847, «Zur Theorie der complexen Zahlen». *Journal für die reine und angewandte Mathematik*, vol. 35, p. 319–326.

[Kummer, 1851] Kummer Ernst Eduard, 1851, «Mémoire sur la théorie des nombres complexes composés de racines de l'unité et de nombres entiers». *Journal de mathématiques pures et appliquées*, vol. 16, p. 377 – 498.

[Kummer, 1975] Kummer Ernst Eduard, 1975, *Ernst Eduard Kummer Collected Papers. Volume I. Contributions tu Number Theory*. Berlin, New York : Springer-Verlag.

[Lacroix, 1800] Lacroix Sylvestre-François, 1800, *Traité des différences et des séries, faisant suittraité du calcul différentiel et du calcul intégral*. Paris : Duprat.

[Lacroix, 1804] Lacroix Sylvestre-François, 1804, *Complément des élémens d'algèbre*. Paris : Courcier, 3^{e} édition.

[Lacroix, 1817] Lacroix Sylvestre-François, 1817, *Complément des élémens d'algèbre*. Paris : Courcier, 4^{e} édition.

[Lagrange, 1769] Lagrange Joseph-Louis, 1769, «Sur la solution des problèmes indéterminés du second degré». *Histoire de l'Académie royale des sciences et des Belles-Lettres de Berlin*, vol. 22, p. 165–310. Repr. in *Œuvres de Lagrange*, éd. J. - A. Serret, t. 2, Paris : Gauthier-Villars, 1868, p. 377-535.

[Lagrange, 1770] Lagrange Joseph-Louis, 1770, «Nouvelle méthode pour résoudre les problèmes indéterminés en nombres entiers». *Histoire de l'Académie royale des sciences et des Belles-Lettres de Berlin*, (Année 1770), p. 134-215 ; (Année 1771), p. 138-253. Repr. in *Œuvres de Lagrange*, éd. J. - A. Serret, t. 2, Paris : Gauthier-Villars, 1868, p. 655-726.

[Lagrange, 1772] Lagrange Joseph-Louis, 1772, «Démonstration d'un théorème d'arithmétique». *Nouveaux mémoires de l'Académie royale des sciences et belles-lettres de Berlin, Année 1770*, p. 123–133. Repr. in *Œuvres de Lagrange*, éd. J. - A. Serret, t. 3, Paris : Gauthier-Villars, 1869, p. 189-201.

[Lagrange, 1772-1773] Lagrange Joseph-Louis, 1772-1773, «Réflexions sur la résolution algébrique des équations». *Nouveaux mémoires de l'Académie royale des sciences et belles-lettres de Berlin*, (Année 1770), p. 134-215 ; (Année 1771), p. 138-253. Repr. in *Œuvres de Lagrange*, éd. J. - A. Serret, t. 3, Paris : Gauthier-Villars, 1869, p. 205 - 421.

[Lagrange, 1773a] Lagrange Joseph-Louis, 1773a, «Démonstration d'un théorème nouveau concernant les nombres premiers». *Nouveaux mémoires de l'Académie royale des sciences et belles-lettres de Berlin, Année 1771*, p. 125–137. Repr. in *Œuvres de Lagrange*, éd. J. - A. Serret, t. 3, Paris : Gauthier-Villars, 1869, p. 425-438.

[Lagrange, 1773b] Lagrange Joseph-Louis, 1773b, «Solution d'un problème d'arithmétique». *Miscellanea Taurinensia*, vol. 4, p. 41–97. Repr. in *Œuvres de Lagrange*, éd. J. - A. Serret, t. I, Paris : Gauthier-Villars, 1867, p. 671-731.

[Lagrange, 1774] Lagrange Joseph-Louis, 1774, «Additions. De l'analyse indéterminée.» Dans *Élémens d'Algèbre d'Euler, traduits de l'allemand, avec des notes et des additions*, vol. 2, Lyon - Paris : Bruyset - Desaint, p. 369–658. Repr. in *Œuvres de Lagrange*, éd. J. - A. Serret, t. VII, Paris : Gauthier-Villars, 1869, p. 5-180.

[Lagrange, 1808] Lagrange Joseph-Louis, 1808, *Traité de la résolution des équations numériques de tous les degrés, avec des notes sur plusieurs points de la théorie des équations algébriques*. Paris : Courcier, 2e édition.

[Lalande, 1932] Lalande André, 1932, *Vocabulaire technique et critique de la philosophie*. Paris : Presses Universitaires de France.

[Lamandé, 1987] Lamandé Pierre, 1987, «Les manuels de Bézout». *Rivista di storia della scienza*, vol. 4, p. 339–375.

[Lamandé, 2004] Lamandé Pierre, 2004, «La conception des nombres en France autour de 1800 : l'œuvre didactique de Sylvestre François Lacroix». *Revue d'histoire des mathématiques*, vol. 10, p. 45–106.

[Lamy, 1996] Lamy Loîc, 1996, «Le *Journal de l'École polytechnique* de 1795 à 1831 : journal savant, journal institutionnel». *Sciences et techniques en perspective*, vol. 32, p. 4–96.

[Lamé, 1847a] Lamé Gabriel, 1847a, «Mémoire sur la résolution, en nombres complexes, de l'équation $A^5 + B^5 + C^5 = 0$». *Journal de mathématiques pures et appliquées*, vol. 12, p. 137–171.

[Lamé, 1847b] Lamé Gabriel, 1847b, «Mémoire sur la résolution, en nombres complexes, de l'équation $A^n + B^n + C^n = 0$». *Journal de mathématiques pures et appliquées*, vol. 12, p. 172–184.

[Laplace, 1812] Laplace Pierre-Simon, 1812, «Leçons de mathématiques données à l'école normale, en 1795». *Journal de l'École polytechnique*, 7ème cahier, vol. 2, p. 2–278.

[Laubenbacher et Pengelley, 2010] Laubenbacher Reinhard et Pengelley David, 2010, «"Voici ce que j'ai trouvé" : Sophie Germain's grand plan to prove Fermat's Last Theorem». *Historia Mathematica*, vol. 37 (4), p. 641–692.

[Lebesgue, 1829] Lebesgue Victor-Amédée, 1829, «Extrait d'un Mémoire inédit sur les congruence d'un degré quelconque à une seule inconnue». *Bulletin du Nord*, vol. 1, 1er cahier (janvier 1829), p. 23-43 ; 3ème (mars 1829), p. 255-274 ; vol. 2, 5ème cahier (mai 1829), p. 19-33.

[Lebesgue, 1837a] Lebesgue Victor-Amédée, 1837a, «Note sur l'équation $x^p = 1$». *Comptes rendus hebdomadaires des séances de l'Académie des sciences*, vol. 5, p. 722–725.

[Lebesgue, 1837b] Lebesgue Victor-Amédée, 1837b, «Recherches sur les nombres». *Journal de mathématiques pures et appliquées*, vol. 2, p. 253–292.

[Lebesgue, 1838] Lebesgue Victor-Amédée, 1838, «Recherches sur les nombres (suite)». *Journal de mathématiques pures et appliquées*, vol. 3, p. 113–144.

[Lebesgue, 1839] Lebesgue Victor-Amédée, 1839, «Recherches sur les nombres (suite)». *Journal de mathématiques pures et appliquées*, vol. 4, p. 9–59.

[Lebesgue, 1840a] Lebesgue Victor-Amédée, 1840a, «Note sur une formule de Cauchy». *Journal de mathématiques pures et appliquées*, vol. 5, p. 186–188.

[Lebesgue, 1840b] Lebesgue Victor-Amédée, 1840b, «Sommation de quelques séries». *Journal de mathématiques pures et appliquées*, vol. 5, p. 42–71.

[Lebesgue, 1842] Lebesgue Victor-Amédée, 1842, «Démonstration de quelques théorèmes relatifs aux résidus et aux non-résidus quadratiques». *Journal de mathématiques pures et appliquées*, vol. 7, p. 137–159.

[Lebesgue, 1844] Lebesgue Victor-Amédée, 1844, «Formule pour la résolution de l'équation auxiliaire de degré m, relative à l'équation $x^p = 1$, en supposant $p = m\varpi + 1$ et premier». *Comptes rendus hebdomadaires des séances de l'Académie des sciences*, vol. 18, p. 696–699.

[Lebesgue, 1847a] Lebesgue Victor-Amédée, 1847a, «Démonstration nouvelle et élémentaire de la loi de réciprocité quadratique de Legendre, par M. Eisenstein, précédée et suivie de remarques sur d'autres démonstrations qui peuvent être tirées du même principe». *Journal de mathématiques pures et appliquées*, vol. 12, p. 456–473.

[Lebesgue, 1847b] Lebesgue Victor-Amédée, 1847b, «Sur le symbole $\left(\frac{a}{b}\right)$ et quelques-unes de ses applications». *Journal de mathématiques pures et appliquées*, vol. 12, p. 497–517.

[Lebesgue, 1849] Lebesgue Victor-Amédée, 1849, «Exercices d'analyse numérique, forma un traité de la théorie des nombres». *Nouvelles annales de mathématiques*, vol. 8, p. 87.

[Lebesgue, 1850a] Lebesgue Victor-Amédée, 1850a, «Note sur les congruences». *Nouvelles annales de mathématiques*, vol. 9, p. 436–439.

[Lebesgue, 1850b] Lebesgue Victor-Amédée, 1850b, «Suite du Mémoire sur les applications du symbole $\left(\frac{a}{b}\right)$». *Journal de mathématiques pures et appliquées*, vol. 15, p. 215–237.

[Lebesgue, 1854] Lebesgue Victor-Amédée, 1854, «Démonstration de quelques formules d'un Mémoire de Jacobi». *Journal de mathématiques pures et appliquées*, vol. 19, p. 289–300.

[Lebesgue, 1922] Lebesgue Henri, 1922, «L'œuvre mathématique de Georges Humbert, quelques mots sur Camille Jordan (Extrait de la leçon inaugurale de mathématiques donnée au Collège de France le 6 janvier 1922)». *Bulletin des sciences mathématiques*, vol. 57, p. 220 – 233.

[Lecointe, 1859] Lecointe Léon, 1859, *Cours d'algèbre élémentaire*. Bruxelles : Flatau.

[Legendre, 1788] Legendre Adrien-Marie, 1788, «Recherches d'analyse indéterminée». *Histoire de l'Académie royale des sciences, avec les Mémoires de mathématiques et de physique, Année 1785*, p. 465–559.

[Legendre, 1798] Legendre Adrien-Marie, 1798, *Essai sur la théorie des nombres*. Paris : Duprat.

[Legendre, 1808] Legendre Adrien-Marie, 1808, *Essai sur la théorie des nombres*. Paris : Courcier, 2e édition.

[Legendre, 1827] Legendre Adrien-Marie, 1827, «Recherches sur quelques objets d'analyse indéterminée et particulièrement sur le théorème de Fermat». *Mémoires de l'Académie royale des sciences de l'Institut de France*, vol. 6, p. 1–60.

[Legendre, 1830] Legendre Adrien-Marie, 1830, *Théorie des nombres*. Paris : Firmin Didot, 3e édition.

[Legendre, 1832] Legendre Adrien-Marie, 1832, «Mémoire sur la détermination des fonctions Y et Z qui satisfont à l'équation $4(X^n-1) = (X-1)(Y^2 \pm nZ^2)$, n étant un nombre premier $(4i \mp 1)$». *Mémoires de l'Académie Royale des Sciences de l'Institut de France*, vol. 11, p. 81–100.

[Legendre et Jacobi, 1875] Legendre Adrien-Marie et Jacobi Carl Gustav Jacob, 1875, «Correspondance mathématique entre Legendre et Jacobi, communiquée par

C.-W. Borchardt.» *Journal für die reine und angewandte Mathematik*, vol. 80, p. 205–279.

[Lehmer, 1941] Lehmer Derrick Henry, 1941, *Guide to the Tables in the Theory of Numbers*. Washington, D. C. : National Research Council.

[Lemmermeyer, 2000] Lemmermeyer Franz, 2000, *Reciprocity Laws : from Euler to Eisenstein*. Berlin : Springer-Verlag.

[Lemmermeyer, 2009] Lemmermeyer Franz, 2009, «Jacobi and Kummer's Ideal Numbers». *Abhandlungen aus dem mathematischen Seminar der Universität Hamburg*, vol. 79 (2), p. 165–187.

[Libri, 1829] Libri Guglielmo, 1829, *Mémoire de mathématique et de physique*. Florence : Ciardetti.

[Libri, 1832a] Libri Guglielmo, 1832a, «Mémoire sur la théorie des nombres». *Journal für die reine und angewandte Mathematik*, vol. 9, p. 54–80, 169–188, 261–279.

[Libri, 1832b] Libri Guglielmo, 1832b, «Notice sur M^{lle} Sophie Germain». *Journal des Débats politiques et litéraires*, p. 1.

[Libri, 1838] Libri Guglielmo, 1838, «Mémoire sur la théorie des nombres». *Mémoires présentés par divers savants à l'Académie royale des sciences de l'Institut de France ; sciences mathématiques et physiques*, vol. 5, p. 1–75.

[Libri et Poisson, 1836] Libri Guglielmo et Poisson Siméon Denis, 1836, «Rapport sur un Mémoire de M. Lebesgue sur les résidus». *Comptes rendus hebdomadaires des séances de l'Académie des sciences*, vol. 3, p. 439–441.

[Liouville, 1843] Liouville Joseph, 1843, «Sur la division du périmètre de la lemniscate, le diviseur étant un nombre entier réel ou complexe quelconque». *Journal de mathématiques pures et appliquées*, vol. 8, p. 507–512.

[Liouville, 1847] Liouville Joseph, 1847, «Sur la loi de réciprocité dans la théorie des résidus quadratiques». *Comptes rendus hebdomadaires des séances de l'Académie des sciences*, vol. 24, p. 577–578.

[Lucas, 1891] Lucas Edouard, 1891, *Récréations mathématiques*. Paris : Gauthier-Villars.

[Lützen, 1982] Lützen Jesper, 1982, «Joseph Liouville's Contribution to the Theory of Integral Equations». *Historia Mathematica*, vol. 9, p. 371–391.

[Maccioni Ruju et Mostert, 1995] Maccioni Ruju P. Alessandra et Mostert Marco, 1995, *The Life and Times of Guglielmo Libri (1802-1869), Scientist, Patriot, Scholar, Journalist and Thief. A Nineteenth Century Story.* Hilversum : Verloren.

[Maigre, 2007] Maigre Lise, 2007, *La Théorie des nombres de Legendre. Les différentes éditions et le rôle des travaux de Gauss*. Master d'histoire des sciences et des techniques, Centre François Viète, Université de Nantes.

[Martin, 1996] Martin Thierry, 1996, *Probabilités et critique philosophique selon Cournot*. Paris : Vrin.

[Meyer et Molk, 1904 - 1916] Meyer Franz et Molk Jules (eds), 1904 - 1916, *Encyclopédie des sciences mathématiques pures et appliquées, tome I : arithmétique et algèbre (4 vols)*.

[Midy, 1845] Midy E., 1845, «Analyse indéterminée du premier degré». *Nouvelles annales de mathématiques*, vol. 4, p. 146–152.

[Miller, 1903] Miller George Abram, 1903, «Appreciative Remarks on the Theory of Groups». *The American Mathematical Monthly*, vol. 10 (4), p. 87–89.

[Minding, 1832] Minding Ferdinand, 1832, *Anfangsgründe der höheren Arithmetik*. Berlin : Reimer.

[Neumann, 1979-1980] Neumann Olaf, 1979-1980, «Bemerkungen aus heutiger Sicht über Gauss' Beiträge zu Zahlentheorie, Algebra und Funktionentheorie.» *NTM-Schriftenreihe*, vol. 16 (2), p. 22-39 ; vol. 17 (1), p. 32-48 ; vol. 17 (2), p. 38-58.

[Neumann, 2005] Neumann Olaf, 2005, «Carl Friedrich Gauss's Disquisitiones Arithmeticae (1801)». Dans Grattan-Guinness I. (ed.), *Landmark Writings in Western Mathematics 1640-1940*, Amsterdam : Elsevier, p. 303–315.

[Neumann, 2007a] Neumann Olaf, 2007a, «Cyclotomy : From Euler through Vandermonde to Gauss». Dans Bradley Robert E. et Sandifer Ed (eds), *Leonhard Euler : Life, Work and Legacy*, Amsterdam : Elsevier, p. 323–362.

[Neumann, 2007b] Neumann Olaf, 2007b, «The *Disquisitiones Arithmeticae* and the Theory of Equations». Dans Goldstein Catherine, Schappacher Norbert et Schwermer Joachim (eds), *The Shaping of Arithmetic after C. F. Gauss's Disquisitiones Arithmeticae*, Berlin : Springer, p. 107–127.

[Nielsen, 1923] Nielsen Niels, 1923, *Traité élémentaire des nombres de Bernoulli*. Paris : Gauthier-Villars.

[Nový, 1968] Nový Luboš, 1968, «L'École algébrique anglaise». *Revue de synthèse*, 3ème série, vol. 49-52, p. 211–222.

[Ore, 1957] Ore Oystein, 1957, *Niels Henrik Abel : Mathematician Extraordinary*. Minneapolis : University of Minnesota Press.

[Patterson, 2007] Patterson Samuel James, 2007, «Gauss Sums». Dans Goldstein Catherine, Schappacher Norbert et Schwermer Joachim (eds), *The Shaping of Arithmetic after C. F. Gauss's Disquisitiones Arithmeticae*, Berlin : Springer, p. 505–528.

[Peacock, 1834] Peacock George, 1834, «Report on the Recent Progress and Present State of Certain Branches of Analysis». Dans *Report of the Third Meeting of the British Association for the Advancement Of Science*, London : Murray, p. 185–352.

[Peiffer, 1978] Peiffer Jeanne, 1978, *Les premiers exposés globaux de la théorie des fonctions de Cauchy*. Thèse de doctorat, EHESS, Paris.

[Peiffer, 1983] Peiffer Jeanne, 1983, «Joseph Liouville (1809-1882) : ses contributions à la théorie des fonctions d'une variable complexe». *Revue d'histoire des sciences*, vol. 36 (3-4), p. 209–248.

[Peiffer, 1998] Peiffer Jeanne, 1998, «Faire des mathématiques par lettres». *Revue d'histoire des mathématiques*, vol. 4, p. 143–157.

[Petri et Schappacher, 2002] Petri Birgit et Schappacher Norbert, 2002, «From Abel to Kronecker : Episodes from 19th Century Algebra». Dans Laudal Olav Arnfin et Piene Ragni (eds), *The Legacy of Niels Henrik Abel*, Berlin, New York : Springer-Verlag, p. 227–266.

[Pieper, 1993] Pieper Herbert, 1993, «On Euler's Contributions to the Four-Squares Theorem». *Historia Mathematica*, vol. 20, p. 12–18.

[Pieper, 2007] Pieper Herbert, 2007, «A Network of Scientific Philanthropy : Humboldt's Relations with Number Theorists». Dans Goldstein Catherine, Schappacher Norbert et Schwermer Joachim (eds), *The Shaping of Arithmetic after C. F. Gauss's Disquisitiones Arithmeticae*, Berlin : Springer, p. 201–233.

[Poinsot, 1808] Poinsot Louis, 1808, «Analyse du Traité de la résolution des équations numériques... par J. - L. Lagrange». *Magasin encyclopédique, ou Journal des sciences, des lettres et des arts*, vol. 4, p. 343–375.

[Poinsot, 1810] Poinsot Louis, 1810, «Mémoire sur les polygones et les polyèdres». *Journal de l'École polytechnique*, vol. 10^{e} cahier, Tome IV, p. 16–49.

[Poinsot, 1818] Poinsot Louis, 1818, «Extrait de quelques recherches nouvelles sur l'algèbre et la théorie des nombres». *Mémoires de la classe des sciences mathématiques et physiques de l'Institut de France*, vol. 14, p. 381–392.

[Poinsot, 1820] Poinsot Louis, 1820, «Mémoire sur l'application de l'algèbre à la théorie des nombres». *Journal de l'École polytechnique*, 18ème cahier, vol. 11, p. 342–410.

[Poinsot, 1845] Poinsot Louis, 1845, «Réflexion sur les principes fondamentaux de la théorie des nombres». *Journal de mathématiques pures et appliquées*, vol. 10, p. 1–101.

[Poinsot et Bailhache, 1975] Poinsot Louis et Bailhache Patrice, 1975, *La théorie générale de l'équilibre et du mouvement des systèmes*. Paris : Vrin. Édition critique et commentaires par Patrice Bailhache.

[Prouhet, 1845a] Prouhet Eugène, 1845a, «Note sur le nombre qui indique combien il y a d'entiers inférieurs et premiers à un nombre donné». *Nouvelles annales de mathématiques*, vol. 4, p. 75–81.

[Prouhet, 1845b] Prouhet Eugène, 1845b, «Note sur les nombres associés ; généralisation du théorème de Wilson». *Nouvelles annales de mathématiques*, vol. 4, p. 273–278.

[Prouhet, 1846] Prouhet Eugène, 1846, «Mémoire sur la théorie des résidus dans les progressions géométriques». *Nouvelles annales de mathématiques*, vol. 5, p. 175–187.

[Prouhet, 1850] Prouhet Eugène, 1850, «Irréductibilité de l'équation $X = 1 + x + \ldots + x^{p-1} = 0$, p étant un nombre premier». *Nouvelles annales de mathématiques*, vol. 9, p. 348–349.

[Revel, 1996] Revel Jacques, 1996, *Jeux d'échelles. La micro-analyse à l'expérience.* Paris : Seuil/Gallimard.

[Ritter, 2004] Ritter Jim, 2004, «Reading Strasbourg 368 : a Thrice-Told Tale». Dans Chemla Karine (ed.), *History of Science, History of Text*, Dordrecht : Springer, p. 177–200.

[Réalis, 1843] Réalis S., 1843, «De la résolution algébrique de l'équation $x^p - 1 = 0$, quand l'exposant p est un nombre premier». *Nouvelles annales de mathématiques*, vol. 2, p. 147–156.

