Etudes sur les équations de Ramanujan-Nagell et de Nagell-Ljunggren ou semblables

Benjamin Dupuy

numéro d'ordre : 3819

THESE

pour l'obtention du Grade de

DOCTEUR DE L'UNIVERSITE BORDEAUX I

spécialité : Mathématiques Pures

soutenue le 3 juillet 2009 par

Dupuy Benjamin

Directeur de thèse : Y. Bilu

ETUDES SUR LES EQUATIONS DE RAMANUJAN-NAGELL ET DE NAGELL-LJUNGGREN OU SEMBLABLES

---

composition du jury

D. Benois	Université de Bordeaux	examinateur
Y. Bilu	Université de Bordeaux	examinateur
Y. Bugeaud	Université de Strasbourg	rapporteur
H. Cohen	Université de Bordeaux	examinateur
F. Luca	Université nationale autonome de Mexico	rapporteur
N. Ratazzi	Université Paris Sud	examinateur

–2009–

A la mémoire de ma mère

"[1]Passant, sous ce tombeau repose Diophante.
Ces quelques vers tracés par une main savante
Vont te faire connaître à quel âge il est mort.
Des jours assez nombreux que lui compta le sort,
Le sixième marqua le temps de son enfance ;
Le douzième fut pris par son adolescence.
Des sept parts de sa vie, une encore s'écoula,
Puis s'étant marié, sa femme lui donna
Cinq ans après un fils qui, du destin sévère
Reçut de jours hélas, deux fois moins que son père.
De quatre ans, dans les pleurs, celui-ci survécut.
Dis, tu sais compter, à quel âge il mourut."

[1]Extrait d'Eutrope, publié en 369 dans "L'Abrégé de l'Histoire Romaine", traduit en alexandrins par Emile Fourrey (Récréations Mathématiques, 1899).

Remerciements

Tout d'abord, je tiens à exprimer ma plus profonde gratitude à mon directeur de Thèse Yuri Bilu, pour ses encouragements, ses conseils, sa disponibilité et sa gentillesse.

Je remercie le professeur Florian Luca pour les discussions que l'on a eu. Elles ont grandement contribué à améliorer les résultats du chapitre 3 et du chapitre 5, ainsi qu'à simplifier les démonstrations de ce dernier.

Merci à Gaëlle, qui, malgré une épreuve personnelle très difficile, m'a toujours soutenu de façon indéfectible. Je suis également très reconnaissant envers mes parents Mireille, Lucien et ma soeur Delphine pour tout ce qu'ils ont fait pour moi.

Enfin, qu'il me soit permis de rendre ici un dernier hommage à ma mère, décédée quelques semaines après la soutenance de cette thèse. Elle fut non seulement une mère fantastique, mais aussi un très brillant professeur. Je dédie cette thèse à sa mémoire.

Table des matières

Introduction

Dans cette thèse on étudie deux types d'équation diophantiennes. Les premières sont de la forme $\frac{x^p+y^p}{x+y} = p^e z^q$, $(x, y, z) = 1$, c'est à dire de type Nagell-Ljunggren. Ce type d'équation avec $y = -1$, p, q premiers impairs distincts a récemment été étudié par Mihăilescu, notamment suite à sa résolution du problème de Catalan $x^p - y^q = 1$. Dans [54] il a montré pour une certaine classe de premiers $p \neq q$, que l'existence de solutions entières à $\frac{x^p-1}{x-1} = py^q$ n'est possible que si q est un diviseur premier de h_p^-, essayant ainsi de généraliser un critère de Bugeaud et Hanrot (voir [20]) sur l'équation de Catalan.

Dans le premier chapitre, on se propose d'étendre son résultat en montrant que $q > 2$ est bien alors un diviseur premier de h_p^- sans aucune condition sur p autres que $p \neq q$, $p > 3$. On trouvera à la fin du chapitre deux, un nouvel exemple de couples de premiers impairs distincts (p, q) pour lesquels $q \nmid h_p^-$. On s'appuiera sur un résultat récent (1998) de Steiner (voir [73]). L'étude de cette équation sera prolongée au chapitre 6 et 7 pour $y = y_0$ fixé vérifiant certaines conditions. On en déduira de nouveaux critères d'existence de solutions à des équations du type $X^p + Y_0^p = BZ^q$.

Pour ce type de solutions, l'extension d'un théorème de Bugeaud-Hanrot sur les idéaux de Mihăilescu généralisés nous permettra également de donner une borne de X en termes de p, q et Y_0 sous certaines conditions portant sur p, q et B. Le cas $B = 1$, c'est à dire l'équation $X^p + Y_0^p = Z^q$ fera l'objet d'un traitement à part. Des arguments "locaux" d'une part, et notre théorème sur les idéaux de Mihăilescu généralisés d'autre part, nous permettra de montrer que q est un facteur premier de h_{pq}^- en cas d'existence de solutions primitives. Le cas $Y_0 = 1$ redonne par exemple une version faible (par le critère de Masley-Montgomery) du critère de Bugeaud-Hanrot sur Catalan. Divers autres applications seront donnés, comme une extension des résultats de Terai sur l'équation du même nom.

Le cas $p = q$, c'est à dire $X^p + Y_0^p = BZ^p$ a été traité. On a étudié d'abord l'équation de Nagell-Ljunggren dite diagonale $\frac{x^p+y^p}{x+y} = p^e z^p$. Si elle admet des solutions primitives vérifiant $xy(x^2 - y^2) \neq 0 \bmod p$, on peut montrer que le p-rang du groupe des classes relatives du p-ième corps cyclotomique est strictement supèrieur à $\sqrt{p}$: c'est une simple adaptation de la démonstration d'un résultat d'Eichler sur le problème de Fermat. Le cas

$p|x$ est plus difficile. Mihăilescu a réussi à montrer dans [53] le critère très intéressant $p|h_p^+$ pour $y = 1$,$p > 17$ et $p^3|x$. Au chapitre 5, on prolonge cette étude au cas $p|x$, $y = y_0 \neq 0$ entier fixé, $p > 17$. On commencera par donner une nouvelle borne particulièrement petite de $|x|$ en fonction de $|y_0|$ et p. Si $|y_0| < \frac{p}{19}$, on montrera également que la condition $p|h_p^+$ reste valide. On en déduira de nouveaux résultats sur les équations diophantiennes du type $X^p + Y_0^p = BZ^p$, habituellement étudiées pour de petites valeurs de p (voir [5]).

L'étude de l'existence de solutions primitives à $X^p + Y_0^p = BZ^q$, dans le cas $q = 2$ fera l'objet du chapitre 3. On y étudiera plus précisément les équations de la forme $CX^2+b^{2m}D = Y^n$, n et b premiers. On montrera sous certaines conditions portant sur C, D et n que nécessairement $n = 3$ ou 5. Le cas $n = 3$ sera complètement résolu : des conditions nécessaires et suffisantes à l'existence de solutions primitives seront données ; si elles sont satisfaites, on donnera les valeurs explicites de ces solutions. Dans le cas $n = 5$, on donnera également des conditions nécessaires et suffisantes à l'existence de solutions primitives ; si elles sont satisfaites, on montrera qu'il existe un entier k tel que $Y = U_{3k+1}$ ou U_{3k+2}, U étant la suite de Lucas ou de Fibonacci. Une borne explicite sur k sera fournie. Diverses applications seront données. Par exemple, on caractérisera toutes les puissances entières de 3 de la forme $a^m - b^n$, précisant au passage les valeurs de (a, b, m, n). On appliquera également nos résultats à l'équation d'Aigner $X^2 + 4D = Y^p$, $(X, Y) = 1$, $p \nmid h(-D)$ que l'on résoudra complètement, affinant ainsi un résultat de Bugeaud. Très récemment (2008), Muriefah a résolu complètement dans [60] l'équation $px^2+2^{2m} = y^p$, $x \neq 0$, où $p \neq 7 \bmod 8$ est premier impair. On complètera son travail en résolvant complètement $Cx^2 + 2^{2m} = y^p$, $x \neq 0$, où $C \neq 7 \bmod 8$ est un entier sans facteur carré. Le cas où 2 est remplacé par un premier $q \neq p$ sera également traité, complétant également [60].

Le chapitre 8 est un chapitre indépendant des autres. On y donne deux nouvelles démonstrations de la valeur de la signature du Frobenius d'un corps fini. La première est nettement plus simple que toutes celles déjà données dans [36] et [79]. En guise d'application, on en déduit immédiatement la parité du nombre de polynômes unitaires irréductibles à coefficients dans un corps fini, et de degrés divisant un entier fixé à l'avance.

Chapitre 1

A class number criterion for the equation $\frac{x^p-1}{x-1} = py^q$

1.1 Introduction

Let p be an odd prime number and let

$$\Phi(x) = \Phi_p(x) = \frac{x^p - 1}{x - 1}$$

be the p-th cyclotomic polynomial. It is well-known that, for $x \in \mathbb{Z}$, the integer $\Phi(x)$ is divisible by at most the first power of p. More precisely, $p \nmid \Phi(x)$ if $x \not\equiv 1 \bmod p$, and $p \parallel \Phi(x)$ if $x \equiv 1 \bmod p$.

Indeed, if $p \mid \Phi(x)$ then $x^p \equiv 1 \bmod p$, which implies $x \equiv 1 \bmod p$. Now, using the binomial formula, we obtain

$$\Phi(x) = \frac{(1 + (x-1))^p - 1}{x - 1} = p + \sum_{k=2}^{p-1} \binom{p}{k} (x-1)^{k-1} + (x-1)^{p-1} \equiv p \bmod p^2,$$

which implies $p \parallel \Phi(x)$.

Let q be another prime number. A classical Diophantine problem, studied, most recently, by Mihăilescu [55, 54], is whether the p-free part of $\Phi(x)$ can be a q-th power. The can be rephrased as follows : given $e \in \{0, 1\}$, does the equation $\Phi(x) = p^e y^q$ have a non-trivial solution in integers x and y? (By *trivial* solutions we mean those with $x = e = 0$ and $x = e = 1$.)

The case $e = 0$, that is, the equation $\Phi(x) = y^q$ is (a particular case of) the classical *Nagell-Ljunggren equation*. It is known to have several non-trivial solutions, and it is commonly believed that no other solutions exist. See [15] for a comprehensive survey of results on this equation and methods for its analysis.

In the present note we study the case $e = 1$, that is, the equation

$$\frac{x^p - 1}{x - 1} = py^q. \tag{1.1}$$

(As we have seen above, any solution of this equation must satisfy $x \equiv 1 \bmod p$.)

Let h_p^- be the p-th relative class number. Mihăilescu [54, Theorem 1] proved that (1.1) has no non-trivial solutions if $q \nmid h_p^-$ and, in addition, some complicated technical condition involving p and q is satisfied. In this note we show that this technical condition is not required.

Theorem 1.1.1 *Let p and q be distinct odd prime numbers, $p \geq 5$. Assume that q does not divide the relative class number h_p^-. Then (1.1) has no solutions in integers $x, y \neq 1$.*

In particular, since $h_p^- = 1$ for $p \leq 19$, equation (1.1) has no non-trivial solutions when $5 \leq p \leq 19$. (Neither does it have solutions when $p = 3$, as it was shown long ago by Nagell [62].)

The interest to equation (1.1) was inspired by the fact that it is closely related to the celebrated equation of Catalan $x^p - z^q = 1$. In fact, Cassels [27] showed that any non-trivial solution of Catalan's equation gives rise to a solution of (1.1). All major contributions to the theory of Catalan's equation, including Mihăilescu's recent solution [7, 56], have Cassels' result as the starting point.

This article is strongly inspired by the work of Mihăilescu [56, 55, 54]. In particular, the argument in the case $q \not\equiv 1 \bmod p$ (see Section 1.6) can be found in [55]. However, the case $q \equiv 1 \bmod p$ (see Section 1.7) requires new ideas.

1.2 The cyclotomic field

Let p be an odd prime number and let $\zeta = \zeta_p$ be a primitive p-th root of unity. In this section we collect several facts about the p-th cyclotomic field $K = \mathbb{Q}(\zeta)$. As usual, we denote by $K^+ = K \cap \mathbb{R} = \mathbb{Q}(\zeta + \bar{\zeta})$ the maximal real subfield of K. (Here and below $z \mapsto \bar{z}$ stands for the "complex conjugation" map.) We denote by $\mathcal{O}$ the rings of integers of K; it is well-known that $\mathcal{O} = \mathbb{Z}[\zeta]$.

We denote by $\mathfrak{p}$ the principal ideal $(1 - \zeta)$. It is the only prime ideal of the field K above p, and $\mathfrak{p}^{p-1} = (p)$. For $k \not\equiv \ell \bmod p$ the algebraic number

$$\frac{\zeta^k - \zeta^\ell}{1 - \zeta}$$

is a unit of K (called *cyclotomic* or *circular* unit); in other words, we have

$$\left(\zeta^k - \zeta^\ell\right) = \mathfrak{p}.$$

In particular,

$$\zeta^k + \zeta^\ell = \frac{\zeta^{2k} - \zeta^{2\ell}}{1-\zeta} \Big/ \frac{\zeta^k - \zeta^\ell}{1-\zeta}$$

is a unit in K. All this will also be frequently used without special reference.

Finally, recall that $h_p^+ \mid h_p$, where h_p and h_p^+ are the class numbers of K and K^+, respectively, and the relative class number is defined by $h_p^- = h_p/h_p^+$.

The proofs of all statements above can be found in the first chapters of any course of the theory of cyclotomic fields; see, for instance, [77].

The following observation provides a convenient tool for calculating traces of algebraic integers from K modulo p. We denote by $\mathbb{F}_p$ the field of p elements, and we let $\mathrm{Tr} : K \to \mathbb{Q}$ be the trace map.

Proposition 1.2.1 *Let $\rho : \mathcal{O} \to \mathbb{F}_p$ be the reduction modulo $\mathfrak{p}$. Then for any $a \in \mathcal{O}$ we have*

$$\rho(a) \equiv -\mathrm{Tr}(a) \bmod p. \tag{1.2}$$

Proof We have $\rho(\zeta^n) = 1$ for all $n \in \mathbb{Z}$, and

$$\mathrm{Tr}(\zeta^n) = \begin{cases} -1, & p \nmid n, \\ p-1, & p \mid n \end{cases} \tag{1.3}$$

Hence (1.2) holds for $a = \zeta^n$. By linearity, it extends to $\mathcal{O} = \mathbb{Z}[\zeta]$. ■

Here is an example of how one can use this.

Corollary 1.2.2 *For any $u \in \mathbb{Z}$ put*

$$\chi_u = \frac{\zeta^u - \zeta}{(1+\zeta^u)(1-\zeta)}. \tag{1.4}$$

Then

$$2\mathrm{Tr}(\chi_u) \equiv u - 1 \bmod p. \tag{1.5}$$

In particular, $\mathrm{Tr}(\chi_u) \not\equiv 0 \bmod p$ unless $u \equiv 1 \bmod p$.

Proof For $u \equiv 1 \bmod p$ we have $\chi_u = 0$ and there is nothing to prove. Now let $u \not\equiv 1 \bmod p$. We may assume that $u > 0$. We have

$$\rho\left(\frac{\zeta^u - \zeta}{1-\zeta}\right) = \rho\left(-\zeta - \zeta^2 - \cdots - \zeta^{u-1}\right) = 1 - u.$$

Also, since $1 + \zeta^u$ is a unit, we have

$$\rho\left(\frac{1}{1+\zeta^u}\right) = \rho(1+\zeta^u)^{-1} = \frac{1}{2}.$$

Hence $\rho(\chi_u) = (1-u)/2$, which implies (1.5). ■

In the following example we cannot use (1.2) because the number we are interested in is not an algebraic integer.

Proposition 1.2.3 *We have*

$$\mathrm{Tr}\left(\frac{\zeta}{(1-\zeta)^2}\right) = \frac{1-p^2}{12}.$$

Proof Consider the rational function

$$F(t) = \sum_{k=1}^{p-1} \frac{\zeta^k t}{(1-\zeta^k t)^2}.$$

Using (1.3), we obtain

$$\begin{aligned} F(t) &= -\sum_{k=1}^{p-1}\sum_{n=1}^{\infty} n\zeta^{kn}t^n = -\sum_{n=1}^{\infty} n\mathrm{Tr}(\zeta^n)t^n \\ &= \sum_{n=1}^{\infty} nt^n - p^2\sum_{n=1}^{\infty} nt^{pn} = -\frac{t}{(1-t)^2} + \frac{p^2t^p}{(1-t^p)^2}. \end{aligned}$$

When $t \to 1$ we have

$$\begin{aligned} \frac{t}{(1-t)^2} &= \frac{1}{(t-1)^2} + \frac{1}{t-1}, \\ \frac{p^2t^p}{(1-t^p)^2} &= \frac{1}{(t-1)^2} + \frac{1}{t-1} + \frac{1-p^2}{12} + o(1). \end{aligned}$$

Hence

$$\mathrm{Tr}\left(\frac{\zeta}{(1-\zeta)^2}\right) = F(1) = \frac{1-p^2}{12}.$$ ■

1.3 Binomial power series

We shall need a property of binomial power series in the non-archimedean domain. As usual, we denote by $\mathbb{Z}_p$ and $\mathbb{Q}_p$ the ring of p-adic integers and the field of p-adic numbers, and we extend the standard p-adic absolute value from $\mathbb{Q}_p$ to the algebraic closure $\bar{\mathbb{Q}}_p$.

Given $a \in \mathbb{Z}_p$, we let

$$R_a(t) = (1+t)^a = 1 + at + \binom{a}{2}t^2 + \binom{a}{3}t^3 + \dots$$

be the binomial power series. Its coefficients are p-adic integers, and for any τ, algebraic over $\mathbb{Q}_p$ and with $|\tau|_p < 1$, our series converges at $t = \tau$ in the field $\mathbb{Q}_p(\tau)$. For any $n = 0, 1, \dots$ we have the obvious inequality

$$\left| R_a(\tau) - \sum_{k=0}^{n} \binom{a}{k}\tau^k \right|_p \leq |\tau|_p^{n+1}.$$

When a is p-adically small, a sharper inequality may hold. For instance,

$$|R_p(\tau) - (1+p\tau)|_p \leq p|\tau|_p^2$$

when $|\tau|_p$ is sufficiently small. We shall need a result of this kind for the second order Taylor expansion.

It will be convenient to use the familiar notation $O(\cdot)$ in a slightly non-traditional fashion : we say $\tau = O(\upsilon)$ if $|\tau|_p \leq |\upsilon|_p$.

Proposition 1.3.1 *Assume $p \geq 5$ and that $|\tau| \leq p^{-1/(p-3)}$. Then*

$$R_a(\tau) = 1 + a\tau - \frac{a}{2}\tau^2 + O\left(a^2\tau^2\right) + O\left(a\tau^3\right). \tag{1.6}$$

Proof Since

$$\frac{a(a-1)}{2}\tau^2 = -\frac{a}{2}\tau^2 + O\left(a^2\tau^2\right),$$

equality (1.6) is an immediate consequence of

$$R_a(\tau) = 1 + a\tau + \frac{a(a-1)}{2}\tau^2 + O\left(a\tau^3\right), \tag{1.7}$$

so it suffices to prove the latter.

We prove (1.7) by induction in the p-adic order of a. When $|a|_p = 1$, equality (1.7) is an immediate consequence of the binomial formula (and holds even under the weaker

assumption $|\tau|_p < 1$). Now assume that (1.7) holds for certain $a \in \mathbb{Z}_p$, and let us show that it holds with a replaced by pa.

By the induction hypothesis, $R_a(\tau) = 1 + \upsilon$, where

$$\upsilon = a\tau + \frac{a(a-1)}{2}\tau^2 + O\left(a\tau^3\right).$$

Then

$$\begin{aligned} R_{pa}(\tau) = (1+\upsilon)^p &= 1 + p\upsilon + \frac{p(p-1)}{2}\upsilon^2 + O\left(p\upsilon^3\right) + O\left(\upsilon^p\right) \\ &= 1 + pa\tau + \frac{pa(a-1)}{2}\tau^2 + \frac{pa^2(p-1)}{2}\tau^2 + O\left(pa\tau^3\right) + O\left((a\tau)^p\right) \\ &= 1 + pa\tau + \frac{pa(pa-1)}{2}\tau^2 + O\left(pa\tau^3\right) + O\left((a\tau)^p\right). \end{aligned} \tag{1.8}$$

Since $|\tau| \le p^{-1/(p-3)}$, we have $|(a\tau)^p|_p \le |pa^p\tau^3|_p \le |pa\tau^3|_p$. Hence the term $O\left((a\tau)^p\right)$ in (1.8) can be disregarded. This completes the proof of (1.7) and of the proposition. ■

1.4 A special unit of the cyclotomic field

We start the proof of Theorem 1.1.1. We fix, once and for all, distinct odd prime numbers p and q, and rational integers $x, y \neq 1$ satisfying (1.1). Recall that

$$x \equiv 1 \bmod p,$$

this congruence being frequently used in the sequel without special reference. Also, we use without special reference the notation of Section 1.2.

In this section, we construct a special unit of the field K, which plays the central role in the proof of Theorem 1.1.1. Our starting point is the following well-known statement.

Proposition 1.4.1 *Put*

$$\alpha = \frac{x - \zeta}{1 - \zeta}.$$

Then we have the following.

1. *The principal ideal (α) is a q-th power of an ideal of K.*
2. *Assume that q does not divide the relative class number h_p^-. Then $\bar{\alpha}/\alpha$ is a q-th power in K.*

Though the proof can be found in the literature, we include it here for the reader's convenience. We closely follow [10].

Proof Since

$$\Phi_p(x) = (x-\zeta)\cdots(x-\zeta^{p-1}),$$
$$p = \Phi_p(1) = (1-\zeta)\cdots(1-\zeta^{p-1}),$$

we may re-write equation (1.1) as

$$\prod_{k=1}^{p-1} \frac{x-\zeta^k}{1-\zeta^k} = y^q. \tag{1.9}$$

Since $p = \mathfrak{p}^{p-1} \mid (x-1)$, we have $\mathfrak{p} \parallel (x-\zeta^k)$ for $k = 1, \ldots, p-1$. Hence the numbers

$$\alpha_k = \frac{x-\zeta^k}{1-\zeta^k} \qquad (k = 1, \ldots, p-1)$$

are algebraic integers coprime with $\mathfrak{p}$.

On the other hand, since

$$(1-\zeta^k)\alpha_k - (1-\zeta^\ell)\alpha_\ell = \zeta^\ell - \zeta^k,$$

the greatest common divisor of α_k and α_ℓ should divide $\mathfrak{p} = \left(\zeta^k - \zeta^\ell\right)$. Hence the numbers $\alpha_1, \ldots, \alpha_{p-1}$ are pairwise coprime. (In particular, α and $\bar{\alpha}$ are coprime, to be used in the proof of Proposition 1.4.2.) Now (1.9) implies that each of the principal ideals (α_k) is a q-th power of an ideal. This proves part 1.

Now write $(\alpha) = \mathfrak{a}^q$, where $\mathfrak{a}$ is an ideal of K. If $q \nmid h_p^-$ then the class of $\mathfrak{a}$ belongs to the real part of the class group. In other words, we have $\mathfrak{a} = \mathfrak{b}(\gamma)$, where $\gamma \in K^*$ and $\mathfrak{b}$ is a "real" ideal of K (that is, $\mathfrak{b} = \bar{\mathfrak{b}}$). Further, $\mathfrak{b}^q$ is a principal real ideal; in other words, $\mathfrak{b}^q = (\beta)$, where $\beta \in K^+$. We obtain $(\alpha) = (\beta\gamma^q)$, that is, α is equal to $\lambda\gamma^q$ times a unit of K.

Now recall that if η is a unit of cyclotomic field then $\bar{\eta}/\eta$ is a root of unity. Since $\bar{\beta} = \beta$, we obtain that $\bar{\alpha}/\alpha$ is $(\bar{\gamma}/\gamma)^q$ times a root of unity. Since every root of unity in K is a q-th power, we have shown that $\bar{\alpha}/\alpha$ is a q-th power. This proves part 2. ■

From now on **we assume that q does not divide h_p^-**. In particular, Proposition 1.4.1 implies that there exists $\mu \in K$ such that $\bar{\alpha}/\alpha = \mu^q$. Moreover, this μ is unique because K does not contain non-trivial q-th roots of unity. Similarly, the field K contains exactly one q-th root of $\alpha/\bar{\alpha}$. Since both $\bar{\mu}$ and μ^{-1} are q-th roots of $\alpha/\bar{\alpha}$, we have

$$\mu^{-1} = \bar{\mu} \tag{1.10}$$

This will be used in Section 1.5.

Now we are ready to construct the promised unit.

Proposition 1.4.2 *Let u be the inverse of q modulo p (that is, we have $uq \equiv 1 \bmod p$). Then the algebraic number $\phi = \alpha(\mu + \zeta^u)^q$ is a unit of the field K.*

Proof Write the principal ideal (μ) as $\mathfrak{a}\mathfrak{b}^{-1}$, where $\mathfrak{a}$ and $\mathfrak{b}$ are co-prime integral ideals of K. Then $(\bar{\alpha}/\alpha) = \mathfrak{a}^q\mathfrak{b}^{-q}$. Moreover, since α and $\bar{\alpha}$ are coprime (see the proof of Proposition 1.4.1), we have $(\bar{\alpha}) = \mathfrak{a}^q$ and $(\alpha) = \mathfrak{b}^q$.

Further, we have $(\mu + \zeta^u) = \mathfrak{c}\mathfrak{b}^{-1}$, where $\mathfrak{c}$ is yet another integral ideal of K. We obtain $(\phi) = \mathfrak{b}^q\mathfrak{c}^q\mathfrak{b}^{-q} = \mathfrak{c}^q$, which shows that ϕ is an algebraic integer.

Next, put

$$\phi' = \alpha^{q-1}\left(\sum_{k=0}^{q-1}\mu^k(-\zeta^u)^{q-1-k}\right)^q.$$

The same argument as above yields that ϕ' is an algebraic integer as well. Further,

$$\phi\phi' = \alpha^q\left((\mu+\zeta^u)\sum_{k=0}^{q-1}\mu^k(-\zeta^u)^{q-1-k}\right)^q = \left(\alpha\left(\mu^q+\zeta^{uq}\right)\right)^q.$$

Now recall that $\mu^q = \bar{\alpha}/\alpha$ and that $uq \equiv 1 \bmod p$. The latter congruence implies that $\zeta^{uq} = \zeta$, and we obtain

$$\phi\phi' = \left(\alpha\left(\bar{\alpha}/\alpha + \zeta\right)\right)^q = (\bar{\alpha} + \zeta\alpha)^q = (1+\zeta)^q.$$

Since $1 + \zeta$ is a unit of K, so are ϕ and ϕ'. ■

1.5 An analytic expression for μ

We shall work in the local field $K_{\mathfrak{p}} = \mathbb{Q}_p(\zeta)$. As before, we extend p-adic absolute value from $\mathbb{Q}_p$ to $K_{\mathfrak{p}}$, so that $|1-\zeta|_p = p^{-1/(p-1)}$.

Since p totally ramifies in K, every automorphism σ of $K/\mathbb{Q}$ extends to an automorphism of $K_{\mathfrak{p}}/\mathbb{Q}_p$. In particular, the "complex conjugation" $z \mapsto \bar{z}$ extends to an automorphism of $K_{\mathfrak{p}}/\mathbb{Q}_p$ (we continue to call it "complex conjugation").

Let $R_a(t)$ be the binomial power series, introduced in Section 1.3. Since the automorphisms of $K_{\mathfrak{p}}/\mathbb{Q}_p$ (in particular the "complex conjugation") are continuous in the $\mathfrak{p}$-adic topology, for any $\tau \in K_{\mathfrak{p}}$ with $|\tau|_p < 1$ and for any $\sigma \in \mathrm{Gal}(K_{\mathfrak{p}}/\mathbb{Q}_p)$ we have $R_a(\tau)^\sigma = R_a(\tau^\sigma)$. In particular, $\overline{R_a(\tau)} = R_a(\bar{\tau})$.

Put

$$\lambda = \frac{x-1}{1-\zeta},$$

so that

$$\alpha = 1+\lambda, \qquad \bar{\alpha} = 1+\bar{\lambda} = 1-\zeta\lambda$$

(recall that α is defined in Proposition 1.4.1). Then

$$|\lambda|_p = |x-1|_p p^{1/(p-1)} \le p^{-\frac{p-2}{p-1}} < 1,$$

and similarly for $\bar{\lambda}$. In particular, for any $a \in \mathbb{Z}_p$, the series $R_a(t)$ converges at $t = \lambda$ and $t = \bar{\lambda}$.

We wish express the quantity μ, introduced in Section 1.4, in terms of the binomial power series. Since both μ and $R_{1/q}(\bar{\lambda})R_{-1/q}(\lambda)$ are q-th roots of $\bar{\alpha}/\alpha$, we have

$$\mu = R_{1/q}(\bar{\lambda})R_{-1/q}(\lambda)\xi, \tag{1.11}$$

where $\xi \in K_{\mathfrak{p}}$ is a q-th root of unity. We want to show that $\xi = 1$.

The field $\mathbb{Q}_p(\xi)$ is an unramified sub-extension of the totally ramified extension $K_{\mathfrak{p}}$. Hence $\mathbb{Q}_p(\xi) = \mathbb{Q}_p$, that is, $\xi \in \mathbb{Q}_p$. It follows that ξ is stable with respect to all automorphisms of $K_{\mathfrak{p}}/\mathbb{Q}_p$; in particular, it is stable with respect to the "complex conjugation" : $\bar{\xi} = \xi$.

Applying the "complex conjugation" to (1.11) and using (1.10), we obtain $\mu^{-1} = R_{1/q}(\lambda)R_{-1/q}(\bar{\lambda})\xi$ which, together with (1.11), implies that $\xi^2 = 1$. Since ξ is a q-th root of unity, this is possible, only if $\xi = 1$.

We have shown that

$$\mu = R_{1/q}(\bar{\lambda})R_{-1/q}(\lambda) = R_{1/q}(-\zeta\lambda)R_{-1/q}(\lambda), \tag{1.12}$$

The rest of the proof splits into two cases, depending on whether $q \not\equiv 1 \bmod p$ or $q \equiv 1 \bmod p$. The arguments in both cases are quite similar, but the latter case is technically more involved.

1.6 The case $q \not\equiv 1 \bmod p$

We have

$$\mu = R_{1/q}(-\zeta\lambda)R_{-1/q}(\lambda) = 1 - \frac{1+\zeta}{q}\lambda + O\left(\lambda^2\right),$$

where, as in Section 1.3, we say that $\tau = O(\upsilon)$ if $|\tau|_p \le |\upsilon|_p$.

Hence, for the quantity ϕ, introduced in Proposition 1.4.2, we have

$$\begin{aligned}
\phi &= (1+\lambda)\left(1 + \zeta^u - \frac{1+\zeta}{q}\lambda + O\left(\lambda^2\right)\right)^q \\
&= (1+\zeta^u)^q\,(1+\lambda)\left(1 - \frac{1+\zeta}{1+\zeta^u}\lambda\right) + O\left(\lambda^2\right) \\
&= (1+\zeta^u)^q\left(1 + \frac{\zeta^u - \zeta}{1+\zeta^u}\lambda\right) + O\left(\lambda^2\right) \\
&= (1+\zeta^u)^q\,(1 + (x-1)\chi_u) + O\left(\lambda^2\right),
\end{aligned} \tag{1.13}$$

where χ_u is defined in (1.4).

Since the automorphisms of $K/\mathbb{Q}$ extend to automorphisms of $K_{\mathfrak{p}}/\mathbb{Q}_p$, the same is true for the norm and the trace maps : for any $a \in K$ we have

$$\mathcal{N}_{K_{\mathfrak{p}}/\mathbb{Q}_p}(a) = \mathcal{N}_{K/\mathbb{Q}}(a), \qquad \mathrm{Tr}_{K_{\mathfrak{p}}/\mathbb{Q}_p}(a) = \mathrm{Tr}_{K/\mathbb{Q}}(a).$$

In the sequel, we shall simply write $\mathcal{N}(a)$ and $\mathrm{Tr}(a)$. Also, since the automorphisms are continuous, we have $|\mathcal{N}(a)|_p \leq |a|_p^{p-1}$ and $|\mathrm{Tr}(a)|_p \leq |a|_p$.

Taking the norm in (1.13), we obtain

$$\mathcal{N}\left(\frac{\phi}{(1+\zeta^u)^q}\right) = 1 + (x-1)\mathrm{Tr}(\chi_u) + O(\lambda^2).$$

Since both ϕ and $1+\zeta^u$ are units, the norm on the left is ± 1. Since $-1 \not\equiv 1 \bmod p$, the norm is 1, and we obtain $(x-1)\mathrm{Tr}(\chi_u) = O(\lambda^2)$.

But, since $q \not\equiv 1 \bmod p$, we have also $u \not\equiv 1 \bmod p$. Corollary (1.2.2) implies that $\mathrm{Tr}(\chi_u)$ is not divisible by p. We obtain

$$|x-1|_p \leq |\lambda|_p^2 = |x-1|_p^2 p^{2/(p-1)}.$$

which implies $|x-1|_p \geq p^{-2/(p-1)}$. Since $p \mid (x-1)$, this is impossible as soon as $p \geq 5$.

This proves the theorem in the case $q \not\equiv 1 \bmod p$.