[Schappacher, 1997] Schappacher Norbert, 1997, «Some Milestones of Lemniscatomy». Dans Sertöz Sinan (ed.), *Algebraic Geometry. Proceedings Bilkent Summer School, Ankara 1995*, New York : Dekker, p. 257–290.

[Schappacher, 1998] Schappacher Norbert, 1998, «On the History of Hilbert's Twelfth Problem. A comedy of errors». Dans *Matériaux pour l'histoire des mathématiques au XX^e siècle. Actes du colloque à la mémoire de Jean Dieudonné (Nice, 1996)*, Paris : Société Mathématique de France, p. 243–273.

[Serret, 1848] Serret Joseph-Alfred, 1848, «Sur un théorème relatif aux nombres entiers». *Journal de mathématiques pures et appliquées*, vol. 13, p. 12–14.

[Serret, 1849] Serret Joseph-Alfred, 1849, *Cours d'algèbre supérieure.* Paris : Bachelier.

[Serret, 1854] Serret Joseph-Alfred, 1854, *Cours d'algèbre supérieure.* Paris : Bachelier, 2^e édition.

[Serret, 1866] Serret Joseph-Alfred, 1866, *Cours d'algèbre supérieure*, vol. 2. Paris : Gauthier-Villars, 3^e édition.

[Shallit, 1994] Shallit Jeffrey, 1994, «Origins of the Analysis of the Euclidean Algorithm». *Historia Mathematica*, vol. 21, p. 401–419.

[Sinaceur, 1991] Sinaceur Hourya, 1991, *Corps et modèles.* Paris : Vrin.

[Smith, 1859-1865] Smith Henry J. S., 1859-1865, «Report on the Theory of Numbers». Dans *Report of the British Association for the Advancement of Science*, Oxford

Clarendon Press, 1859, p. 228-267 ; 1860, p. 120-169 ; 1861, p. 292-340 ; 1862, p. 503-526 ; 1863, p. 768-786 ; 1865, p. 322-37. Repr. in *The collected mathematical papers*, éd. J.W.L. Glaisher, vol. 1, Oxford : Clarendon Press, 1894, p. 38-364.

[Stern, 1832] Stern Moritz Abraham, 1832, «Bemerkungen zur höheren Arithmetik». *Journal für die reine und angewandte Mathematik*, vol. 9, p. 97–98.

[Stern, 1834] Stern Moritz Abraham, 1834, «Démonstration de quelques théorèmes sur les nombres». *Journal für die reine und angewandte Mathematik*, vol. 12, p. 288–291.

[Stichweh, 1991] Stichweh Rudolf, 1991, *Études sur la genèse du système scientifique moderne*. Lille : Presses Universitaires Septentrion.

[Stupuy, 1879] Stupuy Hyppolyte, 1879, *Œuvres philosophies de Sophie Germain*. Paris : Ritti.

[Suzuki, 2007] Suzuki Jeff, 2007, «Euler and Number Theory : A Study in Mathematical Invention». Dans Bradley Robert E. et Sandifer C. Edwards (eds), *Leonhard Euler : Life, Work and Legacy*, Elsevier, p. 363–384.

[Taton, 1947] Taton René, 1947, «Les mathématiques dans le « Bulletin de Férussac »». *Archives internationales d'histoire des sciences*, vol. 26, p. 100–125.

[Taton, 1990] Taton René, 1990, «La Société Philomathique de Paris et les sciences exactes, premiers tiers du XIX^{e} siècle». Dans *Actes du colloque du bicentenaire de la Société Philomathique*, vol. I, p. 37–54.

[Terquem, 1843] Terquem Olry, 1843, «Théorème de Wilson d'après M. Gauss». *Nouvelles annales de mathématiques*, vol. 2, p. 193–195.

[Terquem, 1844] Terquem Olry, 1844, «Théorie élémentaire des nombres. D'après Euler, Legendre, MM. Gauss et Cauchy». *Nouvelles annales de mathématiques*, vol. 3, p. 204–208, 214–219, 337–344.

[Terquem, 1845] Terquem Olry, 1845, «Généralisation de la théorie des associés et théorèmes y relatifs». *Nouvelles annales de mathématiques*, vol. 4, p. 379–382.

[Terquem, 1848] Terquem Olry, 1848, «Théorème arithmologique de M. Steiner». *Nouvelles annales de mathématiques*, vol. 7, p. 268–269.

[Terquem, 1849] Terquem Olry, 1849, «Nouvelle démonstration de l'irréductibilité de l'équation $1 + x + x^{+} \ldots + x^{p-1} = 0$; p étant un nombre premier. D'après M. L. Kronecker, étudiant à Berlin». *Nouvelles annales de mathématiques*, vol. 8, p. 419–421.

[Vandermonde, 1774] Vandermonde Alexandre-Théophile, 1774, «Mémoire sur la résolution des équations». *Histoire de l'Académie royale des sciences, avec les Mémoires de mathématiques et de physique, Année 1771*, p. 365–416.

[Verdier, 2009] Verdier Norbert, 2009, *Le Journal de Liouville et la presse de son temps : une entreprise d'édition et de circulation des mathématiques au XIX^{e} siècle (1824 - 1885)*. Thèse de doctorat, Université Paris 11, Paris.

[Vuillemin, 1993] Vuillemin Jules, 1993, *La philosophie de l'algèbre*. Paris : Presses Universitaires de France, 2^{e} édition.

[Waring, 1770] Waring Edward, 1770, *Meditationes Algebraicæ*. Cambridge : Typis Academis.

[Weil, 1949] Weil André, 1949, «Numbers of Solutions of Equations in Finite Fields». *Bulletin of the American Mathematical Society*, vol. 55, p. 497–508.

[Weil, 1984] Weil André, 1984, *Number Theory : An Approach through History from Hammurapi to Legendre*. Boston : Birkhäuser.

[White et al., 1867-1872] White Henry, McLeod Herbert et Morley Henry Forester (eds), 1867-1872, *Catalogue of Scientific Papers (1800-1863)*. London : Royal Society of London.

[Wronski, 1847] Wronski Josef Hoëné, 1847, *Messianisme ou réforme absolu du savoir humain ; nommément : réforme des mathématiques comme prototype de l'accomplissement final des sciences et réforme de la philosophie comme accomplissement final de la religion*. Paris : Firmin Didot.

[Wussing, 1984] Wussing Hans, 1984, *The Genesis of the Abstract Group Concept*. Cambridge, MA : MIT Press.

Annexes

Annexe A

Construction du corpus

I *History of the Theory of Numbers*, Dickson (1919-1023) : table des matières et textes non référencés

1 - Table des matières des trois volumes de [Dickson, 1919-1923]

Nous avons indiqué en gras les sections dont le titre mentionne explicitement des résidus, des congruences, des résultats modulo un nombre.

TOME 1	
I. 1	Perfect, multiply perfect, and amicable numbers
I. 2	Formulas for the number and sum of divisors, problems of Fermat and Wallis
I. 3	**Fermat's and Wilson's theorems, generalizations and converses ; symmetric functions of** $1, 2, \ldots, p-1$**, modulo** p
I. 4	**Residue of** $(u^{p-1}-1)/p$ **modulo** p
I. 5	Euler's ϕ-function, generalizations ; Farey series
I. 6	Periodic decimal fractions ; periodic fractions ; factors of $10^n \pm 1$
I. 7	**Primitive roots, exponents, indices, binomial congruences**
I. 8	**Higher congruences**
I. 9	Divisibility of factorials and multinomial coefficients
I. 10	Sum and number of divisors
I. 11	Miscellaneous theorems on divisibility, greatest common divisor, least common multiple
I. 12	Criteria for divisibility by a given number
I. 13	Factor tables, lists of primes
I. 14	Methods of factoring
I. 15	Fermat numbers $F_n = 2^{2^n} + 1$
I. 16	Factors of $a^n \pm b^n$
I. 17	Recurring series ; Lucas' u_n, v_n
I. 18	Theory of prime numbers
I. 19	Inversion of functions ; Möbius' function $\mu(n)$; numerical integrals and derivatives
I. 20	Properties of the digits of numbers
TOME 2	
II. 1	Polygonal, pyramidal and figurate numbers
II. 2	**Linear diophantine equations and congruences**
II. 3	Partitions
II. 4	Rational right triangles
II. 5	Triangles, quadrilaterals, and tetrahedra
II. 6	Sum of two squares
II. 7	Sum of three squares

II. 8	Sum of four squares
II. 9	Sum of n squares
II. 10	**Number of solutions of quadratic congruences in n unknowns**
II. 11	Liouville's series of eighteen articles
II. 12	Pell equation ; $ax^2 + bx + c$ made a square
II. 13	Further single equations of the second degree
II. 14	Squares in arithmetical or geometrical progression
II. 15	Two or more linear functions made squares
II. 16	Two quadratic functions of one or two unknowns made squares
II. 17	Systems of two equations of degree two
II. 18	Three or more quadratic functions of one or two unknowns made squares
II. 19	Systems of three or more equations of degree two in three or more unknowns
II. 20	Quadratic form made an nth power
II. 21	Equations of degree three
II. 22	Equations of degree four
II. 23	Equations of degree n
II. 24	Sets of integers with equal sums of like powers
II. 25	Waring's problem and related results
II. 26	**Fermat's last theorem, $ax^r + by^s = cz^t$, and the congruence $x^n + y^n \equiv z^n \pmod p$**
TOME 3	
III. 1	Reduction and equivalence of binary quadratic forms, representation of integers
III. 2	Explicit values of x, y in $x^2 + \Delta y^2 = g$
III. 3	Composition of binary quadratic forms
III. 4	Orders and genera ; their composition
III. 5	Irregular determinants
III. 6	Number of classes of binary quadratic forms with integral coefficients
III. 7	Binary quadratic forms whose coefficients are complex integers or integers of a field
III. 8	Number of classes of binary quadratic forms with complex integral coefficients
III. 9	Ternary quadratic forms
III. 10	Quaternary quadratic forms
III. 11	Quadratic forms in n variables
III. 12	Binary cubic forms
III. 13	Cubic forms in three or more variables
III. 14	Forms of degree $n \geqq 4$
III. 15	Binary Hermitian forms
III. 16	Hermitian forms in n variables and their conjugates
III. 17	Bilinear forms, matrices, linear substitutions
III. 18	**Representation by polynomials modulo p**
III. 19	Congruencial theory of forms

2 - Ce qu'il n'y a pas dans Dickson

Voici la liste des textes inclus dans notre corpus, après analyse supplémentaire du *Catalogue of Scientific Papers* et des autres sources indiquées dans notre premier chapitre, ainsi que des périodiques listés dans le troisième chapitre, et qui ne sont pas référencés pour leurs utilisation des résidus et des congruences dans [Dickson, 1919-1923] et [Cooper, 1926] :

Mémoires liés à la théorie des résidus et des congruences de 1801 à 1850 non référencés dans [Dickson, 1919-1923] et [Cooper, 1926] du point de vue de la théorie des résidus et des congruences				
Date	**Auteur**	**Titre**	**Publication**	**Ref. publication**
1808	Lagrange, J. - L.	Traité de la résolution numérique des équations	éd. 3	
1808	Poinsot, L.	Commentaire sur le Traité de la résolution numérique des équations de Lagrange	Magasin encyclopédique	4, p. 342-374
1811	Gauss, C. F.	Summatio quarundam serierum singularium	Göttingen Comment.	I,
1828	Jacobi, C. G. J.	Beantwortung der Aufgabe S. 212 dises Band : - « Kann $a^{\mu-1}-1$, wenn μ eine Primzahl und a eine ganze Zahl und kleiner als μ und grösser als 1 ist, druch μ theilbar sein	Journal de Crelle	3, p. 301-302
1830	Lebesgue, V. A.	Note sur les résidus des puissances	Bull. Férussac	15, p. 158-159
1831	Germain, S.	Note sur la manière dont se décomposent les valeurs de y et z dans l'équation $\frac{4(x^p-1)}{x-1} = y^2 \pm pz^2$, et celles de Y' et Z' dans l'équation $\frac{4(x^{p^2}-1)}{x-1} = Y'^2 \pm pZ'^2$	Journal de Crelle	7, p. 201-204
1832	Legendre, A. M.	Mémoire sur la détermination des fonctions Y et Z qui satisfont à l'équation $4(Xn-1) = (X-1)(Y^2+nZ^2)$, n étant un nombre premier $(4i \mp 1)$	Mémoires Académie	11, p. 81-99
1832	Lejeune-Dirichlet, G.	Démonstration d'une propriété analogue à la loi de réciprocité qui existe entre deux nombres premiers quelconques	Journal de Crelle	9, p. 379-389
1834	Peacock, G.	Théory of equations	Report on the recent Progress and present State of certain Branches of Analysis.	p. 296 ? 322
1837	Lejeune-Dirichlet, G.	Sur l'usage des intégrales définies dans la sommation des séries finies ou infinies.	Journal de Crelle	17, p. 57-67
1838	Ostrogradsky, M.	Tables des racines primitives pour tous les nombres premiers audessous de 200, avec les tables pour trouver l'indice d'un nombre donné, et pour trouver le nombre d'après l'indice	Mém. Ac. Imp. Sc. St Petersbourg	s. 6, v. 1, p. 359-385
1839	Cauchy, L. A.	Sur la théorie des nombres et en particulier sur les formes quadratiques des nombres premiers	CRAS	9, p. 473-474

Mémoires liés à la théorie des résidus et des congruences de 1801 à 1850 non référencés dans [Dickson, 1919-1923] et [Cooper, 1926] du point de vue de la théorie des résidus et des congruences				
Date	**Auteur**	**Titre**	**Publication**	**Ref. publication**
1839	Cauchy, L. A.	Sur la théorie des nombres et en particulier sur les formes quadratiques des puissances d'un nombre premier, ou du quadruple de ces puissances	CRAS	9, p. 473, 519-526
1839	Cauchy, L. A. et Liouville, J.	Rapport sur le mémoire de M. Lamé relatif au dernier théorème de Fermat	CRAS	9, p. 359-363
1839	Jacobi, C. G. J.	Ueber die complexen Primzahlen, welche in der Theorie der Reste der 5ten, 8ten und 12ten Potenzen zu betrachten sind	Journal de Crelle	19, p. 314-318
1839	Jacobi, C. G. J.	Ueber die complexen Primzahlen, welche in der Theorie der Reste der 5ten, 8ten und 12ten Potenzen zu betrachten sind	Berlin, Bericht	p. 86-91
1839	Lejeune-Dirichlet, G.	Démonstration de cette proposition : toute progression arithmétique dont le premier terme et la raison sont des entiers sans diviseur commun, contient une infinité de nombres premiers	Journal de Liouville	4, p. 393-422
1840	Cauchy, L. A.	Sur la sommation de certaines puissances d'une racine primitive d'une équation binôme, et en particulier des puissances qui offrent pour exposants les résidus cubiques inférieurs au module donné	Journal de Liouville	5, p. 169-183
1840	Cauchy, L. A.	Suite des observations sur les formes quadratiques de certaines puissances des nombres premiers. Théorèmes relatifs aux exposants de ces puissances.	CRAS	10, p. 181-190
1840	Cauchy, L. A.	Discussion des formes quadratiques sous lesquelles se présentent certaines puissances des nombres premiers. Réduction des exposants de ces puissances.	CRAS	10, p. 229-243
1840	Cauchy, L. A.	Théorèmes relatifs aux formes quadratiques des nombres premiers et de leurs puissances	CRAS	10, p. 51-61
1840	Cauchy, L. A.	Méthode simple et nouvelle pour la détermination complète des sommes alternées, formées avec les racines primitives des équations binômes	CRAS	10, p. 560-572

Mémoires liés à la théorie des résidus et des congruences de 1801 à 1850 non référencés dans [Dickson, 1919-1923] et [Cooper, 1926] du point de vue de la théorie des résidus et des congruences				
Date	**Auteur**	**Titre**	**Publication**	**Ref. publication**
1840	Cauchy, L. A.	Sur la sommation de certaines puissances d'une racine primitive d'une équation binôme, et en particulier des puissances qui offrent pour exposants les résidus cubiques inférieurs au module donné	CRAS	10, p. 594-606
1840	Cauchy, L. A.	Observations nouvelles sur les formes quadratiques des nombres premiers et de leurs puissances	CRAS	10, p. 85-100
1840	Lebesgue, V. A.	Sommation de quelques séries	Journal de Liouville	5, p. 42-71
1842	Kummer, E. E.	Eine Aufgabe, betreffend die Theorie der cubischen Reste.	Journal de Crelle	23, p. 285-286
1843	Arndt, F.	Beweis eines arithmetischen Lehrsatzes	Archiv Math.	3, p. 210-213
1843	Jacobi, C. G. J.	Sur les nombres premiers complexes que l'on doit considérer dans la théorie des résidus de cinquième, huitième et douzième puissance	Journal de Liouville	8, p. 268-272
1843	Lamé, G.	Mémoire sur la démonstration d'un nouveau cas du dernier théorème de Fermat	Mémoire Académie Savants étrangers	8, p. 421-437
1844	Eisenstein, G.	Beitreige zur Kreistheilung	Journal de Crelle	27, p. 269-278
1844	Eisenstein, G.	Über die Anzahl der quadratischen Formen in den verschiedenen complexen Theorieen	Journal de Crelle	27, p. 311-316
1844	Eisenstein, G.	Neuer und elementarer Beweis des Legendre'schen Reciprocitätssatze	Journal de Crelle	27, p. 322-329
1844	Eisenstein, G.	Einfacher Beweis und Verallgemeinerung des Fundamentaltheorems für die biquadratischen Reste	Journal de Crelle	28, p. 223-248
1844	Eisenstein, G.	Geometrischer Beweis und Verallgemeinerung des Fundamentaltheorems für die quadratischen Reste	Journal de Crelle	28, p. 246-248
1844	Eisenstein, G.	Nachtrag zum cubischen Reciprocitätssatze für die aus dritten Wurzeln der Einheit zusammengesetzen complexen Zahlen. Criterien des cubischen Characters der Zahl Drei und ihere Theiler	Journal de Crelle	28, p. 28-35

Mémoires liés à la théorie des résidus et des congruences de 1801 à 1850 non référencés dans [Dickson, 1919-1923] et [Cooper, 1926] du point de vue de la théorie des résidus et des congruences				
Date	**Auteur**	**Titre**	**Publication**	**Ref. publication**
1844	Eisenstein, G.	La loi de réciprocité tirée des formules de Mr. Gauss, sans avoir déterminé préalablement le signe du radical	Journal de Crelle	28, p. 41-43
1844	Eisenstein, G.	Lois de réciprocité	Journal de Crelle	28, p. 53-67
1844	Kummer, E. E.	De numeris complexis, qui radicibus unitatis et numeris integris realibus constant	Academiae Albertinae Regiomontanae secularia tertia celebranti gratulatur Academia Vratislaviensis	p. 1-28
1844	Lebesgue, V. A.	Formule pour la résolution de l'équation auxiliaire de degré m relative à l'équation $x^p = 1$, en supposant $p = m\pi + 1$ et premier	CRAS	18, p. 696-699
1844	Lejeune-Dirichlet, G.	Recherches sur la théorie des nombres complexes	Journal de Liouville	9, p. 245-269
1845	Arndt, F.	Disquisitiones de congruentiis omnium graduum et residuis ordinis cujuscunque	Archiv Math.	6, p. 380-399
1845	Cauchy, L. A.	Note sur quelques propositions relatives à la théorie des nombres	Ex. Analyse	29e livraison (9/12/1845)
1845	Drot	Note sur les chiffres qui peuvent terminer les puissances quelconques des nombres entiers	Nouv. Ann. Math.	4, p. 637-644
1845	Eisenstein, G.	Applications de l'algèbre à l'arithmétique transcendante	Journal de Crelle	29, p. 177-184
1845	Kronecker, G.	Beweis dass für jede Primzahl p die Gleichung $1+x+x^2+\ldots+x^{p-1} = 0$ irreductibel ist	Journal de Crelle	29, p. 280
1845	Midy, E.	Analyse indéterminée du premier degré	Nouv. Ann. Math.	4, p. 146-152
1846	Arndt, C. F.	Bermerkungen über die Verwandlung der irrationalen Quadratwurzeln in einen Kettenbruch	Journal de Crelle	31, p. 343-358
1846	Arndt, F.	Demonstratio duorum theorematum Gaussianis his generaliorum...	Journal de Crelle	31, p. 326-328
1846	Arndt, F.	Disquisitiones de residuis cujusvis ordinis	Journal de Crelle	31, p. 333-342

Mémoires liés à la théorie des résidus et des congruences de 1801 à 1850 non référencés dans [Dickson, 1919-1923] et [Cooper, 1926] du point de vue de la théorie des résidus et des congruences				
Date	**Auteur**	**Titre**	**Publication**	**Ref. publication**
1846	Eisenstein, G.	Beiträge zur Theorie der elliptischen Functionen. I. Ableitung des biquadratischen Fundamentaltheorems aus der Theorie der Lemniscatenfunctionen, nebst Bemerkungen zu den Multiplications- und Transformationsfor	Journal de Crelle	30, p. 185-210
1846	Jacobi, C. G. J.	Mittheilung über die Kreistheilung und ihre Anwendung auf die Zahlentheorie	Journal de Crelle	30, p. 166-182
1846	Kummer, E. E.	Ueber die Divisoren gewisser Formen der Zahlen, welche aus der Theorie der Kreistheilung, entstehen	Journal de Crelle	30, p. 107-116
1846	Kummer, E. E.	De residuis cubicis disquisitiones non-nullae analyticae	Journal de Crelle	32, p. 341-359
1846	Kummer, E. E.	Vervollständigung der Theorie der complexen Zahlen	Berlin, Bericht	p. 87-96
1847	Cauchy, L. A.	Mémoire sur la théorie des équivalences algébriques substituées à la théorie des imaginaires	Ex. Analyse	IV, p. 87 ? 110
1847	Cauchy, L. A.	Sur la décomposition d'un nombre entier en facteurs radicaux	CRAS	24, p. 1022-1030
1847	Cauchy, L. A.	Mémoire sur une nouvelle théorie des imaginaires, et sur les racines symboliques des équations et des équivalences		24, p. 1120-1130
1847	Cauchy, L. A.	Mémoire sur les racines des équations algébriques à coefficients entiers, et sur les polynômes radicaux	CRAS	24, p. 407-414
1847	Cauchy, L. A.	Mémoire sur de nouvelles formules relatives à la théorie des polynômes radicaux, et sur le dernier théorème de Fermat	CRAS	24, p. 469-481, 516-528, 578-584, 633-636, 661-666
1847	Cauchy, L. A.	Mémoire sur l'application de la nouvelle théorie des imaginaires aux diverses branches des sciences mathématiques	CRAS	25, p. 129-132
1847	Cauchy, L. A.	Mémoire sur diverses propositions relatives à la théorie des nombres	CRAS	25, p. 132-136, 177-182, 242-243
1847	Cauchy, L. A.	Mémoire sur la disposition des nombres entiers en facteurs radicaux	CRAS	25, p. 46-54