1.7 The case $q \equiv 1 \bmod p$

We have (1.12). Also, $u \equiv 1 \bmod p$ and $\chi_u = 0$, which means that the first order Taylor expansions are no longer sufficient. We shall use the second order expansion. Put $a = (q-1)/q$, so that $|a|_p \leq p^{-1}$, and re-write (1.12) as

$$\mu = (1-\zeta\lambda)R_{-a}(-\zeta\lambda)(1+\lambda)^{-1}R_a(\lambda). \tag{1.14}$$

For $p \geq 5$ we have

$$|\lambda|_p \leq p^{-\frac{p-2}{p-1}} \leq p^{-1/(p-3)},$$

which means that Proposition 1.3.1 applies to $\tau = \lambda$. We obtain

$$R_{-a}(-\zeta\lambda) = 1 + a\zeta\lambda + \frac{\zeta^2}{2}a\lambda^2 + O\left(a\lambda^3\right) + O\left(a^2\lambda^2\right),$$
$$R_a(\lambda) = 1 + a\lambda - \frac{a}{2}\lambda^2 + O\left(a\lambda^3\right) + O\left(a^2\lambda^2\right).$$

Substituting this in (1.14), we get

$$\begin{aligned}\mu =&(1-\zeta\lambda)\left(1+a\zeta\lambda+\frac{a}{2}\zeta^2\lambda^2\right)(1+\lambda)^{-1}\left(1+a\lambda-\frac{a}{2}\lambda^2\right)\\&+O\left(a\lambda^3\right)+O\left(a^2\lambda^2\right)\\=&\left(1+(-\zeta+a+a\zeta)\lambda-\frac{(1+\zeta)^2}{2}a\lambda^2\right)(1+\lambda)^{-1}\\&+O\left(a\lambda^3\right)+O\left(a^2\lambda^2\right).\end{aligned}$$

It follows that

$$\begin{aligned}\phi =&(1+\lambda)(\mu+\zeta)^q\\=&\left(1+(-\zeta+a+a\zeta)\lambda-\frac{(1+\zeta)^2}{2}a\lambda^2+\zeta(1+\lambda)\right)^q(1+\lambda)^{1-q}\\&+O\left(a\lambda^3\right)+O\left(a^2\lambda^2\right)\\=&(1+\zeta)^q\left(1+a\lambda-\frac{1+\zeta}{2}a\lambda^2\right)^{1+a/(1-a)}(1+\lambda)^{-a/(1-a)}\\&+O\left(a\lambda^3\right)+O\left(a^2\lambda^2\right).\end{aligned}$$

Applying Proposition 1.3.1 with the exponents $\pm a/(1-a)$ and taking into account the inequality $|a|_p<1$, we find :

$$\begin{aligned}\left(1+a\lambda-\frac{1+\zeta}{2}a\lambda^2\right)^{a/(1-a)}&=1+\frac{a^2}{1-a}\lambda+O\left(a^2\lambda^2\right),\\(1+\lambda)^{-a/(1-a)}&=1-\frac{a}{1-a}\lambda+\frac{a}{2(1-a)}\lambda^2+O\left(a\lambda^3\right)\\&=1-\frac{a}{1-a}\lambda+\frac{a}{2}\lambda^2+O\left(a\lambda^3\right)+O\left(a^2\lambda^2\right).\end{aligned}$$

Taking everything together, we obtain

$$\begin{aligned}\frac{\phi}{(1+\zeta)^q}=&\left(1+a\lambda-\frac{1+\zeta}{2}a\lambda^2\right)\left(1+\frac{a^2}{1-a}\lambda\right)\left(1-\frac{a}{1-a}\lambda+\frac{a}{2}\lambda^2\right)\\&+O\left(a\lambda^3\right)+O\left(a^2\lambda^2\right)\\=&1-\frac{\zeta}{2}a\lambda^2+O\left(a\lambda^3\right)+O\left(a^2\lambda^2\right)\\=&1-\frac{\zeta}{2(1-\zeta)^2}a(x-1)^2+O\left(a\lambda^3\right)+O\left(a^2\lambda^2\right).\end{aligned}$$

Now we complete the proof in the same fashion as in Section 1.6. Taking the norm, we find

$$\pm 1=1-\frac{1}{2}\mathrm{Tr}\left(\frac{\zeta}{(1-\zeta)^2}\right)a(x-1)^2+O\left(a\lambda^3\right)+O\left(a^2\lambda^2\right). \tag{1.15}$$

The -1 on the left is again impossible, and if we have 1 on the left of (1.15), then, in view of Proposition 1.2.3, we must have the inequality

$$\begin{aligned} |x-1|_p^2 &\leq \max\left\{|\lambda|_p^3, |a|_p|\lambda|_p^2\right\} \\ &= \max\left\{|x-1|_p^3 p^{3/(p-1)}, |a|_p|x-1|_p^2 p^{2/(p-1)}\right\}, \end{aligned}$$

which means that either $|x-1|_p \geq p^{-3/(p-1)}$ or $|a|_p \geq p^{-2/(p-1)}$. But, for $p \geq 5$, neither of the latter inequalities can hold, because $|x-1|_p \leq p^{-1}$ and $|a|_p \leq p^{-1}$. The theorem is proved in the case $q \equiv 1 \bmod p$ as well.

1.8 On the equation $1 + x + x^2 = 3y^q$.

In this paragraph, we recall a Nagell's result and give a proof wich can be found in [28]. We begin by the following result :

Proposition 1.8.1 *Let $t \in \mathbb{N}^*$ and let p be an odd prime not dividing the class number of the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-t})$. The equation $ty^2 + 1 = 4x^p$ has no integer solution except for $t = 3$, for which it has the solutions $(x, y) = (1, \pm 1)$ for any p.*

Proof If the equation has a solution then $ty^2 \equiv 3 \bmod 4$, so y is odd, and hence $t \equiv 3 \bmod 4$. Furthermore, writing $-t = Df^2$ for a fundamental discriminant D, our equation is equivalent to $-D(fy)^2+1 = 4x^p$, so we may assume that $-t$ is a fundamental discriminant. In K our equation can be written $\beta\overline{\beta} = x^p$ with $\beta = \frac{1+y\sqrt{-t}}{2}$. Let $\mathbb{Z}_K$ be the ring of algebraic integers of K. Since $\beta + \overline{\beta} = 1$, the ideals $\beta\mathbb{Z}_K$ and $\overline{\beta}\mathbb{Z}_K$ are coprime, so that each is a pth power of an ideal. Since p does not divide the class number of K, we deduce that there exist $\alpha \in \mathbb{Z}_K$ and a unit ϵ of K such that $\beta = \epsilon\alpha^p$. Since K is imaginary quadratic, ϵ is a pth power, except perhaps in the case $(p, t) = (3, 3)$. Suppose $(p, t) \neq (3, 3)$, so that we can simply write $\beta = \alpha^p$. Setting $\alpha = \frac{a+b\sqrt{-t}}{2}$ with $a, b \in \mathbb{Z}$, since p is odd the equation $\beta + \overline{\beta} = 1$ translates into $(\gamma + a)^p - \gamma^p = 1$, with $\gamma = -\overline{\alpha} = \frac{-a+b\sqrt{-t}}{2} \in \mathbb{Z}_K$. Expanding the left-hand side of this equation by the binomial theorem we see that it is divisible by a, so that a is a unit, and therefore $a = \pm 1$. On the other hand, looking at the equation modulo $p\mathbb{Z}_K$ gives $a \equiv a^p \equiv 1 \bmod p$, so that we must have $a = 1$ since $p \neq 2$. Since $\gamma \neq 0$ (otherwise $\beta = (-\overline{\gamma})^p = 0$), we deduce that $P(\gamma) = 0$ where

$$P(X) = \frac{(X+1)^p - X^p - 1}{pX}.$$

Since p is prime, from the binomial theorem, $P \in \mathbb{Z}[X]$, P is monic with constant term 1, so that the roots of P are units. When $t \neq 3$, the units of K are ± 1, so the equation

$P(\gamma) = 0$ with $\gamma \in K$ implies that $\gamma = \pm 1$, so that

$$\frac{1 + y\sqrt{-t}}{2} = \beta = (-\overline{\gamma})^p = \pm 1$$

wich is impossible. When $t = 3$, the units of K are the 6th roots of unity, so similarly $\beta = \frac{1+y\sqrt{-3}}{2} = (-\overline{\gamma})^p$ is a 6th root of unity. The 6th root of unity of the form $\frac{1+y\sqrt{-3}}{2}$ being $\frac{1\pm\sqrt{-3}}{2}$, we have $y = \pm 1$, giving the two solutions for $t = 3$, and if $-t = -3f^2$ for $f > 1$ it also shows that there are no solutions for such t.

Suppose $(p, t) = (3, 3)$. There is ϵ a 6th root of unity such that $\beta = \epsilon\alpha^3$, $\alpha = \frac{a+b\sqrt{-3}}{2}$. We have $a = 1$ in this case too ($\beta + \overline{\beta} = 1$). Suppose $\epsilon = \pm 1$. This is a 3th power. As before, there is no integer solution. Suppose $\epsilon = \pm\frac{1+\sqrt{-3}}{2}$. There exist A, $B \in \mathbb{Z}$ such that

$$\frac{1 + y\sqrt{-3}}{2} = \beta = \frac{1 + \sqrt{-3}}{2}\left(\frac{A + B\sqrt{-3}}{2}\right)^3, \quad A = \pm 1.$$

Using the binomial theorem we find that $A = 1$, $B = \pm 1$ and $Y = -1$. Suppose $\epsilon = \pm\frac{1-\sqrt{-3}}{2}$. By the same method, we find that $A = -1$, $B = \pm 1$ and $Y = 1$. ■

Corollary 1.8.2 *(Nagell). Let $p \geq 3$ be a prime. The only integer solutions to the equation $1 + x + x^2 = 3y^p$ are $(x, y) = (1, 1)$ and $(x, y) = (-2, 1)$.*

Proof This equation is equivalent to $(2x + 1)^2 + 3 = 12y^p$; it follows that $3|(2x + 1)$. Setting $2x + 1 = 3z$, we obtain $3z^2 + 1 = 4y^p$, and the result follows from the proposition. ■

Chapitre 2

Théorèmes de factorisation, théorème de Steiner, théorèmes de Gannoukh, application diophantienne

Dans cette partie, on se fixe un nombre premier impair p. On note $\mathbb{K}$ le corps cyclotomique $\mathbb{Q}(\zeta)$, avec ζ racine primitive p-ième de l'unité. p étant fixé, on notera par h^-, au lieu de h_p^-, le nombre de classes relatives de $\mathbb{K}$.

2.0.1 Quelques lemmes préliminaires.

On se fixe une racine primitive modulo p, que l'on note g, avec $1 < g < p$. Si $n \in \mathbb{N}$, alors g_n désigne l'unique entier de $\{1, \ldots, p-1\}$, tel que $g^n \equiv g_n[p]$. Si x est un entier premier à p, il existe un unique entier $n \in \{1, \ldots, p-1\}$ tel que $x \equiv g^n \bmod p$. On note cet entier $Ind_g(x)$.

On se fixe aussi une racine primitive $p-1$ de l'unité, que l'on note ξ. Soient également les polynômes suivants :

$$F_p(X) = \sum_{n=0}^{p-2} g_n X^n. \tag{2.1}$$

On a alors :

Théorème 2.0.3

$$h^- = (2p)^{-\frac{p-3}{2}} \left| \prod_{n=0}^{\frac{p-3}{2}} F_p(\xi^{2n+1}) \right|. \tag{2.2}$$

Comme il est d'usage, on note Φ_k le k-ième polynôme cyclotomique. De plus, si m et un entier positif, on pose

$$\Omega_m(X) = \prod_{1 \le \mu \le m}^{*} (X - \rho^\mu), \quad \rho = e^{\frac{2i\pi}{m}} \tag{2.3}$$

où $*$ signifie que μ décrit les entiers impairs.

Lemme 2.0.4 *Si $m = 2^l m'$, avec m' impair, alors*

$$\Omega_m(X) = \prod_{\delta|m'} \Phi_{\frac{m}{\delta}}(X). \tag{2.4}$$

Preuve On a

$$\Omega_m(X) = \prod_{1\leq\mu\leq m}^{*} (X - \rho^\mu) = \prod_{\delta|m'} \prod_{(t,\frac{m}{\delta})=1} \left(X - \rho^{t\delta}\right) = \prod_{\delta|m'} \Phi_{\frac{m}{\delta}}(X).$$

□

Lemme 2.0.5 *Si $G(X) = G_p(X) = \sum_{n=0}^{p-2} g_n X^{p-n-2}$, alors*

$$h_p^- = (2p)^{-\frac{p-3}{2}} \prod_{n=0}^{\frac{p-3}{2}} G_p(\xi^{2n+1}). \tag{2.5}$$

Preuve Par définition de G_p, on a

$$G_p(X) = X^{p-2} F_p(X^{-1}). \tag{2.6}$$

En prenant $X = \xi^{2n+1}$ et en passant au module, on trouve

$$\left|G_p(\xi^{2n+1})\right| = |\xi^{2n+1}| \left|F_p(\xi^{-2n-1})\right| = \left|F_p(\xi^{2n'+1})\right|, n' = \frac{p-3}{2} - n. \tag{2.7}$$

Donc, on a la relation souhaitée, au signe près. Mais si n est un entier tel que $n \in \{0, \ldots, \frac{p-3}{2}\}$ et $n \neq n'$, alors, on peut ordonner le produit des $G_p(\xi^{2n+1})$ de sorte qu'apparaissent $|G_p(\xi^{2n+1})|^2$. Si $n = n'$ est impossible, le produit des $G_p(\xi^{2n+1})$ est donc positif et on a fini. Si $n = n'$ est possible, alors $n = n' = \frac{p-3}{2} - n$, ie $p \equiv 3[4]$, et $\xi^{2n+1} = -1$. Comme $p \equiv 3[4]$, $G_p(\xi^{2n+1}) = ph(\sqrt{-p}) \geq 0$. Dans tous les cas le produit est positif et on a la relation souhaitée.□

2.0.2 Première factorisation.

Soit P un polynôme de $\mathbb{Z}[X]$ unitaire. Soit $R(P)$ ses racines dans $\overline{\mathbb{Q}}$. Soit k un entier fixé. On pose

$$\Phi_k^*(P) = \prod_{r\in R(P)} \Phi_k(r). \tag{2.8}$$

Comme P est unitaire, $\Phi_k^*(P) = Res(\Phi_k, P) \in \mathbb{Z}$. L'application Φ_k^* est appelée la fonction de Pierce.

Théorème 2.0.6 *On pose $p-1=2^l w$, avec w impair. Le nombre de classes relatives h^- a un développement en produit d'entiers suivant :*

$$(2p)^{\frac{p-3}{2}}h^- = (-1)^{\frac{p-1}{2}}\prod_{d|w} Res(\Phi_{2^l d}, G_p) \tag{2.9}$$

Preuve Par le lemme (2.0.5), on a

$$\begin{aligned}
(2p)^{\frac{p-3}{2}}h^- &= \prod_{n=0}^{\frac{p-3}{2}} G_p(\xi^{2n+1}) \\
&= Res(G_p(X), \Omega_{p-1}(X)) \\
&= (-1)^{\frac{(p-1)(p-2)}{2}} Res(\Omega_{p-1}(X), G_p(X)) \\
&= (1)^{\frac{p-1}{2}} \prod_{i=0}^{p-1} \Omega_{p-1}(\alpha_i) \\
&= (1)^{\frac{p-1}{2}} \prod_{i=0}^{p-1} \prod_{\delta|w} \Phi_{\frac{p-1}{\delta}}(\alpha_i) \\
&= (1)^{\frac{p-1}{2}} \prod_{i=0}^{p-1} \prod_{d|w} \Phi_{2^l d}(\alpha_i) \\
&= (1)^{\frac{p-1}{2}} \prod_{d|w} \prod_{i=0}^{p-1} \Phi_{2^l d}(\alpha_i) \\
&= (1)^{\frac{p-1}{2}} \prod_{d|w} \Phi^*_{2^l d}(G_p).
\end{aligned} \tag{2.10}$$

□

2.0.3 Un théorème de Kummer.

Definition 2.0.7 *Soit p un nombre premier impair. On pose $p-1=2^\lambda w$, avec w impair. Soit d un diviseur de w. Soit q un nombre premier, avec $(q, 2pd) = 1$. On dit que le premier q est caractéristique si et seulement si $q|\Phi^*_{2^\lambda w}(G_p)$. On dit que q^μ est un facteur caractéristique primaire, si et seulement si $q^\mu||\Phi^*_{2^\lambda w}(G_p)$.*

On a le théorème suivant :

Théorème 2.0.8 *Soit q un facteur premier caractéristique de $\Phi^*_{2^\lambda w}(G_p)$. Alors, si $\nu_q(\Phi^*_{2^\lambda w}(G_p)) = v$, on a*

$$q^v \equiv 1[2^\lambda d]. \tag{2.11}$$

En particulier, dans le cas d'un premier de Fermat, on a

Corollaire 2.0.9 *Soit $p = 2^{2^n}+1$ un nombre premier de Fermat. Soit q un facteur premier de h_p^-, tel que $q \equiv 1 + 2^m[2^{m+1}]$, avec $m \leq 2^n$. Alors $q^{2^{2^n-m}}$ divise h_p^-.*

Preuve En effet, par le théorème (2.0.6), si $q|h_p^-$, alors q divise $\Phi^*_{2^{2^n}}(G_p)$. Soit v la valuation q-adique de ce dernier. Par le théorème de Kummer précédent, on doit donc avoir $q^v \equiv 1[2^{2^n}]$. Or l'ordre de q modulo 2^{2^n} est 2^{2^n-m}. Donc, on a

$$q^{2^{2^n-m}}|h_p^-. \tag{2.12}$$

□ On verra une généralisation de ce résultat, en utilisant (entre autres) un théorème de Steiner.

2.0.4 Un théorème de Lehmer.

Dans ce qui suit, e désignera toujours un entier qui divise $p-1$ tel que $\frac{p-1}{e}$ est impair. On pose

$$\tau = \frac{e}{(e, Ind(2))}, \quad \alpha = e^{\frac{2i\pi}{e}}, \quad \gamma = \frac{\varphi(e)}{\varphi(\tau)}. \tag{2.13}$$

Si k est un entier, on pose

$$\chi_e(k) = \begin{cases} \alpha^{Ind_g(k)} & \text{si } p \nmid k, \\ 0 & \text{sinon.} \end{cases}$$

On pose aussi

$$M_e(p) = \sum_{k=0}^{p-1} k\chi_e(k), \quad m_e(p) = \sum_{k=0}^{\frac{p-1}{2}} \chi_e(k). \tag{2.14}$$

On a le lemme suivant :

Lemme 2.0.10 *Si $(r, e) = \delta$ et si $e = e_1\delta$, alors*

$$\prod_{(t,e)=1} (X - e^{\frac{2i\pi rt}{e}}) = \Phi_{e_1}(X)^{\frac{\varphi(e)}{\varphi(e_1)}}. \tag{2.15}$$

Preuve Le polynôme

$$\Psi(X) = \prod_{(t,e)=1} \left(X - e^{\frac{2i\pi rt}{e}} \right)$$

est unitaire de degrés $\varphi(e)$. Ses racines sont les racines primitives e_1-ième de l'unité et elles ont même multiplicité. Il existe donc un entier ν tel que

$$\Psi(X) = \left(\Phi_{e_1}(X)\right)^{\nu}.$$

En prenant les degrés, il vient $\varphi(e) = \nu\varphi(e_1)$, doù le lemme.□

Lemme 2.0.11 *Soit $\mathbb{K} = \mathbb{Q}(\alpha)$. On a alors*

$$\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(2 - \chi_e(2)) = \Phi_\tau(2)^\gamma. \tag{2.16}$$

Preuve En effet, on applique le lemme précédent avec $X = 2, r = Ind_g(2), e_1 = \frac{e}{(e,r)} = \tau$. On a alors

$$\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(2 - \chi_e(2)) = \Phi_{e_1}(2)^{\frac{\varphi(e)}{\varphi(e_1)}} = \Phi_\tau(2)^\gamma. \tag{2.17}$$

□

Lemme 2.0.12 *On a*

$$(2 - \overline{\chi_e})M_e(p) = -pm_e(p). \tag{2.18}$$

Preuve Le caractère χ_e est impair, ie $\chi_e(-1) = -1$. En effet

$$\chi_e(-1) = \alpha^{Ind_g(-1)} = \alpha^{\frac{p-1}{2}} = e^{\frac{i\pi(p-1)}{e}} = (-1)^f = -1.$$

Soit $M' = \sum_{k<p/2} k\chi_e(k)$. Alors

$$M_e(p) - M' = \sum_{\frac{p}{2}<k<p} k\chi_e(k).$$

Soit $r = p - k$. Il vient

$$M_e(p) - M' = \sum_{r<\frac{p}{2}} (p-r)\chi_e(p-r) = \sum_{r<\frac{p}{2}} (p-r)\chi_e(-r) = p\chi_e(-1)m_e(p) - \chi_e(-1)M',$$

d'où

$$M_e(p) = 2M' - pm_e(p). \tag{2.19}$$

D'un autre côté, on a

$$M_e(p) = \sum_{2|k} \chi_e(k) + \sum_{2\nmid k} \chi_e(k),$$

ie

$$M_e(p) = \sum_{k<\frac{p}{2}} 2k\chi_e(2k) + \sum_{k<\frac{p}{2}} (2k+1)\chi_e(2k+1).$$

La première somme est égale à $2\chi_e(2)M'$. Par le changement d'indice $k' = \frac{p-1-2k}{2}$, la seconde somme devient $\sum_{k<\frac{p}{2}} (p-2k)\chi_e(p-2k)$. On a donc

$$\begin{aligned} M_e(p) &= 2\chi_e(2)M' + \sum_{k<\frac{p}{2}} (p-2k)\chi_e(p-2k) \\ &= 2\chi_e(2)M' - p\chi_e(2)\sum_{k<\frac{p}{2}} \chi_e(k) + 2\chi_e(2)\sum_{k<\frac{p}{2}} k\chi_e(k) \\ &= 4\chi_e(2)M' - p\chi_e(2)m_e(p), \end{aligned}$$

ie

$$\overline{\chi_e}(2)M_e(p) = 4M' - pm_e(p). \tag{2.20}$$

En multipliant (2.19) par 2 et en soustrayant (2.20), on obtient le lemme.□

Théorème 2.0.13 *On a*

$$\Phi_e^*(G_p) = Res(\Phi_e(p), G_p) = \frac{(-1)^{\varphi(e)} p^{\varphi(e)} \mathcal{N}_e(m_e(p))}{\Phi_\tau(2)^\gamma}. \tag{2.21}$$

Preuve Par propriétés du résultant

$$\begin{aligned}
Res\left(\Phi_e, G_p\right) &= (-1)^{\varphi(e)(p-2)} Res\left(G_p, \Phi_e\right) \\
&= (-1)^{\varphi(e)} \prod_{(t,e)=1} G_p\left(\alpha^t\right) \\
&= (-1)^{\varphi(e)} \prod_{(t,e)=1} \sum_{n=1}^{p-1} g_n \alpha^{t(p-n-2)} \\
&= (-1)^{\varphi(e)} \prod_{(t,e)=1} \alpha^{t(p-2)} \prod_{(t,e)=1} \sum_{n=1}^{p-1} g_n \alpha^{-tn} \\
&= (-1)^{\varphi(e)} \mathcal{N}_e(\alpha)^{p-2} \prod_{(t,e)=1} \sum_{n=1}^{p-1} g_n \alpha^{-tn} \\
&= \prod_{(t,e)=1} \sum_{n=1}^{p-1} g_n \alpha^{tn} \\
&= \mathcal{N}_e\left(\sum_{n=1}^{p-1} g_n \alpha^n\right).
\end{aligned}$$

Comme $Ind_g(g_n) = n$, on a

$$\sum_{n=1}^{p-1} g_n \alpha^n = \sum_{k=1}^{p-1} k \chi_e(k) = M_e(p),$$

ie

$$Res\left(\Phi_e, G_p\right) = \mathcal{N}_e\left(M_e(p)\right).$$

Le théorème découle donc des lemmes (2.0.11) et (2.0.12).□ On pose

$$W_e(p) = W_e(p,t) = \sum_{n=1}^{\frac{p-1}{2}} \left(\epsilon_n - \epsilon_{n-1}\right) \alpha^{nt},$$

où

$$\epsilon_n = \begin{cases} 1 & \text{si } g_n < \frac{p}{2}, \\ 0 & \text{sinon.} \end{cases}$$

On a alors :

Lemme 2.0.14

$$(1-\alpha) m_e(p) = 2 W_e(p,1). \tag{2.22}$$

Preuve Posons $p = 2r + 1$. On a

$$\alpha^r = \left(\alpha^{\frac{e}{2}}\right)^f = (-1)^f = -1,$$

et

$$g_{n+r} \equiv g^r g^n \equiv -g^n \bmod p,$$

ie $g_{n+r} = p - g_n$ et $\epsilon_{n+r} = 1 - \epsilon$. On a alors

$$\begin{aligned}
m_e(p) &= \sum_{k=1}^{r} \alpha^{Ind_g(k)} = \sum_{t=0}^{p-2} \epsilon_t \alpha^t \\
&= \sum_{t=0}^{p-2} \epsilon_t \alpha^t \\
&= \sum_{\nu=0}^{r-1} \epsilon_\nu \alpha^\nu + \epsilon_{\nu+r} \alpha^{\nu+r} \\
&= \sum_{\nu=0}^{r-1} \epsilon_\nu \alpha^\nu - \sum_{\nu=0}^{r-1} (1 - \epsilon_\nu) \alpha^\nu \\
&= 2 \sum_{\nu=0}^{r-1} \epsilon_\nu \alpha^\nu - \sum_{\nu=0}^{r-1} \alpha^\nu \\
&= 2 \sum_{\nu=0}^{r-1} \epsilon_\nu \alpha^\nu - \frac{2}{1-\alpha}.
\end{aligned}$$

Il vient

$$\begin{aligned}
(1-\alpha) m_e(p) &= 2 \sum_{\nu=0}^{r-1} \epsilon_\nu \alpha^\nu - 2 \sum_{\nu=0}^{r-1} \epsilon_\nu \alpha^{\nu+1} - 2 \\
&= 2 \sum_{\nu=0}^{r-1} \epsilon_\nu \alpha^\nu - 2 \sum_{\nu=1}^{r} \epsilon_{\nu-1} \alpha^\nu - 2 \\
&= 2 \sum_{\nu=1}^{r} (\epsilon_\nu - \epsilon_{\nu-1}) \alpha^\nu,
\end{aligned}$$

car $\epsilon_r = 0$, ie

$$(1-\alpha) m_e(p) = 2 W_e(p, 1).$$

Le lemme est prouvé.□

Lemme 2.0.15 *(Lebesgue) Soit $n > 1$ un entier. Alors*

$$\Phi_n(1) = \begin{cases} p & \text{si } n = p^l, \ p \text{ premier,} \\ 1 & \text{sinon} \end{cases}$$

Preuve (Arnaudiès)

Le groupe des racines primitives n-ième de l'unité est la réunion disjointe des racines primitives d-ième de l'unité, d parcourant les diviseurs de n. En particulier

$$\prod_{d|n} \Phi_d(1) = X^n - 1,$$

d'où

$$\prod_{d|n, d\neq 1} \Phi_d(1) = n.$$

Posons

$$\lambda_n = \begin{cases} \Phi_n(1) & \text{si } n > 1, \\ 1 & \text{sinon.} \end{cases}$$

Par ce qui précède

$$\prod_{d|n} \lambda_d = n.$$

Par la formule d'inversion de Möebius, on a donc $\lambda_n = \prod_{d|n} d^{\mu\left(\frac{n}{d}\right)}$. Posons également

$$\Lambda_n = \begin{cases} p & \text{si } n = p^\alpha, \ p \text{ premier}, \\ 1 & \text{sinon.} \end{cases}$$

Il est facile de vérifier que $\prod_{d|n} \Lambda_d = n$. La formule d'inversion de Möebius montre alors que $\Lambda_n = \lambda_n$.□

Lemme 2.0.16 *Soit e un entier. On suppose que e n'est pas une puissance d'un nombre premier impair. On pose*

$$J(e) = \begin{cases} \varphi(e) - 1 & \textit{si } e = 2^k, k \geq 1, \\ \varphi(e), & \textit{sinon.} \end{cases}$$

On a alors

$$\mathcal{N}_e(m_e(p)) = 2^{J(e)} \mathcal{N}_e(W_e(p, 1)). \tag{2.23}$$

Preuve Par le lemme précédant,

$$(1 - \alpha) m_e(p) = 2 W_e(p, 1).$$

Prenons la norme de cette égalité. Il vient

$$\mathcal{N}_e\,(1 - \alpha)\,\mathcal{N}_e\,(m_e(p)) = 2^{\varphi(e)} \mathcal{N}_e\,(W_e(p, 1))\,.$$

Par le lemme précédent

$$\Phi_e(1) = \begin{cases} 2 & \text{si } e = 2^k, k \geq 1, \\ 1 & \text{sinon,} \end{cases}$$

d'où le lemme.□

Théorème 2.0.17 *On pose* $h_e(p) = p^{[e/(p-1)]} N_e(W_e(p,1)) \Phi_\tau(2)^{-\gamma}$. *On a alors*

$$h_p^- = \prod_{e, 2 \nmid \frac{p-1}{2}} h_e(p). \tag{2.24}$$

Preuve p étant un nombre premier impair, on pose $p-1 = 2^\lambda w$, w impair. Soit e un diviseur de $p-1$ de codiviseur impair. On pose $e = 2^\lambda d$ avec $d|w$. On a par le théorème (2.0.6)

$$(2p)^{\frac{p-3}{2}} h^- = (-1)^{\frac{p-1}{2}} \prod_{d|w} Res(\Phi_e, G_p). \tag{2.25}$$

Par le théorème (2.0.13), on a

$$Res(\Phi_e, G_p) = \frac{(-1)^{\phi(e)} p^{\phi(e)} \mathcal{N}_e(m_e(p))}{\Phi_\tau(2)^\gamma}. \tag{2.26}$$

Par le lemme (2.0.16)

$$\mathcal{N}_e(m_e(p)) = 2^{J(e)} \mathcal{N}_e(W_e(p,1)). \tag{2.27}$$

On a donc

$$\begin{aligned} (2p)^{\frac{p-3}{2}} h^- &= (-1)^{\frac{p-1}{2}} \prod_{d|w} \frac{(-1)^{\phi(e)} p^{\phi(e)} 2^{J(e)} \mathcal{N}_e(W_e(p,1))}{\Phi_\tau(2)^\gamma} \\ &= (-1)^{\frac{p-1}{2}} (-1)^{\sum_{d|w} \phi(2^\lambda d)} p^{\sum_{d|w} \phi(2^\lambda d)} \prod_{d|w} \frac{2^{J(e)} \mathcal{N}_e(W_e(p,1))}{\Phi_\tau(2)^\gamma} \end{aligned} \tag{2.28}$$

On a par la relation d'Euler

$$\begin{aligned} \sum_{d|w} \phi(2^\lambda d) &= \sum_{d|p-1} \phi(d) - \sum_{d|w} \sum_{i=0}^{\lambda-1} \phi(2^i d) \\ &= p - 1 - \sum_{d|w} \phi(d)(2^{\lambda-1}) \\ &= p - 1 - 2^{\lambda-1} \left(\frac{p-1}{2^\lambda} \right) \\ &= \frac{p-1}{2}. \end{aligned} \tag{2.29}$$

On a donc

$$\begin{aligned}(2p)^{\frac{p-3}{2}}h_p^- &= p^{\frac{p-1}{2}}2^{\sum_{d|w}J(e)}\prod_{d|w}\frac{\mathcal{N}_e(W_e(p,1))}{\Phi_\tau(2)^\gamma}\\ &= p^{\frac{p-1}{2}}2^{J(2^\lambda)+\sum_{d|w,d\neq 1}J(2^{\lambda d})}\prod_{d|w}\frac{\mathcal{N}_e(W_e(p,1))}{\Phi_\tau(2)^\gamma}\\ &= p^{\frac{p-1}{2}}2^{\phi(2^\lambda)-1+\sum_{d|w,d\neq 1}\phi(2^{\lambda d})}\prod_{d|w}\frac{\mathcal{N}_e(W_e(p,1))}{\Phi_\tau(2)^\gamma}\\ &= p^{\frac{p-1}{2}}2^{\frac{p-3}{2}}\prod_{d|w}\frac{\mathcal{N}_e(W_e(p,1))}{\Phi_\tau(2)^\gamma}.\end{aligned} \tag{2.30}$$

D'où

$$\begin{aligned}h_p^- &= p\prod_{d|w}\frac{\mathcal{N}_e(W_e(p,1))}{\Phi_\tau(2)^\gamma}\\ &= \prod_{d|w}\frac{p^{\left[\frac{e}{p-1}\right]}\mathcal{N}_e(W_e(p,1))}{\Phi_\tau(2)^\gamma} = \prod_e h_e(p).\end{aligned} \tag{2.31}$$

□

Exemple 2.0.18 *Montrons que* $h_{19}^- = 1$. *Dans ce cas,* $g = 3$, $Ind_g(2) = 7$, *et les entiers* g_n, $n = 1, \ldots, 9$ *sont respectivement* $3, 9, 8, 5, 15, 7, 2, 6, 18$. *En particulier,* $\epsilon_n = 0$ *ssi* $n \in \{5, 9\}$. *De plus, les différentes valeurs possibles pour* e *sont* 2, 6 *et* 18. *En posant* $\alpha_e = e^{\frac{2i\pi}{e}}$, *on a donc*

$$W_e(19,1) = -\alpha_e^5 + \alpha_e^6 - \alpha_e^9.$$

Si $e = 2$, $\alpha = -1$ *et* $\mathcal{N}_e(W_e(19,1)) = W_e(19,1) = 3$. *Comme* $Ind_g(2) = 7$, $\tau = 2$, $\gamma = 1$, *donc* $\Phi_\tau(2) = 3$, *puis* $h_2(19) = 1$.

Si $e = 6$, *on a* $\alpha_e = e^{\frac{i\pi}{3}}$ *donc*

$$W_e(19,1) = -\alpha_e^5 + \alpha_e^6 - \alpha_e^9 = 2 - \alpha^2,$$

puis $\mathcal{N}_e(W_e(19,1)) = 5-4(\alpha^2+\alpha^{-2}) = 3$. *On a* $\tau = 6$, $\gamma = 1$, *donc* $\Phi_\tau(2) = (2-\alpha)(2-\alpha^5) = 3$, *puis* $h_6(19) = 1$.

Si $e = 18$, *de même, on a* $\mathcal{N}_e(W_e(19,1)) = 3$ *et* $\Phi_\tau(2) = \Phi_{18}(2) = 57$. *Comme* $\left[\frac{e}{p-1}\right] = 1$, *on a* $h_{18}(18) = 19 \cdot \frac{3}{57} = 1$. *Au final,* $h_{19}^- = 1$.