Mémoires liés à la théorie des résidus et des congruences de 1801 à 1850 non référencés dans [Dickson, 1919-1923] et [Cooper, 1926] du point de vue de la théorie des résidus et des congruences				
Date	**Auteur**	**Titre**	**Publication**	**Ref. publication**
1847	Cauchy, L. A.	Mémoire sur les indices modulaires des polynômes radicaux que fournissent les puissances et produits des racines de la résolvante d'une équation binôme	CRAS	25, p. 93-99
1847	Eisenstein, G.	Neue Theoreme der höheren Arithmetik	Journal de Crelle	35, p. 117-136
1847	Eisenstein, G.	Note sur la représentation d'un nombre par la somme de cinq carrés	Journal de Crelle	35, p. 368-369
1847	Kummer, E. E.	Sur les nombres complexes qui sont formés avec les nombres entiers réels et les racines de l'unité	Journal de Liouville	12, p. 185-212
1847	Kummer, E. E.	Zur Theorie der complexen Zahlen	Journal de Crelle	35, p. 319-326
1847	Kummer, E. E.	Ueber die Zerlegung der aus Wurzeln der Einheit gebildeten complexen Zahlen in ihre Primfactoren	Journal de Crelle	35, p. 327-367
1847	Lamé, G.	Mémoire sur la résolution, en nombres complexes, de l'équation $A^5 + B^5 + C^5 = 0$	Journal de Liouville	12, p. 137-171
1847	Lebesgue, V. A.	Démonstration nouvelle et élémentaire de la loi de réciprocité de Legendre, par M. Eisenstein, précédée et suivie de remarques sur d'autres démonstrations qui peuvent être tirées du même principe	Journal de Liouville	12, p. 457-473
1847	Lebesgue, V. A.	Sur le symbole $\left(\frac{a}{b}\right)$ et quelques-unes de ses applications	Journal de Liouville	12, p. 497-517
1847	Liouville, J.	Sur la loi de réciprocité dans la théorie des résidus quadratiques	Journal de Liouville	12, p. 95-96
1847	Liouville, J.	Sur la loi de réciprocité dans la théorie des résidus quadratiques	CRAS	24, p. 577-578
1847	Schaar, M.	Nouvelles démonstrations de la loi de réciprocité pour les résidus quadratiques	Bull. Ac. Belgique	14, p. 79-83
1848	Terquem, O.	Théorème arithmologique de M. Steiner, démontré par M. Jacobi	Nouv. Ann. Math.	7, p. 268-269
1849	Binet, J. P. M.	Théorie des nombres	CRAS	28, p. 686-687
1849	Serret, J. A.	Cours d'algèbre supérieure	Édition 1	

Mémoires liés à la théorie des résidus et des congruences de 1801 à 1850 non référencés dans [Dickson, 1919-1923] et [Cooper, 1926] du point de vue de la théorie des résidus et des congruences				
Date	**Auteur**	**Titre**	**Publication**	**Ref. publication**
1849	Terquem, O.	Nouvelle démonstration de l'irréductibilité de l'équation $1 + x + x^2 + \ldots + x^{p-1} = 0$; p étant un nombre premier. D'après M. L. Kronecker, étudiant à Berlin	Nouv. Ann. Math.	8, p. 419-421
1850	Eisenstein, G.	Lehrsätze ? Über irreductible Congruenzen	Journal de Crelle	39, p. 182
1850	Eisenstein, G.	Ueber ein einfaches Mittel zur Auffindung der höheren Reciprocitätsgesetze und der mit ihnen zu verbindenden Ergänzungssätze	Journal de Crelle	39, p. 351-364
1850	Eisenstein, G.	Beweis der allgemeinsten Reciprocitätsgesetze zwischen und complexen Zahlen	Berlin, Bericht	p. 189-198
1850	Kummer, E. E.	Zwei besondere Untersuchungen über die Classen-Anzahl und über die Einheiten der aus λ^{ten} Wurzeln der Einheit gebildeten complexen Zahlen	Journal de Crelle	40, p. 117-129
1850	Kummer, E. E.	Bestimmung der Anzahl nicht äquivalenter Classen für die aus λ^{ten} Wurzeln der Einheit gebildeten complexen Zahlen und die idealen Factorenderselben	Journal de Crelle	40, p. 93-116
1850	Kummer, E. E.	Allgemeine Reciprocitätsgesetze für beliebig hohe Potenzreste	Berlin, Bericht	p. 154-165
1850	Lejeune-Dirichlet, G.	Ueber die Zerlegbarkeit der Zahlen in drei Quadrate	Journal de Crelle	40, p. 228-232
1850	Prouhet, E.	Irréductibilité de l'équation $X = 1 + x + \ldots + x^{p-1} = 0$, p étant un nombre entier	Nouv. Ann. Math.	9, p. 348-349

II Contenu du corpus : des bilans par auteur

Les tableaux ci-dessous ont été construits à partir de la liste des publications donnée dans la section suivante.

1 - Nombre de textes publiés par auteur

Les textes publiés n fois ont été comptés n fois.

Nombre d'articles par auteur et par période						
Auteur	**TOTAL**	**1801-1810**	**1811-1820**	**1821-1830**	**1831-1840**	**1841-1850**
Cauchy, A. - L.	34	0	1	4	14	15
Lejeune-Dirichlet, G.	20	0	0	5	10	5
Eisenstein, G.	19	0	0	0	0	19
Kummer, E. E.	13	0	0	0	0	13
Lebesgue, V. - A.	13	0	0	2	5	6
Arndt, C. F.	11	0	0	0	0	11
Jacobi, C. G. J.	10	0	0	2	6	2
Stern, M.	8	0	0	1	5	2
Crelle, A. L.	6	0	0	0	4	2
Gauss, C. F.	6	2	2	1	1	0
Poinsot, L.	6	1	2	1	0	2
Bouniakowsky, V.	5	0	0	0	2	3
Libri, G.	5	0	1	2	2	0
Schönemann, T.	5	0	0	0	2	3
Terquem, O.	5	0	0	0	0	5
Binet, J. P. M.	4	0	0	0	1	3
Prouhet, E.	4	0	0	0	0	4
Liouville, J.	3	0	0	0	1	2
Schaar, M.	3	0	0	0	0	3
Galois, E.	2	0	0	1	0	1
Grunert, J. A.	2	0	0	0	1	1
Ivory, J.	2	1	0	1	0	0
Lamé, G.	2	0	0	0	0	2
Ostrogradsky, M.	2	0	0	0	2	0
Serret, J. - A.	2	0	0	0	0	2
Barlow, P.	1	0	1	0	0	0
Catalan, E.	1	0	0	0	0	1
Collins, E.	1	0	0	1	0	0
Erlerus, H. G.	1	0	0	0	0	1
Horner, W. G.	1	0	0	1	0	0
Lacroix, S. F.	1	1	0	0	0	0
Lagrange, J. - L.	1	1	0	0	0	0
Minding, F.	1	0	0	0	1	0
Murphy, R.	1	0	0	0	0	1
Peacock, G.	1	0	0	0	1	0
Richelot, F. J.	1	0	0	0	1	0
Staudt, C.	1	0	0	0	1	0
Verhulst, P. F.	1	0	0	1	0	0
Wronski, H.	1	0	0	0	0	1
Nombre d'auteurs	**39**	**5**	**5**	**13**	**18**	**25**
Nombre d'articles	**206**	**6**	**7**	**23**	**60**	**110**

2 - Nombre de textes publiés entre 1801 et 1850 dans lesquels chacun des savants de notre corpus sont cités

Les savants non indiqués dans ce tableau ne sont pas cités dans les textes de notre corpus.

Périodes	**TOTAL**	**1801-1810**	**1811-1820**	**1821-1830**	**1831-1840**	**1841-1850**
Gauss	128	4	3	17	38	66
Legendre	74	4	4	8	21	37
Euler	53	6	3	11	12	21
Jacobi	44	0	0	4	16	24
Dirichlet	41	0	0	3	10	28
Lagrange	37	4	4	7	12	10
Libri	20	0	0	4	10	6
Poinsot	20	0	0	5	7	8
Cauchy	16	0	0	2	6	8
Kummer	8	0	0	0	0	8
Stern	6	0	0	0	1	5
Vandermonde	6	2	2	2	0	0
Abel	5	0	0	2	1	2
Eisenstein	5	0	0	0	0	5
Kronecker	5	0	0	0	0	5
Lebesgue	5	0	0	0	4	1
Waring	4	2	1	1	0	0
Binet	3	0	0	1	0	2
Clausen	3	0	0	0	2	1
Lamé	3	0	0	0	1	2
Zornov	3	0	0	0	2	1
Fourier	2	0	0	1	1	0
Ivory	2	0	0	1	1	0
Lambert	2	1	0	0	0	1
Liouville	2	0	0	0	1	1
Rosenhain	2	0	0	0	1	1
Germain	1	0	0	1	0	0
Grunert	1	0	0	0	0	1
Hermite	1	0	0	0	0	1
Hirsch	1	0	0	0	1	0
Krafft	1	0	0	0	0	1
Kunze	1	0	0	0	0	1
Laplace	1	0	0	0	1	0
Pessuti	1	0	0	0	0	1
Poisson	1	0	0	0	1	0
Seeber	1	0	0	0	0	1
Sturm	1	0	0	0	0	1
Wantzel	1	0	0	0	0	1

3 - Références données par les principaux auteurs de notre corpus

Références données par les principaux auteurs de notre corpus														
Auteurs	***Cauchy***	**Eisenstein**	**Jacobi**	**Kummer**	**Lamé**	**Lebesgue**	**Dirichlet**	**Libri**	**Poinsot**	**Binet**	**Prouhet**	**Terquem**	**Stern**	**Schönemann**
	cite	*cite*	*cite*	*cite*	*cite*	*cite*	*cite*	*cite*	*cite*	*cite*	*cite*	*cite*	*cite*	*cite*
Gauss	15	12	7	7	1	10	16	16	6	0	1	3	4	2
Legendre	7	2	3	3	1	8	9	9	4	1	2	2	1	1
Jacobi	11	6	0	5	1	9	4	4	0	0	0	0	2	0
Dirichlet	5	7	3	9	2	6	0	0	0	0	0	1	1	1
Euler	5	0	0	0	0	0	6	6	5	1	2	3	0	0
Lagrange	3	0	0	1	0	1	7	7	5	1	0	2	0	1
Libri	8	0	0	0	0	4	0	1	0	1	0	0	2	0
Cauchy	0	1	0	0	0	7	1	1	0	1	0	1	1	0
Poinsot	8	0	0	0	0	3	0	0	0	0	0	0	0	0
Kummer	5	2	0	0	0	0	0	0	0	0	0	0	0	0
Kronecker	0	0	0	4	0	0	0	0	0	0	0	1	0	0
Lebesgue	3	0	0	1	0	0	0	0	0	0	0	0	1	0
Stern	2	1	0	1	0	1	0	0	0	0	0	0	0	0
Eisenstein	0	0	0	1	0	2	0	0	0	0	0	0	0	1
Vandermonde	0	0	0	0	0	0	0	0	4	0	0	0	0	0
Binet	3	0	0	0	0	0	0	0	0	0	0	0	0	0
Clausen	0	0	0	1	0	0	0	0	0	0	0	0	1	0
Lamé	2	0	0	0	0	0	0	0	0	0	0	0	0	0
Liouville	2	0	0	0	0	0	0	0	0	0	0	0	0	0
Rosenhain	0	0	2	0	0	0	0	0	0	0	0	0	0	0
Abel	0	1	0	0	0	0	0	0	0	0	0	0	0	0
Fourier	1	0	0	0	0	0	0	0	0	0	0	0	0	0
Hirsch	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Krafft	0	0	0	0	0	0	0	0	0	0	0	1	0	0
Poisson	1	0	0	0	0	0	0	0	0	0	0	0	0	0
Seeber	0	1	0	0	0	0	0	0	0	0	0	0	0	0
Sturm	0	0	0	0	0	0	0	0	0	1	0	0	0	0
Wantzel	0	0	0	0	0	0	0	0	0	0	0	1	0	0

III La théorie des résidus et des congruences dans les publications de 1801 à 1850

La liste ci-dessous correspond à la liste de textes recensés à l'aide de la méthode indiquée dans l'introduction et décrite dans le chapitre 1.

Mémoires liés à la théorie des résidus et des congruences de 1801 à 1850							
Date	**Auteur**	**Titre**	**Publication**	**Ref. publication**	**Références données**	**Remarques**	**Nb pages**
1801	Gauss, C. F.	Disquisitiones Arithmeticae			Euler, Lagrange, Lambert, Legendre, Waring		
1804	Lacroix, S. F.	Compléments d'algèbre			Legendre, Gauss		
1806	Ivory, J.	Demonstration of a Theorem respecting Prime Numbers	New series of the mathematical repository	1, part. 2, p. 6-8	Euler, Legendre		3
1808	Gauss, C. F.	Theorematis arithmetici demonstratio nova	Göttingen Comment.	16, p. 69-74	Legendre, Euler, Lagrange		6
1808	Lagrange, J. - L.	Traité de la résolution numérique des équations	éd. 3		Euler, Gauss, Vandermonde	Note 14	
1808	Legendre, A. M.	Essai sur la théorie des nombres		2ème édition	Lagrange, Waring, Euler, Gauss		
1808	Poinsot, L.	Commentaire sur le Traité de la résolution numérique des équations de Lagrange	Magasin encyclopédique	4, p. 342-374	Vandermonde, Lagrange, Gauss, Euler		
1811	Barlow, P.	An elementary investigation of the Theory of Numbers			Waring, Lagrange, Legendre, Gauss, Euler		
1811	Gauss, C. F.	Summatio quarundam serierum singularium	Göttingen Comment.	1	X		
1813	Cauchy, L. A.	Recherches sur les nombres	J. E. P.		Lagrange, Legendre		24
1817	Poinsot, L.	Extrait de quelques recherches nouvelles sur l'algèbre et sur la théorie des nombres	Mémoires Académie	p. 381-392	Lagrange, Euler, Legendre, Gauss, Vandermonde		12

Mémoires liés à la théorie des résidus et des congruences de 1801 à 1850 (suite)							
Date	**Auteur**	**Titre**	**Publication**	**Ref. publication**	**Références données**	**Remarques**	**Nb pages**
1818	Gauss, C. F.	Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et ampliationes novae	Göttingen Comment.	4, p. 3-20	X		18
1820	Libri, G.	Memoria sopra la teoria die numeri		Florence	*Pas d'accès au texte*		
1820	Poinsot, L.	Mémoire sur l'application de l'algèbre à la théorie des nombres	J. E. P.	11, p. 342-410	Euler, Legendre, Vandermonde, Lagrange, Gauss		69
1822	Collins, E.	Theorematis arithmetici Demonstratio	Mém. Ac. Imp. Sc. St Petersbourg	8, p. 242-246	Gauss		5
1824	Ivory, J.	Addendum to Volume Fourth - Equations	Encyclopaediae Britannica (Supplement)	4, p. 698	Lagrange, Gauss, Legendre, Vandermonde, Euler		
1824	Poinsot, L.	Mémoire sur l'application de l'algèbre à la théorie des nombres	Mémoires Académie	p. 99-183	Euler, Legendre, Vandermonde, Lagrange, Gauss	Publié dans le JEP en 1820.	
1825	Cauchy, L. A. et Ampère, A. - M.	Analyse de la Théorie des nombres par G. Libri	Bull. Férussac	3, p. 77-81	Libri, Poinsot, Fourier,		5
1825	Legendre, A. M.	Recherche sur quelques objets d'analyse indéterminée et particulièrement sur le théorème de Fermat	Mémoires Académie	6, p. 1-60	Euler, Germain, Dirichlet		60
1826	Horner, W. G.	Extension of a Theorem of Fermat	Annals Phil.	11, p. 81-83 (new series)	Euler, Ivory		
1827	Jacobi, C. G. J.	De residuis cubiscis commentatio numerosa	Journal de Crelle	2, p. 66-69	Gauss		4
1827	Verhulst, P. F.	Théorème de Wilson. Démonstration de M. Verhulst	Corr. Math. Phys. Quetelet	3, p. 71-72	Euler, Gauss		2

Mémoires liés à la théorie des résidus et des congruences de 1801 à 1850 (suite)							
Date	**Auteur**	**Titre**	**Publication**	**Ref. publication**	**Références données**	**Remarques**	**Nb pages**
1828	Gauss, C. F.	Theoria residuorum biquadraticorum, Commentatio prima	Göttingen Comment.	6, p. 27-56	X	Lu en 1825	30
1828	Jacobi, C. G. J.	Beantwortung der Aufgabe S. 212 dises Band : - « Kann $a^{\mu-1}-1$, wenn μ eine Primzahl und a eine ganze Zahl und kleiner als μ und grösser als 1 ist, druch μ theilbar sein	Journal de Crelle	3, p. 301-302	X		2
1828	Dirichlet, G.	Recherches sur les diviseurs premiers d'une classe de formules du quatrième degré	Journal de Crelle	3, p. 35-69	Gauss, Legendre		35
1828	Dirichlet, G.	Mémoire sur l'impossibilité de quelques équations indéterminées du 5^e degré	Journal de Crelle	3, p. 354-375	Euler, Legendre		22
1828	Dirichlet, G.	Démonstrations nouvelles de quelques théorèmes relatifs aux nombres	Journal de Crelle	3, p. 390-393	Gauss, Euler		4
1828	Dirichlet, G.	Question d'analyse indéterminée	Journal de Crelle	3, p. 407-408	X		2
1828	Dirichlet, G.	De formis linearibus, in quibus continentur divisores primi quarumdam formularum graduum superiorum commentatio			Euler, Gauss, Lagrange		15
1829	Cauchy, L. A.	Mémoire sur la théorie des nombres	Bull. Férussac	12, p. 205-221	Gauss, Poinsot, Jacobi		20
1829	Lebesgue, V. A.	Extrait d'un Mémoire inédit sur les congruence d'un degré quelconque à une seule inconnue	Bulletin du Nord, Moscou	23-43, 255-274, 19-33	Gauss, Poinsot, Legendre, Jacobi, Dirichlet, Lagrange		56
1829	Cournot, A. - A.	Nouvelle démonstration des théorèmes de Fermat et de Wilson	Bull. Férussac	7, p. 354	Gauss, Legendre		1
1829	Libri, G.	Mémoire sur la théorie des nombres	Mémoire de Mathématique et de Physique	1, p. 47-140	Gauss, Euler, Lagrange, Legendre, Poinsot	Reproduit en 1832 dans le journal de Crelle	

Mémoires liés à la théorie des résidus et des congruences de 1801 à 1850 (suite)							
Date	**Auteur**	**Titre**	**Publication**	**Ref. publication**	**Références données**	**Remarques**	**Nb pages**
1829	Cauchy, L. A.	Sur diverses propositions relatives à l'algèbre et à la théorie des nombres	Ex. Math.	4, p.217-252	Euler, Lagrange, Gauss, Legendre, Libri, Poinsot, Binet		99
1829	Cauchy, L. A.	Sur la résolution des équivalences dont les modules se réduisent à des nombres premiers	Ex. Math.	4, p.253-292	Gauss, Libri		44
1830	Galois, Evariste	Sur la théorie des nombres	Bull. Férussac	13, p. 428-435	Gauss, Abel, Libri		8
1830	Lebesgue, V. A.	Note sur les résidus des puissances	Bull. Férussac	15, p. 158-159	Jacobi, Dirichlet		2
1830	Legendre, A. M.	Théorie des nombres		3ème édition	Gauss, Waring, Euler, Lagrange, Jacobi, Abel, Cauchy		
1830	Libri, G.	Sur les racines primitives des nombres premiers	Bull. Férussac	13, p. 272-273	Cauchy		2
1830	Stern, M.	Bemerkungen über höhere Arithmetik	Journal de Crelle	6, p. 147-158	Gauss		12
1831	Binet, J. P. M.	Mémoire sur la résolution des équations indéterminées du premier degré en nombres entiers	J. E. P.	13, p. 289-296	Legendre, Libri		8
1831	Bouniakowsky, V.	Sur les congruences du second degré	Mém. Ac. Imp. Sc. St Petersbourg	Série 6 ; tome 1, p. 563-582	Gauss, Lagrange, Euler		20
1831	Cauchy, L. A.	Sur la théorie des nombres	Bull. Férussac	15, p. 137-139	X		4
1831	Germain, S.	Note sur la manière dont se décomposent les valeurs de y et z dans l'équation $\frac{4(x^p-1)}{x-1} = y^2 \pm pz^2$, et celles de Y' et Z' dans l'équation $\frac{4(x^{p^2}-1)}{x-1} = Y'^2 \pm pZ'^2$	Journal de Crelle	7, p. 201-204	Legendre, Gauss		