Enfin, on rappelle le résultat suivant :

Théorème 2.0.19 *Soit p un nombre premier impair. Soit e un diviseur de $p-1$, dont le codiviseur f est impair ($p-1=ef$). Soit q un diviseur premier de f. Alors q divise h_{eq} si et seulement q divise h_e.*

Preuve On a déjà vu que

$$Res(\Phi_{eq}, G_p) = \mathcal{N}_{eq}\left(M_{eq}(p)\right) = \prod_{(t,eq)=1} \sum_{n=1}^{p-1} g_n \alpha_1^{tn},$$

où $\alpha_1 = e^{\frac{2i\pi}{eq}}$ (et donc $\alpha_1^q = \alpha$). Il vient alors

$$Res(\Phi_{eq}, G_p)^q \equiv \prod_{(t,eq)=1} \sum_{n=1}^{p-1} g_n^q \alpha^{tn} \equiv \left(\prod_{(t,e)=1} \sum_{n=1}^{p-1} g_n \alpha^{tn} \right)^{\frac{\varphi(eq)}{\varphi(e)}} \bmod q,$$

ie

$$\Phi_{eq}^* \equiv \Phi_e^{*\mu} \bmod q$$

où

$$\mu = \begin{cases} 1 & \text{si } q|e, \\ q-1 & \text{sinon.} \end{cases}$$

En particulier, $q|\Phi_{eq}^*$ ssi $q|\Phi_e^*$, d'où le théorème par définition de $h_e(p)$ et $h_{eq}(p)$.□

2.0.5 Interprétation de $h_e(p)$ pour e de la forme 2^a.

Soit e un diviseur de $p-1$ dont le codiviseur est impair. Soit K_e l'unique sous-corps de $\mathbb{Q}(\zeta)$ tel que $[K_e : \mathbb{Q}] = e$. Soit $h^-(K_e)$ son nombre de classes relatif. Si e est une puissance de deux, alors $h^-(K_e)$ coïncide avec $h_e(p)$. On commence par rappeler quelques résultats intermédiaires.

Lemme 2.0.20 *Soit χ_e le caractère de $\mathbb{Q}(\zeta)$ défini par*

$$\chi_e(k) = \begin{cases} \alpha^{Ind_g(k)} & \textit{si } p \nmid k, \\ 0 & \textit{si } p|k. \end{cases}$$

Le groupe engendré par χ_e est le groupe des caractères de K_e.

Preuve Le groupe de Galois de $\mathbb{Q}(\zeta)/K_e$ est engendré par σ^e, où $\sigma(\zeta) = \zeta^g$. On a alors

$$\chi_e(\sigma^e) = \chi_e(g^e) = \alpha^e = 1.$$

Le groupe engendré par χ_e agit donc trivialement sur $\mathrm{Gal}(\mathbb{Q}(\zeta)/K_e)$. Par conséquent, c'est un sous-groupe du groupe des caractères de K_e. Mais ce dernier est d'ordre e, qui est l'ordre de χ_e, d'où le lemme.□

Lemme 2.0.21 *Une extension cyclique imaginaire de degrés une puissance de deux, ne peut contenir un sous-corps imaginaire propre.*

Preuve En effet, soit L une telle extension. Ses sous-corps sont emboîtés les uns dans les autres. Soit L^+ son sous-corps réel maximal. Comme $[L : L^+] = 2$, les sous-corps propres de L sont donc tous inclus dans L^+, donc réel.□

On peut alors montrer le

Théorème 2.0.22 *Soit p un nombre premier impair et $e = 2^d$ la plus grande puisance de deux qui divise $p-1$. Alors, le nombre de classes relatif de K_e est $h_e(p)$.*

Preuve Remarquons d'abord que le caractère χ_e est impair. En effet

$$\chi_e(-1) = \alpha^{\frac{p-1}{2}} = -1.$$

Soit X un sous-groupe du groupe engendré par χ_e. Soit K le sous-corps associé, $K \subset K_e$. Comme K_e est une extension cyclique imaginaire de degrés une puissance de deux, le lemme précédent montre que K est réel ou $K = K_e$. Par conséquent, $< \chi_e >$ ne possède pas de sous-groupe propre à générateur impair. Soit Q_e l'indice de Hasse de K_e et w_e le nombre de racine de l'unité qu'il contient. On a $Q_e = 1$ (voir le lemme (2.2.4)ci-après) et $w_e = 2$ (respectivement $w_e = 2p$) si $e \neq p-1$ (respectivement si $e = p-1$). Par la formule du nombre de classe

$$h^-(K_e) = \begin{cases} 2\mathcal{N}_e\left(-\frac{1}{2}B_{1,\chi_e}\right) & \text{si } e \neq p-1, \\ 2p\mathcal{N}_e\left(-\frac{1}{2}B_{1,\chi_e}\right) & \text{si } e = p-1 = 2^d, \end{cases}$$

où

$$B_{1,\chi_e} = \frac{1}{p}\sum_{1 \leq a \leq \frac{p-1}{2}} \chi_e(a)a = \frac{1}{p}M_e(p).$$

Par le lemme (2.0.12)

$$B_{1,\chi_e} = -\frac{1}{2 - \overline{\chi_e}(2)}m_e(p).$$

On a alors

$$\begin{aligned}
h_e(p) &= p^{\left[\frac{e}{p-1}\right]}\mathcal{N}_e\left(W_e(p,1)\right)\Phi_\tau(2)^{-\gamma} \\
&= p^{\left[\frac{e}{p-1}\right]}2^{-J(e)}\mathcal{N}_e\left(m_e(p)\right)\Phi_\tau(2)^{-\gamma} && \text{(lemme (2.0.16))} \\
&= p^{\left[\frac{e}{p-1}\right]}2^{-J(e)}(-1)^{\varphi(e)}\mathcal{N}_e\left(2-\overline{\chi_e}(2)\right)\mathcal{N}_e\left(B_{1,\chi_e}\right)\Phi_\tau(2)^{-\gamma} \\
&= p^{\left[\frac{e}{p-1}\right]}2^{-J(e)}(-1)^{\varphi(e)}\Phi_\tau(2)^{\gamma}\mathcal{N}_e\left(B_{1,\chi_e}\right)\Phi_\tau(2)^{-\gamma} && \text{(lemme (2.0.11))} \\
&= p^{\left[\frac{e}{p-1}\right]}2^{-J(e)}(-1)^{\varphi(e)}\mathcal{N}_e\left(B_{1,\chi_e}\right).
\end{aligned}$$

Si p est un nomre premier de Fermat, c'est à dire $p-1=e=2^d$, alors $K_e=\mathbb{Q}(\zeta)$ et $J(e)=\varphi(e)-1$ (voir le lemme (2.0.16)). On obtient

$$\begin{aligned}
h_e(p) &= p2^{-J(e)}(-1)^{\varphi(e)}\mathcal{N}_e\left(B_{1,\chi_e}\right) \\
&= p\frac{1}{2^{\varphi(e)-1}}\mathcal{N}_e\left(-B_{1,\chi_e}\right) \\
&= 2p\mathcal{N}_e\left(-\frac{1}{2}B_{1,\chi_e}\right) \\
&= h^-\left(K_e\right)=h_p^-.
\end{aligned}$$

Le théorème est prouvé dans ce cas. Supposons $p-1\neq e$. Alors

$$\begin{aligned}
h_e(p) &= 2^{-J(e)}(-1)^{\varphi(e)}\mathcal{N}_e\left(B_{1,\chi_e}\right) \\
&= \frac{1}{2^{\varphi(e)-1}}\mathcal{N}_e\left(-B_{1,\chi_e}\right) \\
&= 2\mathcal{N}_e\left(-\frac{1}{2}B_{1,\chi_e}\right) \\
&= h^-\left(K_e\right).
\end{aligned}$$

■

Exemple 2.0.23 *Prenons $p=13$ et calculons $h^-(K_4)$. On peut prendre $g=2$, donc $Ind_g(2)=1$. Pour $e=4$, $\alpha:=\alpha_e=e^{\frac{2i\pi}{4}}=i$ et*

$$\tau=\frac{4}{(4,1)}=4,\quad \Phi_4(X)=X^2+1,\quad \Phi_4(2)=5,\quad \gamma=\frac{\varphi(e)}{\varphi(\tau)}=1.$$

Les différentes valeurs de g_n pour $n=0,\ldots,6$ sont respectivement $1,2,4,8,3,6,12,11$. En particulier, $\epsilon_n=0$ ssi $n=3$, $n=6$. Il vient

$$W_4(13,1)=\sum_{n=1}^{6}\left(\epsilon_n-\epsilon_{n-1}\right)\alpha^n=-i^3+i^4-i^6=2+i,$$

d'où

$$\mathcal{N}_4\left(W_4(13,1)\right) = \mathcal{N}_{\mathbb{Q}(i)/\mathbb{Q}}\left(2+i\right) = 5.$$

Par suite on a

$$h^-(K_4) = \mathcal{N}_4\left(W_4(13,1)\right)\Phi_4(2)^{-1} = 1.$$

2.1 Sur certains facteurs premiers de h_p^-.

2.1.1 Un théorème de Steiner.

Lemme 2.1.1 *Soit K un corps de type CM, de sous-corps réel maximal K^+. Soit j la conjugaison complexe. Soient ϕ et ψ deux pongements de K dans $\mathbb{C}$. Alors*

$$\forall \alpha \in K, \phi^{-1}(j\phi(\alpha)) = \psi^{-1}(j\psi(\alpha)) \tag{2.32}$$

Preuve L'extension $\phi(K)/\phi(K^+)$ est quadratique, donc normale, et la conjugaison complexe fixe $\phi(K^+)$. Donc

$$j\phi(K) = \phi(K). \tag{2.33}$$

En particulier, $\phi^{-1}j\phi$ est un automorphisme de K. Idem pour $\psi^{-1}j\psi$. Comme K est de type CM, ces deux automorphismes ne peuvent être l'identité de K. Comme le groupe de Galois de K/K^+ est d'ordre 2, ils ont donc égaux. □

On rappelle maintenant le résultat suivant de la théorie du corps de classes :

Théorème 2.1.2 *Soit L/K une extension de corps de nombres. Supposons que cette extension ne contienne aucune sous-extension non ramifiée abélienne qui n'est pas triviale sur K. Alors, la norme associée à L/K est surjective sur K.*

Preuve Soient d'abord F, M, k et K des corps de nombres tels que les extensions K/k et M/F soient abéliennes. On suppose aussi que $M \cap k = F$. Soit $\mathfrak{p}$ un idéal premier de k non ramifié dans K/k. Soit $\mathcal{P}$ un premier de K au-dessus de $\mathfrak{p}$. Soit $\tilde{\mathfrak{p}}$ le premier de F en-dessous de $\mathfrak{p}$. Soit $\tilde{\mathcal{P}}$ un premier de M au-dessus de $\tilde{\mathfrak{p}}$. On suppose que $\tilde{\mathfrak{p}}$ est non ramifié dans M/F. Soit f le degrés résiduel de $\mathfrak{p}/\tilde{\mathfrak{p}}$. Soit $\sigma = \left[\frac{K/k}{\mathfrak{p}}\right]$. Soit aussi $\tau = \left[\frac{M/F}{\tilde{\mathfrak{p}}^f}\right]$. Soit $\sigma' = \sigma_{|M}$. On a

$$\tau = \sigma'. \tag{2.34}$$

Supposons maintenant que M soit le corps de clases de F, et que K soit le corps de classes de k. La restriction des éléments de $\mathrm{Gal}(Mk/k)$ à M donne

$$\mathrm{Gal}(Mk/k) \simeq \mathrm{Gal}(M/F). \tag{2.35}$$

On note ψ un tel isomorphisme. Soit f_k (application d'Artin) l'isomorphisme entre le groupe des classes de k et $\mathrm{Gal}(K/k)$. Soit de même pour f_F. Soit $\mathcal{N}$ l'application norme du group des classes de k vers celui de F. L'égalité précédente $\tau = \sigma'$ donne

$$\psi\left(f_k(\mathfrak{p})\right) = f_M\left(\mathcal{N}(\mathfrak{p})\right). \tag{2.36}$$

On en déduit en particulier que l'application $\mathcal{N}$ est surjective. On peut apliquer ce qui précède à $k = L$ et $F = K$, par hypothèse sur L/K. □

Remarque 2.1.3 *En particulier, le nombre de clases de K divise celui de L. On redémontre ainsi que h_p^+ divise h_p.*

Soit maintenant un groupe abélien A, noté additivement. On supose que j agit sur A. On a la proposition suivante :

Proposition 2.1.4 *Supposons que A soit un groupe fini d'ordre impair. Il existe deux sous-groupes de A, notés A^+ et A^- tels que*

$$A = A^+ \oplus A^-. \tag{2.37}$$

De plus, $A^+ = Ker(1-j)$ et $A^- = Ker(1+j)$.

Preuve A étant d'ordre impair, on pose $|A| = 2m+1$. Parle théorème de Lagrange

$$\forall a \in A, a \in 2A. \tag{2.38}$$

Donc $A = 2A$. En particulier, on pose

1. $A^+ = \frac{1+j}{2}A$.
2. $A^- = \frac{1-j}{2}A$.

Montrons que $A^+ = Ker(1-j)$ et $A^- = Ker(1+j)$. En effet, soit $a \in A^+$. Il existe un élément a_1 de A tel que

$$a = \frac{1-j}{2}a_1, \tag{2.39}$$

d'où $(1-j)a = 0$, car $(1+j)(1-j) = 0$. Inversement, si $a = ja$, alors

$$a = (1+j)a - a, \tag{2.40}$$

d'où $a = \frac{1+j}{2}a$. On a donc bien $A^+ = Ker(1-j)$. De même on montre $A^- = Ker(1+j)$. Il reste à montrer que $A = A^+ \oplus A^-$. Soit $a \in A$. On a

$$a = \frac{1-j}{2}a + \frac{1+j}{2}a, \tag{2.41}$$

d'où l'égalité $A = A^+ + A^-$. De plus, si $a \in A^+ \cap A^-$, alors $a = ja = -ja$, ie $2a = 0$, ie $a = 0$, et on a donc bien

$$A = A^+ \oplus A^-. \tag{2.42}$$

□

On peut maintenant démontrer le théorème suivant de Steiner :

Théorème 2.1.5 *Soient p et q deux nombres premiers impairs. Soit $t = \nu_2(p-1)$ et soit $d = 2^t$. Soit aussi f l'ordre de q modulo d. Supposons que $t > \nu_2(q-1)$. Alors si $q|h(K_p)^-$ on a*

$$q^f | h(K_p)^-, \tag{2.43}$$

où K_p est le sous-cors de degrés d sur $\mathbb{Q}$ du p-ième corps cyclotomique.

Preuve Comme K_p est une extension galoisienne de $\mathbb{Q}$, dont le groupe de Galois est un 2-groupe, et qui, parmi les premiers fini, ramifie seulement en deux. On en déduit que $h(K_p)^-$ est impair. Soit A le sous-groupe du groupe des classes de K_p, formé de éléments d'ordre 1 ou q. A est un q-groupe, et q est impair. Par la proposition précédente

$$A = A^+ \oplus A^-, \tag{2.44}$$

avec

1. $A^+ = \frac{1+j}{2} A$.
2. $A^- = \frac{1-j}{2} A$.

En tant que sous-extension de $\mathbb{Q}(\zeta_p)$, il existe σ un élément d'ordre d, tel que

$$G = \mathrm{Gal}(K_p/\mathbb{Q}) = < \sigma > . \tag{2.45}$$

Le groupe G opère sur A^-. Soit $v \in A^-$ et soit Ω_v l'orbite de v sous G.

Lemme 2.1.6 *Si $|\Omega_v| < d$, il existe i tel que $0 < i < d$, $i|\frac{d}{2}$ et $\sigma^i(v) = v$.*

Preuve (du lemme)

Comme $|\Omega_v| < d$, il existe $k < l$ tels que $\sigma^k(v) = \sigma^l(v)$ ie $\sigma^{l-k}(v) = v$. Il existe donc un plus petit entier $i > 0$ tel que $\sigma^i(v) = v$. En notant r le reste de la division euclidienne de d par i, il vient $\sigma^i(v) = v$ donc $r = 0$ car $0 \leq r < i$, ie $i|d$. Comme $i < d$ et d puissance de deux, en fait $i|\frac{d}{2}$.□

Supposons qu'il existe un élément de A^- dont l'orbite sous G a au plus $d-1$ éléments. Par le lemme, il existe i tel que $\sigma^i(v) = v$, avec $i|d$ et $i < d$. Comme $d = 2^t$, $i|\frac{d}{2}$, donc

$\sigma^{\frac{v}{2}}(v) = v$, ie $j(v) = v$. D'après la proposition précédente, $A^- = Ker(1+j)$. Donc on a aussi $j(v) = -v$. Finalement, $j(v) = v = -v$, ie $2v = 0$ ie $v = 0$. Ainsi, l'orbite de tout élément non nul de A^- a exactement d éléments. Soit $(v_i)_{i\in I}$ un système de représentant de ces orbites. Comme elles réalisent une partition de A^-, on a

$$\left|A^-\right| = \sum_{i\in I} |\Omega_{v_i}|. \tag{2.46}$$

En particulier, $|A^-| \equiv 1[d]$. Supposons que $|A^-| = q^m$. On aurait alors $q^m \equiv 1[d]$. Donc, f étant l'ordre de q modulo d, on aurait $f|m$. On aurait donc $q^f| \, |A^-|$.

Mais on a montré que lapplication norme $1+j$ réalise une surjection de $cl(K)$ sur $cl(K^+)$. En particulier, on a

$$|Ker(1+j)| = h_K^-. \tag{2.47}$$

Si on restreint l'action de $1+j$ à A^-, on a

$$Ker((1+j)_{|A}) = \frac{1-J}{2}A = A^-. \tag{2.48}$$

On en déduit que $|A^-|h_K^-$, d'où $q^f|h_K^-$. □

Corollaire 2.1.7 *Soit p un nombre premier et soit $n = \nu_2(p-1)$. Soit K_p le sous-corps de $\mathbb{Q}(\zeta_p)$ de degrés 2^n sur $\mathbb{Q}$. Soit $0 < m \leq n$, et soit q un nombre premier tel que $q \equiv 1 + 2^m[2^{m+1}]$. Supposons que $q|h(K_p)^-$. Alors*

$$q^{2^{n-m}}|h(K_p)^-. \tag{2.49}$$

De plus, si $q^\mu||h(K_p)^-$, alors $\mu = 2^{n-m}l$, où l est un entier.

Preuve Si $n = m$, il n'y a rien à faire. On peut donc supposer $n > m$.

On commence par montrer le lemme suivant

Lemme 2.1.8 *L'entier q est d'ordre 2^{n-m} modulo 2^n.*

Preuve Pour $n = 2$ et donc $m = 1$, il n'y a rien à faire. On peut donc supposer $n \geq 3$.

Montrons par récurrence sur n que

$$q^{2^{n-m-1}} \equiv 1 + 2^{n-1} \bmod 2^n, \quad q^{2^{n-m}} \equiv 1 + \bmod 2^n.$$

Supposons $n = m+1$. Comme $q \equiv 1+2^m \bmod 2^{m+1}$, en particulier $q \equiv 1+2^{n-1} \bmod 2^n$ et comme $q \equiv 1 \bmod 2^m$, on a $q^2 \equiv 1 \bmod 2^{m+1}$ ie $q^2 \equiv 1 \bmod 2^n$. Supposons le lemme vrai pour $n \geq m+1$ et montrons le pour $n+1$. On a

$$q^{2^{n-m}} \equiv 1 \bmod 2^n \Rightarrow \left(q^{2^{n-m}}\right)^2 \equiv 1 \bmod 2^{n+1},$$

d'où $q^{2^{n+1-m}} \equiv 1 \bmod 2^{n+1}$. Il reste à montrer que $q^{2^{n-m}} \equiv 1+2^n \bmod 2^{n+1}$. Or, par hypothèse de récurrence

$$2^n | q^{2^{n-m-1}} - 2^{n-1} - 1,$$

donc

$$2^{n+1} | \left(q^{2^{n-m-1}} - 2^{n-1} - 1\right)\left(q^{2^{n-m-1}} + 2^{n-1} + 1\right),$$

ie

$$2^{n+1} | q^{2^{n-m}} - 2^n - 1 - 2^{2n-2}.$$

Comme $n \geq 3$, $2^{n+1} | 2^{2n-2}$, donc $2^{n+1} | q^{2^{n-m}} - 2^n - 1$.□ En particulier, comme q divise $h(K_p)^-$, par le théorème de Steiner (théorème (2.1.5))

$$q^{2^{n-m}} | h(K_p)^-. \tag{2.50}$$

Supposons que $q^\mu || h(K_p)^-$. q^μ est donc un facteur caractéristique primaire. Par le théorème de Kummer, $2^{n-m} | \mu$, ie il existe un entier l tel que $\mu = 2^{n-m} l$. □

2.2 Une application diophantienne.

Soit K_p le sous-corps maximal de $\mathbb{Q}(\zeta)$ de degrés une puissance de deux. Dans ce paragraphe on commence par donner une majoration du nombres de classes relatif $h(K_p)^-$ en fonction de p et de la valuation 2-adique de p que l'on note t pour la suite. Cette majoration nous permettra de donner un exemple de couples de nombres premiers impairs distincts (p, q) pour lesquels $q \nmid h_p^-$.

2.2.1 Une majoration de $h(K_p)^-$ en termes de t et p.

Lemme 2.2.1 *(voir [48] et [77])*

1. *Le nombre de classes $h(-p)$ du corps quadratique imaginaire $\sqrt{-p}$, $p \equiv 3 \bmod 4$, vérifie l'inégalité*

$$h(-p) < \frac{\sqrt{p}}{2\pi}\left(log(p) + c_1\right). \tag{2.51}$$

où $c_1 = +2 + \gamma - log(\pi)$, γ étant la constante d'Euler.

2. *Soient N un corps imaginaire de degrés $2n \geq 2$, N^+ son sous-corps réel maximal, W_N le nombre de racines de l'unité dans N, h_N^- son nombre de classes relatif, et Q_N son indice de Hasse. Soit A_N le quotient des discriminants de N et N^+. L'entier h_N^- vérifie l'inégalité*

$$h_N^- \leq Q_N W_N \sqrt{A_N} \left(\frac{1}{4\pi n} log(A_N) + \frac{c_1}{4\pi} \right)^n. \tag{2.52}$$

Lemme 2.2.2 *(formule du discriminant de Hasse) Soient K un corps de nombres, de groupe des caractères X_K. Soient $d(K)$ le discriminant de K, et $2r_2$ le nombre de $\mathbb{Q}$-plongement complexes de K. On a la relation suivante :*

$$d(K) = (-1)^{r_2} \prod_{\chi \in X_K} f_\chi,$$

où f_χ est le conducteur du caractère χ.

Ces deux lemmes permettent de démontrer la proposition suivante :

Proposition 2.2.3 *Soit $t = \nu_2(p-1)$, et soit K_p le sous-corps de $\mathbb{Q}(\zeta)$ dont le degrés sur $\mathbb{Q}$ est 2^t, et dont le nombre de classes relatif est noté $h_{K_p}^-$. Si $K_p \neq Q(\zeta)$, c'est à dire si p n'est pas un nombre premier de Fermat, alors*

$$h_{K_p}^- \leq 2p^{2^{t-2}} \left(\frac{1}{4\pi} log(p) + \frac{c_1}{4\pi} \right)^{2^{t-1}}. \tag{2.53}$$

Preuve Appliquons l'inégalité (2.52) au corps $N = K_p$, $n = 2^{t-1}$, et $Q_N = Q_p$ l'indice de Hasse du corps K_p. Comme $K \neq \mathbb{Q}(\zeta)$, 1 et -1 sont seules racines de l'unité que le corps K contienne, c'est à dire $W_p = 2$. L'indice Q_p vaut 1. En effet, on a le lemme suivant du à Latimer :

Lemme 2.2.4 *Tout sous-corps imaginaire pur K de $\mathbb{Q}(\zeta)$ a un indice de Hasse Q égal à 1.*

Preuve Soit $H = \mathrm{Gal}(K/\mathbb{Q})$, dont on note σ un générateur. Soit $n = [K : \mathbb{Q}]$ (qui est pair car K est imaginaire pur). Pour montrer que Q_K, il suffit de montrer que si u est une unité de K, alors il existe une racine de l'unité η telle que $\frac{\overline{u}}{u} = \eta^2$. En effet, l'unité $u\eta$ est alors réelle, et $u = u\eta \cdot \overline{\eta}$.

Posons $v = uu^\sigma \dots u^{\sigma^{n/2}-1}$. On a alors

$$\frac{\overline{u}}{u} = \frac{v^\sigma}{v},$$

et $v\overline{v}$ est la norme de u qui vaut donc 1 (-1 est impossible car cette norme doit être positive). Comme H opère trivialement sur le groupe des racines de l'unité modulo les carrés, en particulier, le quotient $\frac{v^\sigma}{v}$ est le carré d'une racine de l'unité, disons η^2. $\square$

Enfin, par la formule du discrimiant de Hasse (lemme (2.2.2)), étant donné que le caractère principal est de conducteur 1, et que tout caractère non principal de K_p est de conducteur p (car $K_p \subset \mathbb{Q}(\zeta)$), il vient :

$$d_{K_p} = (-1)^{r_2} \prod_{\chi \in \chi \in X_{K_p}} f_\chi = p^{2^t-1}, \quad (2|r_2).$$

Pour le sous-corps réel maximal K_p^+ de K_p, comme $\mathrm{Gal}\big(K_p/K_p^+\big) = \{1; j\}$, j conjugaison complexe, on a

$$d_{K_p^+} = (-1)^{r_2} \prod_{\chi \in \chi(-1)=1} f_\chi = p^{2^{t-1}-1}, \quad (r_2 = 0).$$

Le quotient $A_p = \frac{d_{K_p}}{d_{K_p^+}} = p^{2^{t-1}}$. L'inégalité (2.53) de la proposition (2.2.3) donne :

$$h_{K_p}^- \leq 2p^{2^{t-2}} \left(\frac{log(p) + c_1}{4\pi} \right)^{2^{t-1}}.$$

■

Remarque 2.2.5 *Si $K_p = \mathbb{Q}(\zeta)$, c'est à dire si p est un nombre premier de Fermat, on montre de la même façon (voir [34]) que*

$$h_{K_p}^- \leq 2p^{2^{t-2}+1} \left(\frac{1}{4\pi} log(p) + \frac{c_1}{4\pi} \right)^{2^{t-1}}.$$

2.2.2 Un nouveau critère pour $q \nmid h_p^-$.

Désignons par $\wp$ l'ensemble des nombres premiers et par $\wp'$ l'ensemble des nombres premiers qui sont congrus à 3 modulo 4. On adopte les notations suivantes ($A > 0$ entier) :

$$\Pi_t = \left\{ p \in \wp : \quad \frac{p-1}{2^t} \in \wp' \right\}, \quad \Pi_t(A) = \{ p \in \Pi_t : p \geq A \}.$$

Si un nombre premier p est un élément de Π_t pour un certain $t \geq 1$, on pose $\tilde{p} = \frac{p-1}{2^t}$, qui est donc un nombre premier.

On peut maintenant montrer le nouveau résultat suivant :

Proposition 2.2.6 *Soit $t \geq 1$ un entier. Il existe une constante effective $C(t)$ ne dépendant que de t (avec $C(1) = C(2) = 7$), telle que si $p \in \Pi_t(C(t))$, alors, $\tilde{p} \nmid h_p^-$.*

Preuve Soient donc p, q deux nombres premiers impairs tels que $p-1=2^tq$ et $q\equiv 3 \bmod 4$. Soit $h_{2^t}^-$ le nombre de classes relatif du sous-corps K_{2^t} de $\mathbb{Q}(\zeta)$ et de degrés 2^t sur $\mathbb{Q}$. D'après les théorèmes (2.0.17), (2.0.19) et (2.0.22), il existe un entier h_{2^tq} tel que

$$\left\{\begin{array}{l} h_p^- = h_{2^t}^- h_{2^tq}, \\ q|h_{2^tq} \Leftrightarrow q|h_{2^t}^-. \end{array}\right. \tag{2.54}$$

Supposons que $q|h_p^-$. Ce qui précède montre que $q|h_{2^t}^-$. Comme $q\equiv 1+2 \bmod 4$, le corollaire (2.1.7) montre que $q^{2^{t-1}}|h_{2^t}^-$. Or on a montré précédemment que l'on peut majorer $h_{2^t}^-$ comme suit :

$$h_{2^t}^- \leq 2p^{2^{t-2}}\left(\frac{1}{4\pi}\log(p)+c_1\right)^{2^{t-1}},$$

où on a posé $c_1=\frac{2+\gamma-\log(\pi)}{4\pi}$, γ étant la constante d'Euler. Cette majoration montre alors :

$$q^{2^{t-1}} \leq 2p^{2^{t-2}}\left(\frac{1}{4\pi}\log(p)+c_1\right)^{2^{t-1}},$$

c'est à dire

$$\left(\frac{p-1}{2^t}\right)^{2^{t-1}} \leq 2p^{2^{t-2}}\left(\frac{1}{4\pi}\log(p)+c_1\right)^{2^{t-1}},$$

ce qui donne le résultat souhaité, cette inégalité montrant au passage que $C(1)=C(2)=7$.□

2.2.3 Autre preuve de la proposition (2.2.6) si $p=1+2q$, q premier.

Dans le cas où $p=1+2q$, on peut montrer d'une autre façon que $(q,h_p^-)=1$, quoique cette façon puisse paraître parachutée. Avec les notations de la preuve de la proposition (6.1.3) ξ est alors une racine primitive q-ième de l'unité. Raisonnons par l'absurde et supposons qu'il existe un facteur premier $\mathfrak{q}$ de q dans $\mathbb{Q}(\zeta)$ tel que $h_p^- = \mathcal{O}(\mathfrak{q})$. Par la proposition (6.1.3), on a en particulier (en prenant $a=1$ par exemple) $E(p,1,1)=\mathcal{O}(\mathfrak{q})$. Il existe un entier k de $\{0,\ldots,r\}$ tel que (notation de la preuve de la proposition (6.1.3)) $P_{1,1}(\xi^k)=\mathcal{O}(\mathfrak{q}')$, où $\mathfrak{q}'$ est l'unique premier de $\mathbb{Q}(\zeta,\xi)$ au-dessus de $\mathfrak{q}$. Le premier $\mathfrak{q}$ étant totalement ramifié dans l'extension $\mathbb{Q}(\zeta,\xi)/\mathbb{Q}(\zeta)$ (voir le lemme 3.3.30 de [28]), on a alors en notant par $\mathbf{Tr}$ la trace relative à l'extension $\mathbb{Q}(\zeta,\xi)/\mathbb{Q}(\zeta)$ (rappelons que $\mathbf{Tr}(\xi)=-1$) :

$$(q-1)Z+\mathbf{Tr}\left(\sum_{k=1}^{r} Z^{\sigma^k}\xi^k\right)=\mathcal{O}(\mathfrak{q}), \quad Z=\frac{1}{1-\zeta_0}-\frac{1}{1-\overline{\zeta_0}}.$$

Comme

$$(q-1)Z - \sum_{k=1}^{r} Z^{\sigma^k} = qZ - \sum_{k=0}^{r} Z^{\sigma^k} = qZ - h(-p)\sqrt{-p},$$

on a donc

$$qZ - h(-p)\sqrt{-p} = \mathcal{O}(\mathfrak{q}). \tag{2.55}$$

La relation (2.55) montre $q|h(-p)$, donc en particulier $q = \frac{p-1}{2} \leq h(-p)$. Comme $p \equiv 3 \bmod 4$, le lemme (2.2.1) montre que c'est imposible. Le nombre rationnel $E(p,1,1)$ est donc premier à q, et la proposition (6.1.3) montre donc que $(q, h_p^-) = 1$.□

Remarque 2.2.7 *Lors de cette preuve, le fait que $h(-p)$ intervienne est du à (2.54).*

Notons que si l'on se fixe un entier t, on ne sait toujours pas si l'ensemble Π_t est infini.

2.2.4 Application à $1 + x + \ldots + x^{p-1} = py^q$.

Soit donc $m \geq 1$ et p premier impair tel que $p \in \Pi_m\,(C(m))$. Considérons l'équation diophantienne

$$1 + x + \ldots x^{p-1} = py^{\tilde{p}}, \quad x, y \in \mathbb{Z}. \tag{2.56}$$

Si $x \neq 1$, alors le théorème (1.1.1) montre que $\tilde{p}|h_p^-$, en contradiction avec la proposition (2.2.6). Ainsi (2.56) admet $x = y = 1$ pour seule solution entière.

Chapitre 3

Etude de l'équation $CX^2 + b^{2m}D = Y^n$

3.1 Introduction

On se fixe C, D deux entiers naturels premiers entre eux, avec D sans facteur carré et premier à 3. Soit également $b = 1$ ou b un nombre premier. Dans la suite, on notera par $\mathbb{K}$ le corps quadratique imaginaire $\mathbb{Q}(\sqrt{-CD})$. On désignera par h son nombre de classes. On étudie l'équation diophantienne suivante :

$$CX^2 + b^{2m}D = Y^n, \quad (2X, Y) = 1. \tag{3.1}$$

On peut supposer sans perte de généralité que C est aussi sans facteur carré. Fixons nous maintenant quelques notations pour la suite. On notera dorénavant, par ϕ_n (respectivement ψ_n) le n-ième terme de la suite de Fibonacci (respectivement de Lucas). Rappelons que la suite de Fibonacci est définie par : $\phi_0 = 0, \phi_1 = 1$ et $\phi_{n+2} = \phi_{n+1} + \phi_n$, tandis que la suite de Lucas est définie par $\psi_0 = 2$, $\psi_1 = 1$ et $\psi_{n+2} = \psi_{n+1} + \psi_n$.

Si $n \geq 2$ est un entier, on note $p(n)$ le plus grand de ses facteurs premiers. Dans ce chapitre, on se propose de montrer d'abord le nouveau théorème suivant :

Théorème 3.1.1 *Soit n un nombre premier impair, tel que $(n, h) = 1$. On suppose $n > 3$ pour $CD \equiv 3 \bmod 4$. Si $b > 2$, on suppose que $b|D$ ou que $b \neq \left(-\frac{CD}{b}\right) \bmod n$. Si l'équation (3.1) admet une solution en nombres entiers X, Y, alors $n = 3$ ou $n = 5$. De plus :*

1. *Si $C = 1$, $n = 3$, alors de deux choses l'une :*
   - *soit il existe un entier A tel que $A^2 = 1 + 3^{2m-3}D$, et alors on a $b = 3$, $X = \pm A\,(9 - 8A^2)$, $Y = 4A^2 - 3$ et $m > 0$;*
   - *soit il existe un entier A tel que $3A^2 = \epsilon + b^{2m}D$ avec $\epsilon = \pm 1$, et alors $X = \pm A\,(3\epsilon - 8A^2)$, $Y = 4A^2 - \epsilon$.*
2. *Si $C > 1$, $n = 3$, alors*

– *soit il existe un entier A tel que $A^2C - \epsilon = 3^{2m-3}D$ avec $\epsilon = \pm 1$, et alors*

$$b = 3, \quad X = \pm A\left(9\epsilon - 8A^2C\right), \quad Y = 4A^2C - 3\epsilon, \quad m > 0;$$

– *soit il existe des entiers A avec $\epsilon = \pm 1$ tel que $3A^2C - \epsilon = b^{2m}D$ et alors*

$$X = \pm A\left(3\epsilon - 8A^2C\right), \quad Y = 4A^2C - \epsilon;$$

– *soit il existe des entiers A et k tels que $8D = sb^m + 3^{k+1}\epsilon$ et $A^2C = 3D - 3^k\epsilon$ avec $\epsilon = \pm 1$, $s = \pm 1$, et alors $X = \pm A3^k$, $Y = 4D - 3^k\epsilon$;*

– *soit il existe des entiers A et k tels que $8b^{2m}D = s + 3^{k+1}$ et $A^2C = 3b^{2m}D - 3^k$ avec $s = \pm 1$, et alors $X = \pm A3^k$, $Y = 4b^{2m}D - 3^k$. Dans ce dernier cas, si $b = 3$, alors $m = 0$.*

3. *Si $C = 1$, $n = 5$, alors de deux choses l'une :*
   – *soit $b = 5$, $m = 1$, $D = 10$, $X = \pm 401$ et $Y = 11$,*
   – *soit $b^m = 1$, $D = 19$, $X = \pm 22434$, $Y = 55$,*
   – *soit $b^m = 1$, $D = 341$, $X = \pm 2759646$, $Y = 377$.*
4. *Si $C > 1$, $n = 5$, alors $Y = V_k$, où V désigne la suite de Lucas ou de Fibonacci. L'entier k est de la forme $3l + 1$ ou $3l + 2$, où l'entier l vérifie*

$$l \leq Sup\left(4, \frac{b+2}{3}, \frac{p(CD)+2}{3}, \frac{1}{3}\sqrt{\frac{b^{2m}D}{C} + \frac{1}{C}\sqrt{\frac{b^m}{5} + \frac{4}{5}b^{4m}D^2}} + \frac{2}{3}\right).$$

Si $b = 2$ et D impair, on a en fait

$$l \leq Sup\left(4, \frac{b+2}{3}, \frac{p(CD)+2}{3}, \frac{1}{3}\sqrt{\frac{4^mD}{C} + \frac{1}{C}\sqrt{\frac{1}{5} + \frac{4^{2m+1}D^2}{5}}} + \frac{2}{3}\right).$$

Une fois démontré, nous illustrerons ce théorème au paragraphe (3.4) en retrouvant les solutions entières de certaines équations diophantiennes.

En guise de première application du théorème (3.1.1), on obtient :

Corollaire 3.1.2 *Soit $\mathcal{S}$ l'ensemble des solutions (x, y, m, n) de l'équation*

$$x^2 + 3^m = y^n, n > 2, x \neq 0. \tag{3.2}$$

On pose $\mathcal{S}_i = \{(x, y, m, n) \in \mathcal{S} | m \equiv i \bmod 3\}$. On a $\mathcal{S} = \mathcal{S}_1 \cup \mathcal{S}_2$, avec

$$\mathcal{S}_1 = \left\{(\pm 46 \cdot 27^{m_0}, 13 \cdot 9^{m_0}, 4 + 6m_0, 3) : m_0 \in \mathbb{N}\right\},$$
$$\mathcal{S}_2 = \left\{(\pm 10 \cdot 27^{m_0}, 7 \cdot 9^{m_0}, 5 + 6m_0, 3) : m_0 \in \mathbb{N}\right\}.$$

Ce corollaire complète un résultat récent de Tao Liqun (voir [75]) qui résout l'équation $x^2 + 3^{2m} = y^n$, $(x, y) = 1$.

Definition 3.1.3 *Soient $m, n \geq 2$ deux entiers. Soit $z \in \mathbb{N}^*$. On dit que z est de type (m, n) ssi il existe $a, b \in \mathbb{N}^*$, tels que $z = a^m - b^n$.*

On peut énoncer le résultat précédent comme suit :

Corollaire 3.1.4 *1. Le nombre 3^m est de type $(3, 2)$ si et seulement si $m \equiv 4$ ou $5 \bmod 6$.*

2. Soit m, n deux entiers tels que $n > 3$. Alors 3^m n'est jamais de type $(n, 2)$.

Le cas de l'équation $x^p + 3^{mp} = y^q$, $(3, x) = 1$ sera également étudié : voir le chapitre 6, exemple (6.1.27) et proposition (6.1.28).

On donne également toutes les solutions à l'équation d'Aigner : si D est un entier sans facteur carré et si $p > 2$ est un nombre premier tel que $(h(-D), p) = 1$, alors, on appelle équation d'Aigner, l'équation diophantienne suivante :

$$X^2 + 4D = Y^p, \quad (X, Y) = 1 \tag{3.3}$$

Dans [25], les auteurs affirment que (3.3) n'admet pour $p = 3$ que les solutions suivantes :

1. $7^2 + 76 = 5^3$, $1015^2 + 76 = 101^3$
2. $155^2 + 364 = 29^3$, $10681^2 + 364 = 485^3$

Plus précisément, ils montrent pour $p > 3$, que l'équation d'Aigner n'admet aucune solution et affirment que Aigner l'a complètement résolue dans le cas $p = 3$, les seules solutions étant dans ce cas, les valeurs précédemment citées. Ils en déduisent donc que ces valeurs sont les seules solutions de (3.3).

En fait, dans [2], **Aigner montre seulement** que $D = 19$ et $D = 91$ sont les seuls entiers pour lesquels il existe un nombre premier impair p, tel que (3.3) admet plus d'une solution (X, Y) avec $X > 0$. **Mais contrairement à ce qui est affirmé dans [25]**, on peut trouver des entiers D pour lesquels il existe un nombre premier p, tels que (3.3) admet au moins une solution (X, Y) avec $X > 0$. Par exemple, si $D = 7$, alors $X = 225$ et $Y = 37$ conviennent $(h(-7) = 1)$. Comme autre conséquence du théorème (3.1.1), on se propose de donner la résolution **complète** de (3.3). Commençons par poser la définition suivante :

Definition 3.1.5 *Soit D un entier sans facteur carré. On dit que D est convenable si 3 est premier à $h(-D)$, et s'il existe un entier A tel que $D = 3A^2 - 16\epsilon$ ou bien $D = \frac{3A^2+1}{4}$ avec $\epsilon = \pm 1$.*

On obtient alors comme nouveau résultat, la résolution **complète** suivante :

Corollaire 3.1.6 *Soit D un entier sans facteur carré. L'équation (3.3) n'a aucune solution entière (X, Y) si $p > 3$. Si $p = 3$, alors l'équation d'Aigner admet des solutions si et seulement si D est convenable. Si c'est le cas, on a les relations suivantes : soit $D = \frac{3A^2+1}{4}$, $X = \pm A\left(8A^2 + 3\right)$, $Y = 4A^2 + 1$, soit $D = 3A^2 - 16\epsilon$, $X = \pm A\left(A^2 - 6\epsilon\right)$, $Y = \frac{A^2+D}{4}$. De plus, $D = 19$ et $D = 91$ sont les seuls entiers convenables pour lesquels l'équation (3.3) admet plus d'une solution positive (X, Y).*

Par exemple, 7 est un entier convenable au sens de la définition (3.1.5). En effet, $h(-7) = 1$ et $7 = \frac{3\cdot 3^2+1}{4}$. Le corollaire précédent montre alors que l'équation $X^2 + 28 = Y^3$ admet des solutions entières vérifiant $(X, Y) = 1$. Celles-ci sont données par : $X = \pm 3\left(8 \cdot 3^2 + 3\right) = \pm 225$ et $Y = 4 \cdot 3^2 + 1 = 37$.

On résout aussi l'équation suivante, en entiers strictement positifs X et n :

$$2X^2 + 1 = 3^n. \tag{3.4}$$

Il est affirmé dans [25], suite à une erreur de Maohua Le, que les seules solutions sont $(1, 1)$ et $(2, 2)$. Néanmoins, Ming-Guan Leu et Guan-Wei Li remarquent que $(11, 5)$ est aussi solution, et montrent dans [57] qu'il n'y en a pas d'autres. Ils utilisent pour cela des résultats de Beukers (voir [6]).

Néanmoins, soulignons ici que ce résultat est en fait une conséquence du théorème classique de Nagell-Ljunggren ; voir la fin du Paragraphe 3.7.2. On montrera que ce résultat est aussi une conséquence d'une application séquentielle du théorème (3.1.1). Plus précisément, on va montrer le théorème suivant (dont la démonstration et le théorème (3.1.1) permettront en particulier de résoudre (3.4)) :

Théorème 3.1.7 *Soit $C > 0$, $C \neq 1, 3$ un entier sans facteur carré. Soit $h = h(-C)$ le nombre de classes du corps quadratique imaginaire $\mathbb{Q}(\sqrt{-C})$. Soient m un entier naturel, l un nombre premier impair, $b = 1$ ou b un nombre premier tels que $l = C + b^{2m}$.*

On considère la suite $(b_n)_n$ définie par $b_0 = 1, \quad b_1 = b^m$ et $b_{n+2} = 2b^m b_{n+1} - l b_n$.

L'ensemble $\mathcal{E}$ désigne l'ensemble des entiers $n \geq 1$, tels que les assertions suivantes soient vérifiées :

- *$b_n = \pm b^m$,*
- *$n = 1$ ou il existe un nombre premier p tel que $p|n$ et $(p, 6h) = 1$,*
- *$b \neq \left(\frac{-C}{b}\right) \bmod n$ si $b > 2$.*

On désigne par $\mathcal{E}'$ l'ensemble des entiers $n \geq 1$ tels que $b_n = \pm b^m$.

On a alors $\mathcal{E} = \{1\}$, sauf si $l = 3$. Dans ce cas, on a $\mathcal{E} = \{1, 5\}$. De plus, $\mathcal{E}'$ est effectif.

La démonstration du résultat précédent permettra aussi de montrer la proposition suivante (sans utiliser le théorème des diviseurs primitifs) :

Proposition 3.1.8 *Soit l un nombre premier impair. On pose $l = C + 1$. On suppose que C est sans facteur carré. Soit (b_n) la suite d'entiers définie par $b_0 = b_1 = 1$, et $b_{n+2} = 2b_{n+1} - lb_n$.*

Soit $\mathcal{E}$ les entiers $n > 0$ tels que $b_n = \pm 1$. On a les assertions suivantes :

1. *Si $l = 3$, alors $|\mathcal{E}| = 3$.*
2. *Si $l = 7$, alors $|\mathcal{E}| = 2$.*
3. *Dans les autres cas, on a $|\mathcal{E}| = 1$.*

On se propose également en guise d'application du théorème (3.1.1) d'étudier les équations de la forme

$$Cx^2 + q^m = y^n, \quad x \neq 0,$$

où $m \geq 0$ est un entier, $q \geq 2$ est un nombre premier, C un entier sans facteur carré.

Dans un premier temps, on étudie le cas $q = 2$. On se propose alors de **résoudre complètement l'équation** si m pair et $C \neq 7 \bmod 8$; puis si m est impair sans aucune hypothèse cette fois sur la valeur de $C \bmod 8$. Cette résolution du cas $q = 2$ étend un résultat très récent (2008) de Muriefah qui montre dans [60] (théorème 2.2) que l'équation précédente, cas $q = 2$, est sans solution entière pour $n > 3$, m pair, $m > 0$ et $(x, y) = 1$. Cela généralise également le théorème 2.3 de [60] qui montre que le cas $q = 2$, $n > 3$ est bien sans solution entière, mais uniquement pour C premier impair.

On commence par redémontrer le corollaire suivant en tant que conséquence seule du théorème (3.1.1) et de sa démonstration. On retrouve ainsi, outre le résultat du théorème 2.2 de [60], les résultats du théorème 1.1 de [59] :

Corollaire 3.1.9 *Soit n un nombre premier impair, $m > 0$ un entier, et soit $C > 0$ un entier impair sans facteur carré. On suppose que $(h(-C), n) = 1$. Alors, l'équation*

$$CX^2 + 2^{2m} = Y^n, (X, Y) = 1 \tag{3.5}$$

n'admet aucune solution entière si $n \geq 5$.

De plus, si $n = 3$, alors il existe des solutions si et seulement s'il existe un entier b tel que $Cb^2 = \frac{1+2^{m+3}}{3}$ et m est pair, ou $Cb^2 = \frac{2^{2m}-1}{3}$. Dans le premier cas, on a $X = \pm b\left(\frac{2^m-1}{3}\right), Y = \frac{1+2^{m+1}}{3}$, et dans le second cas, $X = \pm b\left(\frac{8.4^m+1}{3}\right), Y = \frac{4^{m+1}-1}{3}$.

Remarque 3.1.10 *1. Si $C = n$, l'hypothèse $(h(-C), n) = 1$ peut être omise (voir [32]).*

2. *Indépendamment des résultats, on peut montrer (voir [59]) que l'équation* $Cx^2+2^{2m} = y^n, (x,y) = 1$ *où* $C > 1, m > 0$ *et* $(h(-C), n) = 1$ *, n premier impair, possède au plus une solution* (x, y) *en entiers positifs.*

Notons en particulier le

Corollaire 3.1.11 *Soit C un entier impair sans facteur carré, soit* $m > 0$ *un entier et soit* $n > 3$ *un nombre premier tel que* $(n, h(-C)) = 1$*. Alors, l'équation*

$$Cx^2 + 2^{2m} = y^n, (x,y) = 1 \tag{3.6}$$

n'a aucune solution.

On peut maintenant résoudre de façon complète le cas $q = 2$, m pair et $C \neq 7 \bmod 8$ comme annoncé précédemment, généralisant ainsi le théorème 2.3 de [60] :

Théorème 3.1.12 *Soit* $n \geq 3$ *un nombre premier. Soit* $C \geq 1$, $C \neq 7 \bmod 8$*, un entier impair sans facteur carré tel que* $n \nmid h(-C)$*. Soit* $m > 0$ *un entier. Supposons que l'équation*

$$Cx^2 + 2^{2m} = y^n, \quad x \neq 0, \tag{3.7}$$

admette une solution entière. Alors on est dans l'un des cas suivant

- $C = 1$, $m > 0$, $n|2m+1$, $(x,y) = \left(\pm 2^m, 2^{\frac{2m+1}{n}}\right)$,
- $C = 1$, $3|m-1$, $n = 3$, $(x,y) = \left(\pm 11 \cdot 2^{m-1}, 5 \cdot 4^{\frac{m-1}{3}}\right)$,
- $C = 3$, $n|m+1$, $(x,y) = \left(\pm 2^m, 4^{\frac{m+1}{n}}\right)$,
- $C > 1$, $n = 3$*, il existe un entier* b *et un entier* $u < m$ *divisible par* 3 *tels que*

$$Cb^2 = \frac{1 + 2^{m-u+3}}{3}, \quad 2|m-u,$$

ou

$$Cb^2 = \frac{2^{2m-2u} - 1}{3}.$$

Dans le premier cas

$$x = \pm b \cdot \frac{2^m - 2^u}{3}, \quad y = 2^{\frac{2u}{3}} \cdot \frac{1 + 2^{m-u+1}}{3}.$$

Dans le second cas

$$x = \pm b \cdot \frac{2^{2m-u+3} + 2^u}{3}, \quad y = 2^{\frac{2u}{3}} \cdot \frac{4^{m-u+1} - 1}{3}.$$

En particulier si $n > 3$ et $C > 1$, l'équation (3.7) n'admet aucune solution entière.

Si on prend $C = n > 3$, le théorème précédent redonne le théorème principal de [60] comme annoncé précédemment. (Le nombre de classes de $\mathbb{Q}(\sqrt{-n})$ est toujours premier à n si n est premier).

Exemple 3.1.13 *Considérons l'équation $85x^2 + 2^{14} = y^n$, $n > 2$ premier. Si $x = 0$ convient, alors $2^{14} = y^n$ donc $n = 7$, $y = 4$. Si $x \neq 0$, comme $h(-85) = 4$ on peut appliquer le corollaire (3.1.12). Nécessairement $n = 3$. Il existera une solution ssi il existe des entiers b et u tels que*

$$85b^2 = \frac{2^{14-2u} - 1}{3}, \quad 3|u, \quad 0 \leq u < 7,$$

ou

$$85b^2 = \frac{1 + 2^{10-u}}{3}, \quad 3|u, \quad 2 \nmid u, 0 < u < 7.$$

Dans ce dernier cas, au plus $u = 3$ mais cela donnerait $C = 43$. Dans le premier cas, on trouve $u = 3$ comme seule possibilité. Les solutions cherchées pour $n = 3$ sont donc

$$x = \pm\left(\frac{2^{14} + 2^3}{3}\right) = \pm 5464, \quad y = 4 \cdot \frac{4^5 - 1}{3} = 1364.$$

On s'intéresse maintenant au cas $q = 2$ et m impair. On redémontre le théorème suivant comme conséquence du théorème (3.1.1)

Théorème 3.1.14 *(Muriefah) Soit $n \geq 3$ un nombre premier. Soit $C \geq 1$ un entier impair sans facteur carré tel que $n \nmid h(-C)$ et $m \geq 0$ un entier. Supposons qu'il existe des entiers X, Y tels que*

$$CX^2 + 2^{2m+1} = Y^n, \quad (X, Y) = 1. \tag{3.8}$$

Alors, nécessairement $n = 3$. Il existe des solutions entières si et seulement s'il existe un entier A tel que $A^2C = \frac{2^{2m+1}+1}{3}$. Si c'est le cas, on a

$$X = \pm A\left(\frac{4^{m+2} - 1}{3}\right), \quad Y = \frac{2^{2m+3} + 1}{3}.$$

On en déduit le nouveau

Corollaire 3.1.15 *Soit $n \geq 3$ un nombre premier. Soit $C \geq 1$ un entier impair sans facteur carré tel que $n \nmid h(-C)$ et $m \geq 0$ un entier. Supposons qu'il existe des entiers x, y tels que*

$$Cx^2 + 2^{2m+1} = y^n, \quad x \neq 0. \tag{3.9}$$

Alors on est dans l'un des cas suivant :

– *$n = 3$, il existe des entiers A et u tels que*

$$A^2C = \frac{2^{2(m-u)+1}+1}{3}, \quad 3|u$$

et alors

$$x = \pm A 2^u \left(\frac{4^{m-u+2}-1}{3}\right), \quad y = 2^{\frac{2u}{3}} \frac{2^{2(m-u)+3}+1}{3}.$$

– *soit $n = 5$, $C = 1$, $5|2m+1$ et alors*

$$x = \pm 2^{m+1} \cdot 11, \quad y = 2^{\frac{2m+1}{5}} \cdot 3.$$

Exemple 3.1.16 *Considérons l'équation $11x^2 + 2^{17} = y^n$, $x \neq 0$, avec $n > 2$ nombre premier. Alors nécessairement $n = 3$. De plus, il existe des solutions entières s'il existe un entier $u \leq 8$ divisible par 3 et un entier A tels que*

$$11A^2 = \frac{2^{17-2u}+1}{3}.$$

On vérifie que seule la valeur $u = 6$ convient, valeur pour laquelle $A = \pm 1$. Les seules solutions entières de l'équation sont donc

$$x = \pm 2^6 \frac{4^4-1}{3} = \pm 5440, \quad y = 2^4 \frac{2^7+1}{3} = 688.$$

Muriefah s'est également intéréssée aux équations de la forme $pX^2+q^{2m} = Y^p$, $(X, Y) = 1$, avec p, q premiers impairs distincts. Toujours dans [60], elle a montré que si $p \neq 3 \bmod 4$, $p > 3$, $m > 0$, alors l'existence de solutions (X, Y), Y n'étant pas de la forme $pA^2 + 1$, n'est possible que si $p = 5$, Y étant alors un nombre de Lucas ou de Fibonacci (voir les commentaires (3.12.1)), sans préciser toutefois de borne explicite pour les indices possibles des termes de Lucas ou Fibonacci. Notre théorème (3.1.1) nous donne plus généralement

Corollaire 3.1.17 *Soient b, p deux nombres premiers impairs, $p > 3$, $m \geq 0$ un entier et $C \neq 7 \bmod 8$ un entier sans facteur carré tel que $p \nmid h(-C)$. On suppose que $b \neq \left(\frac{-C}{b}\right) \bmod n$ si $m > 0$. Alors l'équation*

$$CX^2 + b^{2m} = Y^p, (X, Y) = 1, \tag{3.10}$$

n'a aucune solution (X, Y) si $p > 5$. De plus, si $p = 5$ et s'il existe une solution (X, Y), alors il existe un entier $E > 0$ et un entier B éventuellement négatif divisant b^m tel que

$$\frac{b^m}{B} + 4B^4 = 5E^2.$$

Alors $Y = E + 2B^2$ *et il existe un entier* k *tel que* $Y = \phi_{3k+1}, \phi_{3k+2}, \psi_{3k+1}$ *ou* ψ_{3k+2}. *De plus, cet entier* k *vérifie*

$$k \leq Sup\left(4, \frac{b+2}{3}, \frac{p(C)+2}{3}, \frac{1}{3}\sqrt{\frac{b^{2m}}{C} + \frac{1}{C}\sqrt{\frac{b^m}{5} + \frac{4}{5}b^{4m}} + \frac{2}{3}}\right).$$

Ce corollaire contient le résultat de Muriefah précédemment cité (voir les commentaires après la preuve du corollaire). De plus, notre corollaire précise une borne effective sur k dans le cas $p = 5$.

Exemple 3.1.18 *Considérons un entier impair* C *sans facteur carré et* $n > 3$ *un nombre premier tel que* $n \nmid h(-2C)$. *Supposons qu'il existe des entiers* X, Y, *tels que*

$$2CX^2 + 1 = Y^n.$$

Le théorème précédent montre que nécessairement $n = 5$. *On a pour cette équation* $B = \pm 1$ *et* $\pm 1 + 4 = 5E^2$. *On doit donc avoir* $B = 1$, $E = 1$, $Y = 3$. *On trouve alors que* $2CX^2 = 2 \cdot 11^2$. *On doit donc avoir* $C = 1$ *et les solutions entières sont donc* $X = \pm 11$, $Y = 3$.

Corollaire 3.1.19 *Soient* b, p *deux nombres premiers impairs,* $p > 3$, $m \geq 0$ *un entier et* C *un entier sans facteur carré tel que* $p \nmid h(-C)$ *et* $Cb \neq 7 \bmod 8$. *Alors l'équation*

$$CX^2 + b^{2m+1} = Y^p, (X, Y) = 1,$$

n'a aucune solution (X, Y) *si* $p > 5$. *De plus, si* $p = 5$ *et s'il existe une solution* (X, Y), *alors il existe un entier* $E > 0$ *et un entier* B *éventuellement négatif divisant* b^m *tel que*

$$\frac{b^m}{B} + 4B^4b^2 = 5E^2.$$

Alors $Y = E + 2B^2$ *et il existe un entier* k *tel que* $Y = \phi_{3k+1}, \phi_{3k+2}, \psi_{3k+1}$ *ou* ψ_{3k+2}. *De plus, cet entier* k *vérifie*

$$k \leq Sup\left(4, \frac{b+2}{3}, \frac{p(C)+2}{3}, \frac{1}{3}\sqrt{\frac{b^{2m+1}}{C} + \frac{1}{C}\sqrt{\frac{b^m}{5} + \frac{4}{5}b^{4m+2}} + \frac{2}{3}}\right).$$

Dans le cas où l'on ne fait plus d'hypothèse sur la valeur de $b \bmod n$ dans (3.1), on obtient :

Théorème 3.1.20 *On fait les hypothèses suivantes :*

1. *Il existe* $X, Y \in \mathbb{N}$, *tels que* $CX^2 + b^{2m}D = Y^n$, *où* n *est un nombre premier,* $n \geq 5$.
2. $(2X, Y) = 1$.
3. $(n, h) = 1$.

On a l'inégalité suivante :

$$n \leq 1 + c_0 H^2 + \frac{11\pi c_0 H^2 + \log(8b^m)}{\log(\sqrt{D_0}/2)}.$$

où on a posé

$$c_0 = 8.87, \quad D_0 = Sup(12, C + D), \quad H = H(n) = 7.38 + \log\left(\frac{n}{68.9} + \frac{n}{22\pi + \log(3)}\right).$$

On a aussi les assertions suivantes :

- *Si* $16b^m \leq \sqrt{D}$, *alors il existe une constante absolue effective* N_1 *telle que* $n \leq N_1$.
- *Il existe une constante absolue effective* N_2, *telle que si* $n \geq N_2$, *alors* $X \leq \frac{4b^{2m}D}{C}$.

Remarque 3.1.21 *On verra au cours de la démonstration que l'on peut prendre* $N_1 = 139297$, *et* $N_2 = 307451$.

Par exemple, si on applique le théorème précédent à l'équation d'Aigner, on obtient $n \leq 139303$. On obtient une meilleure borne que celle de Le, qui montre dans [43], que $n < 10^6$. Notons que Le fut le premier à montrer dans [43] que l'équation d'Aigner est sans solution pour n premier et $n > 10^6$.

Dans la suite, l'abréviation HRG signifie hypothèse de Riemann généralisée. On appelle conjecture GS (pour Granville-Soundararajan) la conjecture suivante faite dans [35] :

Conjecture 3.1.22 *Si* χ *est un caractère primitif modulo* q, *on a l'inégalité suivante :*

$$\left|\sum_{n \leq x} \chi(n)\right| \leq \left(\frac{e^\gamma}{\pi} + o(1)\right)\sqrt{q}\log\log(q). \tag{3.11}$$

Enfin, si n n'est plus supposé premier et si CD est encore quelconque modulo 4, on a le théorème suivant :

Théorème 3.1.23 *Supposons qu'il existe* $X, Y \in \mathbb{N}$ *tels que (3.1) admette une solution, avec* $n \in \mathbb{N}$, $n > 1$, $CD > 1$, $CD \neq 3$ *et* $(2b, Y) = 1$. *On définit l'entier* $t \in \{0; 1\}$ *comme suit : si* $CD \neq 3 \bmod 4$, *on pose* $t = 1$, *et* $t = 0$ *sinon.*

Alors, on a l'inégalité suivante

$$n \leq \frac{c_0 H^2 \left(11\pi + M \log\left(\sqrt{C}\right)\right) + \log\left(2Mb^m\sqrt{5D}\right)}{\log(\sqrt{3})} + c_0 M H^2.$$

où $M = \frac{1}{2^{1-t}\pi(2-\chi(2))}(1+o(1))\sqrt{CD}\log(4^t CD)$, *avec* $o(1)$ *infiniment petit lorsque* CD *tend vers l'infini. Sous HRG, on peut prendre* $M = \frac{2^{t+2}e^\gamma}{\pi(2-\chi(2))}(1+o(1))\sqrt{CD}\log\log(4^t CD)$, *et sous GS on peut prendre* $M = \frac{2^{t+1}e^\gamma}{\pi(2-\chi(2))}(1+o(1))\sqrt{CD}\log\log(4^t CD)$.

3.2 Paires de Lucas et de Lehmer.

3.2.1 Définitions et notations.

Une paire de Lucas est une paire (α, β) d'entiers algébriques tels que $\alpha+\beta$ et $\alpha\beta$ soient des entiers relatifs premiers entre eux et $\frac{\alpha}{\beta}$ ne soit pas une racine de l'unité. Si (α, β) est une paire de Lucas, on lui associe la suite des nombres de Lucas $(u_n(\alpha, \beta))$ définie par

$$u_n = u_n(\alpha, \beta) = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad (n = 0, 1, 2 \ldots).$$

Une paire de Lehmer est une paire (α, β) d'entiers algébriques tels que $(\alpha+\beta)^2$ et $\alpha\beta$ soient des entiers relatifs premiers entre eux et $\frac{\alpha}{\beta}$ ne soit pas une racine de l'unité. Si (α, β) est une paire de Lehmer, on lui associe la suite des nombres de Lehmer

$$\tilde{u}_n = \tilde{u}_n(\alpha, \beta) = \begin{cases} \frac{\alpha^n - \beta^n}{\alpha - \beta} & \text{si } n \text{ est impair,} \\ \frac{\alpha^n - \beta^n}{\alpha^2 - \beta^2} & \text{sinon.} \end{cases}$$

Definition 3.2.1 *Soit* p *un nombre premier et soit* (α, β) *une paire de Lucas. On dit que* p *est un diviseur primitif de* $u_n(\alpha, \beta)$ *si et seulement si* p *divise* $u_n(\alpha, \beta)$, *mais ne divise pas* $(\alpha - \beta)^2 u_1 \ldots u_{n-1}$.

Definition 3.2.2 *Soit* p *un nombre premier et soit* (α, β) *une paire de Lehmer. On dit que* p *est un diviseur primitif de* $\tilde{u}_n(\alpha, \beta)$ *si et seulement si* p *divise* $\tilde{u}_n(\alpha, \beta)$, *mais ne divise pas* $(\alpha^2 - \beta^2)^2 \tilde{u}_1 \ldots \tilde{u}_{n-1}$.

Definition 3.2.3 *Une paire de Lucas (respectivement de Lehmer)* (α, β) *est dite* n*-défectueuse si et seulement si* $u_n(\alpha, \beta)$ *(respectivement* $\tilde{u}_n(\alpha, \beta)$*) n'a aucun diviseur primitif.*

3.2.2 Quelques résultats classiques.

Proposition 3.2.4 *Soient (α, β) une paire de Lehmer et $(\tilde{u}_n)$ la suite des nombres de Lehmer correspondante. On a les assertions suivantes :*

1. *Pour tout entier positif n, on a $(\alpha\beta, \tilde{u}_n) = 1$.*
2. *Si d est un diviseur de n, alors $\tilde{u}_d | \tilde{u}_n$ et $\left(\frac{\tilde{u}_n}{\tilde{u}_d}, \tilde{u}_d\right)$ divise $\frac{n}{d}$.*
3. *Pour tout entier positif m et n, on a $(\tilde{u}_m, \tilde{u}_n) = \tilde{u}_{(m,n)}$.*
4. *Si un nombre premier p ne divise pas $\alpha\beta\left(\alpha^2 - \beta^2\right)^2$, alors p divise $\tilde{u}_{p-1}\tilde{u}_{p+1}$.*
5. *Si un nombre premier p divise $\tilde{u}_m$ alors p divise $\frac{\tilde{u}_{mp}}{\tilde{u}_m}$.*
6. *Dans l'assertion précédente, si $p > 2$, alors p divise exactement*[1] $\frac{\tilde{u}_{mp}}{\tilde{u}_m}$.
7. *Si $4 | \tilde{u}_m$, alors 2 divise exactement $\frac{\tilde{u}_{2m}}{\tilde{u}_m}$.*
8. *Si un nombre premier $p > 2$ divise $(\alpha - \beta)^2$ alors p divise $\tilde{u}_p$; si $p > 3$ alors p divise exactement $\tilde{u}_p$.*
9. *Si un nombre premier p divise $(\alpha + \beta)^2$ alors p divise $\tilde{u}_{2p}$; si $p > 3$ alors p divise exactement $\tilde{u}_{2p}$.*

Preuve On définit la suite $\tilde{v}_n = \tilde{v}_n(\alpha, \beta)$ par

$$\tilde{v}_n = \begin{cases} \frac{\alpha^n + \beta^n}{\alpha + \beta} & \text{si } n \text{ est impair,} \\ \alpha^n + \beta^n & \text{sinon.} \end{cases}$$

Dans la suite de la preuve, $A_0, A_1, \ldots, A_n$ désignent des entiers algébriques.

– preuve de l'assertion (1) : On a

$$(\alpha + \beta)^{2n} = \alpha^{2n} + \beta^{2n} + \alpha\beta A_0 = v_{2n} + \alpha\beta A_0.$$

Comme $(\alpha\beta, (\alpha + \beta)^2) = 1$, on a $(v_{2n}, \alpha\beta) = 1$. De même

$$\frac{\alpha^{2n+1} + \beta^{2n+1}}{\alpha + \beta} = \alpha^{2n} + \beta^{2n} + \sum_{k=1}^{2n-1} (-1)^k \alpha^k \beta^{2n-k} = v_{2n} + \alpha\beta A_1,$$

donc $(v_{2n+1}, \alpha\beta) = 1$. Soit alors n un entier impair :

$$\tilde{u}_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \alpha^{n-1} + \beta^{n-1} + \alpha\beta A_2 = v_{n-1} + \alpha\beta A_2.$$

[1] c'est à dire p le divise mais pas p^2.

Comme $(v_{n-1}, \alpha\beta) = 1$, on a $(\tilde{u}_n, \alpha\beta) = 1$ si n est impair. Fixons n pair.

$$\begin{aligned}\tilde{u}_n &= \frac{\alpha^n - \beta^n}{\alpha^2 - \beta^2} = \frac{\alpha^{n-1} + \beta^{n-1}}{\alpha + \beta} + \alpha\beta\left(\frac{\alpha^{n-2} - \beta^{n-2}}{\alpha^2 - \beta^2}\right) \\ &= \frac{\alpha^{n-1} + \beta^{n-1}}{\alpha + \beta} + \alpha\beta A_3 = v_{n-1} + \alpha\beta A_3,\end{aligned}$$

d'où $(\tilde{u}_n, \alpha\beta) = 1$ si n est pair.
L'assertion (1) est prouvée.