Mémoires liés à la théorie des résidus et des congruences de 1801 à 1850 (suite)							
Date	**Auteur**	**Titre**	**Publication**	**Ref. publication**	**Références données**	**Remarques**	**Nb pages**
1831	Grunert, J. A.	Zahl	Klügel's Mathematische Wörterbuch	5 (2), p. 1-75	Gauss, Euler, Legendre, Lagrange, Cauchy, Jacobi, Dirichlett		
1831	Stern, M.	Aufgaben und Lehrsätze	Journal de Crelle	7, p. 104	Gauss		
1832	Clausen, T.	Auflösung einiger Aufgaben	Journal de Crelle	8, p. 140-141	Stern	Réponse à la question de Stern posée dans le tome 7	2
1832	Crelle, A. L.	Table des racines primitives, etc., pour les nombres premiers depuis 3, jusqu'à 101, précédée d'une note sur le calcul de cette table	Journal de Crelle	9, p. 27-51	Euler		25
1832	Crelle, A. L.	Von einigen Sätzen aus der Theorie der Zahlen	Berlin, Abhandl.	p. 33-68	Euler, Lagrange, Gauss, Legendre, Cauchy, Dirichlet		36
1832	Gauss, C. F.	Theoria residuorum biquadraticorum, Comentatio secunda	Göttingen Comment.	7, p. 89-148	X	1828-1832	60
1832	Jacobi, C. G. J.	Observatio arithmetica de numero classium divisorum quadraticorum formae $yy + Azz$ designante A numerum primum formae $4n + 3$	Journal de Crelle	9, p. 189-192	Legendre		4
1832	Legendre, A. M.	Mémoire sur la détermination des fonctions Y et Z qui satisfont à l'équation $4(Xn - 1) = (X-1)(Y^2+nZ^2)$, n étant un nombre premier $(4i \mp 1)$	Mémoires Académie	11, p. 81-99	X		19
1832	Dirichlet, G.	Démonstration d'une propriété analogue à la loi de réciprocité qui existe entre deux nombres premiers quelconques	Journal de Crelle	9, p. 379-389	Gauss		11

Mémoires liés à la théorie des résidus et des congruences de 1801 à 1850 (suite)							
Date	**Auteur**	**Titre**	**Publication**	**Ref. publication**	**Références données**	**Remarques**	**Nb pages**
1832	Libri, G.	Mémoire sur la théorie des nombres	Journal de Crelle	9, p. 54-80, p. 169-188, p. 261-294	Gauss, Euler, Lagrange, Legendre, Poinsot	Publié en 1829	81
1832	Minding, F.	Anfangsgründe der Höheren Arithmetik			Gauss, Euler, Legendre		
1832	Richelot, F. J.	De resolutione algebraica aequationis $X^{257} = 1$, sive de divisione circuli per bisectionem anguli septies repetitam in partes 257 inter se aequales commentatio coronata.	Journal de Crelle	9, p. 1-26, 146-161, 209-230	Gauss, Legendre		62
1832	Stern, M.	Bemerkungen zur höheren Arithmetik	Journal de Crelle	9, p. 97-98	Clausen, Gauss		2
1833	Cauchy, L. A.	Formules d'interpolation	Résumés Analytiques, Turin	p. 31-36	X		6
1833	Dirichlet, G.	Untersuchungen über die Theorie der quadratischen Formen	Berlin, Abhandl.	p. 101-121	Euler, Lagrange, Legendre, Gauss		21
1834	Dirichlet, G.	Einige neue Sätze über unbestimmte Gleichungen	Berlin, Abhandl.	p. 649-664	Lagrange, Legendre		16
1834	Peacock, G.	Theory of equations	Report on the recent Progress and present State of certain Branches of Analysis.	p. 296 - 322	Poinsot, Gauss, Ivory, Euler, Abel, Libri		
1834	Stern, M.	Démonstration de quelques théorèmes sur les nombres	Journal de Crelle	12, p. 288-291	Libri		4
1835	Jacobi, C. G. J.	Über den Steinerschen Satz von dem Primzahlen im 4ten Hefte des 13ten Bandes dieses Journals	Journal de Crelle	14, p. 64-65	X		

Mémoires liés à la théorie des résidus et des congruences de 1801 à 1850 (suite)							
Date	**Auteur**	**Titre**	**Publication**	**Ref. publication**	**Références données**	**Remarques**	**Nb pages**
1836	Crelle, A. L.	Einige Bermerkungen über unbestimmte Gleichungen vom ersten Grades zwischen zwei ganzen Zahlen	Berlin, Abhandl.	p. 1-53	X		53
1837	Jacobi, C. G. J.	Mittheilung über die Kreistheilung und ihre Anwendung auf die Zahlentheorie	Berlin, Bericht	p. 127-136	Gauss, Dirichlet, Legendre, Rosenhain	Reproduit en 1846 dans le *Journal de Crelle* et traduit en 1856 dans les *Nouvelle Annales.*	10
1837	Lebesgue, V. A.	Recherches sur les nombres	Journal de Liouville	2, p. 253-292	Libri, Cauchy, Gauss, Jacobi		40
1837	Lebesgue, V. A.	Note sur l'équation $x^p = 1$	CRAS	5, p. 722-723	Poinsot, Libri, Legendre		2
1837	Dirichlet, G.	Sur la manière de résoudre l'équation $t^2 - pu^2 = 1$ au moyen des fonctions circulaires	Journal de Crelle	17, p. 286-290	Lagrange, Gauss		5
1837	Dirichlet, G.	Sur l'usage des intégrales définies dans la sommation des séries finies ou infinies.	Journal de Crelle	17, p. 57-67	Gauss, Libri		11
1837	Dirichlet, G.	Über den Satz : dass jede arithmetische Progression, deren erstes Glied und Differenz keinen gemeinschaftlichen Factor haben, unendlich viel Primzahlen enthält	Berlin, Bericht	p. 108-110	X		3
1837	Ostrogradsky, M.	Leçons d'analyse algébrique et transcendante [en russe]			*Pas d'accès au texte*		
1838	Bouniakowsky, V.	Note sur une propriété des nombres premiers	Mém. Ac. Imp. Sc. St Petersbourg	4, p. 65-69	X		5

Mémoires liés à la théorie des résidus et des congruences de 1801 à 1850 (suite)							
Date	**Auteur**	**Titre**	**Publication**	**Ref. publication**	**Références données**	**Remarques**	**Nb pages**
1838	Lebesgue, V. A.	Recherches sur les nombres (suite)	Journal de Liouville	3, p. 113-144	Gauss, Poinsot, Libri, Legendre, Jacobi, Cauchy		32
1838	Dirichlet, G.	Sur l'usage des séries infinies dans la théorie des nombres	Journal de Crelle	18, p. 259-274	Legendre, Gauss, Lagrange, Jacobi, Cauchy		16
1838	Libri, G.	Mémoire sur la théorie des nombres	Mémoire Académie Savants étrangers	5, p. 1-75	Euler, Gauss, Laplace, Lagrange, Fourier, Poinsot	Présenté en 1823	75
1838	Ostrogradsky, M.	Tables des racines primitives pour tous les nombres premiers au-dessous de 200, avec les tables pour trouver l'indice d'un nombre donné, et pour trouver le nombre d'après l'indice	Mém. Ac. Imp. Sc. St Petersbourg	s. 6, v. 1, p. 359-385	X		27
1838	Stern, M.	Aufgaben und Lehrsätze	Journal de Crelle	18, p. 375-376	X		2
1839	Brennecke	Sur le théorème de Wilson	Journal de Crelle	19, p. 319-323	Gauss		5
1839	Cauchy, L. A.	Sur la théorie des nombres et en particulier sur les formes quadratiques des nombres premiers	CRAS	9, p. 473-474	Libri, Gauss, Jacobi	14 octobre 1839	3
1839	Cauchy, L. A.	Sur la théorie des nombres et en particulier sur les formes quadratiques des puissances d'un nombre premier, ou du quadruple de ces puissances	CRAS	9, p. 473, 519-526	Lagrange, Gauss, Poinsot	28 octobre 1839	8
1839	Cauchy, L. A. et Liouville, J.	Rapport sur le mémoire de M. Lamé relatif au dernier théorème de Fermat	CRAS	9, p. 359-363	Euler, Legendre, Dirichlet, Lamé		5
1839	Jacobi, C. G. J.	Ueber die complexen Primzahlen, welche in der Theorie der Reste der 5ten, 8ten und 12ten Potenzen zu betrachten sind	Journal de Crelle	19, p. 314-318	Gauss, Prof. Zornov		5

Mémoires liés à la théorie des résidus et des congruences de 1801 à 1850 (suite)							
Date	**Auteur**	**Titre**	**Publication**	**Ref. publication**	**Références données**	**Remarques**	**Nb pages**
1839	Jacobi, C. G. J.	Ueber die complexen Primzahlen, welche in der Theorie der Reste der 5ten, 8ten und 12ten Potenzen zu betrachten sind	Berlin, Bericht	p. 86-91	Gauss, Prof. Zornov		6
1839	Jacobi, C. G. J.	Canon Arithmeticus Sive Tabulae Quibus Exhibentur Pro Singulis Numeris Primis Vel Primorum Potestatibus Infra 1000 Numeri Ad Datos Indices Et Indices ad Datos Numeros pertinentes			Gauss , Dirichlet		248
1839	Lebesgue, V. A.	Recherches sur les nombres (suite)	Journal de Liouville	4, p. 9-59	Jacobi, Cauchy, Gauss, Dirichlet		51
1839	Dirichlet, G.	Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres	Journal de Crelle	19, p. 324-369 et 21, p. 1-12, 135-155	Euler, Gauss, Lagrange, Legendre, Jacobi		80
1839	Dirichlet, G.	Démonstration de cette proposition : toute progression arithmétique dont le premier terme et la raison sont des entiers sans diviseur commun, contient une infinité de nombres premiers	Journal de Liouville	4, p. 393-422	Legendre, Gauss	Traduit par Terquem	30
1839	Schönemann, T.	Theorie der symmetrischen Funtionen der Wurzeln einer Gleichung. Allgemeine Sätze über Congruenzen nebst einige, Anwendungen derselben.	Journal de Crelle	19, p. 231-243, 289-308	Legendre, Gauss, Hirsch		32
1839	Schönemann, T.	Ueber die Congruenz $x^2 + y^2 \equiv 1 \pmod{p}$	Journal de Crelle	19, p. 93-112	Lagrange		20

Mémoires liés à la théorie des résidus et des congruences de 1801 à 1850 (suite)							
Date	**Auteur**	**Titre**	**Publication**	**Ref. publication**	**Références données**	**Remarques**	**Nb pages**
1840	Cauchy, L. A.	Sur la sommation de certaines puissances d'une racine primitive d'une équation binôme, et en particulier des puissances qui offrent pour exposants les résidus cubiques inférieurs au module donné	Journal de Liouville	5, p. 169-183	Gauss, Jacobi, Libri, Lebesgue	CRAS : 13 avril 1840	15
1840	Cauchy, L. A.	Suite des observations sur les formes quadratiques de certaines puissances des nombres premiers. Théorèmes relatifs aux exposants de ces puissances.	CRAS	10, p. 181-190	X	3 février 1840	11
1840	Cauchy, L. A.	Discussion des formes quadratiques sous lesquelles se présentent certaines puissances des nombres premiers. Réduction des exposants de ces puissances.	CRAS	10, p. 229-243	Jacobi	10 février 1840	17
1840	Cauchy, L. A.	Théorèmes divers sur les résidus et les non-résidus quadratiques	CRAS	10, p. 437-452	Gauss, Liouville, Dirichlet	16 mars 1840	18
1840	Cauchy, L. A.	Théorèmes relatifs aux formes quadratiques des nombres premiers et de leurs puissances	CRAS	10, p. 51-61	Gauss, Jacobi	13 janvier 1840	12
1840	Cauchy, L. A.	Méthode simple et nouvelle pour la détermination complète des sommes alternées, formées avec les racines primitives des équations binômes	CRAS	10, p. 560-572	Gauss, Dirichlet, Lebesgue, Poisson	6 avril 1840	15
1840	Cauchy, L. A.	Sur la sommation de certaines puissances d'une racine primitive d'une équation binôme, et en particulier des puissances qui offrent pour exposants les résidus cubiques inférieurs au module donné	CRAS	10, p. 594-606	Gauss, Jacobi, Libri, Lebesgue	13 avril 1840	15

Mémoires liés à la théorie des résidus et des congruences de 1801 à 1850 (suite)							
Date	**Auteur**	**Titre**	**Publication**	**Ref. publication**	**Références données**	**Remarques**	**Nb pages**
1840	Cauchy, L. A.	Observations nouvelles sur les formes quadratiques des nombres premiers et de leurs puissances	CRAS	10, p. 85-100	Jacobi	20 janvier 1840	18
1840	Cauchy, L. A.	Mémoire sur la théorie des nombres	Mémoires Académie	18, p. 249-768	Gauss, Poinsot, Legendre, Euler, Dirichlet, Jacobi	31 mai 1830	446
1840	Crelle, A. L.	Démonstration élémentaire du théorème de Wilson généralisé	Journal de Crelle	20, p. 29-56	X		28
1840	Lebesgue, V. A.	Sommation de quelques séries	Journal de Liouville	5, p. 42-71	Gauss, Dirichlet, Jacobi, Legendre		30
1840	Dirichlet, G.	Recherches sur diverses applications de l'Analyse infinitésimale à la Théorie des Nombres.	Journal de Crelle	21, p. 1-12, 134-155	Gauss, Jacobi, Legendre		34
1840	Staudt, C.	Beweis eines Lehrsatzes, die Bernoullischen Zahlen betreffen.	Journal de Crelle	21, p. 372-374	Clausen, Gauss		3
1840	Stern, M.	Extrait d'une lettre adressée à M. Liouville	Journal de Liouville	5, p. 216-219	Lebesgue, Jacobi		4
1841	Binet, J. P. M.	Note sur une propriété des nombres premiers, et sur la détermination des nombres associés d'Euler	CRAS	13, p. 210-213	Euler, Wilson, Lagrange, Cauchy		4
1841	Binet, J. P. M.	Note sur une nouvelle méthode pour trouver le plus grand commun diviseur des nombres entiers, ou des polynomes algébriques, et sur l'application de cette méthode aux congruences du premier degré	CRAS	13, p. 349-353	Sturm		5
1841	Bouniakowsky, V.	Nouveaux théorèmes relatifs à la distinction des nombres premiers et à la décomposition des entiers en facteurs	Mém. Ac. Imp. Sc. St Petersbourg	4, p. 447-470	Euler		24

Mémoires liés à la théorie des résidus et des congruences de 1801 à 1850 (suite)							
Date	**Auteur**	**Titre**	**Publication**	**Ref. publication**	**Références données**	**Remarques**	**Nb pages**
1841	Cauchy, L. A.	Mémoire sur la résolution des équations indéterminées du premier degré en nombres entiers	Ex. Analyse	13e livraison	Libri, Binet, Poinsot, Legendre, Jacobi, Stern	Reproduction des CRAS du 10 mai 1841	39
1841	Cauchy, L. A.	Mémoire sur diverses formules relatives à l'algèbre et à la théorie des nombres	CRAS	12, p. 698-711, 813-846	Libri, Binet, Poinsot, Legendre, Jacobi, Stern	26 avril et 10 mai 1841	48
1841	Erlerus, H. G.	Elementa Doctrinae Numerorum			Lamé		
1841	Gorini, P.	Sui residui delle divisioni numeriche	Annali di Fisica, Milano	1, p. 235-257	Gauss, Euler, Legendre		23
1841	Dirichlet, G.	Untersuchungen über die Theorie der complexen Zahlen	Berlin, Abhandl.	p. 141-161	Gauss		21
1841	Dirichlet, G.	Untersuchungen über die Theorie der complexen Zahlen	Berlin, Bericht	p. 190-194	Euler, Lagrange, Legendre, Gauss		5
1841	Murphy, R.	Remark on primitives Radices	Phil. Mag.	19, p. 369	Jacobi		1
1841	Poinsot, L.	Réflexions sur les principes fondamentaux de la théorie des nombres	CRAS	12, p. 803-812	Gauss	Introduction du Mémoire publié en 1845 dans le *Journal de Liouville*	10
1841	Stern, M.	Recherches sur la théorie des résidus quadratiques	Bruxelles, Mém. Couronn.	15, p. 1-62	Gauss, Legendre, Dirichlet, Cauchy, Libri		62
1842	Arndt, C. F.	Von den kubischen Resten	Gym. Prog. Torgau	12, u. 28, s. 4	*Pas d'accès au texte*	Cité dans Dickson	
1842	Arndt, C. F.	De potestatum periodis, radicibus primitivis residuisque quadraticis	Archiv Math.	2, p. 1-41	Gauss, Euler		41
1842	Catalan, E.	Sur les fractions décimales périodiques	Nouv. Ann. Math.	1, p. 457-470	X		13

Mémoires liés à la théorie des résidus et des congruences de 1801 à 1850 (suite)							
Date	**Auteur**	**Titre**	**Publication**	**Ref. publication**	**Références données**	**Remarques**	**Nb pages**
1842	Kummer, E. E.	Eine Aufgabe, betreffend die Theorie der cubischen Reste.	Journal de Crelle	23, p. 285-286	Gauss		2
1842	Lebesgue, V. A.	Démonstration de quelques théorèmes relatifs aux résidus et aux non-résidus quadratiques	Journal de Liouville	7, p. 137-159	Gauss, Jacobi, Libri, Dirichlet, Stern, Legendre, Cauchy		23
1842	Dirichlet, G.	Recherches sur les formes quadratiques à coefficients et à indéterminées complexes	Journal de Crelle	24, p. 291-371	Euler, Lagrange, Legendre, Gauss		81
1843	Arndt, F.	Beweis eines arithmetischen Lehrsatzes	Archiv Math.	3, p. 210-213	Gauss, Kunze, Pessuti		4
1843	Crelle, A. L.	Einige Bermerkungen über die Anwendung der Polynome in der Theorie der Zahlen	Berlin, Abhandl.	49-87	X		39
1843	Jacobi, C. G. J.	Sur les nombres premiers complexes que l'on doit considérer dans la théorie des résidus de cinquième, huitième et douzième puissance	Journal de Liouville	8, p. 268-272	Gauss, Prof. Zornov	Publié pour la première fois en 1839.	5
1843	Lamé, G.	Mémoire sur la démonstration d'un nouveau cas du dernier théorème de Fermat	Mémoire Académie Savants étrangers	8, p. 421-437	Dirichlet, Legendre	Présenté en 1839	17
1843	Terquem, O.	Théorème de Wilson d'après M. Gauss	Nouv. Ann. Math.	2, p. 193-195	Euler, Gauss, Lagrange, Verhulst		3
1844	Bouniakowsky, V.	Note sur l'emploi du binôme factoriel pour la résolution des congruences du premier degré	Mém. Ac. Imp. Sc. St Petersbourg	5, p. 287-296	X		10
1844	Crelle, A. L.	Encyklopädische und elementare Darstellung der Theorie der Zahlen	Journal de Crelle	27, p. 6-74, 107-181, 330-378 ; 28, p. 111-178 ; 29, p. 58-96, 103-176	Euler, Lagrange, Gauss, Legendre, Jacobi, Dirichlet		374
1844	Eisenstein, G.	Beitreige zur Kreistheilung	Journal de Crelle	27, p. 269-278	Gauss, Dirichlet		10

Mémoires liés à la théorie des résidus et des congruences de 1801 à 1850 (suite)							
Date	**Auteur**	**Titre**	**Publication**	**Ref. publication**	**Références données**	**Remarques**	**Nb pages**
1844	Eisenstein, G.	Aufgaben und Lehrsätze	Journal de Crelle	27, p. 281	X		1
1844	Eisenstein, G.	Beweis des Reciprocitätssatzes für die Cubischen Reste in der Theorie der aus dritten Wurzeln Der Einheit zusammengesetzen complexen Zahlen	Journal de Crelle	27, p. 289-310	Gauss, Jacobi, Dirichlet		22
1844	Eisenstein, G.	Über die Anzahl der quadratischen Formen in den verschiedenen complexen Theorieen	Journal de Crelle	27, p. 311-316	Dirichlet, Gauss, Jacobi		2
1844	Eisenstein, G.	Einfacher Algorithmuis zur Bestimmung des Werthes von $\left(\frac{a}{b}\right)$	Journal de Crelle	27, p. 317-318	X		2
1844	Eisenstein, G.	Neuer und elementarer Beweis des Legendre'schen Reciprocitätssatze	Journal de Crelle	27, p. 322-329	Gauss		8
1844	Eisenstein, G.	Einfacher Beweis und Verallgemeinerung des Fundamentaltheorems für die biquadratischen Reste	Journal de Crelle	28, p. 223-248	Gauss		26
1844	Eisenstein, G.	Geometrischer Beweis und Verallgemeinerung des Fundamentaltheorems für die quadratischen Reste	Journal de Crelle	28, p. 246-248	X		3
1844	Eisenstein, G.	Nachtrag zum cubischen Reciprocitätssatze für die aus dritten Wurzeln der Einheit zusammengesetzen complexen Zahlen. Criterien des cubischen Characters der Zahl Drei und ihere Theiler	Journal de Crelle	28, p. 28-35	X		8
1844	Eisenstein, G.	La loi de réciprocité tirée des formules de Mr. Gauss, sans avoir déterminé préalablement le signe du radical	Journal de Crelle	28, p. 41-43	Gauss , Dirichlet		3
1844	Eisenstein, G.	Lois de réciprocité	Journal de Crelle	28, p. 53-67	Gauss, Dirichlet, Legendre		15