– preuve de l'assertion (2) : Si $d|n$, en écrivant $\alpha^n = \left(\beta^d + (\alpha^d - \beta^d)\right)^{\frac{n}{d}}$, il vient

$$\frac{\alpha^n - \beta^n}{\alpha^d - \beta^d} = \frac{n}{d}\beta^{n-d} + \left(\alpha^d - \beta^d\right)\sum_{k=0}^{\frac{n}{d}-2}\binom{n/d}{k}\beta^{kd}\left(\alpha^d - \beta^d\right)^{\frac{n}{d}-k-2}. \tag{3.12}$$

Si $n - d$ est pair, l'égalité précédente multipliée par α^{n-d} devient

$$\alpha^{n-d}\frac{\tilde{u}_n}{\tilde{u}_d} = \frac{n}{d}\left(\alpha\beta\right)^{n-d} + A_4\tilde{u}_d,$$

et si $n - d$ est impair (donc $2|n$, $2 \nmid d$), elle devient

$$\alpha^{n-d}\left(\alpha + \beta\right)\frac{\tilde{u}_n}{\tilde{u}_d} = \frac{n}{d}\left(\alpha\beta\right)^{n-d} + A_5\tilde{u}_d.$$

L'assertion résulte de ces deux égalités et du fait que $(\tilde{u}_n, \alpha\beta) = 1$.

– preuve de l'assertion (3) : soient donc m, n deux entiers positifs. Il existe deux entiers positifs r et s tels que $rm - sn = (m, n)$. Posons $k = rm$ et $l = sn$ de sorte que $k - l = (k, l)$. On vérifie que

$$\left(\alpha^k - \beta^k\right)\left(\alpha^l + \beta^l\right) - \left(\alpha^l - \beta^l\right)\left(\alpha^k + \beta^k\right) = 2\left(\alpha\beta\right)^l\left(\alpha^{k-l} - \beta^{k-l}\right).$$

Comme $k - l = (k, l)$, si $k - l$ est pair, il vient

$$\tilde{u}_k v_l - \tilde{u}_l v_k = 2\left(\alpha\beta\right)^l\tilde{u}_{k-l},$$

et pour $k - l$ impair

$$\begin{aligned}\left(\alpha + \beta\right)^2\tilde{u}_k v_l - \tilde{u}_l v_k &= 2\left(\alpha\beta\right)^l\tilde{u}_{k-l} \quad \text{si } l \text{ est impair,} \\ \tilde{u}_k v_l - \left(\alpha + \beta\right)^2\tilde{u}_l v_k &= 2\left(\alpha\beta\right)^l\tilde{u}_{k-l} \quad \text{si } k \text{ est impair.}\end{aligned}$$

Si 2 ne divise pas $(\tilde{u}_k, \tilde{u}_l)$, l'assertion (1) et les trois égalités précédentes montrent que $(\tilde{u}_k, \tilde{u}_l)\,|\tilde{u}_{k-l}$. Supposons maintenant que 2 divise $\tilde{u}_k$ et $\tilde{u}_l$. Puisque $\frac{\tilde{u}_{2k}}{\tilde{u}_k} = v_k$, on a, en posant $d = k$ et $n = 2k$ dans les deux equations suivant (3.12), que si k est pair

alors $2|v_k$ (rappelons que $(\alpha\beta, \tilde{u}_k) = 1$), tandis que si k est impair, alors $2|(\alpha+\beta)^2 v_k$; et la même chose a lieu avec k remplacé par l. On déduit encore des trois équations précédentes que $(\tilde{u}_k, \tilde{u}_l)\,|\tilde{u}_{k-l}$.

Rappelons que

$$\alpha^n - \beta^n = \prod_{d|n} \Phi_d(\alpha, \beta), \tag{3.13}$$

où

$$\Phi_d(\alpha, \beta) = \prod_{j=1,(j,n)=1}^{n} \left(\alpha - \zeta^j \beta\right),$$

ζ étant une racine primitive d-ième de l'unité. On déduit de (3.13) que $\tilde{u}_m|\tilde{u}_k$ et $\tilde{u}_n|\tilde{u}_l$, donc que $(\tilde{u}_m, \tilde{u}_n)$ divise $(\tilde{u}_k, \tilde{u}_l)$; comme ce dernier divise $\tilde{u}_{k-l} = \tilde{u}_{(m,n)}$, on en déduit donc que $(\tilde{u}_m, \tilde{u}_n)$ divise $\tilde{u}_{(m,n)}$. Comme (3.13) montre que $\tilde{u}_{(m,n)}$ divise $\tilde{u}_m$ et $\tilde{u}_n$, l'assertion est prouvée.

– preuve de l'assertion (4) : si $p > 2$, on a

$$(\alpha - \beta)^2 (\alpha + \beta)^2 \tilde{u}_{p-1}\tilde{u}_{p+1} = \alpha^{2p} + \beta^{2p} - \left(\alpha^2 + \beta^2\right)(\alpha\beta)^{p-1}.$$

Par le petit théorème de Fermat, il vient

$$(\alpha - \beta)^2 (\alpha + \beta)^2 \tilde{u}_{p-1}\tilde{u}_{p+1} \equiv 0 \bmod p,$$

et l'assertion est prouvée si $p > 2$. Supposons $p = 2$. On a

$$\tilde{u}_{p-1}\tilde{u}_{p+1} = \tilde{u}_3 = \alpha^2 + \beta^2 + \alpha\beta.$$

Si $2 \nmid \alpha\beta u_3$, alors il divise $\alpha^2 + \beta^2 + 2\alpha\beta = (\alpha + \beta)^2$. L'assertion est encore prouvée dans ce cas.

– preuve de l'assertion (5) : De l'égalité (3.12), on a pour p premier et $m \geq 1$ entier

$$\frac{\alpha^{mp} - \beta^{mp}}{\alpha^m - \beta^m} = p\beta^{m(p-1)} + \sum_{k=0}^{p-2} \binom{p}{k} \beta^{km} (\alpha^m - \beta^m)^{p-k-1}. \tag{3.14}$$

Supposons d'abord $p > 2$. De (3.14), il vient

$$\frac{\tilde{u}_{mp}}{\tilde{u}_m} = pA_6 + (\alpha^m - \beta^m)^{p-1}. \tag{3.15}$$

Comme $A_7\tilde{u}_m = \alpha^m - \beta^m$, on en déduit que si $p|\tilde{u}_m$, alors $p|\frac{\tilde{u}_{mp}}{\tilde{u}_p}$. Supposons $p = 2$. Dans ce cas, (3.14) donne

$$\frac{\alpha^{2m} - \beta^{2m}}{\alpha^m - \beta^m} = 2\beta^m + (\alpha^m - \beta^m).$$

Or

$$\frac{\alpha^{2m}-\beta^{2m}}{\alpha^m-\beta^m}=\begin{cases}(\alpha+\beta)\,\frac{\tilde{u}_{2m}}{\tilde{u}_m} & \text{si } m \text{ est impair,}\\ \frac{\tilde{u}_{2m}}{\tilde{u}_m} & \text{si } m \text{ est pair.}\end{cases}$$

Si $2|\tilde{u}_m$ avec m pair ou m impair et $2\nmid(\alpha+\beta)^2$, alors comme précédemment, on déduit que $2|\frac{\tilde{u}_{2m}}{\tilde{u}_m}$. Si 2 divise $(\alpha+\beta)^2=\tilde{u}_4+2\alpha\beta$, alors 2 divise $\tilde{u}_4$, et donc par l'assertion (3) ne peut diviser $\tilde{u}_m$ avec m impair. L'assertion est prouvée.

– preuve de l'assertion (6) : De l'égalité (3.14), on peut écrire pour $p>2$

$$\alpha^{m(p-1)}\frac{\tilde{u}_{mp}}{\tilde{u}_m}-p\,(\alpha^m-\beta^m)\,A_8-(\alpha^m-\beta^m)^{p-1}\,\alpha^{m(p-1)}=p\,(\alpha\beta)^{m(p-1)}\,. \tag{3.16}$$

S'il était possible d'avoir $p^2|\alpha^{m(p-1)}\frac{\tilde{u}_{mp}}{\tilde{u}_m}$ pour $p|\tilde{u}_m$, alors (3.16) montrerait que $p|\alpha\beta$, en contradiction avec l'assertion (1). L'assertion (6) est prouvée.

– preuve de l'assertion (7) : C'est une conséquence facile de l'assertion (1) et de l'étude faite dans le cas $p=2$, lors de la preuve de l'assertion (5).

– preuve de l'assertion (8) : pour avoir la première partie, il suffit de prendre $m=1$ dans (3.15). Supposons que $p>3$ divise $(\alpha-\beta)^2$. De (3.12) appliqué avec $m=1$, alors

$$\tilde{u}_p\equiv p\beta^{p-1} \bmod p^2.$$

Par l'assertion (1), on a donc $p||\tilde{u}_p$.

– preuve de l'assertion (9) : idem que précédemment en prenant $m=2$.

□

Corollaire 3.2.5 *Soit (α,β) une paire de Lehmer et $(\tilde{u}_n)$ la suite associée des nombres de Lehmer. Soit p un nombre premier ne divisant pas $\alpha\beta$. Il existe alors un entier m tel que p divise $\tilde{u}_m$. Soit m_p le plus petit entier jouissant de cette propriété. On a alors*

$$p|\tilde{u}_m \Longleftrightarrow m_p|m, \tag{3.17}$$

et

$$\begin{array}{ll} m_p=p & \textit{si } p>2 \textit{ et } p|(\alpha-\beta)^2,\\ m_p=2p & \textit{si } p|(\alpha+\beta)^2,\\ m_p|(p\pm1) & \textit{sinon.}\end{array}$$

Preuve L'existence d'un entier m tel que $p|\tilde{u}_m$ résulte de la conjonction des asssertions (4), (8) et (9) de la proposition précédente.

L'implication " $\Leftarrow$ " dans (3.17) résulte de l'assertion (2), et l'implication " $\Rightarrow$ " résulte de (3).

Le fait que $m_p = p$ si $p > 2$ et $p|(\alpha-\beta)^2$, résulte de l'assertion (8). Le fait que $m_p|(p\pm 1)$ si $p \nmid (\alpha^2-\beta^2)^2$ résulte de l'assertion (4). Le cas $p = 2$ et $p \nmid (\alpha+\beta)^2$ résulte aussi de (4). Dans ce dernier cas $m_2 = 3$. Il nous reste à montrer $m_p = 2p$ si $p|(\alpha+\beta)^2$. Si $p = 2$, il n'y a rien à faire. Supposons $p > 2$. Par la formule du binôme

$$\alpha^p - \beta^p \equiv (\alpha-\beta)^p \bmod p. \tag{3.18}$$

Comme $pgcd\,((\alpha+\beta)^2, (\alpha-\beta)^2)$ divise 4, le nombre algébrique $\alpha-\beta$ est premier à p. Par (3.18), il vient

$$\tilde{u}_p(\alpha,\beta) \equiv (\alpha-\beta)^{p-1} \bmod p. \tag{3.19}$$

Comme le terme de gauche de (3.19) est premier à p, il en est de même de $\tilde{u}_p(\alpha,\beta)$, ie $m_p \neq p$. Or par l'assertion (9) de la proposition précédente, p divise $\tilde{u}_{2p}(\alpha,\beta)$ et (3.17) montre que m_p divise $2p$. Comme $m_p \neq 2$ et $m_p \neq p$, on a donc $m_{2p} = 2p$. ■

3.2.3 Nombres de Lucas ou de Lehmer sans diviseur primitif.

Pour les paires de Lucas ou de Lehmer (α,β) qui sont réelles, (c'est à dire α et β réels), Carmichael et Ward ont montré le résultat suivant :

Théorème 3.2.6 *Soit $n > 12$ un entier. Il n'existe aucune paire de Lucas ou de Lehmer n-défectueuse.*

Dans le cas général, la classification des triplets (α,β,n) tels que (α,β) soit une paire de Lucas ou de Lehmer n-défectueuse a été obtenue par Bilu, Hanrot et Voutier : voir [12].

3.3 Démonstration du théorème (3.1.1).

Considérons les idéaux principaux de $\mathbb{K} = \mathbb{Q}\left(\sqrt{-CD}\right)$ suivant :

$$\mathcal{I}_+ = \left(CX + b^m\sqrt{-CD}\right), \quad \mathcal{I}_- = \left(CX - b^m\sqrt{-CD}\right).$$

D'après (3.1), on a en termes d'idéaux de $\mathbb{K}$

$$\mathcal{I}_+\mathcal{I}_- = (C)(Y)^n. \tag{3.20}$$

Soit $\delta = (\mathcal{I}_+, \mathcal{I}_-)$. On a

$$\delta = \left(C, \sqrt{-CD}\right).$$

En effet, posons $\delta' = \left(C, \sqrt{-CD}\right)$. On a $\delta'^2 = (C)$ car $(C, D) = 1$. Par définition de $\mathcal{I}_+$ et de $\mathcal{I}_-$, $\delta'|\delta$. Supposons que $\mathcal{I}_+\delta'^{-1}$ et $\mathcal{I}_-\delta'^{-1}$ ne soient pas premiers entre eux. Comme $\delta'^2 = (C)$, il existe donc d'après (3.20), un premier $\mathfrak{p}$ de $\mathcal{O}_\mathbb{K}$, l'anneau des entiers de $\mathbb{K}$, qui divise $\mathcal{I}_+$, $\mathcal{I}_-$ et Y. Il divise donc en particulier $2CX$ et Y. Mais l'entier Y est premier à $2X$, et $\mathfrak{p}$ divise donc C et Y. Il existe donc un nombre premier p qui divise Y et C. Par (3.1), il divise aussi $b^{2m}D$. p ne peut pas diviser D car sinon $(C, D) \neq 1$. p ne peut pas diviser b^{2m} car sinon $b = p$, vu que, si $b \neq 1$, b est premier, et donc $b|Y$; alors, $b|b^m$ et $b|Y$, donc $b^2|CX^2$ par (3.1), donc $b|X$, car C est sans facteur carré, en contradiction avec $(X, Y) = 1$. Donc $\delta = \delta'$. Les idéaux $\mathcal{I}_+\delta^{-1}$ et $\mathcal{I}_-\delta^{-1}$ sont donc premiers entre eux. Il existe donc un idéal entier $\mathcal{I}$ de $\mathcal{O}_\mathbb{K}$ tel que

$$\left(CX + b^m\sqrt{-CD}\right) = \delta\mathcal{I}^n, \tag{3.21}$$

c'est à dire en élevant (3.21) au carré

$$\left(CX + b^m\sqrt{-CD}\right)^2 = (C)\mathcal{I}_1^n,$$

où $\mathcal{I}_1 = \mathcal{I}^2$. Comme $(n, h) = 1$, il existe $Z \in \mathcal{O}_\mathbb{K}$ tel que

$$\left(CX + b^m\sqrt{-CD}\right)^2 = CZ^n. \tag{3.22}$$

(Si $CD = 3$, en particulier $CD \equiv 3 \bmod 4$ et alors par hypothèse $n > 3$; l'unité qui devrait alors apparaître dans l'égalité précédente est une puissance n-ième dans $\mathcal{O}_\mathbb{K}$; quitte à modifier Z, on peut la supposer égale à 1.) Comme n est impair, il existe donc $U, V \in \mathbb{Z}$ de même parité tels que

$$CZ = \left(\frac{U + V\sqrt{-CD}}{2}\right)^2. \tag{3.23}$$

Supposons d'abord que $CD \neq 3 \bmod 4$. Alors en fait U et V sont pairs. On note encore U au lieu de $\frac{U}{2}$ et V au lieu de $\frac{V}{2}$:

$$CZ = \left(U + V\sqrt{-CD}\right)^2. \tag{3.24}$$

Posons $CU' = U$. Par (3.24), $U' \in \mathbb{Z}$ car C est sans facteur carré. En effet, comme on se place d'abord dans le cas $CD \neq 3 \bmod 4$, il existe des entiers a et b tels que $Z = a + b\sqrt{-CD}$. En identifiant les parties réelles dans (3.24), il vient

$$\begin{aligned} Ca &= U^2 - CDV^2 \\ &= C^2U'^2 - CDV^2, \end{aligned}$$

ie $CU'^2 = a + DV^2 \in \mathbb{Z}$. Comme C est sans facteur carré, nécessairement $U' \in \mathbb{Z}$. Il existe donc $U', V \in \mathbb{Z}$ tels que

$$Z = \left(U'\sqrt{C} + V\sqrt{-D}\right)^2. \tag{3.25}$$

En reportant (3.25) dans (3.22), il existe donc $A = \pm U', B = \pm V$ tels que

$$X\sqrt{C} + b^m\sqrt{-D} = \left(A\sqrt{C} + B\sqrt{-D}\right)^n.$$

Si $CD \equiv 3 \bmod 4$, en particulier, C est impair. En reprenant les calculs précédents, il existe $U', V \in \mathbb{Z}$ tels que

$$Z = \left(\frac{U'\sqrt{C} + V\sqrt{-D}}{2}\right)^2. \tag{3.26}$$

Comme $CU' = U$ et C impair, U' et V ont même parité. Comme précédemment, il existe $A = \pm U', B = \pm V$ tels que

$$X\sqrt{C} + b^m\sqrt{-D} = \left(\frac{A\sqrt{C} + B\sqrt{-D}}{2}\right)^n, \quad A \equiv B \bmod 2.$$

Ainsi, que CD soit congru à 3 modulo 4 ou pas, il existe des entiers A et B de même parité tels que l'équation précédente ait lieu. Notons que si B (et donc A) est impair, alors nécessairement $CD \equiv 3 \bmod 4$.

On pose $\epsilon = \frac{A\sqrt{C}+B\sqrt{-D}}{2}$. L'égalité précédente s'écrit aussi

$$X\sqrt{C} + b^m\sqrt{-D} = \epsilon^n. \tag{3.27}$$

En particulier $\epsilon\overline{\epsilon} = Y$, c'est à dire

$$4Y = CA^2 + B^2D. \tag{3.28}$$

De plus, $(\epsilon + \overline{\epsilon})^2 = (A\sqrt{C})^2 = A^2C$. Posons $\alpha = \epsilon$ et $\beta = \overline{\epsilon}$. α, β sont donc deux entiers algébriques (car leur puissance n-ième en est un), tels que $\alpha\beta, (\alpha+\beta)^2 \in \mathbb{Z}$ et même $\alpha + \beta \in \mathbb{Z}$ si $C = 1$. Si $\alpha + \beta = 0$, alors $A = 0$. Or, en égalisant les parties rélles dans (3.27), on vérifie que A divise X, donc que $A \neq 0$. On a donc bien $\alpha + \beta \neq 0$. De même $\alpha\beta = Y \neq 0$. Supposons qu'il existe une racine de l'unité ζ de $\mathbb{Q}(\sqrt{C}, \sqrt{-D})$ telle que $\frac{\alpha}{\overline{\alpha}} = \frac{\alpha}{\beta} = \zeta$. ζ serait alors en fait une racine de l'unité de $\mathbb{Q}(\sqrt{-CD})$. En effet, ζ peut se mettre sous la forme :

$$\zeta = \frac{A\sqrt{C} + B\sqrt{-D}}{A\sqrt{C} - B\sqrt{-D}} = \frac{AC + B\sqrt{-CD}}{AC - B\sqrt{-CD}} \in \mathbb{Q}\left(\sqrt{-CD}\right).$$

On a $\zeta \in \{\pm 1, \pm\sqrt{-1}, \pm\frac{1\pm\sqrt{-3}}{2}\}$. Si $\zeta = \pm 1$, on aurait $A = 0$ ou $B = 0$. On a déjà vu que le premier cas est impossible. Si $B = 0$, par (3.27), on aurait nécessairement $b = 0$, ce qui n'est pas. Si $\zeta = \pm\sqrt{-1}$, $A\sqrt{C} = \pm B\sqrt{D}$. Comme $4Y = CA^2 + B^2D$, on aurait $2Y = CA^2 = B^2D$. Comme Y est impair, $2|C$ et $2|D$, en contradiction avec $(C, D) = 1$. Enfin, si $\zeta = \pm\frac{1\pm\sqrt{-3}}{2}$ (donc $CD = 3$ ie $C = 3$, $D = 1$ car $3 \nmid D$), on vérifie que cela donne $A = B = 0$ ce qui est absurde.

De plus, $(\alpha\beta, (\alpha+\beta)^2) = 1$. En effet, $\alpha\beta = Y$, $(\alpha+\beta)^2 = CA^2$, et $(Y, C) = 1$. Supposons qu'il existe un nombre premier l qui divise Y et A. Comme $4Y = CA^2 + B^2D$, il divise aussi B^2D, donc b^{2m} ou D. Si $l|b^{2m}$, alors $m > 0$ et $l = b$, donc $b|Y$, d'où $b^2|CX^2$. Comme $(X, Y) = 1$, on a $b^2|C$, ce qui est impossible car C est sans facteur carré. Donc, $l \neq b$, $l|D$ et $l|Y$, d'où $l|CX^2$. Comme $(C, D) = 1$, on a $l|X^2$. Donc l^2 divise $Y^n - CX^2 = b^{2m}D$. Comme $l \neq b$, $l^2|D$, ce qui est impossible car D est sans facteur carré.

On a donc bien $(\alpha\beta, (\alpha + \beta)^2) = 1$.

On vient donc de montrer que α et β sont des entiers algébriques, tels que $\frac{\alpha}{\beta}$ n'est pas une racine de l'unité et tels que $\alpha\beta$, $(\alpha+\beta)^2$ soient des entiers premiers entre eux. De plus, $\alpha + \beta \in \mathbb{Z}$ si $C = 1$. Le couple (α, β) définit donc une paire de Lehmer (respectivement de Lucas) si $C > 1$ (respectivement si $C = 1$). Posons

$$u_n = u_n(\alpha, \beta) = \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

Si $C = 1$, c'est un nombre de Lucas. Si $C > 1$ c'est un nombre de Lehmer. Dans les deux cas

$$u_n = \frac{2b^m}{B}.$$

Si B est impair, u_n est alors divisible par 2. Comme $Y = \alpha\beta$ est impair, le corollaire (3.2.5) montre que $m_2|n$. Ce même corolaire montre que

$$m_2 = \begin{cases} 4 & \text{si } 2|\,(\alpha+\beta)^2 = CA^2, \\ 3 & \text{sinon.} \end{cases}$$

Comme A et B ont même parité, A est impair. De plus, B impair n'est possible que si $CD \equiv 3 \bmod 4$ et donc C est impair. On a donc $m_2 = 3$ divise n ie $n = 3$. Or on a supposé que $n > 3$ si $CD \equiv 3 \bmod 4$. L'entier B (et donc A) est pair.

Notons encore par B (respectivement par A) l'entier $\frac{B}{2}$ (respectivement l'entier $\frac{A}{2}$). On pose

$$\alpha = A\sqrt{C} + B\sqrt{-D}, \quad \beta = A\sqrt{C} - B\sqrt{-D},$$

de sorte que

$$X\sqrt{C} + b^m\sqrt{-D} = \alpha^n. \tag{3.29}$$

et

$$u_n = \frac{b^m}{B}. \tag{3.30}$$

On a la proposition suivante :

Proposition 3.3.1 *L'entier u_n est sans diviseur primitif.*

Preuve Si $b = 1$ ou $m = 0$, il n'y a rien à faire car alors $u_n = \pm 1$. On peut donc supposer $b > 1$ et $m > 0$.

Supposons que $b = 2$. Si $u_n = \pm 1$, il n'y a rien à faire. Sinon, comme $\alpha - \beta = 2B\sqrt{-D}$, et que le seul diviseur premier de u_n est 2 on a le résultat.

Supposons que $b > 2$ et que $b|D$. Comme $\alpha - \beta = 2B\sqrt{-D}$, il n'y a rien à faire.

Supposons $b > 2$ et que b vérifie $b \neq \left(\frac{-CD}{b}\right) \bmod n$. Comme $\alpha - \beta = 2B\sqrt{-D}$, si le premier b divise B, l'entier u_n est bien sans diviseur primitif. On peut donc supposer que $B = \pm 1$. Notons que l'entier A est premier à b. En effet, dans le cas contraire, en identifiant les parties réelles dans (3.27), il vient

$$X = \sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k+1} A^{2k+1} C^k \left(B\sqrt{-D}\right)^{n-2k-1}.$$

En particulier, A et donc b divise X. Comme $m > 0$, on déduit de l'équation $CX^2 + b^{2m}D = Y^n$, que $b|Y$ en contradiction avec $(X, Y) = 1$.

L'entier algébrique $(\alpha^2 - \beta^2)^2 = -16A^2CD$ est donc premier à b. Supposons que $\left(\frac{-CD}{b}\right) = -1$. Il vient

$$\begin{aligned}
\alpha^b &\equiv A^b C^{\frac{b-1}{2}}\sqrt{C} + B^b(-D)^{\frac{b-1}{2}}\sqrt{-D} \\
&\equiv AC^{\frac{b-1}{2}}\sqrt{C} + B(-D)^{\frac{b-1}{2}}\sqrt{-D} \\
&\equiv \pm\beta \bmod b,
\end{aligned}$$

d'où $\alpha^{b+1} \equiv \pm\alpha\beta \bmod b$. De même $\beta^{b+1} \equiv \pm\alpha\beta \bmod b$ (avec le même signe). Comme $(\alpha^2 - \beta^2)^2$ est premier à b, il vient $\tilde{u}_{b+1}(\alpha, \beta) \equiv 0 \bmod b$. Raisonnons par l'absurde et supposons que b soit un diviseur primitif de u_n. Avec les notations du corollaire (3.2.5), on doit donc avoir $m_b = n$. Comme $\tilde{u}_{b+1} \equiv 0 \bmod b$, ce même corollaire montre que $m_b|b+1$, ie $n|b+1$, ie $b \equiv \left(\frac{-CD}{b}\right) \bmod n$ en contradiction avec les hypothèses du théorème.

Dans le cas $\left(\frac{-CD}{b}\right) = 1$, on obtient

$$\begin{aligned}\alpha^b &\equiv A^b C^{\frac{b-1}{2}}\sqrt{C} + B^b(-D)^{\frac{b-1}{2}}\sqrt{-D} \\ &\equiv AC^{\frac{b-1}{2}}\sqrt{C} + B(-D)^{\frac{b-1}{2}}\sqrt{-D} \\ &\equiv \pm\alpha \bmod b,\end{aligned}$$

d'où $\alpha^{b-1} \equiv \pm 1 \bmod b$, car $\alpha\beta = Y$ est premier à b. De même $\beta^{b-1} \equiv \pm 1 \bmod b$ (avec le même signe). Comme $\left(\alpha^2 - \beta^2\right)^2$ est premier à b, il vient $\tilde{u}_{b-1}(\alpha, \beta) \equiv 0 \bmod b$. Raisonnons par l'absurde et supposons que b soit un diviseur primitif de u_n. Le corollaire (3.2.5) montre comme avant que l'on a alors $b \equiv 1 \equiv \left(\frac{-CD}{b}\right) \bmod n$ en contradiction avec les hypothèses du théorème.□ Remarquons que dans le cas où $b = 2$ et D impair, on peut montrer plus précisément que $u_n = \pm 1$. En effet, on a le lemme suivant :

Lemme 3.3.2 *Si $b = 2$ et si D est impair, alors $B = \pm 2^m$.*

Preuve Supposons $b = 2$. Alors, d'après (3.27)

$$2^m = \sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k+1} (A\sqrt{C})^{n-2k-1}(-D)^k B^{2k+1}. \tag{3.31}$$

En particulier, $B|2^m$. Si $m = 0$, il n'y a rien à faire. Supposons donc $m > 0$. En particulier, comme Y est impair, C l'est aussi d'après (3.1). Supposons que $2|\frac{2^m}{B}$. La somme de droite dans (3.31), divisée par B est donc paire. Comme $Y = CA^2 + B^2D \equiv 1[2]$, et $(D, 2) = 1$, A et B sont donc de parité différente. En effet, si $2|B$, comme Y impair, alors A l'est aussi. Si $B = \pm 1$, alors, comme $(2, D) = 1$, B^2D est impair, donc $2|CA^2$, car Y impair. Mais $(2, C) = 1$, donc $2|A$.

Ainsi, A et B sont donc bien de parité différente. On a donc en particulier $2|AB$. Comme la somme de droite de (3.31) divisée par B est paire, il vient

$$2|nA^{n-1}C^{\frac{n-1}{2}} + (-D)^{\frac{n-1}{2}}B^{n-1},$$

ce qui est impossible car $(2, D) = 1$ et A, B de différente parité. Donc $\frac{2^m}{B}$ est impair, ie $B = \pm 2^m$. □

On peut alors appliquer les résultats de [12] (complétés dans [1]). On trouve que le nombre premier n vérifie $n = 3$ ou 5. On est alors amené à distinguer les quatre cas suivants $(n = 3, C = 1)$, $(n = 3, C > 1)$, $(n = 5, C = 1)$, $(n = 5, C > 1)$.

3.3.1 Cas $C = 1, n = 3$.

Il existe alors des entiers $m_0 \geq 0, \epsilon_0 = \pm 1$,
$\epsilon = \pm 1$ et $k \geq 0$ tels que

$$\begin{cases} 2A = m_0\epsilon_0; \\ 4B^2D = 3m_0^2 - 3^k \cdot 4\epsilon; \end{cases}$$

Si $k > 0$, alors, comme par hypothèse $(D, 3) = 1$, on doit avoir $3|B$, avec B qui est une puissance de b, $b = 1$ ou b nombre premier. Donc $b = 3, m > 0$. Montrons que l'on a aussi $k = 1$. En effet, en utilisant les deux relations précédentes, on a

$$B^2D = 3A^2 - 3^k\epsilon.$$

Comme $9|B^2$, si $k > 1$, on a alors $3|A$. On a aussi montré au paragraphe précédent la relation suivante (relation (3.28)) :

$$Y = CA^2 + B^2D.$$

Comme $3|A$ et $3|B$, on a $3|Y$, et donc $3|X$ car $b = 3, m > 0$, en contradiction avec $(X, Y) = 1$. Donc on a bien $k = 1$ si $k > 0$. On a donc en prenant $k = 1$

$$B^2D + 3\epsilon = 3A^2.$$

De plus, comme $n = 3$ et $b = 3$, en prenant la partie imaginaire dans (3.27), on a

$$3^m = 3A^2B - B^3D.$$

On a donc les relations suivantes :

$$\begin{cases} 3^m + B^3D = 3A^2B; \\ B^2D + 3\epsilon = 3A^2; \end{cases}$$

On en déduit que $B = 3^{m-1}\epsilon$, et $A^2 - \epsilon = 3^{2m-3}D$. Comme dans ce cas $(A, 3) = 1$, on a $A^2 \equiv 1 \bmod 3$, d'où $\epsilon = 1$. Comme $Y = CA^2 + B^2D$, on vérifie alors que $Y = 4A^2 - 3$. En identifiant les parties réelles de (3.27), il vient

$$X = \sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k} B^{2k}(-D)^k A^{n-2k} C^{\frac{n-1}{2}-k}. \tag{3.32}$$

Comme $C = 1, n = 3, B^2D + 3 = 3A^2$, on obtient en particulier $X = \pm A\,(9 - 8A^2)$.

Si $k = 0$, on a

$$B^2D + \epsilon = 3A^2.$$

Comme avant

$$\begin{cases} b^m + B^3D = 3A^2B; \\ B^2D + \epsilon = 3A^2; \end{cases}$$

Il vient $B = \epsilon b^m$, et $3A^2 - b^{2m}D = \epsilon$. On vérifie alors que $Y = 4A^2 - \epsilon, X = \pm A\,(3\epsilon - 8A^2)$.

3.3.2 Cas $C > 1, n = 3$.

Supposons maintenant que $n = 3$ et $C > 1$. Par [12], il existe des entiers $q, k \geq 0$ et $\epsilon = \pm 1$ tels que

$$\begin{cases} 4A^2C = q + 3^k\epsilon; \\ 4B^2D = 3q - 3^k\epsilon; \end{cases}$$

ou bien

$$\begin{cases} 4A^2C = 3q - 3^k\epsilon; \\ 4B^2D = q + 3^k\epsilon; \end{cases}$$

Remarquons, vu que $Y = CA^2 + B^2D$, que l'on a $q = Y$. Etudions d'abord le premier cas. Si $k > 0$, on a $k = 1$, $b = 3$. En effet, si $k > 0$, 3 divise $3q - 3^k\epsilon = 4B^2D$. Comme $(D, 3) = 1$, 3 divise B, qui divise b^m. Donc $b = 3$ et $m > 0$. Montrons que $k = 1$. Sinon $k \geq 2$ et 9 divise $3q = 4B^2D + 3^k\epsilon$, donc $3|q = Y$. Comme $m > 0$ et $b = 3$, 9 divise aussi $CX^2 = Y^3 - 3^{2m}D$. C étant sans facteur carré, $3|X$, en contradiction avec $(X, Y) = 1$. Ainsi, si $k > 0$, $k = 1, b = 3$.

Comme $3^m = 3A^2BC - B^3D$, on obtient :

$$\begin{aligned} 4.3^m &= 3B.4A^2C - B.4B^2D \\ &= 3B(q + 3\epsilon) - B(3q - 3\epsilon) \\ &= 12B\epsilon. \end{aligned}$$

On a alors :

$$\begin{cases} B = 3^{m-1}\epsilon; \\ A^2C - \epsilon = 3^{2m-3}D; \end{cases}$$

On obtient $Y = 4A^2C - 3\epsilon$. On vérifie $X = \pm A\,(9\epsilon - 8A^2C)$.

Si $k = 0$, alors $B = b^m\epsilon$ et $3A^2C - \epsilon = b^{2m}D$. On vérifie comme avant les valeurs de X, Y.

Etudions maintenant le second cas. Comme $Y = CA^2 + B^2D$, on en déduit que $q = Y$. De plus,

$$b^m = 3A^2BC - B^3D = B(3A^2C - B^2D).$$

On en déduit

$$\begin{aligned}\frac{4b^m}{B} &= 3\left(3q - 3^k\epsilon\right) - q - 3^k\epsilon \\ &= 8q - 4.3^k\epsilon,\end{aligned}$$

d'où

$$8B^2D = \frac{b^m}{B} + 3^{k+1}\epsilon.$$

Supposons d'abord $b \neq 3$. L'un des entiers B^2 et $\frac{b^m}{B}$ est donc premier à b, ie $B = s$ ou bien $B = sb^m, s = \pm 1$. Supposons d'abord $B = s$. Les relations précédentes donnent $8D = sb^m + 3^{k+1}\epsilon$ et $A^2C = 3D - 3^k\epsilon$. Comme $q = Y$, on en déduit $Y = 4D - 3^k\epsilon$ et $X = \pm A.3^k$.

Supposons $B = b^m s$. Comme précédemment, il vient

$$\begin{cases} 8b^{2m}D = s + 3^{k+1}\epsilon; \\ A^2C = 3b^{2m}D - 3^k\epsilon; \end{cases}$$

On a alors $\epsilon = 1, q = Y = 4b^{2m}D - 3^k$ et $X = \pm A.3^k$.

Supposons maintenant que $b = 3$. On doit alors avoir $m = 0$. En effet, supposons $m > 0$. Comme $8B^2D = \frac{3^m}{B} + 3^{k+1}\epsilon$, on a $3|B$ et $3|\frac{3^m}{B}$. Si $k > 0$, comme $4B^2D = q + 3^k\epsilon$, on aurait $3|q = Y$. Comme $m > 0$ et $CX^2 + 3^{2m}D = Y^3$, il vient $3|X$ et donc $(X, Y) \neq 1$, en contradiction avec les hypothèses. On a donc $k = 0$. On obtient :

$$8B^2D = \frac{3^m}{B} + 3\epsilon,$$

c'est à dire

$$8\frac{B^2}{3}D - \frac{3^{m-1}}{B} = \epsilon.$$

Comme $\frac{B^2}{3}$ est divisible par 3, on doit avoir $B = \pm 3^{m-1}$, donc $8.3^{2m-3}D = \epsilon \pm 1$, ce qui est impossible. Donc si $b = 3$, on doit avoir $m = 0$, et $8D = s + 3^{k+1}\epsilon$.

3.3.3 Cas $C = 1, n = 5$.

Supposons maintenant que $C = 1$ et $n = 5$. On trouve $2A = 2\epsilon$ et $4B^2D = 40$, ou $2A = 12\epsilon$ et $4B^2D = 76$, ou $2A = 12\epsilon$ et $4B^2D = 1364$, $\epsilon = \pm 1$. Donc $A = \epsilon, B = \pm 1$ et $D = 10$, ou $A = 6\epsilon, B = \pm 1$ et $D = 19$ ou $A = 6\epsilon, B = \pm 1$ et $D = 341$.

Dans le premier cas, on a $A^2 = B^2 = C = 1, D = 10$. On en déduit que $Y = 11$ et (3.32) donne $X = \pm 401$. On a alors $b^{2m} = 25$, ie $m = 1, b = 5$.

Dans le second cas, $D = 19$, $A^2 = 36$, $B^2 = 1$, $Y = 36 + 19 = 55$; (3.32) donne $X = \pm 22434$. On a alors $b^{2m} \cdot 19 = 55^5 - 22434^2 = 19$, ie $b^m = 1$.

Dans le troisième cas, on obtient $D = 341$, $Y = 377$, $X = \pm 2759646$, et $b^m = 1$ en utilisant la relation (3.28).

3.3.4 Cas $C > 1, n = 5$.

Plaçons nous maintenant dans le cas où $n = 5$ et $C > 1$. On désigne par V_k, le k-ième terme de la suite de Fibonacci ou de Lucas. Il existe alors $\epsilon = \pm 1$ et un entier k tel que

$$\begin{cases} 4A^2C = V_{k-2\epsilon}; \\ 4B^2D = 4V_k - V_{k-2\epsilon}; \end{cases} \tag{3.33}$$

ou bien

$$\begin{cases} 4B^2D = V_{k-2\epsilon}; \\ 4A^2C = 4V_k - V_{k-2\epsilon}; \end{cases} \tag{3.34}$$

On en déduit que $Y = \phi_k =$ ou ψ_k. Mais Y est impair, donc $k = 3l + 1$ ou $3l + 2$. Il nous reste à démontrer la majoration de l en termes de b, C et D qui sera utile pour des applications pratiques du théorème. On commence par montrer le lemme suivant :

Lemme 3.3.3 *Soit $n > 12$ un entier et V_n le n-ième terme de la suite de Lucas ou de Fibonacci. On a alors l'inégalité*[2]

$$n - 1 \leq p\,(V_n).$$

Preuve Comme $n > 12$, le théorème (3.2.6) montre que V_n a au moins un diviseur primitif p que l'on se fixe. Par définition de m_p (voir le corollaire (3.2.5)) $m_p = n$. La paire d'entiers algébriques associée à la suite V est $(\alpha, \beta) = \left(\frac{1-\sqrt{5}}{2}, \frac{1+\sqrt{5}}{2}\right)$. Comme $(\alpha + \beta)^2 = 1 = -\alpha\beta$, le corollaire (3.2.5) montre que $m_p \leq p + 1$, d'où $n - 1 \leq p \leq p\,(V_n)$.□

Dans notre cas, on a $Y = V_k$ avec $4A^2C = V_{k-2\epsilon}$ ou $4B^2D = V_{k-2\epsilon}$, $\epsilon = \pm 1$. Le lemme précédent montre donc

$$k - 2\epsilon - 1 \leq Sup\,(11, b, p(CD), p(A)),$$

[2]Rappelons que $p(y)$ est par définition le plus grand nombre premier divisant l'entier y.

d'où

$$k \leq Sup\,(14, b+3, p(CD)+3, p(A)+3).$$

Par (3.27), en identifiant les parties imaginaires, on obtient

$$b^m = \sum_{k=0}^{2} \binom{5}{2k+1} B^{2k+1}(-D)^k (A\sqrt{C})^{4-2k},$$

d'où

$$5A^2C\left(A^2C - 2B^2D\right) = \frac{b^m}{B} - B^4D^2.$$

On en déduit

$$p(A) \leq \sqrt{\frac{b^{2m}D}{C} + \frac{1}{C}\sqrt{\frac{b^m}{5} + \frac{4}{5}b^{4m}D^2}},$$

d'où

$$k \leq Sup\left(14, b+3, p(CD)+3, \sqrt{\frac{b^{2m}D}{C} + \frac{1}{C}\sqrt{\frac{b^m}{5} + \frac{4}{5}b^{4m}D^2}} + 3\right).$$

Si $b = 2$ et D impair, le lemme (3.3.2) montre que $B = \pm 2^m$. On obtient dans ce cas comme meilleure borne :

$$k \leq Sup\left(14, b+3, p(CD)+3, \sqrt{\frac{4^mD}{C} + \frac{1}{C}\sqrt{\frac{1}{5} + \frac{4^{2m+1}D^2}{5}}} + 3\right).$$

Le théorème (3.1.1) est prouvé. ■

On donne maintenant quelques exemples.

3.4 Exemples.

On illustre le théorème (3.1.1) en retrouvant les solutions entières de quelques équations diophantiennes classiques.

3.4.1 Résolution de l'équation de Mordell $x^2 = y^3 + k$.

Soit $k < -1$ un entier. Soit $h(k)$ le nombre de classes du corps quadratique imaginaire $\mathbb{Q}(\sqrt{k})$. On suppose que l'entier k est sans facteur carré, vérifie $k \neq 1 \bmod 4$, et est tel que $(3, h(k)) = 1$. On considère l'équation de Mordell suivante :

$$x^2 = y^3 + k. \tag{3.35}$$

Mordell a démontré le théorème suivant :

Théorème 3.4.1 *(voir [58]) L'équation (3.35) a au moins une solution en nombres entiers, si et seulement s'il existe un entier a tel que* $k = \pm 1 - 3a^2$*, et alors* $x = \pm a\,(a^2 + 3k)$ *et* $y = a^2 - k$*.*

Ce théorème est une conséquence du théorème (3.1.1). En effet, supposons que (3.35) admette une solution entière (x, y). Comme k est sans facteur carré, les entiers x et y sont premiers entre eux. De plus $(3, h(k))) = 1$ et $k \neq 1 \bmod 4$. On peut appliquer le théorème (3.1.1). Le cas "$C = 1, n = 3$" montre qu'il existe des entiers A et $\epsilon = \pm 1$ tels que $3A^2 = \epsilon - k$. Toujours par le théorème (3.1.1), pour de tels entiers, on a alors $x = \pm A\,(3\epsilon - 8A^2)$ et $y = 4A^2 - \epsilon$. Comme $k = \epsilon - 3A^2$, on obtient $x = \pm A\,(A^2 + 3k)$ et $y = A^2 - k$.

3.4.2 Résolution de l'équation de Lebesgue $X^2 + 1 = Y^n$, $n > 1$, $Y > 0$.

Si n est une puissance de deux, on écrit $1 = Y^n - X^2$ et on arrive facilement à $X = 0, Y = 1$. Si n n'est pas une puissance de deux, fixons p un facteur premier impair de n. On pose $Z = Y^{\frac{n}{p}}$. Supposons que (X, Y) ne soit pas la solution triviale $(0, 1)$. Comme $h(-1) = 1$, et "$CD = b = 1$", le théorème (3.1.1) montre que $p = 3$ ou $p = 5$. Si $p = 3$, on obtient $A = X = 0$: contradiction. Si $p = 5$, on obtient aucune solution. Donc, la seule solution est la solution triviale $X = 0$, $Y = 1$.

Remarque 3.4.2 *On trouvera une démonstration plus éclairante, ie plus spécifique à l'anneau des entiers de Gauss* $\mathbb{Z}[i]$ *dans [64].*

Remarque 3.4.3 *Le théorème de Lebesgue démontre en particulier que les nombres de Fermat ne sont jamais des puissances entières propres.*

3.4.3 Résolution de $2x^2 + 19 = y^n$.

Soit à résoudre l'équation d'inconnue (x, y, n)

$$2x^2 + 19 = y^n, n > 1, (n, 6) = 1. \tag{3.36}$$

L'entier 19 étant sans facteur carré, les entiers x et y sont premiers entre eux. Comme $h(-38) = 6$, le théorème (3.1.1) implique que le seul facteur premier de n est 5. Il existe un entier A tel que $y^{\frac{n}{5}} = 2A^2 + 19$ et il existe des entiers k et $\epsilon = \pm 1$, tels que

$$\begin{cases} 8A^2 = V_{k-2\epsilon}; \\ 76 = 4V_k - V_{k-2\epsilon}; \end{cases}$$

ou bien

$$\begin{cases} 76 = V_{k-2\epsilon}; \\ 8A^2 = 4V_k - V_{k-2\epsilon}; \end{cases}$$

où V est la suite de Lucas ou de Fibonacci.

Etudions d'abord le premier cas. Dans le cas de la suite de Fibonacci, les seuls termes qui sont le double d'un carré sont $\phi_2 = 2$ et $\phi_5 = 8$ (voir [66]). Ici seul $k - 2\epsilon = 5$ convient et $A^2 = 1$. On a alors $k = 7, \epsilon = 1$ ou $k = 3, \epsilon = -1$. On vérifie que seul $k = 7$ convient. Dans ce cas, $B = \pm 1$, d'où $y^{\frac{n}{5}} = 21$. Donc $y = 21, n = 5$, et $x = \pm 1429$. Dans le cas de la suite de Lucas, seul les termes d'indice 0 et 6 sont le double d'un carré (voir [66]). On vérifie que cela ne conduit à aucune solution (A, B).

Dans le second cas, $76 = V_{k-2\epsilon}$. C'est impossible pour la suite de Fibonacci. Pour la suite de Lucas, cela implique $k - 2\epsilon = 9$, ie $k = 7$ ou $k = 11$. On doit alors avoir $8A^2 = 4\psi_7 - \psi_9 = 40$, ou bien $8A^2 = 4\psi_{11} - \psi_9 = 720$. On obtient aucune nouvelle solution.

Donc, les seules solutions (x, y, n) de

$$2x^2 + 19 = y^n, n > 1, (n, 6) = 1.$$

sont $(\pm 1429, 21, 5)$.

3.4.4 Résolution de $2x^2 + 1 = y^n, n > 2$.

Déterminons tous les entiers x, y, n avec $n > 2$ tels que

$$2x^2 + 1 = y^n, n > 2, x \neq 0. \tag{3.37}$$

Soit donc (x, y, n) une solution de cette équation.

Si $4|n$, on pose $X = x, Y = y^{\frac{n}{4}}$ et $Z = 1$. Les entiers X, Y, Z vérifient

$$Y^4 - Z^4 = 2X^2.$$

L'équation (3.37) s'écrit alors

$$\left(Y^2 - 1\right)\left(Y^2 + 1\right) = 2X^2. \tag{3.38}$$

En particulier, les entiers $Y^2 - 1$, $Y^2 + 1$ sont pairs, et (3.38) peut s'écrire dans $\mathbb{Z}$ sous la forme

$$\left(Y^2 - 1\right)\left(\frac{Y^2 + 1}{2}\right) = X^2. \tag{3.39}$$

Supposons $Y \neq \pm 1$. La différence de Y^2-1 et Y^2+1 valant 2, les entiers Y^2-1 et $\frac{Y^2+1}{2}$ sont premiers entre eux. L'équation (3.39) montre donc qu'il existe donc un entier Z tel que $Y^2-1=Z^2$, d'où $Y=\pm 1$: contradiction. On a donc bien $y=\pm 1$, et $x=0$, montrant ainsi que l'équation (3.37) est sans solution entière.

On suppose maintenant que $\nu_2(n)<2$. Comme $n>2$, n possède donc un facteur premier impair p. On pose $X=x, Y=y^{\frac{n}{p}}$. Comme $h(-2)=1$, le théorème (3.1.1) implique que $p=3$ ou $p=5$.

Supposons d'abord que $p=3$. Le théorème (3.1.1) appliqué dans le cas "$C=2, p=3$" montre qu'il n'existe pas de solution (on trouve en effet uniquement la possibilité $X=0, Y=1$, or $x\neq 0$).

Supposons maintenant que $p=5$. La démonstration du théorème (3.1.1) montre que l'on doit considérer deux cas.

Dans le premier, on doit trouver tous les doubles de carrés dans les suites de Fibonacci et de Lucas. Seul 8 convient, c'est à dire $A^2=1$ et $k-2\epsilon=5$. Seule l'égalité $4\phi_3-\phi_5=4B^2$ est possible, soit $B^2=1$. On a alors $Y=y^{n/5}=3$. Donc $n=5$, et $y=3$. On vérifie alors que $x=\pm 11$. Le cas des suites de Lucas ne donne que la solution triviale $x=0$ qui est exclue.

Dans le second cas, on doit trouver tous les entiers k tels que $4=V_k$ où V est la suite de Lucas ou de Fibonacci. On obtient $4=\psi_{k-2\epsilon}$, avec $k-2\epsilon=3$ ie $k=5$ ou $k=1$. Comme on a alors $8A^2=4\psi_k-4$, il vient $A^2=5$ ou $A^2=0$, ce qui implique que $x=0$, ce qui est exclu.

Les solutions cherchées sont donc $(\pm 11, 3, 5)$

3.4.5 Résolution de $x^2+2^{m'}=y^n, n>2$.

Soit donc (x,y) une solution entière de

$$x^2+2^{m'}=y^n, n>2, x\neq 0$$

où n n'est pas une puissance de deux. On peut supposer $m'>0$ car sinon, il n'y a pas de solution par le théorème de Lebesgue (voir le paragraphe (3.4.2)). On a $(x,y)|2^{m'}$. On pose $x=2^u x_1, y=2^v y_1$, avec $(x_1 y_1, 2)=1$. On va distinguer les cinq cas suivants :

1. $m'=2m, u=m$.
2. $m'=2m, u<m$.
3. $m'=2m, u>m$.
4. $m'=2m+1, m'>2u$.
5. $m'=2m+1, m'<2u$.

Dans le premier cas, $u = m, nv = 2u + 1$ et x_1, y_1 sont solutions de :

$$x_1^2 + 1 = 2y_1^n.$$

Par [64], $x_1 = \pm 1, y_1 = 1$. On doit donc avoir $n|2m + 1, x = \pm 2^m, y = 2^{\frac{2m+1}{n}}$.

Plaçons nous dans le second cas. Par hypothèse, il existe un nombre premier impair p tel que $p|n$. On pose $X = x_1, Y = y_1^{\frac{n}{p}}$. x_1, y_1 sont solutions de :

$$X^2 + 2^{2m-2u} = Y^p.$$

Par le théorème (3.1.1), $p = 3$ ou $p = 5$. Si $p = 5$, on obtient aucune solution. Si $p = 3$, le cas "$C = 1, p = 3$" montre qu'il existe un entier $A \neq 0$ tel que $3A^2 + 1 = 2^{2m-2u}$. Si $m - u = 1$, $A = 1$ convient. Par la proposition (6.7.1), l'équation $3T^2 + 1 = 2^l$ n'admet aucune solution entière avec $l > 2$. On a donc comme seule possibilité $A = \pm 1$ et $m-u = 1$. Comme ici $b = 2$ et $D = 1$ impair, $B = \pm 2^{m-u} = \pm 2$, par le lemme (3.3.2). Comme $A^2 = 1$, on a $y_1^{\frac{n}{3}} = Y = A^2 + B^2 = 5$. On doit donc avoir $n = 3, y_1 = 5$ et $x_1 = \pm 11$. Comme $u = m - 1$ et $nv = 2u$, $3|m - 1$. Il vient alors $x = \pm 11.2^{m-1}, y = 5.4^{\frac{m-1}{3}}$.

Dans le troisième cas x_1, y_1 sont solutions de

$$(2^{u-m}x_1)^2 + 1 = y_1^n.$$

Cette équation est sans solution par le théorème de Lebesgue.

Dans le quatrième cas, on pose $X = x_1, Y = y_1^{\frac{n}{p}}$. Par le théorème (3.1.1), $p = 3$ ou $p = 5$, et X, Y sont solutions de

$$X^2 + 2^{2m-2u}.2 = Y^p.$$

Si $p = 5$, comme $C = 1$, on obtient aucune solution. Si $p = 3$,

$$X^2 + 2^{2m-2u}.2 = Y^3.$$

Il existe alors un entier A et $\epsilon = \pm 1$ tels que

$$3A^2 = \epsilon + 2^{2(m-u)+1}.$$

Si $m - u \geq 1$, alors $3A^2 \equiv \epsilon \bmod 4$. Comme A est impair, $\epsilon = -1$ et $3A^2 + 1 = 2^{2(m-u)+1}$. Cette équation est sans solution.

Si $m = u$, alors $\epsilon = 1, A^2 = 1$ et $X = \pm 5, y^{\frac{n}{3}} = Y = 3$, ie $x_1 = \pm 5, y_1 = 3, n = 3$. Comme $3v = nv = 2u$ et $u = m$, on doit avoir $3|m$. On a alors $x = \pm 2^m 5, y = 2^{\frac{2m}{3}} 3$.

Dans le dernier cas, $nv = 2m + 1$ et

$$2(x_1 2^{u-m-1})^2 + 1 = y_1^n.$$

Cette équation a été résolue au paragraphe (3.4.4). On obtient $n = 5, 2^{u-m-1}x_1 = \pm 11, y_1 = 3$. On doit donc avoir $u = m + 1$, $5|2m + 1$. Alors $x = \pm 11 \cdot 2^{m+1}, y = 3 \cdot 2^{\frac{2m+1}{5}}$.

On a donc montré :

1. Soit $m' = 2m > 0$, $n|2m + 1$ et alors $(x, y) = (\pm 2^m, 2^{\frac{2m+1}{n}})$,
2. soit $m' = 2m > 0$, $n = 3$, $3|m - 1$ et alors $(x, y) = (\pm 11.2^{m-1}, 5.4^{\frac{m-1}{3}})$,
3. soit $m' = 2m + 1$, $n = 3$, $3|m$ et alors $(x, y) = (\pm 5.2^m, y = 3.2^{\frac{2m}{3}})$,
4. soit $m' = 2m + 1$, $n = 5$, $5|2m + 1$, et alors $(x, y) = (\pm 11.2^{m+1}, 3.2^{\frac{2m+1}{5}})$.

Remarque 3.4.4 *On trouvera dans [17] une étude de l'équation diophantienne* $x^2 - 2^m = \pm y^n$. *On pourra aussi consulter [18].*

3.4.6 Résolution de l'équation de Brown $2x^2 + 3^{2m} = y^n$.

Déterminons toutes les solutions (x, y, m, n) avec $n > 2$ et $(x, y) = 1$ de

$$2x^2 + 3^{2m} = y^n.$$

Soit donc (x, y, m, n) une telle solution. Si $m = 0$, on est ramené à une équation déjà étudiée précédemment. On peut donc supposer $m > 0$. Soit p un facteur premier de n. On pose

1. $X = x$.
2. $Y = y^{\frac{n}{p}}$.

Si $2|n$, en prenant $p = 2$, comme $m > 0$, on obtient modulo 3

$$2X^2 \equiv Y^2 \bmod 3,$$

c'est à dire vu que $(3, XY) = 1$,

$$2 \equiv 1 \bmod 3,$$

ce qui est impossible. Donc n est impair. Soit alors p un facteur premier impair de n. La méthode de résolution dans le cas $C > 1, p = 3$ donne $m > 1$ et

1. $B = \epsilon 3^{m-1}$.
2. $2A^2 - \epsilon = 3^{2m-3}$.

Supposons d'abord que $\epsilon = 1$. Il existe donc un entier A tel que $2A^2 - 1 = 3^{2m-3}$. Si $2|A$, on a $3^{2m-3} \equiv 7 \bmod 8$. Mais $3^{2m-3} \equiv 3 \bmod 8$. De même, si A est impair, on a $2A^2 - 1 \equiv 1 \bmod 8$ et $3^{2m-3} \equiv 3 \bmod 8$. Donc en fait $\epsilon = -1$, et

$$2A^2 + 1 = 3^{2m-3}.$$

Or on a déjà montré avant, que l'équation $2X_1^2 + 1 = Y_1^l$ donne $l = 5$ ou $l = 1$ ou $l = 2$. Comme $2m - 3$ est impair, on a donc $2m - 3 = 1$ ou $2m - 3 = 5$, ie $m = 2$ ou $m = 4$. Si $m = 2$, on trouve $B = -3$ et $A^2 = 1$, donc $y^{\frac{n}{3}} = Y = 11$. On a alors $n = 3$, $y = Y = 11$. On vérifie alors que $x = \pm 25$. Si $m = 4$, alors $B = -3^3$, $A = \pm 11$ et $y^{\frac{n}{3}} = 971$. On vérifie alors que $x = X = \pm 21935$. On a donc montré que les solutions (x, y, m, n) de

$$2x^2 + 3^{2m} = y^n, (x, y) = 1, n > 2$$

sont

$$(\pm 21395, 971, 4, 3), \quad (\pm 25, 11, 2, 3) \quad (\pm 11, 3, 0, 5).$$

3.5 Sur l'équation $x^2 + 3^m = y^n$.

3.5.1 Etude d'un cas particulier.

Soit donc $x, y, m, n \in \mathbb{N}$ avec $n > 2$ et $m \in \mathbb{N}$ tels que

$$x^2 + 3^{2m} = y^n, (x, y) = 1. \tag{3.40}$$

On peut supposer $m > 0$ car l'équation

$$X^2 + 1 = Y^n$$

n'a aucun couple solution $(X, Y) \in \mathbb{N}^2$, avec $X > 0$ (théorème de Lebesgue). On commence par considérer le cas où l'entier n est sans facteur premier impair, donc de la forme 2^t. Dans ce cas, comme $4|n$, on est ramené à montrer que l'équation (3.40) où $n = 4$ est sans solution. On commence donc par montrer le lemme suivant qui se trouve également dans [75] :

Lemme 3.5.1 *L'équation*

$$x^2 + 3^{2m} = y^4, (x, y) = 1,$$

n'a aucune solution en nombres entiers $x, y, m \in \mathbb{N}$, $m > 0$.

Preuve Raisonnons par l'absurde et supposons qu'il existe $x, y, m \in \mathbb{N}$, $m > 0$ tels que

$$x^2 + 3^{2m} = y^4, (x, y) = 1.$$

On peut mettre cette équation sous la forme

$$(y^2 + x)(y^2 - x) = 3^{2m}.$$

Il existe donc $\epsilon = \pm 1$ et $a, b \in \mathbb{N}$ avec $a + b = 2m$, tels que

1. $y^2 + x = \epsilon 3^a$.
2. $y^2 - x = \epsilon 3^b$.

Comme $x, y \in \mathbb{N}$, il vient :

1. $y^2 + x = 3^a$.
2. $y^2 - x = 3^b$.

En particulier, on obtient

$$2y^2 = 3^a + 3^b.$$

Comme $(3, y) = 1$ car $(x, y) = 1$, on doit avoir $b = 0$ (car $b \leq a$), et on a donc

$$2y^2 = 3^{2m} + 1$$

Comme $m > 0$ on obtient modulo 3

$$2y^2 \equiv 1 \bmod 3.$$

Comme $(3, y) = 1$, $y^2 \equiv 1 \bmod 3$, ce qui donne par ce qui précède $2 \equiv 1 \bmod 3$, ce qui est absurde. On a la contradiction souhaitée et le lemme est prouvé.□ Le lemme précédent montre donc en particulier que n a au moins un facteur premier impair. Soit donc p un facteur premier impair fixé de n. Pour la suite on pose afin d'utiliser les notations du théorème 1.2 :

1. $Y = y^{\frac{n}{p}}$.
2. $X = x$.

L'équation de Le se met sous la forme

$$X^2 + 3^{2m} = Y^p.$$

On a donc $p = 3$ ou $p = 5$. Le cas $p = 5$ est impossible. Donc $p = 3$. On est dans le cas $C = 1, n = 3$. Comme ici $b = 3$, le théorème (3.1.1) montre qu'il existe un entier A tel que $A^2 = 1 + 3^{2m-3}$, c'est à dire

$$(A + 1)(A - 1) = 3^{2m-3}.$$

Il existe donc $\epsilon = \pm 1$ et $a, b \in \mathbb{N}$ tels que $a + b = 2m - 3$ et

1. $A+1=\epsilon 3^a$.
2. $A-1=\epsilon 3^b$.

On a donc $2=\epsilon(3^a-3^b)$. Comme A peut être négatif, il y a deux possibilités, soit $a=0$, $b=1$, $\epsilon=-1$, $A=-2$, soit $b=0$, $\epsilon=1$, $A=2$. Dans les deux cas $A^2=4$ et $m=2$. Par le théorème (3.1.1), on a aussi $y^{\frac{n}{3}}=Y=4\cdot 4-3=13$ et $x=X=\pm 2\,(9-8\cdot 4)=\pm 46$. Donc, $n=p=3$, $y=13$ et $x=\pm 46$. ■

3.5.2 Démonstration du corollaire (3.1.2).

Soit donc (x,y,m,n) une solution de l'équation

$$x^2+3^m=y^n, n>2, x\neq 0.$$

On a $(x,y)|3^m$. On pose $x=3^s x_1$ et $y=3^t y_1$ avec $(x_1y_1,3)=1$. Cela nous permet de ramener la résolution de l'équation à quatre équations que l'on sait résoudre. En effet, supposons d'abord que $(2,m)=1$. Si $m<2s$, alors $m=nt<2s$ et si $m>2s$, alors $2s=nt<m$. Dans le premier cas, comme m est impair, x_1,y_1 et n sont solutions de l'équation

$$3X^2+1=Y^n,\quad (X,Y)=1.$$

Supposons d'abord que n ait un facteur premier impair p. Si $p>3$, le théorème (3.1.1) montre que l'équation précédente est sans solution entière. Supposons $p=3$. Quitte à poser $Y_1=Y^{\frac{n}{3}}$, on peut supposer alors que $n=p$. L'équation s'écrit alors

$$Y^3-1=3X^2.$$

Il existe donc un entier $Z>0$ tel que

$$1+Y+Y^2=3Z^2.$$

Cette équation s'écrit aussi

$$(2Y+1)^2+3=12Z^2.$$

Nécessairement, $3|2Y+1$. Il existe donc un entier $T>0$ tel que $2Y+1=3T$ et

$$3T^2+1=(2Z)^2.$$

On tombe sur une équation de type Pell-Fermat. L'unité fondamentale de $\mathbb{Q}(\sqrt{3})$ étant $2+\sqrt{3}$, on vérifie facilement que la seule solution de $3T^2+1=S^2$ avec S pair est $T=1$, $S=2$, ce qui donne $Y=Z=1$, ie $Y=1$, $X=0$. Ainsi, l'équation $Y^3-1=3X^2$ n'admet que la solution triviale. On vient donc de montrer que si $n>2$ n'est pas une puissance de deux, alors l'équation

$$3X^2+1=Y^n, \quad X\neq 0,$$

n'admet aucune solution entière. Dans le cas où l'entier n est une puissance de deux, comme $n>2$, on peut supposer que $n=4$. Ce cas est traité en détails lors de la preuve de la proposition (6.7.1) : l'équation n'admet pas non plus de solution entière. Le premier cas est clôt.

Remarque 3.5.2 *Plus généralement, on peut montrer le résultat suivant (voir [59], théorème* 1.8*) :*

Proposition 3.5.3 *L'équation diophantienne* $3x^2+2^{2m}=y^p, \quad x\neq 0$ *où* p *est un nombre premier impair, a une solution ssi* $p|m+1$*, et alors* $x=\pm 2^m, y=4^{\frac{m+1}{p}}$.

Plaçons nous dans le second cas. Supposons d'abord que n soit une puissance de deux. Comme $n>2$, $4|n$. On pose $X=x_1$ et $Y=y_1^{\frac{n}{4}}$. X,Y sont solutions de :

$$X^2+3^{m-2s}=Y^4.$$

Cette équation est sans solution. (même démarche qu'au paragraphe (3.5.1)).

Si n n'est pas une puissance de deux, soit p un facteur premier impair de n. Alors $(x_1, y_1^{\frac{n}{p}}, m-2s, n)$ est solution de l'équation :

$$X^2+3^{m-2s}=Y^p, (X,Y)=1.$$

D'après [14], $(x_1, y_1^{\frac{n}{p}}, m-2s, p)=(\pm 10, 7, 5, 3)$. Donc $n=p=3, y_1=7$, $s=\frac{m-5}{2}$. Comme $2s=nt$, on doit avoir $m\equiv 2 \bmod 3$, donc $m\geq 5$, et $t=\frac{m-5}{3}$. Comme $x=3^s x_1$, on a $x=\pm 3^{\frac{m-5}{2}}.10$. De même $y=3^{\frac{m-5}{3}}.7$.

Supposons que $2|m$. Si $m=2s$, alors $m=nt=2s$ et on est ramené à l'équation de Lebesgue qui est sans solution non triviale. Si $m<2s$, alors $m=nt<2s$ et comme $m-2s$ est pair, on est également ramené à l'équation de Lebesgue. Si $m>2s$, alors $2s=nt$, et on est ramené à l'équation de Le, que l'on vient de résoudre. Comme avant on a donc $(x_1, y_1, m-2s, n)=(\pm 46, 13, 4, 3)$. Il vient $s=\frac{m-4}{2}$ et $t=\frac{m-4}{3}$. En particulier, $m\geq 4$, $m\equiv 1[3]$, et $x=\pm 3^{\frac{m-4}{2}}.46$, $y=3^{\frac{m-4}{3}}.13$. En écrivant m sous la forme $m=4+6m_0$ si m est pair et $m\equiv 1 \bmod 3$ (respectivement sous la forme $m=5+6m_0$ si m est impair et $m\equiv 2 \bmod 3$, on obtient les ensembles $\mathcal{S}_1$ et $\mathcal{S}_2$ de l'énoncé.

Inversement, on vérifie que les éléments de $\mathcal{S}_1\cup\mathcal{S}_2$ sont bien solutions.

3.6 Résolution complète de l'équation d'Aigner (corollaire (3.1.6)).

Si $p = D = 3$, on obtient l'équation

$$X^2 + 12 = Y^3, (X, Y) = 1,$$

qui n'a aucune solution entière. En effet, on l'écrit sous la forme :

$$X^2 + 4 = (Y - 2)(Y^2 + 2Y + 4).$$

Les entiers $Y - 2$ et $Y^2 + 2Y + 4$ sont premiers entre eux. En effet, s'il existe un nombre premier l qui les divisent, alors $l|12$. Comme $(X, Y) = 1$, Y est impair, donc $l = 3$. Donc $Y \equiv 2 \bmod 3$. Mais $X^2 \equiv X^2 + 12 \equiv Y^3 \equiv 2 \bmod 3$, ce qui est impossible. $X^2 + 4$ étant somme de deux carrés d'entiers, on en déduit que $Y - 2 \equiv 1 \bmod 4$ ie $Y \equiv 3 \bmod 4$. On a alors $X^2 \equiv 3 \bmod 4$ ce qui est impossible.

Supposons $p > 3$, avec éventuellement $D = 3$. Alors le théorème (3.1.1) montre que l'équation n'admet aucune solution entière.

Supposons $p = 3$ et $D \neq 3$. Si $D \equiv 3 \bmod 4$, il existe et $A_1, B_1 \in \mathbb{Z}$ tels que

$$X + 2\sqrt{-D} = \left(\frac{A_1 + B_1\sqrt{-D}}{2}\right)^3$$

Supposons que $(B_1, 2) = 1$. Comme $B_1|16$, il existe $\epsilon = \pm 1$, tel que

$$X + 2\sqrt{-D} = \left(\frac{A_1 + \epsilon\sqrt{-D}}{2}\right)^3. \tag{3.41}$$

En particulier, on obtient $Y = \frac{A_1^2 + D}{4}$. En identifiant les parties imaginaires dans (3.41), il vient

$$16\epsilon = 3A_1^2 - D,$$

et en identifiant les parties réelles, $X = \pm A_1 (A_1^2 - 6\epsilon)$. Si $D \neq 3 \bmod 4$ ou si $2|B_1$, il existe $A, B \in \mathbb{Z}$ tels que

$$X + 2\sqrt{-D} = \left(A + B\sqrt{-D}\right)^3.$$

Les entiers A, B précédents correspondent à ceux de l'énoncé du théorème (3.1.1). Le cas "$C = 1, n = 3$" du théorème montre qu'il existe $\epsilon = \pm 1$ tel que $\epsilon = 3A^2 - 4D$. A étant impair, en se plaçant modulo 4, on obtient $\epsilon = -1$, donc $D = \frac{3A^2+1}{4}$. Toujours par le théorème (3.1.1), il vient alors $Y = 4A^2 + 1$, et $X = \pm A (8A^2 + 3)$.