Mémoires liés à la théorie des résidus et des congruences de 1801 à 1850 (suite)							
Date	**Auteur**	**Titre**	**Publication**	**Ref. publication**	**Références données**	**Remarques**	**Nb pages**
1844	Kummer, E. E.	De numeris complexis, qui radicibus unitatis et numeris integris realibus constant	Academiae Albertinae Regiomontanae secularia tertia celebranti gratulatur Academia Vratislaviensis	p. 1-28	Gauss, Jacobi, Dirichlet, Kronecker, Lagrange	Reproduit dans le Journal de Liouville en 1847 (vol. 12, p. 185-212)	28
1844	Lebesgue, V. A.	Formule pour la résolution de l'équation auxiliaire de degré m relative à l'équation $x^p = 1$, en supposant $p = m\pi + 1$ et premier	CRAS	18, p. 696-699	Gauss, Legendre		4
1844	Dirichlet, G.	Recherches sur la théorie des nombres complexes	Journal de Liouville	9, p. 245-269	Gauss	Lu en 1841 à l'Ac. De Berlin, tradutcion de Faye	25
1844	Terquem, O.	Théorie élémentaire des nombres, d'après Euler, Legendre, MM. Gauss et Cauchy	Nouv. Ann. Math.	3, p. 204-208, 214-219, 337-344	Euler, Lagrange, Gauss, Legendre, Wantzel, Krafft, Cauchy		18
1845	Arndt, F.	Disquisitiones de congruentiis omnium graduum et residuis ordinis cujuscunque	Archiv Math.	6, p. 380-399	Gauss		20
1845	Cauchy, L. A.	Note sur quelques propositions relatives à la théorie des nombres	Ex. Analyse	29e livraison (9/12/1845)	Euler, Poinsot, Gauss		7
1845	Drot	Note sur les chiffres qui peuvent terminer les puissances quelconques des nombres entiers	Nouv. Ann. Math.	4, p. 637-644	Gauss		8
1845	Eisenstein, G.	Applications de l'algèbre à l'arithmétique transcendante	Journal de Crelle	29, p. 177-184	Abel, Jacobi, Gauss		8
1845	Kronecker, G.	Beweis dass für jede Primzahl p die Gleichung $1 + x + x^2 + \ldots + x^{p-1} = 0$ irreductibel ist	Journal de Crelle	29, p. 280	Gauss, Kummer		1

Mémoires liés à la théorie des résidus et des congruences de 1801 à 1850 (suite)							
Date	**Auteur**	**Titre**	**Publication**	**Ref. publication**	**Références données**	**Remarques**	**Nb pages**
1845	Midy, E.	Analyse indéterminée du premier degré	Nouv. Ann. Math.	4, p. 146-152	Gauss		7
1845	Poinsot, L.	Réflexions sur les principes fondamentaux de la théorie des nombres	Journal de Liouville	10, p. 1-101	Euler, Lagrange, Gauss, Legendre		101
1845	Prouhet, E.	Note sur les nombres associés ; généralisation du théorème de Wilson	Nouv. Ann. Math.	4, p. 273-278	Legendre		6
1845	Prouhet, E.	Note sur le nombre qui indique combien il y a d'entiers inférieurs et premiers à un nombre donné	Nouv. Ann. Math.	4, p. 75-81	Euler, Gauss		7
1845	Prouhet, E.	Mémoire sur la théorie des résidus dans les progressions géométriques	Nouv. Ann. Math.	5, p. 175-187	Euler, Poinsot, Legendre		13
1845	Terquem, O.	Généralisation de la théorie des nombres associés et théorèmes y relatifs. D'après M. Dirichlet	Nouv. Ann. Math.	4, p. 379-382	Dirichlet, Euler, Catalan		4
1846	Arndt, C. F.	Nova solutio problematis determinandi multitudinem numerorum, qui ad numerum aliquem sint primi eoque minores	Journal de Crelle	31, p. 246-248	Gauss, Euler, Grunert,		3
1846	Arndt, C. F.	Bermerkungen über die Verwandlung der irrationalen Quadratwurzeln in einen Kettenbruch	Journal de Crelle	31, p. 343-358	Legendre		16
1846	Arndt, C. F.	Mbermerkungen über die Verwandlung der irrationalen Quadratwurzel in einen Kettenbruch	Journal de Crelle	31, p. 343-358	Legendre		16
1846	Arndt, F.	Nova methodus determinandi multitudinem radicuum congruentiae $x^t \equiv 1 \pmod{M}$ aliaque ad hanc materiam spectautis	Journal de Crelle	31, p. 259-268	Gauss, Jacobi		10
1846	Arndt, F.	Demonstratio duorum theorematum Gaussianis his generaliorum...	Journal de Crelle	31, p. 326-328	X		3

Mémoires liés à la théorie des résidus et des congruences de 1801 à 1850 (suite)							
Date	**Auteur**	**Titre**	**Publication**	**Ref. publication**	**Références données**	**Remarques**	**Nb pages**
1846	Arndt, F.	Demonstratio nova theorematis Wilsoniani a summo Gauss hoc modo generalius enunciati...	Journal de Crelle	31, p. 329-332	Gauss		4
1846	Arndt, F.	Disquisitiones de residuis cujusvis ordinis	Journal de Crelle	31, p. 333-342	Gauss, Legendre		10
1846	Eisenstein, G.	Beiträge zur Theorie der elliptischen Functionen. I. Ableitung des biquadratischen Fundamentaltheorems aus der Theorie der Lemniscatenfunctionen, nebst Bemerkungen zu den Multiplications- und Transformationsfor	Journal de Crelle	30, p. 185-210	Gauss, Jacobi, Legendre		26
1846	Galois, Evariste	Sur la théorie des nombres	Journal de Liouville	11, p. 398-407	Gauss, Abel, Libri	Publié en 1829 dans le Bulletin de Férussac	10
1846	Grunert, J. A.	ueber zwei Sätze aus der Algebra und aus der Zahlenlehre	Archiv Math.	7, p. 367-386	Gauss, Lagrange, Legendre, Euler, Poinsot		20
1846	Jacobi, C. G. J.	Mittheilung über die Kreistheilung und ihre Anwendung auf die Zahlentheorie	Journal de Crelle	30, p. 166-182	Gauss, Dirichlet, Legendre, Rosenhain	Publié en 1837 pour la première fois. Rosenhain est un des auditeurs de Jacobi	15
1846	Kummer, E. E.	Ueber die Divisoren gewisser Formen der Zahlen, welche aus der Theorie der Kreistheilung, entstehen	Journal de Crelle	30, p. 107-116	X		10
1846	Kummer, E. E.	De residuis cubicis disquisitiones non-nullae analyticae	Journal de Crelle	32, p. 341-359	Gauss, Jacobi, Dirichlet, Clausen, Lebesgue, Stern, Legendre		19

Mémoires liés à la théorie des résidus et des congruences de 1801 à 1850 (suite)							
Date	**Auteur**	**Titre**	**Publication**	**Ref. publication**	**Références données**	**Remarques**	**Nb pages**
1846	Kummer, E. E.	Vervollständigung der Theorie der complexen Zahlen	Berlin, Bericht	p. 87-96	Dirichlet, Legendre, Kronecker, Gauss	Reproduit dans le Journal de Crelle en 1847 (vol. 35, p. 319-326)	10
1846	Schönemann, T.	Grundzüge einer allgemeinen Theorie der höhern Congruenzen, derne Modul eine relle Primzahl ist	Journal de Crelle	31, p. 269-325	Gauss, Dirichlet		57
1846	Schönemann, T.	Von denjenigen Moduln, welche Potenzen von Primzahlen sind	Journal de Crelle	32, p. 93-105	X		13
1846	Stern, M.	Eine Bemerkung zur Zahlentheorie	Journal de Crelle	32, p. 89-90	Jacobi		2
1847	Cauchy, L. A.	Mémoire sur la théorie des équivalences algébriques substituées à la théorie des imaginaires	Ex. Analyse	4, p. 87 - 110	Gauss, Kummer, (Euler, Moivre)		
1847	Cauchy, L. A.	Sur la décomposition d'un nombre entier en facteurs radicaux	CRAS	24, p. 1022-1030	Kummer	14 juin 1847	10
1847	Cauchy, L. A.	Mémoire sur les facteurs modulaires des fonctions entières d'une ou plusieurs variables	CRAS	24, p. 1117-1120	X	28 juin 1847	12
1847	Cauchy, L. A.	Mémoire sur une nouvelle théorie des imaginaires, et sur les racines symboliques des équations et des équivalences		24, p. 1120-1130	Gauss, Kummer	28 juin 1847	12
1847	Cauchy, L. A.	Mémoire sur les racines des équations algébriques à coefficients entiers, et sur les polynômes radicaux	CRAS	24, p. 407-414	X	15 mars 1847	9
1847	Cauchy, L. A.	Mémoire sur de nouvelles formules relatives à la théorie des polynômes radicaux, et sur le dernier théorème de Fermat	CRAS	24, p. 469-481, 516-528, 578-584, 633-636, 661-666	Liouville, Dirichlet, Lamé	22 et 29 mars, 5, 12 et 19 avril 1847	46

Mémoires liés à la théorie des résidus et des congruences de 1801 à 1850 (suite)							
Date	**Auteur**	**Titre**	**Publication**	**Ref. publication**	**Références données**	**Remarques**	**Nb pages**
1847	Cauchy, L. A.	Mémoire sur diverses propositions relatives à la théorie des nombres	CRAS	24, p. 996-999 et XXV, 177-182, 242-243	Kummer	7 juin 1847	10
1847	Cauchy, L. A.	Mémoire sur l'application de la nouvelle théorie des imaginaires aux diverses branches des sciences mathématiques	CRAS	25, p. 129-132	X	26 juillet 1847	4
1847	Cauchy, L. A.	Mémoire sur diverses propositions relatives à la théorie des nombres	CRAS	25, p. 132-136, 177-182, 242-243	X	26 juillet, 2 et 9 août 1847	10
1847	Cauchy, L. A.	Mémoire sur les racines des équivalences correspondantes à des modules quelconques premiers et non premiers, et sur les avantages que présente l'emploi de ces racines dans la théorie des nombres	CRAS	25, p. 37-46	X	12 juillet 1847	10
1847	Cauchy, L. A.	Mémoire sur la disposition des nombres entiers en facteurs radicaux	CRAS	25, p. 46-54	Kummer	12 juillet 1847	11
1847	Cauchy, L. A.	Mémoire sur les indices modulaires des polynômes radicaux que fournissent les puissances et produits des racines de la résolvante d'une équation binôme	CRAS	25, p. 93-99	Gauss, Jacobi, Legendre	19 juillet 1847	8
1847	Eisenstein, G.	Neue Theoreme der höheren Arithmetik	Journal de Crelle	35, p. 117-136	Gauss, Jacobi, Seeber, Dirichlet		20
1847	Eisenstein, G.	Note sur la représentation d'un nombre par la somme de cinq carrés	Journal de Crelle	35, p. 368-369	Dirichlet, Gauss		2

Mémoires liés à la théorie des résidus et des congruences de 1801 à 1850 (suite)

Date	Auteur	Titre	Publication	Ref. publication	Références données	Remarques	Nb pages
1847	Kummer, E. E.	Sur les nombres complexes qui sont formés avec les nombres entiers réels et les racines de l'unité	Journal de Liouville	12, p. 185-212	Gauss, Jacobi, Kronecker, Dirichlet	Texte original publié en 1844, non traduit ici (latin)	18
1847	Kummer, E. E.	Zur Theorie der complexen Zahlen	Journal de Crelle	35, p. 319-326	Kronecker, Legendre, Gauss, Dirichlet	Texte publié pour la première fois en 1846. Référence à la thèse de Kronecker.	8
1847	Kummer, E. E.	Ueber die Zerlegung der aus Wurzeln der Einheit gebildeten complexen Zahlen in ihre Primfactoren	Journal de Crelle	35, p. 327-367	Gauss, Jacobi, Eisenstein, Dirichlet		41
1847	Kummer, E. E.	Beweis des Fermatschen Satzes der Unmoglichkeit von $x^{\lambda}-y^{lambda} = z^{\lambda}$ für eine unendliche Anzahl Primzahlen λ	Berlin, Bericht	p. 132-139, 140-141, 305-319	Dirichlet		25
1847	Lamé, G.	Mémoire sur la résolution, en nombres complexes, de l'équation $A^5 + B^5 + C^5 = 0$	Journal de Liouville	12, p. 137-171	Dirichlet, Gauss, Jacobi		35
1847	Lebesgue, V. A.	Démonstration nouvelle et élémentaire de la loi de réciprocité de Legendre, par M. Eisenstein, précédée et suivie de remarques sur d'autres démonstrations qui peuvent être tirées du même principe	Journal de Liouville	12, p. 457-473	Eisenstein, Gauss, Jacobi, Legendre, Cauchy		17
1847	Lebesgue, V. A.	Sur le symbole $\left(\frac{a}{b}\right)$ et quelques-unes de ses applications	Journal de Liouville	12, p. 497-517	Legendre , Jacobi, Gauss, Eisenstein		21
1847	Liouville, J.	Sur la loi de réciprocité dans la théorie des résidus quadratiques	Journal de Liouville	12, p. 95-96	Legendre, Gauss	CRAS : 29 mars 1847	2

Mémoires liés à la théorie des résidus et des congruences de 1801 à 1850 (suite)							
Date	**Auteur**	**Titre**	**Publication**	**Ref. publication**	**Références données**	**Remarques**	**Nb pages**
1847	Liouville, J.	Sur la loi de réciprocité dans la théorie des résidus quadratiques	CRAS	24, p. 577-578	Legendre, Gauss		2
1847	Mösta, W.	Ueber einige Sätze der höheren Arithmetik	Archiv Math.	10, p. 98-107	Libri, Eisenstein, Gauss	Reprend la question d'Eisenstein posée dans Crelle, 27, p. 281 (1844)	10
1847	Schaar, M.	Nouvelles démonstrations de la loi de réciprocité pour les résidus quadratiques	Bull. Ac. Belgique	14, p. 79-83	Gauss, Legendre		5
1847	Wronski, H.	Messianisme ou réforme absolu du savoir humain ; nommément : réforme des mathématiques comme prototype de l'accomplissement final des sciences et réforme de la philosophie comme accomplissement final de la religion	1		Gauss, Euler, Legendre, Lagrange, Lambert		
1848	Bouniakowsky, V.	Notes sur quelques points de l'Analyse indéterminée	Bull. Ac. Sc. St Petersburg	6, col. 196-208	X		
1848	Eisenstein, G.	Szur Theorie der quadratischen Zerfällung der Primzahlen $8n+3$, $7n+2$ und $7n+4$	Journal de Crelle	37, p. 97-126	Stern, Jacobi, Cauchy, Gauss		30
1848	Serret, J. A.	Sur un théorème relatif aux nombres entiers	Journal de Liouville	13, p. 12-14	Legendre		3
1848	Terquem, O.	Théorème arithmologique de M. Steiner, démontré par M. Jacobi	Nouv. Ann. Math.	7, p. 268-269	X		2
1849	Binet, J. P. M.	Théorie des nombres	CRAS	28, p. 686-687	Poinsot		
1849	Čebišev	Theorie der Congruenzen			Gauss, Euler, Legendre, Jacobi		360
1849	Grenoble, E. R.	Démonstration du théorème énoncé par M. Poinsot dans la séance du 7 mai 1849	CRAS	528, p. 665-666	Poinsot	communiqué par Poinsot.	

Mémoires liés à la théorie des résidus et des congruences de 1801 à 1850 (suite)							
Date	**Auteur**	**Titre**	**Publication**	**Ref. publication**	**Références données**	**Remarques**	**Nb pages**
1849	Serret, J. A.	Cours d'algèbre supérieure	Édition 1		Gauss, Poinsot, Euler, Hermite, Legendre	Leçons 23-25	
1849	Terquem, O.	Nouvelle démonstration de l'irréductibilité de l'équation $1 + x + x^2 + \ldots + x^{p-1} = 0$; p étant un nombre premier. D'après M. L. Kronecker, étudiant à Berlin	Nouv. Ann. Math.	8, p. 419-421	Gauss, Legendre, Kronecker		3
1850	Eisenstein, G.	Lehrsätze - Über irreductible Congruenzen	Journal de Crelle	39, p. 182	Schönemann		1
1850	Eisenstein, G.	Ueber ein einfaches Mittel zur Auffindung der höheren Reciprocitätsgesetze und der mit ihnen zu verbindenden Ergänzungssätze	Journal de Crelle	39, p. 351-364	Kummer		14
1850	Eisenstein, G.	Beweis der allgemeinsten Reciprocitätsgesetze zwischen und complexen Zahlen	Berlin, Bericht	p. 189-198	Kummer		10
1850	Kummer, E. E.	Zwei besondere Untersuchungen über die Classen-Anzahl und über die Einheiten der aus λ^{ten} Wurzeln der Einheit gebildeten complexen Zahlen	Journal de Crelle	40, p. 117-129	X		13
1850	Kummer, E. E.	Allgemeiner Beweis des Fermatschen Satzes, dass die Gleichung $x^\lambda + y^\lambda = z^\lambda$ durch ganze Zahlen unlösbar ist, für alle diejenigen Potenz-Exponenten λ, welche ungerade Primzahlen sind und in den Zahlern der ersten $\frac{1}{2}(\lambda - 3)$ Bernoullischen Zahlen als Factoreninocht vorkommen	Journal de Crelle	40, p. 130-138	X	-1849	9

Mémoires liés à la théorie des résidus et des congruences de 1801 à 1850 (suite)							
Date	**Auteur**	**Titre**	**Publication**	**Ref. publication**	**Références données**	**Remarques**	**Nb pages**
1850	Kummer, E. E.	Bestimmung der Anzahl nicht äquivalenter Classen für die aus λ^{ten} Wurzeln der Einheit gebildeten complexen Zahlen und die idealen Factorenderselben	Journal de Crelle	40, p. 93-116	Dirichlet		24
1850	Kummer, E. E.	Allgemeine Reciprocitätsgesetze für beliebig hohe Potenzreste	Berlin, Bericht	p. 154-165	Jacobi, Dirichlet		12
1850	Lebesgue, V. A.	Suite du mémoire sur les applications du symbole $\left(\frac{a}{b}\right)$	Journal de Liouville	15, p. 215-237	Cauchy Dirichlet		23
1850	Lebesgue, V. A.	Note sur les congruences	Nouv. Ann. Math.	9, p. 436-439	Gauss, Cauchy		4
1850	Dirichlet, G.	Ueber die Zerlegbarkeit der Zahlen in drei Quadrate	Journal de Crelle	40, p. 228-232	Gauss, Legendre, Jacobi		5
1850	Prouhet, E.	Irréductibilité de l'équation $X = 1 + x + \ldots + x^{p-1} = 0$, p étant un nombre entier	Nouv. Ann. Math.	9, p. 348-349	X		2
1850	Schaar, M.	Mémoire sur la théorie des résidus quadratiques	Mém. Ac. Belgique	24, p. 1-14	Gauss, , Legendre, Dirichlet,	Présenté le 6 octobre 1840.	14
1850	Schaar, M.	Recherches sur la théorie des résidus quadratiques	Mém. Ac. Belgique	25, p. 1-20	Dirichlet, Euler, Catalan	Présenté le 6 avril 1850.	
1850	Schönemann, T.	Ueber einige von Herrn Dr. Eisenstein aufgestellte Lehresätze, irreductible Congruenzen betreffend	Journal de Crelle	40, p. 185-188	Eisenstein		4

Annexe B

Les résidus et le congruences dans la section 1 du *Bulletin de Férussac*

Nous donnons ici la liste des entrées de la première section du *Bulletin de Férussac* qui font référence à des présentations, ouvrages ou mémoires en lien avec les résidus et les congruences. Dans le tableau, l'année indiquée correspond à l'année de publication du volume du *Bulletin de Férussac* concerné. Les trois colonnes suivantes donnent les références de la publication ou du mémoire inédit qui est référencé dans l'entrée du *Bulletin*. Dans la dernière colonne, on indique quelle est la forme de l'entrée :

- *Académie* : l'entrée consiste en une phrase et relate un événement d'une séance de l'Académie des Sciences de Paris (annonce d'un ouvrage, présentation d'un mémoire, ...) ;
- *CR* : l'entrée est le compte-rendu, fait généralement par Cournot, sur un ouvrage ou un article paru dans un périodique ;
- *Direct* : ne concerne qu'une entrée. Cournot résume un travail que Dirichlet lui a communiqué directement ;
- *Mémoire* : l'entrée est une note ou un mémoire inédit, communiqué directement par l'auteur.