Remarquons que les entiers D pour lesquels il y a deux solutions (au signe près) (X, Y), sont données par :

$$3A^2 - 16\epsilon = \frac{3B^2+1}{4},$$

c'est à dire

$$12A^2 - 3B^2 = 64\epsilon + 1.$$

Donc $\epsilon = -1$ et $B^2 - 4A^2 = 21$, ce qui donne $A = 1$, ou $A = 5$, ie $D = 19$ ou 91. ■

Remarque 3.6.1 *Si $b = 2$, $C = 1$, $p = 5$, et m quelconque, on montre facilement que $2|A_1, B_1$, sans hypothèse sur D. Si D est impair, le lemme (3.3.2) montre alors que $u_n = \pm 1$. Si $2|D$, on vérifie en identifiant les parties imaginaires de (3.27), que $B = \pm 2^m$, ce qui donne encore $u_n = \pm 1$.*

En généralisant une remarque de Le (voir [43]), on peut alors également trouver tous les entiers (x, y, m) solutions de :

$$x^2 + 2^{2m}D = y^5, (x, y) = 1,$$

en appliquant le théorème de Cohn suivant :

Théorème 3.6.2 *(voir [29].) Si ϕ_k est un carré d'entier, alors $\phi_k = 1$ ou $\phi_k = 144$.*

En effet, l'égalité $u_n(\epsilon, \overline{\epsilon}) = \pm 1$ s'écrit aussi

$$\left(2^{2m}D - 5A^2\right)^2 - 20A^4 = \pm 1.$$

Autrement dit, le couple $(2^{2m}D - 5A^2, A^2)$ est solution de l'équation de type Pell-Fermat suivante :

$$x^2 - 20y^2 = \pm 1,$$

qui se résout via le corps $\mathbb{Q}(\sqrt{5})$ dont $\frac{1+\sqrt{5}}{2}$ est l'unité fondamentale. La résolution donne qu'il existe un entier k tel que $4A^2 = \phi_k$. Comme le terme de gauche est un carré d'entier, le théorème de Cohn donne $A = \pm 6$. On obtient $2^{2m}D - 5A^2 = \pm 161$, ie $2^{2m}D = 19$ ou $2^{2m}D = 341$, ie $m = 0, D = 19$ ou $D = 341$. Si $D = 19$, on trouve $Y = 36 + 19 = 55$ et si $D = 341$, on trouve $Y = 36 + 341 = 377$.

En particulier, l'équation d'Aigner est sans solution dans le cas $n = 5$.

3.7 Applications séquentielles du théorème (3.1.1).

3.7.1 Démonstration du théorème (3.1.7).

Soit l'équation suivante d'inconnue $(X, n) \in \mathbb{N}^2$:

$$l^n = b^{2m} + CX^2.$$

On va montrer qu'il y a une correspondance entre les solutions (X, n), $X > 0, n > 0$, et les éléments de $\mathcal{E}'$. En effet, soit donc (X, n) une telle solution. Soit $\Theta = b^m + \sqrt{-C}$. On a alors $\Theta\overline{\Theta} = l$. La décomposition en produit d'idéaux premiers de $(b^m + X\sqrt{-C})(b^m - X\sqrt{-C})$ dans le corps $\mathbb{K} = \mathbb{Q}(\sqrt{-C})$ est donc

$$(\overline{\Theta}^n)(\Theta^n) = (b^m + X\sqrt{-C})(b^m - X\sqrt{-C}).$$

Comme l est premier impair, $(2b, l) = 1$. Les idéaux $(b^m + X\sqrt{-C})$ et $(b^m - X\sqrt{-C})$ sont donc premiers entre eux dans $\mathbb{K}$. Quitte à changer les notations il existe donc un entier $n \geq 0$ tel que

$$\pm\Theta^n = b^m + X\sqrt{-C}. \tag{3.42}$$

On a le lemme suivant :

Lemme 3.7.1 *Pour tout entier naturel n, il existe un unique couple d'entiers (a_n, b_n) tel que $\sqrt{-C}\Theta^n = a_n + b_n\Theta$.*

Preuve (du lemme) Pour $n = 0$, il n'y a rien à faire. Supposons la propriété acquise au rang n. On a alors

$$\begin{aligned}\sqrt{-C}\Theta^{n+1} &= \Theta(a_n + b_n\Theta) = a_n\Theta + b_n(-b^{2m} - C + 2b^m\Theta) \\ &= -(b^{2m} + C)b_n + (a_n + 2b_nb^m)\Theta.\end{aligned}$$

Pour l'unicité, il n'y a rien à faire.□ Par unicité, la démonstration précédente montre que l'on a les relations suivantes :

$$\begin{cases} a_{n+1} = -(b^{2m} + C)b_n; \\ b_{n+1} = a_n + 2b_nb^m; \end{cases}$$

En particulier, on a

$$b_{n+2} = a_{n+1} + 2b_{n+1}b^m = -(b^{2m} + C)b_n + 2b_{n+1}b^m = 2b_{n+1}b^m - lb_n.$$

De plus, par définition, $b_0 = 1$ et $b_1 = b^m$. Par (3.42), on a

$$\begin{aligned}\sqrt{-C}\Theta^n &= \pm\Big(b^m\sqrt{-C} - CX\Big)\\ &= \pm(-CX + b^m(\Theta - b^m))\\ &= \pm\big(-CX - b^{2m} + b^m\Theta\big).\end{aligned}$$

L'entier n est donc tel que $b_n = \pm b^m$, c'est à dire un élément de $\mathcal{E}'$. A la solution (X, n), on associe l'entier n. Inversement, supposons qu'il existe un entier n tel que $b_n = \epsilon b^m$, avec $\epsilon = \pm 1$. On pose alors

$$Z = \left|\frac{\epsilon a_n + b^{2m}}{C}\right| \in \mathbb{Q}.$$

Montrons que $CZ^2 + b^{2m} = l^n$. En effet, on a, vu que $\Theta\overline{\Theta} = l^n$, la relation suivante :

$$Cl^n = (\sqrt{-C}\Theta)(\overline{\sqrt{-C}\Theta}) = (a_n + b_n\Theta)(a_n + b_n\overline{\Theta}) = a_n^2 + 2\epsilon a_n b^{2m} + b^{2m}l. \tag{3.43}$$

On a alors, en utilisant (3.43) et le fait que $l = C + b^{2m}$

$$\begin{aligned}C^2Z^2 + b^{2m}C &= a_n^2 + b^{4m} + 2\epsilon a_n b^{2m} + b^{2m}C\\ &= Cl^n - b^{2m}l + b^{4m} + b^{2m}C\\ &= Cl^n - b^{2m}(C + b^{2m}) + b^{4m} + b^{2m}C\\ &= Cl^n,\end{aligned}$$

c'est à dire

$$CZ^2 + b^{2m} = l^n.$$

Comme C est sans facteur carré, $Z \in \mathbb{N}$. De plus, si (X, n) (X', n') sont telles que $n = n'$, alors $X = X'$, car $X, X' > 0$. Donc on a la correspondance voulue entre les solutions (X, n) et $\mathcal{E}'$.

Soit p un diviseur premier de n, avec $(p, 6h(-C)) = 1$. Le théorème (3.1.1) donne, pour la solution éventuelle $(x, l^{\frac{n}{p}}, p)$ de

$$Cx^2 + b^{2m} = l^n,$$

$p = 5$ et $l^{\frac{n}{5}}$ est une puissance entière propre de Lucas ou de Fibonacci si $n \neq 5$. Mais de telles puissances sont $1, 4, 8$ et 144. Comme $l \neq 2$, on a donc $n = 5$. Comme $C > 1$, le corollaire (3.1.9) montre que $C = 2, m = 0$, c'est à dire $l = 3$. On a donc bien $\mathcal{E} = \{1\}$, sauf si $l = 3$, auquel cas $\mathcal{E} = \{1, 5\}$.

Le fait que $\mathcal{E}'$ soit effectif résulte du fait que n est bornée par une constante $\mathcal{C}(m)$ effective (voir le théorème (3.1.23)). ■

3.7.2 Application : résolution de l'équation (3.4).

Soit (b_n) la suite définie par

$$\begin{cases} b_0 = b_1 = 1; \\ b_{n+2} = 2b_{n+1} - 3b_n; \end{cases}$$

La démonstration précédente montre que les solutions (X, n) de (3.4) sont en correspondance avec les entiers $n \geq 1$ tels que $b_n = \pm 1$ (à (X, n) correspond n). Déterminons d'abord les solutions éventuelles (X, n) où n est une puissance de deux. On va appliquer le théorème de Strassmann (voir [28] par exemple). Considérons en effet le polynôme suivant $f(X) = X^2 - 2X + 3$. Le corps $\mathbb{Q}_{17}$ est un corps de décomposition pour f. En effet, modulo 17, le polynôme réduit de f s'écrit $f(X) = (X - 11)(X - 8)$. Par le lemme de Hensel, il existe donc $\alpha \neq \beta, \alpha, \beta \in \mathbb{Q}_{17}$, tels que $f(\alpha) = f(\beta) = 0$. En appliquant l'algorithme de Newton à ces racines, on obtient :

1. $\alpha \equiv 266 \bmod 17^2$.
2. $\beta \equiv 25 \bmod 17^2$.

Le terme b_n s'exprime en fonction des racines de f :

$$(\beta - \alpha)b_n = \alpha^n(\beta - 1) - \beta^n(\alpha - 1).$$

Soit maintenant un entier $n = 2^t$ tel que $b_n = \pm 1$. Si $t < 4$, alors seul les termes $t = 1$ et $t = 0$ conviennent. On peut donc supposer $t \geq 4$. En particulier, il existe s tel que $n = 16s$. Par le petit théorème de Fermat, comme $\nu_{17}(\alpha\beta) = 0$, $\alpha^{16s} \equiv 1 \bmod 17$ et $\beta^{16s} \equiv 1 \bmod 17$. On pose $a = \alpha^{16} - 1$ et $b = \beta^{16} - 1$. Soit $s \in \mathbb{Z}_{17}$ et soit

$$\Phi(s) = (\beta - \alpha)(b_{16s} - 1) = (\alpha^{16s} - 1)(\beta - 1) - (\beta^{16s} - 1)(\alpha - 1).$$

Comme $a \equiv 0 \bmod 17$ et $b \equiv 0 \bmod 17$, $\Phi(s)$ est bien définie car $\alpha^{16s} = (1 + (\alpha^{16} - 1))^s = exp_{17}(s \log_{17}(1 + a))$ est convergente. Par définition de Φ, on a $\Phi(0) = \Phi(s) = 0$. On pose

$$\Phi(s) = \sum_{j=1}^{+\infty} C_j s^j.$$

On a $C_j = \mathcal{O}(17^2)$ si $j > 1$ et $C_1 \equiv a(\beta - 1) - b(\alpha - 1) \bmod 17^2 \neq 0 \bmod 17^2$. On a donc une fonction analytique au voisinage de 0, qui dans ce voisinage a au moins deux zéros distincts, mais dont le coefficient C_1 est le plus petit p-adiquement. On a une contradiction avec le théorème de Strassmann. Donc seules $n = 1$ et $n = 2$ conviennent parmi les $n = 2^t$.

Soit maintenant une solution éventuelle (X, n) telle que $n > 1$ et n qui n'est pas une puissance de deux. Soit p un facteur premier impair de n. Le théorème (3.1.1) montre que $p = 3$ ou $p = 5$. Les cas $C > 1, p = 3$ et $C > 1, p = 5$ montrent que nécessairement $X = 11, n = 5$. Si $n = 1$, $X = 1$ convient.

Ainsi les seules solutions (X, n) de $3^n = 1+2X^2$ (avec $n = 0$ possible) sont les suivantes :

$$(0, 0), (1, 1), (2, 2), (11, 5). \tag{3.44}$$

Remarquons que ce résultat découle aussi du théorème classique de Nagell-Ljunggren (voir [64]) :

Théorème 3.7.2 *(Théorème de Nagell-Ljunggren.)*

A part les solutions

$$\frac{3^5 - 1}{3 - 1} = 11^2, \quad \frac{7^4 - 1}{7 - 1} = 20^2, \quad \frac{18^3 - 1}{18 - 1} = 7^3,$$

l'équation

$$\frac{x^n - 1}{x - 1} = y^q, \quad x, y > 1, \quad n > 2, q \geq 2,$$

n'en a pas d'autres si l'une des conditions suivantes est satisfaite :

- *soit* $q = 2$,
- *soit* 3 *divise* n,
- *soit* 4 *divise* n,
- *soit* $q = 3$ *et* $n \equiv 5 \bmod 6$.

Mettons en effet l'équation (3.4) sous la forme

$$\frac{3^n - 1}{3 - 1} = X^2.$$

Le théorème (3.7.2), appliqué avec $q = 2$ montre que $n = 1, 2$ ou $n = 5$ et $X = 11$. Si $n = 1$, on trouve que $X = 1$ convient, si $n = 2$, on trouve que $X = 2$ convient. La liste des solutions $(X, n), n > 0$ est donc

$$\{(1, 1), (2, 2), (11, 5)\}.$$

3.7.3 Démonstration de la proposition (3.1.8).

Soit (b_n) la suite définie par

$$\begin{cases} b_0 = b_1 = 1; \\ b_{n+2} = 2b_{n+1} - lb_n; \end{cases}$$

La démonstration du théorème (3.1.7) montre que le nombre de termes de la suite, d'indice non nul, valant ± 1 est égal au nombre de solution (X, n), $X > 0, n > 0$, de

$$\frac{l^n - 1}{l - 1} = X^2.$$

Par le théorème de Nagell-Ljunggren (théorème (3.7.2)), on sait qu'il y en a trois si $l = 3$, qu'il y en a deux si $l = 7$ et une sinon (si un nombre premier l vérifie $l + 1 = Z^2$, alors $l = 3$). ■

3.8 Démonstration du corollaire (3.1.9).

Supposons d'abord que $C \neq 3 \bmod 4$. Soit (X, Y, m) une solution de

$$CX^2 + 2^{2m} = Y^n, (X, Y) = 1.$$

Comme $m > 0$, on a bien $(2X, Y) = 1$. On peut appliquer le théorème (3.1.1). Il montre que $n = 3$ ou $n = 5$. Supposons d'abord que $n = 3$.

Si $C = 1$, le théorème (3.1.1) montre qu'il existe des solutions si et seulement s'il existe un entier A et $\epsilon = \pm 1$, tel que $3A^2 = \epsilon + 2^{2m}$. La preuve du théorème (3.1.1) montre que A divise X. En particulier, A est impair et donc $3A^2 \equiv -1 \bmod 4$. Alors, si $m \geq 2$, on doit avoir $\epsilon = -1$, ie

$$3A^2 + 1 = 2^{2m}, \quad 2m > 2$$

Or l'équation $3X^2 + 1 = Y^n$ est sans solution triviale pour $n > 2$. On a donc $m = 1$ et $3A^2 = \pm 1 + 4$, ie $m = 1$, $\epsilon = 1$, $A^2 = 1$. Le théorème (3.1.1) montre alors que $X = \pm 5$, $Y = 3$. Dans le cas $C = m = 1$, les relations proposées dans l'énoncé du corollaire donnent bien ces valeurs.

Si $C > 1$, le théorème (3.1.1) distingue plusieurs cas possibles. Dans le premier, il existe un entier A impair tel que $3A^2C = \epsilon + 2^{2m}$. Comme C est impair et $C \neq 3 \bmod 4$, donc $C \equiv 1 \bmod 4$, on a $3A^2C \equiv -1 \bmod 4$. Comme $C > 1$, alors $m > 1$, donc $\epsilon = -1$ en se plaçant modulo 4. Il existe donc un entier A tel que $CA^2 = \frac{4^m - 1}{3}$, et alors le théorème (3.1.1) montre que

$$\pm X = A\left(-3 - 8A^2C\right) = A\left(\frac{-1 - 2^{2m+3}}{3}\right), \quad Y = 4A^2C + 1 = \frac{4^{m+1} - 1}{3}.$$

Dans le second cas, il existe un entier A impair (car divisant X), k et $\epsilon = \pm 1$ tels que $A^2C = 3 - 3^k\epsilon$. Cette dernière égalité est impossible car sinon elle impliquerait que CA^2 est pair, ce qui est faux.

Enfin, dans le troisième cas, il existe un entier A, k et $s = \pm 1$ tels que

$$8 \cdot 2^{2m} = s + 3^{k+1}, \quad A^2C = 3 \cdot 2^{2m} - 3^k.$$

Si $k+1$ est impair, alors k est pair et donc $s + 3^{k+1} \equiv 3 + s \bmod 8 \neq 0 \bmod 8$, et donc l'égalité $8 \cdot 2^{2m} = s + 3^{k+1}$ ne peut avoir lieu. Ainsi, $k+1$ est pair, et en se plaçant modulo 8, on voit que $s = -1$. On a donc

$$3^{\frac{k+1}{2}} - 1 = 2, \quad 3^{\frac{k+1}{2}} + 1 = 2^{2m+2},$$

ce qui donne $2^{2m+1} = 1$: absurde.

Supposons maintenant que $n = 5$. Comme $C \neq 3 \bmod 4$, la démonstration du théorème (3.1.1) montre qu'il existe des entiers A, B tels que

$$X\sqrt{C} + 2^m\sqrt{-1} = \left(A\sqrt{C} + B\sqrt{-1}\right)^5.$$

Avec les notations du théorème (3.1.1), $D = 1$. Le lemme (3.3.2) montre que $B = \pm 2^m$. L'égalisation des parties imaginaires donne alors

$$\pm 1 = 5A^4C^2 - 10 \cdot 2^{2m}A^2C + 2^{4m}.$$

Comme $m \geq 1$ et CA impair, modulo 8 cela donne $\pm 1 \equiv 5 \bmod 8$, ce qui est impossible.

Pour terminer la preuve du corollaire, il reste à étudier le cas $C \equiv 3 \bmod 4$. Dans ce cas, si $C > 3$, la preuve du théorème (3.1.1) montre qu'il existe deux entiers A et B de même parité tels que

$$X\sqrt{C} + 2^m\sqrt{-1} = \left(\frac{A\sqrt{C} + B\sqrt{-1}}{2}\right)^n.$$

Si $n > 3$, la preuve du théorème (3.1.1) montre que B est pair, et les résultats du théorème(3.1.1) s'appliquent. On retrouve les résultats précédents. Si $n = 3$ et B pair, idem. Il reste donc à traiter le cas $n = 3$ et B impair. Comme B divise 2^m, c'est étudier le cas $n = 3$, $B = \pm 1$. La preuve du théorème (3.1.1) montre qu'il existe un entier A impair tel que

$$X\sqrt{C} + 2^m\sqrt{-1} = \left(\frac{A\sqrt{C} + B\sqrt{-1}}{2}\right)^3, \quad B = \pm 1.$$

L'égalisation des parties imaginaires donne

$$3A^2C = 2^{m+3} \pm 1.$$

Comme $C \equiv 3 \bmod 4$, seul le signe + convient : il existe donc un entier A tel que

$$3A^2C = 2^{m+3} + 1.$$

Nécessairement m est pair car sinon, $2^{m+3} + 1 \neq 0 \bmod 3$. Comme alors $4Y = CA^2 + B^2$, cela donne $4Y = \frac{2^{m+3}+1}{3} + 1$ ie $Y = \frac{2^{m+1}+1}{3}$. L'égalisation des parties réelles donne $8X = A^3C - 3A = A\left(\frac{8\cdot 2^m+1}{3} - 3\right) = A\left(\frac{8\cdot 2^m-8}{3}\right)$, ie $X = A\left(\frac{2^m-1}{3}\right)$.

Enfin, si $C = 3$, le théorème 1.8 de [59] montre que l'équation

$$3X^2 + 2^{2m} = Y^n, \quad (X, Y) = 1,$$

n'a aucune solution entière. Le corollaire est prouvé. ■

3.9 Démonstration du corollaire (3.1.12).

Si $C = 1$, l'étude a déjà été faite en exemple au paragrahe (3.4.5). On peut donc supposer dans la suite $C > 1$. Par (3.7), (x, y) divise 2^m. Il existe donc des entiers u, v tels que

$$x = 2^u X, \quad y = 2^v Y, \quad (X, Y) = 1.$$

L'équation (3.7) s'écrit

$$C2^{2u}X^2 + 2^{2m} = 2^{nv}Y^n.$$

– Supposons d'abord que $m \leq u$ et $2m \leq nv$. Alors

$$C\left(2^{u-m}X\right)^2 + 1 = 2^{nv-2m}Y^n.$$

Nécessairement $u = m$ ou $nv = 2m$.
Si $u = m$, comme $C \neq 7 \bmod 8$, on doit avoir $nv - 2m = 1$ ou 2, ie

$$CX^2 + 1 = 2Y^n, \quad ou \quad CX^2 + 1 = 4Y^n.$$

Lemme 3.9.1 *([45]) Soit $A \geq 1$ un entier sans facteur carré. Les équations diophantiennes*

$$Ax^2 + 1 = 2y^n, A \equiv 1 \bmod 4, \quad Ax^2 + 1 = 4y^n, A \equiv 3 \bmod 4,$$

n'ont aucune solution en entier positif tels que $y > 1$ impair, $n > 2$ et $n \nmid h(-A)$.

Comme $h(-C)$ est premier à n et Y impair, ce lemme montre donc que $Y = 1$, donc que

$$nv - 2m = 1, C = 1, X = \pm 1, \quad ou \quad nv - 2m = 2, C = 3, X = \pm 1.$$

Dans le pemier cas, $C = 1$, le premier n divise $2m + 1$ et alors $x = \pm 2^m$, $y = 2^{\frac{2m+1}{n}}$.
Dans le second, $C = 3$, le premier n divise $m + 1$, et alors $x = \pm 2^m$, $y = 4^{\frac{m+1}{n}}$.
Si $nv = 2m$, on a $C\left(2^{u-m}X\right)^2 + 1 = Y^n$. Comme C est impair, cette équation est sans solution (voir [61], théorème 25).

– Supposons que $u \leq m$ et $2u \leq nv$. L'équation (3.7) s'écrit

$$CX^2 + 2^{2(m-u)} = 2^{nv-2u}Y^{nv}.$$

Comme CX^2 est impair, soit $m = u$, soit $nv = 2u$. Si $m = u$, comme $C \neq 7 \bmod 8$, on a $nv - 2u = 1$ ou 2 et on est ramené à un cas précédent. Si $nv = 2u$, on est ramené à l'équation

$$CX^2 + 2^{2(m-u)} = Y^n, \quad m - u > 0.$$

Comme $C > 1$ impair, $m - u > 0$ et C impair, le corollaire (3.1.9) montre que $n = 3$, donc $3v = 2u$ et que les entiers X, Y existent si et seulement s'il existe un entier b tel que

$$Cb^2 = \frac{1 + 2^{m-u+3}}{3}, \quad 2|m - u,$$

ou

$$Cb^2 = \frac{2^{2m-2u} - 1}{3}.$$

Dans le premier cas, le corollaire (3.1.9) donne

$$x = \pm 2^u \cdot b \cdot \frac{2^{m-u} - 1}{3} = \pm b \cdot \frac{2^m - 2^u}{3}, \quad y = \pm 2^{\frac{2u}{3}} \cdot \frac{1 + 2^{m-u+1}}{3}.$$

Dans le second cas, le corollaire (3.1.9) donne

$$x = \pm 2^u \cdot b \cdot \frac{8 \cdot 4^{m-u} + 1}{3} = \pm b \cdot \frac{2^{2m-u+3} + 2^u}{3}, \quad y = \pm 2^{\frac{2u}{3}} \cdot \frac{4^{m-u+1} - 1}{3}.$$

– Supposons $nv \leq 2u$ et $nv \leq 2m$. L'équation (3.7) se ramène alors à

$$C2^{2u-nv}X^2 + 2^{2m-nv} = Y^n.$$

Nécessairement $2m = nv$ ou $2u = nv$. Dans le premier cas, on doit résoudre $C\left(2^{u-m}X\right)^2 + 1 = Y^n$ cas déjà étudié avant. Dans le second cas $CX^2 + 2^{2(m-u)} = Y^n$, $m > u$, $nv = 2u$ et on est ramené à un cas déjà étudié.

Le corollaire est prouvé.

3.10 Démonstration du théorème (3.1.14)

On peut directement appliquer le théorème (3.1.1), car $(2X, Y) = 1$ et avec les notations de celui-ci $D = 2$ et donc $CD \neq 3 \bmod 4$. On trouve que $n = 3$ ou $n = 5$.

Supposons $n = 3$. Si $C = 1$, le théorème (3.1.1) montre qu'il existe un entier A et $\epsilon = \pm 1$ tels que

$$3A^2 = \epsilon + 2^{2m+1}.$$

La preuve du théorème (3.1.1) montre que A divise X. En particulier, A est impair, et donc en se plaçant modulo 4, on voit que $\epsilon = -1$ si $m > 0$, ie

$$3A^2 + 1 = 2^{2m+1}$$

si $m > 0$, équation sans solution entière car $2m+1 > 2$. Donc en fait $m = 0$, $\epsilon = 1$, $A^2 = 1$. Le théorème (3.1.1) montre alors que $X = \pm 5$ et $Y = 3$.

Si $C > 1$, il y a plusieurs possibilités. Dans le premier cas, il existe un entier A et $\epsilon = \pm 1$ tels que $3A^2C = \epsilon + 2^{2m+1}$. En se plaçant modulo 3, on voit nécessairement que $\epsilon = 1$, ie

$$A^2C = \frac{2^{2m+1} + 1}{3}.$$

Le théorème (3.1.1) montre alors que

$$X = \pm A\left(\frac{4^{m+2} - 1}{3}\right), \quad Y = \frac{2^{2m+3} + 1}{3}.$$

Dans le second cas, il existe des entiers A, k, $\epsilon = \pm 1$, $s = \pm 1$ tels que

$$A^2C = 6 - 3^k\epsilon, \quad 16 = 2^m s + 3^{k+1}\epsilon.$$

Nécessairement, $m = 0$, et alors $16 - s = 3^{k+1}\epsilon$, ce qui est impossible.

Enfin, dans le dernier cas, il existe des entiers A, k, $\epsilon = \pm 1$, $s = \pm 1$ tels que

$$A^2C = 3 \cdot 2^{2m+1} - 3^k, \quad 2^{2m+4} = s + 3^{k+1}.$$

L'équation $2^{2m+4} = s + 3^{k+1}$ donne $s = 1$ en se plaçant modulo 3. Alors $2^{2m+4} - 1 = 3^{k+1}$ ie $(2^{m+2}+1)(2^{m+2}-1) = 3^{k+1}$, ie $2^{m+2}-1 = 1$, $2^{m+2}+1 = 3^{k+1}$. Comme $m \geq 0$, $2^{m+2}-1 = 1$ est impossible.

Supposons maintenant $n = 5$. On sait qu'il existe des entiers A et B tels que

$$X\sqrt{C} + 2^m\sqrt{-2} = \left(A\sqrt{C} + B\sqrt{-2}\right)^5.$$

En identifiant les parties imaginaires, il vient

$$\frac{2^m}{B} = 5\left(A^2C - 2B^2\right)^2 - 16B^4.$$

En identifiant les parties réelles, on voit que A divise X. En particulier, A est impair. Comme C l'est aussi, l'équation précédente montre que l'entier $\frac{2^m}{B}$ est impair, et donc vaut ± 1, ie

$$\pm 1 = 5\left(A^2C - 2B^2\right)^2 - 2^{4m+4}.$$

Modulo 8, il vient $\pm 1 \equiv 5 \bmod 8$, ce qui est faux.

3.11 Démonstration du théorème (3.1.15).

Soit donc (x, y) une solution de l'équation (3.9), $x \neq 0$. On pose $x = 2^u X$, $y = 2^v Y$, $(XY, 2) = 1$. Les entiers X, Y sont solutions de

$$C2^{2u}X^2 + 2^{2m+1} = 2^{nv}Y^n. \tag{3.45}$$

Si $2m + 1$ est majoré par $2u$ et nv, on obtient à partir de (3.45)

$$2C\left(2^{u-m-1}X\right)^2 + 1 = 2^{nv-2m-1}Y^n.$$

Nécessairement, $nv = 2m + 1$ et

$$2C\left(2^{u-m-1}X\right)^2 + 1 = Y^n.$$

Posons pour simplifier $T = 2^{u-m-1}X$. Pour résoudre cette équation, on va appliquer le théorème (3.1.1). On obtient $n = 3$ ou $n = 5$. Le cas $n = 3$ ne donne aucune solution. Dans le cas $n = 5$, la preuve du théorème (3.1.1) montre qu'il existe des entiers A et $B = \pm 1$ tels que

$$T\sqrt{2C} + \sqrt{-1} = \left(A\sqrt{2C} + B\sqrt{-1}\right)^5.$$

L'identification des parties imaginaires conduit à

$$\pm 1 = 5A^4(2C)^2 - 10A^2(2C) + 1.$$

On obtient ($A \neq 0$ car divise X) $A^2C = 1$, ie $C = A^2 = 1$. L'entier T est donc solution de $2T^2 + 1 = Y^5$, donc $T = \pm 11$, $Y = 3$, ie

$$2^{u-m-1}X = \pm 11, \quad Y = 3.$$

On a donc $u = m+1$, $5v = 2m+1$, $X = \pm 11$, $Y = 3$. Ainsi, $5|2m+1$, et alors

$$x = \pm 2^{m+1} \cdot 11, \quad y = 2^{\frac{2m+1}{5}} \cdot 3.$$

Supposons maintenant que ce soit $2u$ qui est majoré par nv et $2m+1$. Les entiers X et Y sont alors solutuions de

$$CX^2 + 2^{2(m-u)+1} = 2^{nv-2u} Y^n.$$

Comme CX est impair, on doit avoir $nv = 2u$ et donc

$$CX^2 + 2^{2(m-u)+1} = Y^n.$$

Le théorème (3.1.14) montre qu'il existe des solutions entières si et seulement si $n = 3$ et s'il existe un entier A tel que

$$A^2 C = \frac{2^{2(m-u)+1} + 1}{3}.$$

Alors, $3v = 2u$ et les entiers X et Y sont donnés par

$$X = \pm A \left(\frac{4^{m-u+2} - 1}{3} \right), \quad Y = \frac{2^{2(m-u)+3} + 1}{3}$$

On a donc $3|u$ et

$$x = \pm A 2^u \left(\frac{4^{m-u+2} - 1}{3} \right), \quad y = 2^{\frac{2u}{3}} \frac{2^{2(m-u)+3} + 1}{3}.$$

Supposons enfin que ce soit nv qui soit majoré par $2u$ et $2m+1$. Alors X et Y sont solutions de

$$2^{2u-nv} CX^2 + 2^{2m+1-nv} = Y^n.$$

Comme Y est impair, soit $2u = nv$, soit $2m+1 = nv$. Si $2u = nv$, on est ramené au cas précédent. Si $2m+1 = nv$, alors X et Y sont solutions de

$$2^{2u-2m-1} CX^2 + 1 = Y^n,$$

ie

$$2C \left(2^{u-m-1} X \right)^2 + 1 = Y^n.$$

On a déjà montré que cela implique que $n = 5$, $C = 1$, $2^{u-m-1} X = \pm 11$, $Y = 3$. On a donc

$$X = \pm 11, \quad Y = 3, \quad u = m+1, \quad 5v = 2m+1,$$

et on retombe sur un cas déjà traité.

3.12 Démonstration du théorème (3.1.17).

Soit donc (X, Y) une solution entière de (3.10). Notons que Y est impair. En effet, sinon, X l'est et modulo 8, on obtient $(b > 2) : C+1 \equiv 0 \bmod 8$, ie $C \equiv 7 \bmod 8$, en contradiction avec les hypothèses. On a donc bien $(2X, Y) = 1$. Comme $n > 3$ et $b \neq \left(\frac{-C}{b}\right) \bmod n$, on peut appliquer le théorème (3.1.1). Celui-ci montre directement que $n = 5$ et une partie des résultats sur Y. Il reste à montrer l'existence de E et la valeur de Y en fonction de E. Pour cela, on revient à la preuve du théorème (3.1.1) : il existe des entiers A et B tels que

$$X\sqrt{C} + b^m\sqrt{-1} = \left(A\sqrt{C} + B\sqrt{-1}\right)^5.$$

En identifiant les parties imaginaires, il vient

$$\frac{b^m}{B} + 4B^4 = 5\left(A^2C - B^2\right)^2 = 5E^2, \quad E > 0$$

avec $E + 2B^2 = CA^2 + B^2 = Y$. ■

Commentaires 3.12.1 *La preuve du théorème* 3.1 *de [60] est fausse. L'existence des entiers a et b de sa preuve ne convient que si $p \neq 3 \bmod 4$. Sinon, on aura une égalité de la forme*

$$x\sqrt{p} + q^m\sqrt{-1} = \left(\frac{a\sqrt{p} + b\sqrt{-1}}{2}\right)^p, \quad a \equiv b \bmod 2,$$

et il reste à montrer que $2|a, b$ ce qui n'est pas justifié. De plus, deux lignes avant la fin de la preuve, on devrait lire

$$\left(\alpha^2 - \beta^2\right)^2 = -16apb^2 = -16papq^{2j},$$

où l'entier j peut s'annuler. Or elle remplace j par m. Elle en déduit que $(\alpha^2 - \beta^2)^2$ est divisible par q, donc que le théorème des diviseurs primitifs s'applique. Or, en fait on a du q^{2j} et si $j = 0$ on ne peut à priori pas appliquer le théorème. Si $j = 0$, tout ce qu'on peut dire c'est que Y est de la forme $Y = pA^2 + 1$. Donc le théorème 3.1 ***réellement prouvé*** *par Muriefah est le suivant :*

Théorème 3.12.2 *Soit $p \neq 3 \bmod 4$ un nombre premier. Supposons qu'il existe des entiers x, y tels que*

$$px^2 + q^{2m} = y^p, \quad (x, y) = 1, \quad m > 0,$$

où y ne se met pas sous la forme $y = pa^2 + 1$. Alors $p = 5$ et y est un terme de la suite de Lucas ou de Fibonacci.