Résidus et congruences dans le Bulletin de Férussac (1823-1831)					
Année	Auteur	Texte concerné	Ref. publication	Réf. Bulletin Férussac	Type d'entrée
1825	Libri, G.	Théorie des nombres		3, p. 56	Académie
1825	Libri, G.	Analyse de la théorie des nombres par G. Libri. Extrait du raport fait par MM. Ampère et Cauchy...	Séance du 9 août 1824	3, p. 77-81	CR
1825	Poinsot, L.	Mémoire sur l'application de l'algèbre à la théorie des nombres	Mém. Acad.	3, p. 144-145	CR
1825	Lacroix, S. F.	Complément des éléments d'algèbre	5^{e} édition	4, p. 275	Annonce
1826	Cauchy, A.-L.	Exercices de Mathématiques		6, p. 21-25	CR
1826	Libri, G.	Théorie des nombres	Séance du 13 mars 1826	6, p. 87	Académie
1826	Lejeune-Dirichlet, G.	Mémoire sur l'impossibilité de quelques équations indéterminées du 5^{e} degré	lu à l'Académie le 11 juillet 1825	6, p. 89-91	CR
1826	Horner, W. - G.	Extension of a theorem of Fermat	Annals of Philosophy, 27, p. 81	6, p. 161	CR
1827	Jacobi, C. G. J.	De residuis cubiscis commentatio numerosa	Journal de Crelle, 2, p. 66-69	8, p. 302	CR
1827	Lejeune-Dirichlet, G.	Nouvelle démonstration des théorèmes de Fermat et de Wilson	X	7, p. 354-355	Direct
1828	Legendre, A. - M.	Recherche sur quelques objets d'analyse indéterminée et particulièrement sur le théorème de Fermat	Mémoires Académie (1825), 6, p. 1-60	9, p. 355-356	CR
1828	Lejeune-Dirichlet, G.	Recherches sur les diviseurs premiers d'une classe de formules du quatrième degré	Journal de Crelle, 3, p. 35-69	9, P. 356-357	CR
1828	Lejeune-Dirichlet, G.	Mémoire sur l'impossibilité de quelques équations indéterminées du 5^{e} degré	Journal de Crelle, 3, p. 354-375	11, p. 154	CR
1828	Lejeune-Dirichlet, G.	Démonstrations nouvelles de quelques théorèmes relatifs aux nombres	Journal de Crelle, 3, p. 390-393	11, p. 156	CR
1829	Cauchy, A.-L.	Mémoire sur la théorie des nombres	Inédit	12, p. 205-221	Mémoire
1830	Libri, G.	Sur les racines primitives des nombres premiers	Inédit	13, p. 272-273	Mémoire

Résidus et congruences dans le Bulletin de Férussac (1823-1831) (suite)					
Année	Auteur	Texte concerné	Ref. publication	Réf. Bulletin Férussac	Type d'entrée
1830	Galois, É.	Sur la théorie des nombres	Inédit	13, p. 428-435	Mémoire
1830	Legendre, A. - M.	Théorie des nombres	3^{e} édition	14, p. 90-93	CR
1830	Cauchy, A.-L.		Séance du 14 septembre 1829	14, p. 156	Académie
1830	Cauchy, A.-L.		Séance du 9 novembre 1829	14, p. 156	Académie
1831	Cauchy, A.-L.		Séance du 12 juillet 1830	15, p. 118	Académie
1831	Cauchy, A.-L.	Sur la théorie des nombres	Inédit	15, p. 137-139	Mémoire
1831	Lebesgue, V. - A.	Note sur les résidus des puissances	Inédit	15, p. 155-159	Mémoire
1831	Stern, M. A.	Bemerkungen über höhere Arithmetik	Journal de Crelle, 6, p. 147-158	15, p. 173	CR

Annexe C

La théorie des résidus et des congruences dans le *Journal de Liouville* (1836 - 1850)

I *Journal de Liouville* : bilan par auteur (1836-1850)

Résidus et congruences dans le *Journal de Liouville* (1836-1850) : Bilan par auteur			
Auteurs	Nombre de textes	Nombre de textes originaux	Nombre de pages
Cauchy, L. A.	2	0	30
Galois, E.	1	0	10
Jacobi, C. G. J.	1	0	5
Kummer, E. E.	1	0	18
Lamé, G.	1	1	35
Lebesgue, V. A.	8	8	237
Lejeune-Dirichlet, G.	2	0	55
Liouville, J.	1	0	2
Poinsot, L.	1	1	101
Serret, J. A.	1	1	3
TOTAL	**19**		**496**

II À titre comparatif : bilan par auteur pour le *Journal de Crelle* (1836 - 1850)

Résidus et congruences dans le Journal de Crelle (1836-1850) : Bilan		
Auteur	Nombre d'articles	Nombre de pages
Jacobi, C. G. J.	2	25
Lejeune-Dirichlet, G.	7	232
Schönemann, T.	5	126
Staudt, C.	1	3
Kummer, E. E.	8	126
Crelle, A. L.	1	374
Eisenstein, G.	16	212
Arndt, C. F.	5	43
Kronecker, G.	1	1
Stern, M.	1	2
TOTAL	**47**	**1144**

III Liste des textes publiés

Résidus et congruences dans le *Journal de Liouville* (1836-1850) : liste des articles					
Date	Auteur	Titre	Réf. Publication	Sources données par l'auteur	Nb pages
1837	Lebesgue, V. A.	Recherches sur les nombres	2, p. 253-292	Libri, Cauchy, Gauss, Jacobi	40
1838	Lebesgue, V. A.	Recherches sur les nombres (suite)	3, p. 113-144	Gauss, Poinsot, Libri, Legendre, Jacobi, Cauchy	32
1839	Lebesgue, V. A.	Recherches sur les nombres (suite)	4, p. 9-59	Jacobi, Cauchy, Gauss, Dirichlet	51
1839	Lejeune-Dirichlet, G.	Démonstration de cette proposition : toute progression arithmétique dont le premier terme et la raison sont des entiers sans diviseur commun, contient une inifnité de nombres premiers	4, p. 393-422	Legendre, Gauss	30
1840	Cauchy, L. A.	Sur la sommation de certaines puissances d'une racine primitive d'une équation binôme, et en particulier des puissances qui offrent pour exposants les résidus cubiques inférieurs au module donné	5, p. 169-183	Gauss, Jacobi, ibri, Lebesgue	15
1840	Cauchy, L. A.	Méthode simple et nouvelle pour la détermination complète des sommes alternées, formées avec les racines primitives des équations binômes	5, p. 154-168	Gauss, Jacobi, ibri, Lebesgue	15
1840	Lebesgue, V. A.	Sommation de quelques séries	5, p. 42-71	Gauss, Dirichlet, Jacobi, Legendre	30
1842	Lebesgue, V. A.	Démonstration de quelques théorèmes relatifs aux résidus et aux non-résidus quadratiques	7, p. 137-159	Gauss, Jacobi, Libri, Dirichlet, Stern, Legendre, Cauchy	23
1843	Jacobi, C. G. J.	Sur les nombres premiers complexes que l'on dit considérer dans la théorie des résidus de cinquième, huitième et douzième puisance, Traduction de M. Faye	8, p. 268-272	Gauss, Prof. Zornov	5
1844	Lejeune-Dirichlet, G.	Recherches sur la théorie des nombres complexes.	9, p. 245-269	Gauss	25
1845	Poinsot, L.	Réflexions sur les principes fondamentaux de la théorie des nombres	10, p. 1-101	Euler, Lagrange, Gauss, Legendre	101

Résidus et congruences dans le Journal de Liouville (1836-1850) : liste des articles (suite)					
Date	Auteur	Titre	Réf. Publication	Sources données par l'auteur	Nb pages
1846	Galois, Evariste	Sur la théorie des nombres	11, p. 398-407		10
1847	Kummer, E. E.	Sur les nombres complexes qui sont formés avec les nombres entiers réels et les racines de l'unité	12, p. 185-212	Gauss, Jacobi, Kronecker, Dirichlet	18
1847	Lamé, G.	Mémoire sur la résolution, en nombres complexes, de l'équation $A^5 + B^5 + C^5 = 0$	12, p. 137-171	Dirichlet, Gauss, Jacobi	35
1847	Lebesgue, V. A.	Démonstration nouvelle et élémentaire de la loi de réciprocité de Legendre, par M. Eisenstein, précédée et suivie de remarques sur d'autres démonstrations qui peuvent être tirées du même principe	12, p. 457-473	Eisenstein, Gauss, Jacobi, Legendre, Cauchy	17
1847	Lebesgue, V. A.	Sur le symbole $\left(\frac{a}{b}\right)$ et quelques-unes de ses applications	12, p. 497-517	Legendre , Jacobi, Gauss, Eisenstein	21
1847	Liouville, J.	Sur la loi de réciprocité dans la théorie des résidus quadratiques	12, p. 95-96	Legendre, Gauss	2
1848	Serret, J. A.	Sur un théorème relatif aux nombres entiers	13, p. 12-14	Legendre	3
1850	Lebesgue, V. A.	Suite du mémoire sur les applications du symbole $\left(\frac{a}{b}\right)$	15, p. 215-237	Cauchy Dirichlet	23

Annexe D

La théorie des résidus et des congruences dans les *Nouvelles Annales de Mathématiques* (1842 - 1850)

I Les auteurs

Résidus et congruences dans les Nouvelles Annales de Mathématiques (1842-1850) : Bilan		
Auteur	Nombre d'articles	Nombre de pages
Catalan, E.	1	13
Terquem, O.	5	30
Drot	1	8
Midy, E.	1	7
Prouhet, E.	4	28
Lebesgue, V. A.	1	4

II Liste des textes publiés

Résidus et congruences dans les *Nouvelles Annales de Mathématiques* (1842-1850) : liste des articles					
Date	Auteur	Titre	Réf. Publication	Sources données par l'auteur	Nb pages
1842	Catalan, E.	Sur les fractions décimales périodiques	1, p. 457-470	X	13
1843	Terquem, O.	Théorème de Wilson d'après M. Gauss	2, p. 193-195	Euler, Gauss, Lagrange, Verhulst	3
1844	Terquem, O.	Théorie élémentaire des nombres, d'après Euler, Legendre, MM. Gauss et Cauchy	3, p. 204-208, 214-219, 337-344	Euler, Lagrange, Gauss, Legendre, Wantzel, Krafft, Cauchy	18
1845	Drot	Note sur les chiffres qui peuvent terminer les puissances quelconques des nombres entiers	4, p. 637-644	Gauss	8
1845	Midy, E.	Analyse indéterminée du premier degré	4, p. 146-152	Gauss	7
1845	Prouhet, E.	Mémoire sur la théorie des résidus dans les progressions géométriques	5, p. 175-187	Euler, Poinsot, Legendre	13
1845	Prouhet, E.	Note sur les nombres associés ; généralisation du théorème de Wilson	4, p. 273-278	Legendre	6
1845	Prouhet, E.	Note sur le nombre qui indique combien il y a d'entiers inférieurs et premiers à un nombre donné	4, p. 75-81	Euler, Gauss	7
1845	Terquem, O.	Généralisation de la théorie des nombres associés et théorèmes y relatifs. D'après M. Lejeune-Dirichlet	4, p. 379-382	Dirichlet, Euler, Catalan	4
1848	Terquem, O.	Théorème arithmologique de M. Steiner, démontré par M. Jacobi	7, p. 268-269	X	2
1849	Terquem, O.	Nouvelle démonstration de l'irréductibilité de l'équation $1+x+x^2+\ldots+x^{p-1}=0$; p étant un nombre premier. D'après M. L. Kronecker, étudiant à Berlin	8, p. 419-421	Gauss, Legendre, Kronecker	3
1850	Lebesgue, V. A.	Note sur les congruences	9, p. 436-439	Gauss, Cauchy	4
1850	Prouhet, E.	Irréductibilité de l'équation $X=1+x+\ldots+x^{p-1}=0$, p étant un nombre entier	9, p. 348-349	X	2

Annexe E

Petit intermède sur les fractions continues

Dans [Lagrange, 1773b] , Lagrange ne donne aucun détail sur la façon dont l'on obtient une fraction continue, ou sur les propriétés de celles-ci. On va donc détailler rapidement ces propriétés en nous inspirant de ce que Lagrange fait au début de ses *Additions* aux *É lémens d'Algèbre d'Euler*, publiées en 1774[Lagrange, 1774].

Pour déterminer les premiers termes du développement en fraction continue d'un nombre a, il faut tout d'abord avoir une valeur approchée de $\sqrt{a}$, puis il suffit ensuite d'utiliser l'algorithme d'Euclide. On peut donner l'exemple du début du développement en fraction continue de $\sqrt{3}$. On a :

$$\sqrt{3} \simeq 1.732 = \frac{1732}{1000}.$$

On utilise donc l'algorithme d'Euclide :

$$\begin{aligned}
1732 &= 1 \times 1000 + 732,\\
1000 &= 1 \times 732 + 268,\\
732 &= 2 \times 268 + 196,\\
268 &= 1 \times 196 + 72,\\
196 &= 2 \times 72 + 52,\\
72 &= 1 \times 52 + 20,\\
52 &= 2 \times 20 + 12,\\
20 &= 1 \times 12 + 8,\\
12 &= 1 \times 8 + 4,\\
8 &= 2 \times 4 + 0.
\end{aligned}$$

On obtient donc la fraction continue :

$$\sqrt{3} = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \dots}}}$$

Une fois que l'on a : $\sqrt{a} = q + \cfrac{1}{q' + \cfrac{1}{q'' + \cfrac{1}{q''' + \dots}}}$, les fractions $\frac{m}{n}, \frac{M}{N}, \frac{m'}{n'}, \frac{M'}{N'}, \dots,$ correspondent en fait à :

$$\frac{m}{n} = q,\ \frac{M}{N} = q + \frac{1}{q'},$$

$$\frac{m'}{n'} = q + \frac{1}{q' + \dfrac{1}{q''}}, \ldots,$$

ce qui donne : $\dfrac{m}{n} = \dfrac{q}{1}$, $\dfrac{M}{N} = \dfrac{qq'+1}{q'}$, $\dfrac{m'}{n'} = \dfrac{qq'q''}{q'q''+1}$, ..., et ces fractions sont de plus en plus proches de $\sqrt{a}$. De plus, on peut facilement observer qu'elles sont alternativement plus petites et plus grandes que $\sqrt{a}$, car $\dfrac{m}{n} = q < \sqrt{a}$. Puis on a $\dfrac{M}{N} = q + \dfrac{1}{q'}$, or $q' < q' + \dfrac{1}{q'' + \ldots}$, donc $\dfrac{M}{N} > \sqrt{a}$. De la même façon, comme $\dfrac{m'}{n'} = q + \dfrac{1}{q' + \dfrac{1}{q''}}$, et comme $q'' < q'' + \dfrac{1}{q''' + \ldots}$, alors $q' + \dfrac{1}{q''} > q' + \dfrac{1}{q'' + \ldots}$, donc $\dfrac{m'}{n'} < \sqrt{a}$. Et on peut réitérer le raisonnement.

De plus, d'après ce qui précède, on obtient les formules :

$$\begin{array}{rclcrcl}
m & = & q & & n & = & 1, \\
M & = & mq' + 1 & & N & = & q', \\
m' & = & q''(qq'+1) + q & & n' & = & Nq'' + 1, \\
 & = & q''M + m & & & & , \\
M' & = & q'''m' + M & & N' & = & n'q''' + q', \\
 & & & \ldots & & & .
\end{array}$$

Les deux séries de nombres m, M, m', M',..., et n, N, n', N',..., sont croissantes car avec l'algorithme d'Euclide, les nombres q, q', q'',,..., sont tous positifs.

De plus, en croisant chaque couple de fractions consécutives, on obtient :

$$\begin{array}{rcrcl}
1n & - & 0m & = & 1, \\
Mn & - & Nm & = & 1, \\
Mn' & - & Nm' & = & 1, \\
M'n' & - & N'm' & = & 1, \\
M'n'' & - & N'm'' & = & 1, \\
\ldots & & \ldots & \ldots & .
\end{array}$$

Cela montre d'ailleurs que toutes les fractions considérées sont irréductibles.

Il reste enfin à montrer que la différence entre deux fractions consécutives est minimale. En effet, on peut prendre par exemple les fractions $\dfrac{m'}{n'}$ et $\dfrac{M'}{N'}$. Leur différence est :

$$\frac{M'}{N'} - \frac{m'}{n'} = \frac{M'n' - m'N'}{N'n'} = \frac{1}{N'n'}.$$

Supposons qu'il existe une fraction $\frac{c}{d}$ comprise entre les deux fractions $\frac{m'}{n'}$ et $\frac{M'}{N'}$, et dont le dénominateur d est plus petit que n' ou N'. Considérons la différence $\frac{c}{d} - \frac{m'}{n'} = \frac{cn' - dm'}{dn'}$ et déterminons si elle est inférieure à $\frac{1}{N'n'}$. On a que $\frac{c}{d} - \frac{m'}{n'} > \frac{1}{dn'}$, puisque la différence entre les deux fractions est nécessairement positive. Mais, comme $d < N'$, on a que $\frac{1}{dn'} > \frac{1}{N'n'}$. On en déduit donc que $\frac{c}{d} - \frac{m'}{n'} > \frac{M'}{N'} - \frac{m'}{n'}$.

De même, on a $\frac{M'}{N'} - \frac{c}{d} = \frac{M'd - cN'}{N'd} > \frac{1}{N'd} > \frac{1}{N'n'}$, puisque $d < n'$.

Finalement, on a bien que la différence entre deux fractions consécutives est minimale.

Annexe F

Le manuscrit sur la théorie des permutations de Louis Poinsot

I Quand Poinsot a-t-il écrit son texte sur les permutations ?

Comme nous l'avons indiqué précédemment, nous pensons que ce manuscrit correspond au texte sur la théorie des permutations lu par Poinsot à l'Académie des Sciences le 17 mai 1813. Nous allons donc développer ici les raisons de cette hypothèse.

D'une part, nous avons connu l'existence de ce travail sur les permutations grâce au mémoire lu à l'Académie le 5 mai 1817 par Poinsot [1] : après avoir introduit la notion de *théorie de l'ordre*, point commun entre plusieurs de ses travaux, il résume un mémoire de mai 1813 concernant la théorie des permutations sur les quatre premiers paragraphes, et ceux-ci sont très similaires à certains passages du manuscrit sur les permutations. D'autre part, la qualité du manuscrit présent à l'Institut de France est bonne, et l'écriture très lisible, ce qui laisse à penser que ce texte avait été travaillé et était achevé, prêt à être lu ou publié. Il est donc plausible que cela corresponde à un travail à présenter devant l'Académie.

De plus, on retrouve les idées présentées par Poinsot dans ce manuscrit dans plusieurs de ses textes présentés en 1813 ou avant. On retrouve par exemple dans le commentaire du *Traité* de Lagrange (1808) des raisonnements sur des *groupes de racines*, où le mot *groupe* semble déjà avoir la signification que Poinsot utilise dans le manuscrit. Le paragraphe concernant l'équation binôme du 13^{e} degré cité précédemment page 227 de cet article contient des idées très similaires à celles que l'on retrouve dans le manuscrit.

Les Procès Verbaux de l'Académie des Sciences permettent également de confirmer le fait qu'en 1813, Poinsot est convaincu de l'importance de la théorie des permutations dans la théorie générale des équations. En effet, lors de la séance du 27 décembre 1813, Poinsot lit un rapport sur un mémoire de M. Corancez :

> [...] Telle est la méthode nouvelle contenue dans le Mémoire de M. Corancez. Si nous la considérons d'abord du côté de la théorie des équations, nous ne voyons pas qu'elle puisse répandre une lumière nouvelle sur leur résolution générale. Les principes qui regardent ce problème célèbre résident essentiellement dans la théorie des combinaisons et dans celle des nombres. C'est ce qu'on peut démontrer par la nature même des choses, et, sous ce point de vue général, Vandermonde et l'illustre Lagrange semblent avoir porté la recherche presque aussi loin qu'elle pouvait aller ; du moins, s'il est possible de l'avancer encore, ce n'est que par des idées du

1. Voir [Poinsot, 1818].

même genre et par quelques éléments nouveaux qui manquent encore à la théorie des permutations. [2]

Ainsi, il paraît tout à fait cohérent que Poinsot ait fait des recherches sur les permutations à cette époque.

Réciproquement, on retrouve à la page 511 de notre transcription du manuscrit cette remarque de Poinsot :

> Je passe à une exposition plus claire et plus rapide, et qui est tirée de la considération des nouveaux polygones que nous avons fait connaître. Cette théorie des polygones a une liaison intime avec la résolution générale des équations et la théorie des nombres.

Or, les travaux de Poinsot sur les polygones ont été lus en 1809 devant l'Académie, et publiés en 1810 dans le *Journal de l'École Polytechnique*. Cela correspond donc bien à l'appellation « nouveaux polygones ». On peut donc penser que ce manuscrit a été écrit - ou au moins lu - peu de temps après les recherches de Poinsot sur les polygones et les polyèdres.

Finalement, il est très probable que Poinsot ait produit ce manuscrit pour le lire à l'Académie en 1813. Il est même possible que ces idées aient été relativement claires pour Poinsot avant cette période là. Il reste par contre difficile de savoir si Poinsot a développé ces idées dès le début de sa carrière, soit bien avant les travaux de Cauchy. Les travaux de Cauchy, lus en 1812, ont pu lui permettre d'étudier plus facilement les différents groupes de permutations. Néanmoins, on retrouve également dans le texte de ce dernier le fait que les permutations puissent être rangées « en cercle ou plutôt en polygone régulier »[Cauchy, 1815a, p. 75], raisonnement qui est mis en avant dans le texte de Poinsot sur les polygones et polyèdres dès 1809.

II Manuscrit de Poinsot sur la théorie des permutations [3]

Sur le degré des équations d'où dépend une fonction quelconque des racines d'une équation proposée

Soient a, b, c, d, & c. les racines et $(a, b, c, d, \ldots) = \varphi$ la fonction donnée où l'on suppose que les racines a, b, c, d, ... ne sont pas traitées de la même manière ; qu'on représente

2. *Procès - Verbaux des séances de l'Académie*, tome V (An 1812 - 1815), Imprimerie de l'Observatoire d'Abbadia, 1914, page 294.

3. Nous remercions Michèle Vergne et Gérard Laumon, membres de l'Académie des Sciences, ainsi que Mireille Pastoureau, directeur de la Bibliothèque de l'Institut, pour nous avoir donné accès à ce manuscrit. Nous remercions également la Commission des bibliothèques et archives de l'Institut de France ainsi que sa présidente, Madame Hélène Carrère d'Encausse, secrétaire perpétuel de l'Académie française, pour leur autorisation d'insérer ce manuscrit dans nos travaux. Le texte présenté ici est contenu dans les feuillets 92 à 107 du manuscrit MS954. Le manuscrit original ne contient aucune rature.

même plus simplement la fonction φ par la permutation $abcd\ldots$; toutes les valeurs de φ seront représentées par les diverses permutations $abcd\ldots$, $abdc\ldots$, $bacd\ldots$, & c des m lettres a, b, c, d, & c , et la fonction φ aura, comme on sait, $1.2.3.4\ldots m$ valeurs et dépendra immédiatement d'une équation de ce degré dont on pourra calculer tous les coefficients.

Or il s'agit de faire voir que cette équation ne renferme au fond que la difficulté des degrés respectifs 2, 3, 4, $\ldots m$.

Pour nous faire mieux comprendre, considérons seulement l'équation du $5^{\text{ème}}$ degré et ses cinq racines a, b, c, d, e ; on aura $1.2.3.4.5 = 120$ permutations ou valeurs de la fonction φ.

Or, ces 1.2.3.4.5. permutations peuvent être partagées en 5 groupes principaux de 1.2.3.4 permutations chacun et tels que les permutations d'un même groupe ne se séparent jamais malgré tous les échanges qu'on pourrait faire entre les lettres a, b, c, d, e. En effet, mettez ensemble toutes les permutations qui commencent par a ; ensemble toutes celles qui commencent par b, par c, par d, par e ; il est manifeste à [4] l'aspect de ce tableau, que dans tous les échanges possibles des quatre lettres b, c, d, e, le premier groupe où toutes les permutations commencent par a, restera à sa place ; et que dans l'échange de a avec une des quatre autres lettres b, c, d, e, ce groupe passera tout entier à la place d'un autre, lequel reviendra à la place du premier.

a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a
e	b	c	d	e	b	c	d	e	b	c	d	e	b	c	d	e	b	c	d	e	b	c	d
b	e	d	c	c	d	e	b	d	c	b	e	b	e	d	c	c	d	e	b	d	c	b	e
c	d	e	b	d	c	d	e	b	e	d	c	d	c	b	e	b	e	d	c	c	d	e	b
d	c	b	e	b	e	b	c	c	d	e	b	c	d	e	b	d	c	b	e	b	e	d	c
b	b	b	b	b	b	b	b	b	b	b	b	b	b	b	b	b	b	b	b	b	b	b	b
e	a	c	d	e	a	c	d	e	a	c	d	e	a	c	d	e	a	c	d	e	a	c	d
a	e	d	c	c	d	e	a	d	c	a	e	a	e	d	c	c	d	e	a	d	c	a	e
c	d	e	a	d	c	a	e	a	e	d	c	d	c	a	e	a	e	d	c	c	d	e	a
d	c	a	e	a	e	d	c	c	d	e	a	c	d	e	a	d	c	a	e	a	e	d	c
c	c	c	c	c	c	c	c	c	c	c	c	c	c	c	c	c	c	c	c	c	c	c	c
e	a	b	d	e	a	b	d	e	a	b	d	e	a	b	d	e	a	b	d	e	a	b	d
a	e	d	b	b	d	e	a	d	b	a	e	a	e	d	b	b	d	e	a	d	b	a	e
b	d	e	a	d	b	a	e	a	e	d	b	d	b	a	e	a	e	d	b	b	d	e	a
d	b	a	e	a	e	d	b	b	d	e	a	b	d	e	a	d	b	a	e	a	e	d	b
d	d	d	d	d	d	d	d	d	d	d	d	d	d	d	d	d	d	d	d	d	d	d	d
e	a	b	c	e	a	b	c	e	a	b	c	e	a	b	c	e	a	b	c	e	a	b	c
a	e	c	b	b	c	e	a	c	b	a	e	a	e	c	b	b	c	e	a	c	b	a	e
b	c	e	a	c	b	a	e	a	e	c	b	c	b	a	e	a	e	c	b	b	c	e	a
c	b	a	e	a	e	c	b	b	c	e	a	b	c	e	a	c	b	a	e	a	e	c	b
e	e	e	e	e	e	e	e	e	e	e	e	e	e	e	e	e	e	e	e	e	e	e	e
d	a	b	c	d	a	b	c	d	a	b	c	d	a	b	c	d	a	b	c	d	a	b	c
a	d	c	b	b	c	d	a	c	b	a	d	a	d	c	b	b	c	d	a	c	b	a	d
b	c	d	a	c	b	a	d	a	d	c	b	c	b	a	d	a	d	c	b	b	c	d	a
c	b	a	d	a	d	c	b	b	c	d	a	b	c	d	a	c	b	a	d	a	d	c	b

Ainsi l'on aura 5 groupes principaux dont les permutations respectives ne pourront

4. Le tableau suivant est placé à cet endroit dans le manuscrit.

jamais se mêler, celles de l'un avec celles de l'autre.

Actuellement, chaque groupe qui est de 1.2.3.4 permutations pourra se partager en 4 groupes secondaires composés de 1.2.3 permutations.

Par exemple, le premier groupe principal qui commence par a se décomposera en 4 groupes secondaires : le premier composé de toutes les permutations qui ont b à la $2^{\text{ème}}$ place ; le second de toutes celles qui ont c à la $2^{\text{ème}}$ place ; le troisième de toutes celles qui ont d à la $2^{\text{ème}}$ place ; et le quatrième, e à cette même place.

Or il est clair comme tout-à-l'heure, que ces 4 groupes ne se mêleront jamais ensemble malgré l'échange des lettres b, c, d, e les unes dans les autres.

Maintenant chaque groupe secondaire, tel que le premier où toutes les permutations, qui sont au nombre de 1.2.3 , commençant par ab, se décomposera en 3 groupes ternaires composés chacun de 1.2 permutations ; le premier aura c à la $3^{\text{ème}}$ place, le second aura d , et le troisième, e à cette même place.

Enfin, chaque groupe ternaire, tel que le premier, se décomposera en deux permutations simples $abcde$, $abced$ qui seront toujours conjuguées dans tous les échanges possibles des lettres entre elles.

Donc, en remontant, la fonction $\varphi = abcde$ aura 1.2.3.4.5 valeurs, mais toute fonction invariable φ' telle que la somme ou le produit des deux fonctions conjuguées $abcde$, $abced$ n'en aura que 3.4.5 ; de même, toute fonction invariable φ'' des trois fonctions conjuguées φ', n'en aura que 4.5 , et toute fonction invariable φ''' des quatre fonctions conjuguées φ'', n'en aura que 5.

Ainsi, en représentant les fonctions invariables des diverses valeurs conjuguées par des permutations qui les renferment, on aura ce tableau :

φ	φ'	φ''		
	$\overbrace{\quad}$	$\overbrace{\quad}$	$\overbrace{\quad}$	$\overbrace{\quad}$
a	$\overbrace{aa}$	$\overbrace{aa}$	$\overbrace{aa}$	$\overbrace{aa}$
b	bb	bb	bb	bb
c	cc	cc	dd	ee
d	de	de	ce	cd
e	ed	ed	ec	dc

φ'''

$\overbrace{\quad\quad\quad}\ \overbrace{\quad\quad\quad}\ \overbrace{\quad\quad\quad}\ \overbrace{\quad\quad\quad}$

$\overbrace{aa}\ \overbrace{aa}\ \overbrace{aa}\ \overbrace{aa}\ \overbrace{aa}\ \overbrace{aa}\ \overbrace{aa}\ \overbrace{aa}\ \overbrace{aa}\ \overbrace{aa}\ \overbrace{aa}\ \overbrace{aa}$

bb	bb	bb	cc	cc	cc	dd	dd	dd	ee	ee	ee
cc	dd	ee	bb	dd	ee	bb	ce	ec	bb	cc	dd
de	ce	cd	de	be	bd	ce	bc	be	cd	bd	be
ed	ec	dc	ed	eb	db	ec	eb	cb	dc	db	eb

où l'on voit que φ dépend d'une équation du 2$^{\text{d}}$ degré dont φ' est coefficient ; que φ' dépend d'une équation du 3$^{\text{ème}}$ degré dont φ'' est coefficient ; que φ'' dépend d'une équation du 4$^{\text{ème}}$ degré dont φ''' est coefficient, et φ''' enfin d'une équation du 5$^{\text{ème}}$ degré dont tous les coefficients sont connus.

Et ce raisonnement est général quel que soit le nombre des racines, a, b, c, d, & c ou le degré de la proposée ; d'où l'on voit que l'équation supérieure d'où dépend une fonction de ses racines ne renfermera jamais de difficulté supérieure à celle de la proposée elle-même.

Lorsque, sous la fonction φ, deux ou plusieurs racines se trouvent traitées de la même manière, le nombre des permutations se réduit, et les équations successives d'où dépend cette fonction φ s'abaissent.

S'il n'y a dans la fonction φ qu'une partie des racines, on peut prouver comme précédemment que la difficulté n'est jamais supérieure au degré de la proposée.

Soit, comme dans le 1$^{\text{er}}$ exemple, une équation du 5$^{\text{e}}$ degré, et a, b, c, d, e ses racines, et qu'on demande une fonction φ *abc* qui n'en renferme que trois.

On partagera d'abord toutes les permutations qui sont au nombre de 5.4.3 en 5 groupes principaux, le 1$^{\text{er}}$ où l'on voit a partout à la 1$^{\text{ère}}$ place, le 2$^{\text{e}}$ où l'on voit la lettre b, le 3$^{\text{e}}$ c, le 4$^{\text{e}}$ d, et le 5$^{\text{e}}$ e à cette même place.

Le 1$^{\text{er}}$ où, comme on le voit ici, toutes les permutations commencent par a, se partagera en quatre groupes où l'on voit dans chacun les deux mêmes lettres occuper les deux premières places :

$$\begin{array}{cccc} & & \varphi'' & \\ aaa & aaa & aaa & aaa \\ bbb & ccc & ddd & eee \\ cde & bde & bce & bcd \\ \varphi' & \varphi' & \varphi' & \varphi' \end{array}$$

Chacun de ces groupes ne renfermant que trois valeurs, la fonction $\varphi.abc$ dépendra d'une équation du 3$^{\text{e}}$ degré dont φ' sera coefficient ; φ' dépendra d'une équation du 4$^{\text{e}}$ degré dont φ'' sera coefficient ; et φ'' enfin dépendra d'une équation du 5$^{\text{e}}$ degré dont tous les coefficients seront connus.

Et en général, pour trouver une fonction φ de n racines d'une équation proposée du degré m, il suffira de résoudre des équations des degrés respectifs m, $m-1$, $m-2$, jusqu'à n.

On vient de prouver que toutes les valeurs ou permutations φ peuvent être partagées en divers groupes inséparables malgré l'échange des lettres a, b, c, d, ... les unes dans les autres. Dans l'exemple proposé, on a formé les cinq groupes principaux en composant chacun de toutes les permutations où une même lettre occupe la seconde place, ou la 3$^{\text{e}}$, ou la 4$^{\text{e}}$, ou la 5$^{\text{e}}$, ce qui nous fait voir d'abord que le partage des 2.3.4.5 permutations en 5 groupes principaux n'est point unique, mais peut se faire de 5 manières différentes ; ainsi,

l'on peut former 5 tableaux où l'on verra toutes les permutations différemment groupées, mais de telle manière dans chacun d'eux, que les 5 groupes qui le composent ne pourront jamais mêler leurs permutations malgré tous les échanges possibles des lettres a, b, c, d, e entre elles.

De même, chaque groupe principal, en y faisant, pour plus de clarté, abstraction de la lettre commune qui occupe partout la même place, pourra être partagé en 4 groupes secondaires de 4 manières différentes ; chaque groupe secondaire se pourra décomposer de même de 3 manières différentes en groupes ternaires et ainsi de suite.

D'où il résulte en général qu'on a m manières de partager toutes les permutations de m lettres en m groupes principaux, ce qui donne lieu à m tableaux ou systèmes différents ;

Que dans chaque tableau ou système, on a $m-1$ manières de partager les permutations de chaque groupe, ce qui produit $m.m-1$ tableaux différents ;

Que dans chaque tableau, on a $m-2$ manières de grouper les permutations de chaque groupe secondaire ; ce qui fournira $m.m-1.m-2$ tableaux différents ; et ainsi de suite.

Et dans tous ces tableaux, deux permutations conjuguées ne se sépareront jamais ; trois groupes conjugués ne se sépareront jamais ; quatre de ces groupes conjugués ne se sépareront jamais, et ainsi de suite, malgré tous les échanges possibles qu'on voudra faire entre les lettres a, b, c, d, e, & c.

La manière dont nous venons de grouper les permutations en mettant dans les groupes une ou plusieurs lettres aux mêmes places, est la plus naturelle et la plus simple qui puisse s'offrir ; mais quoiqu'elle abaisse les degrés des équations d'où elles dépendent jusqu'au degré de la proposée elle-même, elle ne peut rien apprendre sur la résolution ; par cela même qu'elle considère chaque racine comme servant de chef aux divers groupes, elle renferme essentiellement la difficulté du degré marqué par le nombre de ces racines.

II.

Il nous reste à voir s'il n'y a pas d'autres conjugaisons ou d'autres manières de partager les permutations en divers groupes qui ne puissent jamais se mêler malgré l'échange des lettres a, b, c, d, & c. les unes dans les autres.

Nous avons d'abord assemblé nos permutations par deux, puis ces couples par trois ; ensuite ces groupes résultants par quatre, et ainsi de suite jusqu'à m ; commençons au contraire par assembler nos permutations de m lettres par m, et pour plus de clarté, reprenons l'exemple de cinq lettres a, b, c, d, e.

La manière générale de trouver les permutations qui s'assemblent est de prendre une quelconque de ces permutations, et d'y appeler toutes les lettres dans un nouvel ordre, ce qui fournira une nouvelle permutation, ensuite de tirer de celle-ci, par la même loi, une troisième permutation qui sera dérivée de la $2^{\text{ème}}$ comme la $2^{\text{ème}}$ est dérivée de la $1^{\text{ère}}$;

on continuera de cette manière jusqu'à ce que l'on retombe sur la permutation primitive d'où l'on était parti, et l'on repassera ensuite dans les mêmes à l'infini.

Ces différentes permutations dérivées successivement l'une de l'autre par la même loi seront conjuguées ; c'est-à-dire ne se sépareront jamais malgré tous les échanges possibles entre les lettres, ou ces permutations ne feront que s'échanger les unes dans les autres, ou tout le groupe changera et deviendra un groupe semblable de permutations nouvelles, mais dérivées les unes des autres par la même loi qu'auparavant.

La dérivation la plus simple† est celle d'appeler les lettres dans l'ordre naturel 2^{e} , 3^{e} , 4^{e} , 5^{e} , $1^{ère}$; ou 3^{e} , 4^{e} , 5^{e} , $1^{ère}$, 2^{e} , ou 4^{e} , 5^{e} , $1^{ère}$, 2^{e} , 3^{e} ; & c ; ce qui revient à les avancer toutes d'une place, ou toutes de deux places , & c. ; ainsi, d'après cette règle,

$$a\ b\ c\ d\ e$$

je tire

$$b\ c\ d\ e\ a;$$

de celle-ci je tire de même

$$c\ d\ e\ a\ b;$$

de celle-ci je déduis également

$$d\ e\ a\ b\ c;$$

de celle-ci

$$e\ a\ b\ c\ d,$$

et de celle-ci enfin, je tirerai la $1^{ère}$

$$a\ b\ c\ d\ e$$

d'où j'étais parti. Ainsi l'on a ce groupe de permutations dérivées que j'écris maintenant suivant les lignes verticales de cette manière :

$$\begin{array}{ccccc} a & b & c & d & e \\ b & c & d & e & a \\ c & d & e & a & b \\ d & e & a & b & c \\ e & a & b & c & d \end{array}$$

Si l'on eût dérivé suivant l'ordre 3^{e} , 4^{e} , 5^{e} , $1^{ère}$, 2^{e} , on aurait retrouvé les mêmes permutations, mais rangées différemment ; et de même en dérivant suivant l'ordre 4^{e} , 5^{e} , $1^{ère}$, 2^{e} , 3^{e} , ou 5^{e} , $1^{ère}$, 2^{e} , 3^{e} , 4^{e} , on aurait encore le même groupe.

†. il y a en effet plusieurs manières de dériver les permutations les unes des autres ; pour cinq lettres, on peut dériver de 6 manières différentes ; pour sept lettres, on pourrait faire la même chose de 2.3.4.5 manières différentes, mais nous ne pouvons ici qu'indiquer ces théorèmes.

Considérons en effet la 1ère loi, ou la première manière de dériver les permutations ; nous voyons que la première permutation

$$a\ b\ c\ d\ e$$

fait naître la deuxième

$$b\ c\ d\ e\ a;$$

celle-ci la 3e

$$c\ d\ e\ a\ b;$$

celle-ci la 4e

$$d\ e\ a\ b\ c;$$

celle ci enfin la 5e

$$e\ a\ b\ c\ d.$$

La 2e loi de dérivation ferait naître de la première permutation la 3e ; de celle-ci la 5e ; de celle-ci la 2e ; de celle-ci la 4e , en sautant ainsi de 2 en 2 ; et si 2 ne divise pas le nombre m, comme dans cet exemple où $m = 5$, il faut nécessairement retrouver nos m permutations différentes avant de revenir à la première.

Par la même raison la troisième manière de dériver reproduira les m permutations si 3 n'est pas diviseur de m, et ainsi des autres ; de sorte que m étant un nombre premier, il y aura $m - 1$ lois équivalentes de dérivation. Les m permutations conjuguées seront entre elles dans une dépendance toute semblable, et l'on pourra les considérer indifféremment comme dérivées successivement l'une de l'autre par la loi dont une quelconque d'entre elles dériverait de l'une quelconque des autres à volonté.

Si le nombre m est un nombre composé, en appelant les lettres d'une première permutation dans l'ordre naturel 2, 3, 4, 5, 6, & c., on assemble aussi m permutations différentes qui sont conjuguées entre elles ; mais ces permutations n'offrent point cette même similitude de dépendance mutuelle. Elles ne peuvent pas être envisagées comme formées toutes par la loi dont une quelconque d'entre elles dériverait de l'une quelconque des autres à volonté. Elles se partagent en plusieurs groupes suivant les facteurs premiers de m.

Soient, en effet, nos m permutations formées par la 1ère loi et rangées dans l'ordre où elles naissent d'après cette loi ; si vous vouliez les retrouver par la loi d'où la $n^{\text{ème}}$ dérive de la 1ère et que n fût diviseur de m, vous iriez ainsi de l'une à l'autre en sautant de n en n, et comme n divise exactement m, vous ne passeriez jamais que sur la même partie $\frac{m}{n}$ de vos m permutations ; donc si m est composé, il y aura seulement autant de manières de les former toutes les unes par les autres, qu'il y aura de nombres inférieurs premiers à m.

Soit α l'un des facteurs premiers de m qui sera ainsi de la forme $m = \alpha N$, en dérivant

de la 1ère permutation, d'après l'ordre

$$\alpha + 1,\ \alpha + 2,\ \alpha + 3,\ \&\ \text{c.},$$

vous assemblerez N de vos permutations, et par conséquent les m permutations proposées seront partagées en α groupes conjugués de N permutations.

Soit β l'un des facteurs premiers de N, de sorte qu'on ait $N = \beta N'$; en dérivant d'après l'ordre

$$\beta + 1,\ \beta + 2,\ \beta + 3,\ \&\ \text{c.},$$

vous formerez un groupe de N' permutations conjuguées et par conséquent β groupes semblables des N permutations de chacun des groupes précédents, et ainsi de suite. Pour le cas de $m = \alpha\beta\gamma$, α, β, et γ étant des nombres premiers, le système de vos m permutations dérivées se partagerait donc en α groupes de $\beta\gamma$ permutations, et ces α groupes seraient conjugués entre eux d'une manière toute semblable ; chacun des groupes $(\beta\gamma)$ se partagerait de même en β groupes de γ, et les β groupes seraient conjugués entre eux d'une manière semblable ; enfin les γ permutations de chacun de ces groupes seraient aussi conjuguées entre elles d'une manière semblable, à cause que γ est aussi un nombre premier. Ainsi pour $m = 12$ par exemple, les douze permutations se pourraient partager en deux groupes de six, et chacun de ces groupes en deux autres de trois permutations.

Voilà donc une manière très simple de partager le système des $1.2.3.4 \ldots m$ permutations de m lettres, en $1.2.3.4 \ldots m - 1$ groupes de m permutations conjuguées par la même loi, et qui sont inséparables malgré tous les échanges qu'on pourrait faire entre les m lettres proposées.

Conjugaison mutuelle des groupes

Mais actuellement, il peut y avoir plusieurs de ces groupes qui se conjuguent aussi entre eux d'une manière inséparable, je veux dire qui soient tels que tout échange qui ferait passer une permutation à la place de celle d'un autre groupe, non seulement ferait passer le groupe entier à la place de cet autre, mais ramènerait encore celui-ci à la place du premier ; ou bien, si les groupes s'assemblaient en plus grand nombre, tout échange de lettres ne ferait que les convertir les uns dans les autres, ou changerait à la fois tout le système en l'un des systèmes semblables formés par le reste des autres permutations.

(Dans les permutations dérivées d'un même groupe, il n'y a aucune lettre qui soit à la même place dans deux permutations ; mais dans les groupes conjugués il y a nécessairement autant de permutations où la même lettre occupe la même place.)

Si l'on voulait découvrir à la seule inspection quels sont les groupes qui s'assemblent, on n'aurait qu'à regarder les permutations qui commencent par la même lettre dans ces

divers groupes, et voir quel est l'aspect relatif des $m-1$ lettres restantes : cet aspect doit être le même pour les $m-1$ lettres restantes des autres permutations qui commencent aussi par une autre même lettre, et ainsi de suite. De cette manière, la conversion mutuelle des permutations commençant par la même lettre entraînera la conversion mutuelle des groupes auxquels ces permutations appartiennent, et l'on aura trouvé les groupes qui peuvent se conjuguer.

Mais on y peut également parvenir par le principe analogue à celui qui nous a fait d'abord assembler les permutations d'un même groupe. En effet, si plusieurs groupes sont conjugués d'une manière inséparable, il faut que le même changement d'ordre qui ferait déduire le $2^{\text{ème}}$ du 1^{er}, fit aussi déduire le $3^{\text{ème}}$ du 2^{d} , le $4^{\text{ème}}$ du $3^{\text{ème}}$ et ainsi de suite, jusqu'à ce qu'on retombât sur le 1^{er} groupe d'où l'on est parti.

Or, si dans le 1^{er} groupe de m permutations, nous prenez toutes les lettres de n en n, et que n soit premier à m, vous formerez évidemment un nouveau groupe de permutations conjuguées entre elles par la même loi que les premières : car il est manifeste que dans ces permutations toutes les lettres se suivront aussi entre elles dans le même ordre. Si dans ce nouveau groupe vous prenez de même toutes les lettres de n en n, vous trouverez un troisième groupe de permutations nouvelles, mais conjuguées encore par la même loi, et ainsi de suite, jusqu'à ce que vous retombiez sur le premier groupe d'où vous étiez parti.

Mais il n'est pas difficile de voir et de démontrer que si, dans une permutation, on prend les lettres de n en n, ce qui fournit une nouvelle permutation, et que dans celle-ci on prenne encore les lettres de n en n, ce qui donne une troisième permutation, ce passage de la $1^{\text{ère}}$ à la $3^{\text{ème}}$ peut également se faire en prenant tout d'un coup dans la $1^{\text{ère}}$ les lettres de n^2 en n^2, et de même si l'on continuait à prendre les lettres de n en n dans la $3^{\text{ème}}$ permutation pour arriver à une $4^{\text{ème}}$, ce passage de la $1^{\text{ère}}$ à la $4^{\text{ème}}$ pourrait s'effectuer tout d'un coup en prenant les lettres de n^3 en n^3, et ainsi de suite, en observant que si les nombres n^2, n^3, & c. deviennent supérieurs à m, il faut entendre par ces nombres leurs plus petits résidus par rapport à m.

Ce théorème est très remarquable, il donne une espèce de définition géométrique de ces nombres qu'Euler nomme racines primitives, et qui sont tels que toutes leurs puissances successives laissent par rapport au nombre premier μ que l'on considère des restes tous différents 1, 2, 3, 4, $\ldots \mu - 1$ et qui reparaissent ensuite périodiquement à l'infini.

Si μ lettres sont rangées en cercle comme les angles d'un polygone, il y a toujours des nombres n tels qu'en joignant les points de n en n, ce qui donne un nouveau polygone, puis ceux-ci de n en n, ce qui forme un troisième polygone, et ainsi de suite, vous formez toutes les espèces de polygones de l'ordre μ ; et il y a juste autant de ces nombres ou racines primitives qu'il y a de nombres premiers à $\mu - 1$ et inférieurs à $\mu - 1$. (La raison de ce dernier théorème est qu'il doit y en avoir autant qu'il y a de permutations dérivées entre les $\mu - 1$ lettres qui suivent celle d'où l'on part ; or pour un nombre composé $\mu - 1$, il y a autant de manières de former les permutations dérivées toutes par une même loi qu'il

y a de nombres inférieurs et premiers à ce nombre).

Donc si m est un nombre premier et n un nombre dont toutes les puissances successives laissent des résidus différents 1, 2, 3, 4, $\ldots m-1$, on trouvera $m-1$ groupes conjugués avant de revenir au premier d'où l'on était parti ; et l'on voit en même temps qu'on peut trouver ces $m-1$ groupes sans connaître le nombre n : il suffira de considérer le 1er et d'y prendre d'abord toutes les lettres de 2 en 2, puis de 3 en 3, puis de 4 en 4, & c., et enfin de $m-1$ en $m-1$.

Ainsi dans l'exemple de 5 lettres a, b, c, d, e, prenez dans le 1er groupe

$$\begin{array}{c} a\ b\ c\ d\ e \\ b\ c\ d\ e\ a \\ c\ d\ e\ a\ b \\ d\ e\ a\ b\ c \\ e\ a\ b\ c\ d \end{array}$$

les lettres de 2 en 2, et vous avez :

$$\begin{array}{c} a\ b\ c\ d\ e \\ c\ d\ e\ a\ b \\ e\ a\ b\ c\ d \\ b\ c\ d\ e\ a \\ d\ e\ a\ b\ c\,; \end{array}$$

dans le 1er groupe prenez les lettres de 3 en 3, et ensuite de 4 en 4, et vous aurez ces deux autres :

$$\begin{array}{c} a\ b\ c\ d\ e \\ d\ e\ a\ b\ c \\ b\ c\ d\ e\ a \\ e\ a\ b\ c\ d \\ c\ d\ e\ a\ b \end{array} \qquad\qquad \begin{array}{c} a\ b\ c\ d\ e \\ e\ a\ b\ c\ d \\ d\ e\ a\ b\ c \\ c\ d\ e\ a\ b \\ b\ c\ d\ e\ a \end{array}$$

et ces quatre groupes de 5 permutations seront conjugués d'une manière inséparable.

Mais la première manière de déduire successivement ces groupes l'un de l'autre par la même loi est plus avantageuse en ce qu'elle nous découvre encore une décomposition de ces $m-1$ groupes entre eux, et par l'ordre où elle les fait naître successivement.

En effet, puisque du 1er groupe vous tirez un 2d groupe en prenant les lettres de n en n ; de ce 2d un 3e en prenant les lettres de n en n ; de ce 3e un 4e en y prenant encore les lettres de n en n, et ainsi de suite ; que d'un autre côté, cela reviendrait à déduire toujours du même 1er groupe, d'abord de n en n, puis de n^2 en n^2, puis de n^3 en n^3, & c., et enfin de n^{m-2} en n^{m-2} ; il s'en suit que le système de ces $m-1$ groupes conjugués se

partage lui-même en systèmes partiels aussi conjugués. Car le nombre m étant premier, le nombre $m-1$ est nécessairement composé ; or supposez que α soit un facteur de $m-1$, et dans l'ordre où sont actuellement vos groupes, essayez de les déduire les uns des autres par la loi d'où le $\alpha+1^{\text{ème}}$ dérive du 1^{er}, ce qui revient à prendre toutes les lettres de n^{α} en n^{α}, vous irez ainsi de l'un à l'autre, en sautant de α en α, et comme α est diviseur de $m-1$, vous ne passerez jamais que sur une même partie $\frac{m-1}{\alpha}$ de vos $m-1$ groupes, de sorte que le système sera partagé en α systèmes partiels de $\frac{m-1}{\alpha}$ groupes aussi conjugués entre eux. Et de même si $\frac{m-1}{\alpha}$ a pour diviseur β, vous pourrez subdiviser encore chacun des $\frac{m-1}{\alpha}$ systèmes partiels en β systèmes de $\frac{m-1}{\alpha\beta}$ groupes aussi conjugués entre eux, et ainsi de suite, jusqu'à ce que le système entier n'offre plus dans toutes ses subdivisions que les nombres premiers α, β, ... qui entrent dans la composition du nombre $m-1$; alors il y aura une dépendance mutuelle toute semblable 1°. entre les m permutations d'un même groupe ; 2°. entre les groupes d'un même système partiel ; 3°. entre les systèmes partiels d'un même système supérieur ; et ainsi de suite.

Pour aller plus loin dans la réduction des groupes il faudrait chercher si les $1.2.3.4\ldots m-2$ systèmes pourraient se grouper encore, et ceux-ci à leur tour, & c. par les nombres $m-2$, $m-3$, & c ou par leurs diviseurs ; de sorte que la décomposition entière de toutes les permutations se fît toujours par des nombres inférieurs à m.

Dans le cas où m est un nombre composé, on n'assemble plus immédiatement $m-1$ des groupes comme ci-dessus, mais seulement autant de ces groupes qu'il y a de nombres premiers à m au dessous de lui : pour 4, par exemple, on n'assemble que deux groupes de permutations conjuguées ; cela est facile à conclure de ce qui a été dit précédemment.

Il est bien facile de faire l'application de ces principes aux cas de 3, 4, 5 lettres et de voir la raison métaphysique de la résolution des équations du 3^{e} et du 4^{e} degré, et celle de la réduction de la difficulté dans le cas du 5^{e} degré, à la difficulté d'une équation particulière du 6^{e} .

On a pour le 3^{e} le tableau suivant :

$a\ b\ c$	$a\ b\ c$
$b\ c\ a$	$c\ a\ b$
$c\ a\ b$	$b\ c\ a$;

pour le 4^{e} on a celui-ci :

a	c	b	d	a	b	c	d	a	b	d	c	a	c	d	b	a	c	b	d	a	d	b	c
b	d	c	a	d	a	b	c	b	d	c	a	c	d	b	a	c	b	d	a	d	b	c	a
c	a	d	b	c	d	a	b	d	c	a	b	d	b	a	c	b	d	a	c	b	c	a	d
$\underbrace{d\ b}_{\varphi}$		$\underbrace{a\ c}_{\varphi}$		b	c	d	a	c	a	b	d	b	a	c	d	d	a	c	b	c	a	d	b
$\underbrace{\qquad\qquad}_{\omega}$																							
$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}_{\psi}$																							

On peut remarquer dans ce dernier tableau que les quatre permutations, de chaque groupe, du 1er par exemple, se partagent en deux groupes partiels de deux permutations conjuguées, comme cela doit être. Ainsi la fonction quelconque de a, b, c, d, $f(a,b,c,d)$ peut être regardée comme racine d'une équation du 2e degré dont φ serait coefficient ; φ peut être regardée comme racine d'une équation du 2d degré dont ω serait coefficient ; ω à son tour, comme racine d'une équation du 2d degré dont ψ serait coefficient, et ψ enfin comme la racine d'une équation du 3e degré dont tous les coefficients seraient connus. D'où l'on peut conclure ce théorème qui nous paraît nouveau et remarquable :

L'équation du 24e degré qui donne les 24 valeurs d'une fonction des quatre racines a, b, c, d d'une équation du 4e degré peut se résoudre actuellement à l'aide d'équations du 2d et 3e degré, sans faire sur cette fonction aucun hypothèse particulière qui réduise les 24 valeurs à 3 en les rendant égales 8 à 8.

Cette résolution tient donc essentiellement à la nature du nombre 4 qui permet ainsi de grouper les 24 valeurs par 2 et par 3, et non point au choix qu'on fait de certaines fonctions particulières des racines qui offrent moins de valeurs différentes qu'il n'y a de permutations entre les quatre racines. Il n'en est pas de même dans le 3e degré : à cause du nombre premier 3 on a toujours à résoudre une équation du 3e degré pour obtenir les trois permutations d'un même groupe ; mais par la dépendance semblable de ces trois permutations qui fait qu'elles se produisent également les unes par les autres comme les racines 3èmes de l'unité, cette équation n'a que la difficulté des équations binômes du 3e degré.

Soient en effet vos trois fonctions

$$\begin{array}{ccc} \varphi & \varphi & \varphi \\ a & b & c \\ b & c & a \\ c & a & b \\ A & A' & A'' \end{array};$$

les fonctions A, A', A'' des trois lettres a, b, c sont telles que si A est changée en A', A' l'est en A'' et A'' en A ; si A est changé en A'', A' l'est en A, A'' en A' ; ainsi ces trois fonctions A, A', A'' ne peuvent présenter que ces trois permutations :

$$\begin{array}{ccc} A & A' & A'' \\ A' & A'' & A \\ A'' & A & A' \end{array};$$

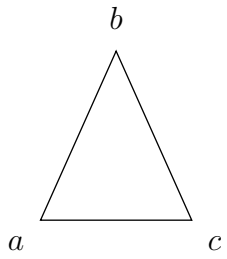
ces fonctions sont donc liées entre elles comme les trois racines de l'unité 1, α, α^2 ; la fonction $(A + \alpha A' + \alpha^2 A'')$ élevée au cube n'a donc qu'une seule valeur pour le 1er groupe.

Par ce que j'ai dit plus haut sur le cas de 5 lettres a, b, c, d, e, on peut voir aussi que la résolvante du 120e degré où l'on est conduit pour la résolution du 5e degré, n'a que la

difficulté d'une équation particulière du 6^{e} , mais qui a résisté jusqu'ici à tous les efforts des géomètres. Nous avons bien trouvé une manière très simple de la réduire elle-même au 5^{e} degré, mais cette réduction paraît inutile, et le problème se replie en quelque sorte lui-même, sans qu'on puisse voir s'il y aurait quelqu'avantage à cette transformation. J'ai à peine le temps d'indiquer la plupart des résultats auxquels je suis parvenu et [5]

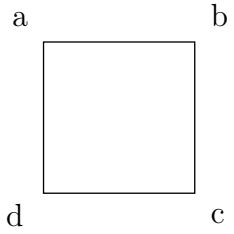
Je passe à une exposition plus claire et plus rapide, et qui est tirée de la considération des nouveaux polygones que nous avons fait connaître. Cette théorie des polygones a une liaison intime avec la résolution générale des équations et la théorie des nombres.

3$^{\text{ème}}$ degré



Ce triangle offre les six permutations des trois lettres a, b, c qui sont aux angles, savoir trois permutations conjuguées qu'on obtient en lisant dans le même ordre en partant successivement de a, de b, de c ; et 3 autre conjuguées en lisant de 2 en 2, ce qui reviendrait ici à renverser.

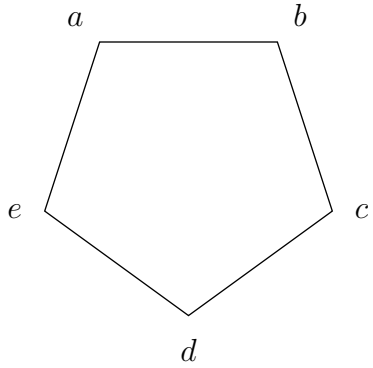
4$^{\text{ème}}$ degré

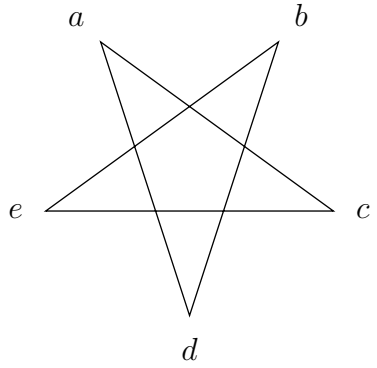


Le carré renferme 8 permutations, savoir 4 en lisant de suite dans le même ordre, et 4 conjuguées en lisant de 3 en 3 ou dans l'ordre renversé.

5$^{\text{ème}}$ degré

5. Cette page n'est pas achevée.





Il y a deux espèces de pentagones réguliers ; chacun d'eux renferme actuellement 10 permutations savoir, 5 en lisant de suite dans le même ordre, et 5 conjuguées en lisant dans l'ordre renversé, ou de 4 en 4 comme vous pouvez le voir ; il en résulte donc 20 permutations conjuguées. Les cinq permutations d'un groupe sont liées entre elles comme les cinq racines cinquièmes de l'unité ; elles ne dépendent au fond que d'une équation binôme du 5^{e} degré ; leurs fonctions semblables ne dépendent que d'une équation du 2^{e} degré, à cause des deux 1^{ers} groupes conjugués ; les fonctions semblables des coefficients de cette équation ne dépendent encore que d'une équation du 2^{d} degré par ce que le 1^{er} couple des groupes est conjugué avec le 2^{d} couple ; enfin les coefficients de cette équation du 2^{d} degré ne dépendent plus que d'une équation du 6^{e} degré dont tous les coefficients sont connus.

Ces résultats s'accordent parfaitement avec ceux que M. Lagrange obtient par son analyse (*Mém. de Berlin*, 1771), mais on voit de plus qu'il n'y a pas réellement d'équation du 4^{e} degré à résoudre, mais bien 2 équations du 2^{d} degré, de sorte que les radicaux cubiques ne proviendront que de la réduite du 6^{e} degré.

Annexe G

Résidus et congruences chez Cauchy

Textes de Cauchy en rapport avec les résidus et les congruences

Textes de Cauchy en rapport avec les résidus et les congruences						
Date	**Titre**	**Publication**	**Ref. publication**	**Références données**	**Remarques**	**Nb pages**
1813	Recherches sur les nombres	J. E. P.		Lagrange, Legendre		24
1829	Mémoire sur la théorie des nombres	Bull. Férussac	12, p. 205-221	Gauss, Poinsot, Jacobi		20
1829	Sur diverses propositions relatives à l'algèbre et à la théorie des nombres	Ex. Math.	4, p.217-252	Euler, Lagrange, Gauss, Legendre, Libri, Poinsot, Binet		99
1829	Sur la résolution des équivalences dont les modules se réduisent à des nombres premiers	Ex. Math.	4, p.253-292	Gauss, Libri		44
1831	Sur la théorie des nombres	Bull. Férussac	15, p. 137-139	X		4
1833	Formules d'interpolation	Résumés Analytiques, Turin	p. 31-36	X		6
1839	Sur la théorie des nombres et en particulier sur les formes quadratiques des nombres premiers	CRAS	9, p. 473-474	Libri, Gauss, Jacobi	14 octobre 1839	3
1839	Sur la théorie des nombres et en particulier sur les formes quadratiques des puissances d'un nombre premier, ou du quadruple de ces puissances	CRAS	9, p. 473, 519-526	Lagrange, Gauss, Poinsot	28 octobre 1839	8
1840	Sur la sommation de certaines puissances d'une racine primitive d'une équation binôme, et en particulier des puissances qui offrent pour exposants les résidus cubiques inférieurs au module donné	Journal de Liouville	5, p. 169-183	Gauss, Jacobi, Libri, Lebesgue	CRAS : 13 avril 1840	15
1840	Suite des observations sur les formes quadratiques de certaines puissances des nombres premiers. Théorèmes relatifs aux exposants de ces puissances.	CRAS	10, p. 181-190	X	3 février 1840	11
1840	Discussion des formes quadratiques sous lesquelles se présentent certaines puissances des nombres premiers. Réduction des exposants de ces puissances.	CRAS	10, p. 229-243	Jacobi	10 février 1840	17
1840	Théorèmes divers sur les résidus et les non-résidus quadratiques	CRAS	10, p. 437-452	Gauss, Liouville, Dirichlet	16 mars 1840	18

Textes de Cauchy en rapport avec les résidus et les congruences (suite)						
Date	**Titre**	**Publication**	**Ref. publication**	**Références données**	**Remarques**	**Nb pages**
1840	Théorèmes relatifs aux formes quadratiques des nombres premiers et de leurs puissances	CRAS	10, p. 51-61	Gauss, Jacobi	13 janvier 1840	12
1840	Méthode simple et nouvelle pour la détermination complète des sommes alternées, formées avec les racines primitives des équations binômes	CRAS	10, p. 560-572	Gauss, Dirichlet, Lebesgue, Poisson	6 avril 1840	15
1840	Sur la sommation de certaines puissances d'une racine primitive d'une équation binôme, et en particulier des puissances qui offrent pour exposants les résidus cubiques inférieurs au module donné	CRAS	10, p. 594-606	Gauss, Jacobi, Libri, Lebesgue	13 avril 1840	15
1840	Observations nouvelles sur les formes quadratiques des nombres premiers et de leurs puissances	CRAS	10, p. 85-100	Jacobi	20 janvier 1840	18
1840	Mémoire sur la théorie des nombres	Mémoires Académie	18, p. 249-768	Gauss, Poinsot, Legendre, Euler, Dirichlet, Jacobi	31 mai 1830	446
1841	Mémoire sur la résolution des équations indéterminées du premier degré en nombres entiers	Ex. Analyse	13e livraison	Libri, Binet, Poinsot, Legendre, Jacobi, Stern	Reproduction des CRAS du 10 mai 1841	39
1841	Mémoire sur diverses formules relatives à l'algèbre et à la théorie des nombres	CRAS	12, p. 698-711, 813-846	Libri, Binet, Poinsot, Legendre, Jacobi, Stern	26 avril et 10 mai 1841	48
1845	Note sur quelques propositions relatives à la théorie des nombres	Ex. Analyse	29e livraison (9/12/1845)	Euler, Poinsot, Gauss		7
1847	Mémoire sur la théorie des équivalences algébriques substituées à la théorie des imaginaires	Ex. Analyse	4, p. 87 ? 110	Gauss, Kummer, (Euler, Moivre)		
1847	Sur la décomposition d'un nombre entier en facteurs radicaux	CRAS	24, p. 1022-1030	Kummer	14 juin 1847	10

Textes de Cauchy en rapport avec les résidus et les congruences (suite)						
Date	**Titre**	**Publication**	**Ref. publication**	**Références données**	**Remarques**	**Nb pages**
1847	Mémoire sur les facteurs modulaires des fonctions entières d'une ou plusieurs variables	CRAS	24, p. 1117-1120	X	28 juin 1847	12
1847	Mémoire sur une nouvelle théorie des imaginaires, et sur les racines symboliques des équations et des équivalences		24, p. 1120-1130	Gauss, Kummer	28 juin 1847	12
1847	Mémoire sur les racines des équations algébriques à coefficients entiers, et sur les polynômes radicaux	CRAS	24, p. 407-414	X	15 mars 1847	9
1847	Mémoire sur de nouvelles formules relatives à la théorie des polynômes radicaux, et sur le dernier théorème de Fermat	CRAS	24, p. 469-481, 516-528, 578-584, 633-636, 661-666	Liouville, Dirichlet, Lamé	22 et 29 mars, 5, 12 et 19 avril 1847	46
1847	Mémoire sur diverses propositions relatives à la théorie des nombres	CRAS	24, p. 996-999 et XXV, 177-182, 242-243	Kummer	7 juin 1847	10
1847	Mémoire sur l'application de la nouvelle théorie des imaginaires aux diverses branches des sciences mathématiques	CRAS	25, p. 129-132	X	26 juillet 1847	4
1847	Mémoire sur diverses propositions relatives à la théorie des nombres	CRAS	25, p. 132-136, 177-182, 242-243	X	26 juillet, 2 et 9 août 1847	10
1847	Mémoire sur les racines des équivalences correspondantes à des modules quelconques premiers et non premiers, et sur les avantages que présente l'emploi de ces racines dans la théorie des nombres	CRAS	25, p. 37-46	X	12 juillet 1847	10
1847	Mémoire sur la disposition des nombres entiers en facteurs radicaux	CRAS	25, p. 46-54	Kummer	12 juillet 1847	11
1847	Mémoire sur les indices modulaires des polynômes radicaux que fournissent les puissances et produits des racines de la résolvante d'une équation binôme	CRAS	25, p. 93-99	Gauss, Jacobi, Legendre	19 juillet 1847	8