3.13 Démonstration du théorème (3.1.20)

Supposons $n \geq 5$. Toute unité du corps quadratique imaginaire $\mathbb{Q}\left(\sqrt{-CD}\right)$ est une puissance n-ième dans son anneau des entiers. Il existe donc des entiers relatifs A, B tels que

$$X\sqrt{C} + b^m\sqrt{-D} = \left(\frac{A\sqrt{C} + B\sqrt{-D}}{2}\right)^n. \tag{3.46}$$

En particulier, comme $A, B \neq 0$,

$$4Y = CA^2 + B^2D \geq D_0,$$

où $D_0 = Sup\,(C + D, 12)$. L'équation (3.46) donne

$$|\epsilon^n - \overline{\epsilon}^n| = |\epsilon - \overline{\epsilon}|\,\frac{2b^m}{|B|}. \tag{3.47}$$

avec $\epsilon = \frac{A\sqrt{C}+B\sqrt{-D}}{2}$. On écrit (3.47) sous la forme

$$|\epsilon - \overline{\epsilon}|\,\frac{2b^m}{|B|} = |\epsilon|^n \left|\left(\frac{\overline{\epsilon}}{\epsilon}\right)^n - 1\right|.$$

Soit log la détermination principale du logarithme. On a le lemme suivant :

Lemme 3.13.1 *Soit $z \in \mathbb{C}$ le corps des nombres complexes. Alors soit $|e^z - 1| > \frac{1}{2}$, soit il existe $k \in \mathbb{Z}$ tel que $|e^z - 1| \geq \frac{1}{2}\left|z - \sqrt{-1}k\pi\right|$.*

Preuve Supposons que $|e^z - 1| \leq \frac{1}{2}$. Soit $Z = e^z - 1$. Comme $|Z| \leq \frac{1}{2}$, on a $|\log(1 + Z)| \leq 2|Z|$. De plus, il existe un entier ℓ tel que $|\log(1 + Z)| = \left|z - \sqrt{-1}\ell\pi\right|$.□

Posons pour la suite $z = \log\left(\left(\frac{\overline{\epsilon}}{\epsilon}\right)^n\right)$. Si $|e^z - 1| > \frac{1}{2}$, alors

$$Y^{\frac{n}{2}} = |\epsilon|^n \leq \frac{8b^m}{|B|}\sqrt{Y}.$$

ie $(n-1)\log(\sqrt{D_0}/2) \leq \log(8b^m)$, et on obtient une inégalité meilleure que celle escomptée. Dans l'autre cas, il existe un entier k tel que $|k| \leq n$ et

$$\log(8b^m) \geq (n-1)\log(\sqrt{Y}) + \log\left|n\log\left(\frac{\overline{\epsilon}}{\epsilon}\right) - k\pi\sqrt{-1}\right|.$$

On pose $\Lambda = \left|n\log\left(\frac{\overline{\epsilon}}{\epsilon}\right) - k\pi\sqrt{-1}\right|$. Pour minorer $\log\Lambda$, on va appliquer le théorème 3 de [50]. Rappelons son énoncé et ses notations. Soit donc $\alpha \in \overline{\mathbb{Q}}$, de module 1 et soit b_1, b_2 deux entiers positifs. On note $h(\alpha)$ le poids de Weil de α. Soit $\lambda = \left|b_1\sqrt{-1}\pi - b_2\log(\alpha)\right| \neq 0$ où

log est une branche quelconque du logarithme. Soit D_0 le degrés de α sur $\mathbb{Q}$ divisé par 2 et soient

$$a = max\{20, 10.98|\log(\alpha)| + D_0 h(\alpha)\},$$
$$H = max\{17, \frac{\sqrt{D}}{10}, D_0 \log(\frac{b_1}{2a} + \frac{b_2}{68.9}) + 2.35D_0 + 5.03\},$$

où $h(\alpha)$ est le poids logarithmique de α. Alors

$$\log(\lambda) \geq -8.87aH^2.$$

On peut appliquer le théorème 3 de [50], car on peut supposer $k \geq 0$, quitte à considérer $\frac{\epsilon}{\overline{\epsilon}}$ (et vu que $\Lambda \neq 0$ car $\epsilon \neq \overline{\epsilon}$, car $A \neq 0$.) Ici, on a $h\left(\frac{\overline{\epsilon}}{\epsilon}\right) \leq \frac{1}{2}\log(Y)$, et on obtient

$$\log(\Lambda) \geq -8.87(11\pi + \frac{1}{2}\log(Y))(7.38 + \log(n/68.9 + k/(22\pi + \log(3))))^2.$$

On pose $H = H(n) = 7.38 + \log\left(\frac{n}{68.9} + \frac{n}{22\pi+\log(3)}\right)$, et $c_0 = 8.87$. Comme $|k| \leq n$, on en déduit

$$n \leq 1 + c_0 H^2 + \frac{11\pi c_0 H^2}{\log(\sqrt{D_0}/2)} + \frac{\log(8b^m)}{\log\left(\sqrt{Y}\right)}.$$

Si $16b^m \leq \sqrt{D}$, comme $4Y = CA^2 + B^2 D$, on a donc $8b^m \leq \sqrt{Y}$, d'où

$$n \leq 2 + c_0 H^2 + \frac{11\pi c_0 H^2}{\log(\sqrt{3})},$$

c'est à dire $n < N_1$, où N_1 est une constante absolue effective. On vérifie que l'on peut prendre $N_1 = 139297$. Dans le cas général, on a

$$n \leq 1 + c_0 H^2 + \frac{11\pi c_0 H^2 + \log(8b^m)}{\log(\sqrt{D_0}/2)}.$$

Supposons maintenant que $\frac{2b^m\sqrt{D}}{\sqrt{C}} < \sqrt{X}$. Considérons

$$\Lambda_1 = \left|\log\left(\frac{CX - b^m\sqrt{-CD}}{CX + b^m\sqrt{-CD}}\right)\right|.$$

On a $\frac{1}{2} > \frac{b^m\sqrt{D}}{\sqrt{CX}}$, donc

$$\Lambda_1 \leq \frac{2}{\sqrt{X}}.$$

L'application du théorème 3 de [50] donne

$$\log\left(\sqrt{X}\right) \leq c_0 H^2 11\pi + c_0 H^2 \log\sqrt{Y} + \log(2).$$

Comme $CX^2 + b^{2m}D = Y^n$, et $CX \geq 4b^{2m}D$, on a $Y^n \leq \frac{5}{4}CX^2$, ce qui donne la minoration suivante

$$\log(X) \geq n\log\sqrt{Y} - \frac{1}{2}\log(5C/4).$$

On a vu dans les démonstrations précédentes, qu'il existe des entiers A, B vérifiant $4Y = CA^2 + B^2D$, donc $\sqrt{Y} \geq \sqrt{C}/2$. On obtient

$$n \leq \frac{22c_0\pi H^2 + \log(4\sqrt{5})}{\log(\sqrt{3})} + 2c_0H^2 + \frac{\log(\sqrt{C}/2)}{\log(\sqrt{Y})}$$

c'est à dire

$$n \leq \frac{22c_0\pi H^2 + \log(4\sqrt{5})}{\log(\sqrt{3})} + 2c_0H^2 + 1.$$

Comme H^2 est un infiniment petit devant n, pour n assez grand c'est à dire $n \geq N_2$ l'inégalité précédente est impossible. On vérifie que l'on peut prendre $N_2 = 307451$. Comme c'est une conséquence du fait que $\sqrt{X} > \frac{2b^m\sqrt{D}}{\sqrt{C}}$, on doit donc avoir $X \leq \frac{4b^{2m}D}{C}$, si $n \geq N_2$. ■

3.14 Calculs généraux et preuve du théorème (3.1.23).

Il existe un idéal J de $\mathbb{K} = \mathbb{Q}(\sqrt{-CD})$ tel que $(CX - b^m\sqrt{-CD})^2 = (C)J^{2n}$. Soit $H = \mathrm{Gal}(\mathbb{K}/\mathbb{Q}) = \{1, j\}$, où j est la conjugaison complexe. On pose $\mathcal{N} = 1 + j$. Soit $\theta = e + fj \in \mathbb{Z}[H]$ fixé de sorte que J^θ soit principal. On pose θ_+ la somme des éléments qui composent θ à coefficients positifs. Par exemple, si $f \geq 0$ et $e < 0$ on pose $\theta_+ = fj$. On pose $\theta_- = \theta - \theta_+$. On appelle norme de θ que l'on note dans la suite $||\theta||$ la quantité $|e| + |f| \in \mathbb{N}$. Le poids de θ est la quantité $W(\theta) = e + f$. On suppose que $j\theta \neq \theta$, c'est à dire θ n'est pas un multiple de $\mathcal{N}$. On suppose aussi que $W(\theta)$ est pair. Il existe un nombre algébrique $\beta = \beta(\theta)$ de $\mathbb{K}$ tel que $\frac{(CX-b^m\sqrt{-CD})^{2\theta_+}}{(CX-b^m\sqrt{-CD})^{-2\theta_-}} = (CX - b^m\sqrt{-CD})^{2\theta} = C^{W(\theta)}\beta^{2n}$, c'est à dire $\frac{(CX-b^m\sqrt{-CD})^{\theta_+}}{(CX-b^m\sqrt{-CD})^{-\theta_-}} = (CX - b^m\sqrt{-CD})^{\theta} = \pm C^{W(\theta)/2}\beta^n$.

Soit $Z = \frac{\overline{\beta}}{\beta}$. On a $Z^n = \frac{\overline{\gamma}}{\gamma}$ avec $\gamma = (CX + b^m\sqrt{-CD})^{-\theta_-}(CX - b^m\sqrt{-CD})^{\theta_+}$ entier algébrique.

Le poids de Weil de Z^n, noté $h(Z^n)$, vérifie ($n > 0$) :

$$nh(Z) = h(Z^n) = h\left(\frac{\overline{\gamma}}{\gamma}\right) \leq \frac{1}{2}\log(\mathcal{N}(\gamma)) = \frac{n||\theta||}{2}\log(Y) + \frac{||\theta||}{2}\log(C),$$

donc $h(Z) \leq \frac{||\theta||}{2}\log(Y) + \frac{||\theta||}{2n}\log(C)$.

Soit

$$\Lambda = |\log(Z^n)| = \left|n\log(Z) - k\pi\sqrt{-1}\right|$$

pour un entier k tel que $|k| \leq n$. On a $\Lambda \neq 0$, car $j\theta \neq \theta$ par hypothèse. Si $\frac{2b^m\sqrt{D}}{\sqrt{C}} > X$, on obtient

$$n\log(3) \leq \log(5b^{2m}D),$$

et il n'y a plus rien à faire. On peut donc supposer $\frac{b^m\sqrt{D}}{X\sqrt{C}} \leq \frac{1}{2}$. On a alors

$$\Lambda = \left|\log\left(\left(\frac{1+\frac{b^m\sqrt{-CD}}{CX}}{1-\frac{b^m\sqrt{-CD}}{CX}}\right)^{\theta_+}\left(\frac{1-\frac{b^m\sqrt{-CD}}{CX}}{1+\frac{b^m\sqrt{-CD}}{CX}}\right)^{-\theta_-}\right)\right| \leq \frac{4||\theta||b^m\sqrt{D}}{X\sqrt{C}}.$$

Pour minorer Λ, on va appliquer le théorème 3 de [50]. On a

$$\log(\Lambda) \geq -8.87aH^2,$$

avec

$$a = 11\pi + \frac{||\theta||}{2}\log(Y) + \frac{||\theta||}{2n}\log(C).$$
$$H = H(e,f) = 7.38 + \log\left(\frac{n}{68.9} + \frac{n}{2m}\right).$$

On obtient

$$\log(X) - \log\left(\frac{4||\theta||b^m\sqrt{D}}{\sqrt{C}}\right) \leq 8.87(11\pi + \frac{||\theta||}{2}\log(Y) + \frac{||\theta||}{2n}\log(C))H^2.$$

Comme $\frac{b^m\sqrt{D}}{X\sqrt{C}} \leq \frac{1}{2}$, il vient

$$n\log\sqrt{Y} - \frac{1}{2}\log\left(\frac{5C}{4}\right) \leq \log(X),$$

d'où

$$n \leq \frac{c_0(11\pi + ||\theta||\log\sqrt{C})H^2 + \log\left(2||\theta||b^m\sqrt{5D}\right)}{\log(\sqrt{3})} + c_0||\theta||H^2. \tag{3.48}$$

On peut alors prendre $\theta = 2h(-CD)$. Soit χ le caractère de $\mathbb{K}$. Si $-CD \equiv 2, 3 \bmod 4$ (respectivement si $-CD \equiv 1 \bmod 4$), c'est un caractère primitif modulo $4CD$ (respectivement

modulo CD). On pose $t = 1$ si $CD \neq 3 \bmod 4$ et $t = 0$ sinon. Dans la suite, la notation $\sum'$ signifie que la variable décrit des éléments premier à $2^t CD$. Par la formule analytique du nombre de classes, on a

$$h(-CD) = \frac{1}{2 - \chi(2)} \sum_{0<x<2^{2t-1}CD}{}' \chi(x).$$

Comme le caractère χ est primitif modulo $4^t CD$ et que $4^t CD$ est libre de cube, l'application du théorème 7 de [35] donne alors

$$h(-CD) \leq \frac{1}{2^{1-t}\pi(2 - \chi(2))} (1 + o(1)) \sqrt{CD} \log(4^t CD).$$

Supposons maintenant HRG. On a alors, par le théorème 6 de [35]

$$h(-CD) \leq \frac{2^{t+2} e^{\gamma}}{\pi(2 - \chi(2))} (1 + o(1)) \sqrt{CD} \log\log(4^t CD).$$

Sous GS, on a

$$h(-CD) \leq \frac{2^{t+1} e^{\gamma}}{\pi(2 - \chi(2))} (1 + o(1)) \sqrt{CD} \log\log(4^t CD).$$

■

3.14.1 Un cas particulier.

Supposons maintenant que $D = q$ où q est un nombre premier tel que $q \equiv 3 \bmod 4$. Le caractère de $\mathbb{Q}(\sqrt{-q})$ est alors le symbole de Legendre car il trivialise les carrés. La formule du nombre de classes se met sous la forme $h = \frac{1}{2-\left(\frac{2}{q}\right)} \sum_{x=1}^{\frac{q-1}{2}} \left(\frac{x}{q}\right)$ et on pose dans ce cas $M = \frac{1}{2-\left(\frac{2}{q}\right)} \sum_{x=1}^{\frac{q-1}{2}} \left(\frac{x}{q}\right)$. La formule analytique du nombre de classes fait intervenir les fonctions L. Ici on va donner une deuxième démonstration arithmétique de l'inégalité, ie sans faire intervenir de résultats démontré de façon analytique.

En effet, dans le cas présent, l'extension $\mathbb{K}/\mathbb{Q}$ est une sous-extension quadratique de $\mathbb{L} = \mathbb{Q}(\zeta_q)$ où ζ_q est une racine primitive q-ième de l'unité. Les éléments de $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ sont notés σ_t avec $\sigma_t(\zeta) = \zeta^t$. Soit $\mathcal{I}_q$ son idéal de Stickelberger. Soit $H' = \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{K})$. La réduction de $\mathcal{I}_q$ modulo H', notée $\overline{\mathcal{I}_q}$ définit l'idéal de Stickelberger de $\mathbb{K}$. D'après [41], il annihile le groupe des classes de $\mathbb{K}$. Posons $\vartheta = \frac{1}{q} \sum_{t=1}^{q-1} t\sigma_t^{-1}$. Soit $\overline{\vartheta} \in \overline{\mathcal{I}_q}$ sa réduction modulo H'. Soit $\mathcal{C}(q)$ les résidus quadratiques modulo q. De même, on note $\mathcal{N}(q)$ les non résidus quadratiques modulo q. On pose $\theta = (1 - j)\overline{\vartheta} = (A - B)(1 - j)$, où $qA = \sum_{t \in \mathcal{C}} t$ et $qB = \sum_{t \in \mathcal{N}} t$. Soit $\chi = \left(\frac{\cdot}{q}\right)$ le symbole de Legendre. Comme

$$\left\{ \begin{array}{l} qA = \sum_{t\in\mathcal{C}} t = \frac{1}{2}\sum_{t=1}^{q-1}(1+\chi(t))\,t; \\ qB = \sum_{t\in\mathcal{N}} t = \frac{1}{2}\sum_{t=1}^{q-1}(1-\chi(t))\,t; \end{array} \right.$$

on a

$$A - B = \frac{1}{q}\sum_{t=1}^{q-1}\chi(t)t.$$

Si $j\theta = \theta$, alors $A = B$, donc $\sum_{t=1}^{q-1}\chi(t)t = 0$. On aurait donc $2qA = \frac{q(q-1)}{2}$, ie $2A = \frac{q-1}{2}$, et donc $q \equiv 1 \bmod 4$, en contradiction avec $q \equiv 3 \bmod 4$. Donc $A \neq B$ et $j\theta \neq \theta$. On peut donc appliquer (3.48) avec $||\theta|| = 2(A-B) = \frac{2}{q}\sum_{t=1}^{q-1}\chi(t)t$. On a le lemme suivant

Lemme 3.14.1 *Soit χ un caractère de Dirichlet modulo m d'ordre 2, avec m impair et tel que $\chi(-1) = -1$. On a alors*

$$-(2-\chi(2))\sum_{0<t<q}{}' t\chi(t) = m\sum_{0<t<\frac{q}{2}}{}' \chi(t).$$

Preuve

$$\begin{aligned} -\sum_{0<x<q}{}' x\chi(x) &= -\sum_{0<x<\frac{m}{2}}{}' x\chi(x) - \sum_{0<x<\frac{m}{2}}{}' (m-x)\chi(m-x) \\ &= -2\sum_{0<x<\frac{m}{2}}{}' x\chi(x) + m\sum_{0<x<\frac{m}{2}}{}' \chi(x) \end{aligned}$$

On a aussi

$$\begin{aligned} -\sum_{0<x<q}{}' x\chi(x) &= -\sum_{0<x<m,2|x}{}' x\chi(x) - \sum_{0<x<m,2|x}{}' (m-x)\chi(m-x) \\ &= -4\sum_{0<x<\frac{m}{2}}{}' x\chi(2x) + m\sum_{0<x<\frac{m}{2}}{}' \chi(2x) \\ &= \chi(2)\left(-4\sum_{0<x<\frac{m}{2}}{}' x\chi(x) + m\sum_{0<x<\frac{m}{2}}{}' \chi(x)\right) \end{aligned}$$

c'est à dire

$$-\chi(2)\sum_{0<x<q}{}' x\chi(x) = -4\sum_{0<x<\frac{m}{2}}{}' x\chi(x) + m\sum_{0<x<\frac{m}{2}}{}' \chi(x).$$

On en déduit

$$-(2-\chi(2))\sum_{0<x<q}{}' x\chi(x) = m\sum_{0<x<\frac{m}{2}}{}' \chi(x).$$

□

Remarque 3.14.2 *Ce lemme est également vrai si* $2|m$ *mais on n'en a pas besoin ici.*

Donc, si $D = q$ avec q premier et $q \equiv 3 \bmod 4$, on peut prendre $e = \mathcal{C}(q) - \mathcal{N}(q)$ et $f = -e$. On a alors par le lemme $||\theta|| = 2|e| = \frac{2}{2-\chi(2)} \sum_{t=1}^{\frac{q-1}{2}} \chi(t)$. On retrouve les bornes précédentes.
■

Chapitre 4

L'idéal de Stickelberger de $\mathbb{Q}(\zeta)$.

4.1 Quelques notations.

On se fixe p un nombre premier impair. On désigne par G le groupe de Galois de l'extension $\mathbb{Q}(\zeta)/\mathbb{Q}$. Si t est un entier premier à p, l'élément σ_t de G est défini par $\sigma_t(\zeta) = \zeta^t$. On préfèrera noter par j la conjugaison complexe σ_{-1}. Le caractère cyclotomique ω de G est défini par

$$\omega(\sigma_t) \equiv t \bmod p.$$

Comme il est d'usage, la norme $\sum_{t=1}^{p-1} \sigma_t$ relative à $\mathbb{Q}(\zeta)/\mathbb{Q}$ sera notée $\mathcal{N}$. On pose

$$\mathbb{Z}[G]^- = (1-j)\mathbb{Z}[G].$$

On vérifie que

$$\mathbb{Z}[G]^- = \{x \in \mathbb{Z}[G] : \quad (1+j)x = 0\}.$$

Definition 4.1.1 *Les éléments $\theta \in \mathbb{N}[G]$ sont les éléments dits positifs de $\mathbb{Z}[G]$.*

Si $\theta \in \mathbb{Z}[G]$ est en fait un élément de $\mathbb{N}[G]$, on écrit $\theta \geq 0$.

Definition 4.1.2 *Soit $\theta = \sum_{c=1}^{p-1} n_c \sigma_c \in \mathbb{Z}[G]$. On appelle poids de θ, que l'on note $W(\theta)$, l'entier défini par*

$$W(\theta) = \sum_{c=1}^{p-1} n_c.$$

L'application W ainsi définie vérifie les propriétés suivantes :

Proposition 4.1.3 *Soient $\theta_1, \theta_2 \in \mathbb{Z}[G]$. On a*

$$W(\theta_1 + \theta_2) = W(\theta_1) + W(\theta_2), \quad W(\theta_1\theta_2) = W(\theta_1)\, W(\theta_2),$$

Definition 4.1.4 *L'élément de Stickelberger de $\mathbb{Q}[G]$ est l'élément ϑ défini par*

$$\vartheta = \frac{1}{p} \sum_{\nu=1}^{p-1} \nu \sigma_\nu^{-1}.$$

On pose alors

Definition 4.1.5 *1. L'idéal de Stickelberger $\mathcal{I}_{st}$ est l'idéal de $\mathbb{Z}[G]$ défini par*

$$\mathcal{I}_{st} = \mathbb{Z}[G] \cap \vartheta \mathbb{Z}[G].$$

2. La partie négative de $\mathcal{I}_{st}$, notée $\mathcal{I}_{st}^-$, est définie par

$$\mathcal{I}_{st}^- = \mathcal{I}_{st} \cap \mathbb{Z}[G]^-,$$

autrement dit, $\mathcal{I}_{st}^- = \{x \in \mathcal{I}_{st} : (1+j)x = 0\}$.

3. La partie positive de $\mathcal{I}_{st}$, notée $\mathcal{I}_{st}^+$, est définie par

$$\mathcal{I}_{st}^+ = (1+j)\mathcal{I}_{st}.$$

Proposition-définition 4.1.6 *On a $\mathcal{I}_{st}^+ = \mathbb{Z}\mathcal{N}$. En particulier, si $\theta \in \mathcal{I}_{st}$, il existe un entier $\varsigma(\theta)$ tel que $(1+j)\theta = \varsigma(\theta)\mathcal{N}$. L'entier $\varsigma(\theta)$ est appelé poids relatif de θ. Il est lié au poids de θ par la relation*

$$W(\theta) = \varsigma(\theta)\frac{p-1}{2}. \tag{4.1}$$

Preuve Remarquons d'abord que $(1+j)\vartheta = \mathcal{N}$. En effet

$$jp\vartheta = \sum_{c=1}^{p-1} t\sigma_{p-t}^{-1} = \sum_{c=1}^{p-1} (p-t)\sigma_t^{-1} = p\mathcal{N} - p\vartheta.$$

Ainsi $\mathbb{Z}\mathcal{N} \subset \mathcal{I}_{st}^+$. Inversement, montrons que $\mathcal{I}_{st}^+ \subset \mathbb{Z}\mathcal{N}$. Il suffit de montrer que $\mathcal{I}_{st}^+ \subset \mathbb{Q}\mathcal{N}$, vu que $\mathbb{Z}\mathcal{N} = \mathbb{Q}\mathcal{N} \cap \mathbb{Z}[G]$. Pour $\theta \in \mathcal{I}_{st}^+$ on a $(1+j)\theta = 2\theta$, d'où

$$2\mathcal{I}_{st}^+ = (1+j)\mathcal{I}_{st}^+ \subset (1+j)\mathcal{I}_{st} \subset (1+j)\vartheta\mathbb{Z}[G] = \mathcal{N}\mathbb{Z}[G] = \mathbb{Z}\mathcal{N},$$

d'où $\mathcal{I}_{st}^+ \subset \mathbb{Q}\mathcal{N}$, comme voulu.

Soit maintenant $\theta \in \mathcal{I}_{st}$. Il existe un entier $\varsigma(\theta)$ tel que $(1+j)\theta = \varsigma(\theta)\mathcal{N}$. En passant aux poids

$$2W(\theta) = W((1+j)\theta) = W(\varsigma(\theta)\mathcal{N}) = \varsigma(\theta)(p-1),$$

d'où (4.1). ■

4.2 Généralités.

4.2.1 Eléments de Kummer.

Soit g une racine primitive modulo p. Si ν est un entier relatif, on désigne par g_ν l'unique entier compris entre 1 et $p-1$ tel que g^ν et g_ν soit dans la même classe modulo p. De plus, si x est un entier relatif, il existe un unique entier l positif, infèrieur à $p-1$, tel que x et g^l soit dans la même classe modulo p. On notera dans la suite un tel entier l, plutôt par $Ind(x)$. Si $\sigma = \sigma_g$, remarquons que $\sigma_{g_\nu} = \sigma^\nu$. Soit $1 \leq d \leq p-2$. On pose

$$I_d = \{\nu : \quad 1 \leq \nu \leq p-1, \quad g_{\pi-\nu} + g_{\pi-\nu+ind(d)} > p\}.$$

Definition 4.2.1 *Les annihilateurs K_d de Kummer sont les éléments de $\mathcal{R}$ de la forme*

$$K_d = \sum_{\nu \in I_d} \sigma^\nu.$$

Lemme 4.2.2

$$g_{\pi-\nu} + g_{\pi-\nu+ind(d)} \equiv g_{\pi-\nu+ind(d+1)} \bmod p.$$

Preuve En effet, par définition, on a

$$\begin{aligned} g_{\pi-\nu} + g_{\pi-\nu+ind(d)} &\equiv g^{\pi-\nu} + g^{\pi-\nu+ind(d)} \bmod p \\ &\equiv g^{\pi-\nu}(1+d) \bmod p \equiv g_{\pi-\nu+ind(d+1)} \bmod p. \end{aligned}$$

■

Soit 1_{I_d} la fonction caractéristique de I_d définie sur $\{1, \ldots, p-1\}$. Par le lemme précédant

$$g_{\pi-\nu} + g_{\pi-\nu+ind(d)} - g_{\pi-\nu+ind(d+1)} = p1_{I_d}(\nu).$$

Remarquons aussi que

$$g_{\pi-\nu} = p - g_{-\nu}.$$

Il vient alors

$$g_{-\nu} + g_{-\nu+ind(d)} - g_{-\nu+ind(d+1)} = p(1 - 1_{I_d}(\nu)). \tag{4.2}$$

Lemme 4.2.3 *Le poids de K_d, qui est aussi l'ordre de I_d, vaut $\frac{p-1}{2}$.*

Preuve On pose

$$A_- = \left\{1, \ldots, \frac{p-1}{2}\right\} - I_d, \quad A_+ = \left\{1, \ldots, \frac{p-1}{2}\right\} \cap I_d.$$

De même

$$B_- = \left\{\frac{p+1}{2}, \ldots, p-1\right\} - I_d, \quad B_+ = \left\{\frac{p+1}{2}, \ldots, p-1\right\} \cap I_d.$$

Soit $\nu \in A_-$. L'entier $\frac{p-1}{2} + \nu$ est alors un élément de B_+. En effet, en utilisant (4.2), on obtient

$$\begin{aligned} g_{\pi-(\pi+\nu)} + g_{\pi-(\pi+\nu)+Ind(d)} &= g_{-\nu} + g_{-\nu+Ind(d)} \\ &= p + g_{-\nu+ind(d+1)} > p, \end{aligned}$$

c'est à dire $\pi + \nu \in I_d$. Soit maintenant $\nu \in A_+$. Montrons que l'entier $\frac{p-1}{2} + \nu$ est alors un élément de B_-. En effet, par (4.2), on a

$$\begin{aligned} g_{\pi-(\pi+\nu)} + g_{\pi-(\pi+\nu)+Ind(d)} &= g_{-\nu} + g_{-\nu+Ind(d)} \\ &= g_{-\nu+ind(d+1)} < p. \end{aligned}$$

On a donc

$$A_+ \hookrightarrow B_-, \quad A_- \hookrightarrow B_+.$$

Mais $|A_+| + |A_-| = |B_+| + |B_-| = \frac{p-1}{2}$, d'où $|A_+| = |B_-|$ et $|A_-| = |B_+|$. Comme $|A_+| + |A_-| + |B_+| + |B_-| = p - 1$, il vient

$$|A_+| + |B_+| = \frac{p-1}{2},$$

ce qu'on voulait.□

Lemme 4.2.4 *On a $K_d = K_{2\pi-d}$.*

Preuve Soit $d' = 2\pi - d$. On a alors

$$d' = p - 1 - d \equiv g_\pi(d+1) \bmod p,$$

et

$$ind(d') \equiv \pi + ind(d+1) \bmod p - 1.$$

De même,

$$d' + 1 \equiv g_\pi \cdot g^{ind(d)} \bmod p,$$

et

$$ind(d' + 1) \equiv \pi + ind(d) \bmod p - 1.$$

Il vient alors

$$\begin{aligned} g_{-\nu+ind(d'+1)} - g_{-\nu+ind(d')} &= g_{-\nu+\pi+ind(d)} - g_{-\nu+\pi+ind(d+1)} \\ &= g_{-\nu+ind(d+1)} - g_{-\nu+ind(d)}. \end{aligned}$$

Ce qui précède et (4.2) donnent le résultat. ■

4.2.2 Génération de $\mathcal{I}_{st}$.

Definition 4.2.5 *Les éléments de Fueter de $\mathcal{R}$ sont définis par*

$$\phi_d = \sum_{\nu=1}^{p-1} \left(\left[\frac{(d+1)\nu}{p} \right] - \left[\frac{d\nu}{p} \right] \right) \sigma_\nu^{-1}.$$

On pose

$$\psi_d = \sum_{\nu=1}^{p-1} \left[\frac{(d+1)\nu}{p} \right] \sigma_\nu^{-1}.$$

Alors $\psi_1 = \phi_1$, et si $2 \leq d \leq p-2$,

$$\psi_d - \psi_{d-1} = \phi_d.$$

Ceci donne

$$\psi_d = \sum_{\nu=1}^{d} \phi_\nu. \tag{4.3}$$

Lemme 4.2.6 *Les éléments de Kummer et les éléments de Fueter vérifient l'identité*

$$\phi_d = \mathcal{N} - K_d, \quad 1 \leq d \leq p-2.$$

Preuve En effet, soit $1 \leq d \leq p-2$. On a

$$dg_{-\nu} - g_{-\nu+ind(d)} \equiv 0 \bmod p.$$

Il existe donc un entier positif r tel que

$$dg_{-\nu} = g_{-\nu+ind(d)} + rp,$$

soit

$$\frac{dg_{-\nu}}{p} = \frac{g_{-\nu+ind(d)}}{p} + r.$$

On a $\frac{g_{-\nu+ind(d)}}{p} \in [0;1[$. Donc $r = \left[\frac{dg_\nu}{p}\right]$. Soit $s = \left[\frac{(d+1)g_\nu}{p}\right]$. On a alors

$$(d+1)g_{-\nu} = g_{-\nu+ind(d+1)} + sp, \quad dg_{-\nu} = g_{-\nu+ind(d)} + rp.$$

On a donc :

$$p(s-r) = g_{-\nu} + g_{-\nu+ind(d)} - g_{-\nu+ind(d+1)}.$$

Ceci, avec (4.2) donnent

$$\left[\frac{(d+1)g_{-\nu}}{p}\right] - \left[\frac{dg_{-\nu}}{p}\right] = 1 - 1_{I_d}.$$

Par définition de ϕ_d et ce qui précède, il vient

$$\begin{aligned}
\phi_d &= \sum_{\nu=1}^{p-1} \left(\left[\frac{(d+1)(p-\nu)}{p}\right] - \left[\frac{d(p-\nu)}{p}\right] \right) \sigma_\nu \\
&= \sum_{\nu=1}^{p-1} \left(\left[\frac{(d+1)g_{-\nu}}{p}\right] - \left[\frac{dg_{-\nu}}{p}\right] \right) \sigma_\nu \\
&= \sum_{\nu=1}^{p-1} (1 - 1_{I_d}(\nu))\, \sigma_\nu \\
&= \mathcal{N} - K_d,
\end{aligned}$$

ce qu'on voulait. ■

Ce lemme, avec (4.2.4) montrent

Lemme 4.2.7

$$\phi_d = \phi_{2\pi-d}. \tag{4.4}$$

On en déduit

Proposition 4.2.8 *L'idéal $\mathcal{I}$ est engendré sur $\mathbb{Z}$ par la norme et les éléments de Fueter $\phi_1, \ldots, \phi_\pi$.*

Preuve Soit $\mathcal{L}$ le sous-groupe de $\mathcal{R}$, engendré sur $\mathbb{Z}$ par la norme et $\phi_1, \ldots, \phi_\pi$. Par le lemme précédent, $\mathcal{L}$ est aussi engendré par la norme $\mathcal{N}$ et $\phi_1, \ldots, \phi_{p-2}$. Les identités (4.3) et (4.2.6) montrent que $\mathcal{L}$ est engendré par la norme $\mathcal{N}$ et $\psi_1, \ldots, \psi_{p-2}$.

D'un autre côté, les éléments de $\mathcal{I}$, sont les éléments de $\mathcal{R}$ de la forme $x\vartheta$ où $x = \sum_{\nu=1}^{p-1} x_\nu \sigma_\nu \in \mathcal{R}$. Posons

$$x = \sum_{\nu=1}^{p-1} x_\nu(\sigma_\nu - \nu) + y, \quad y = \sum_{\nu=1}^{p-1} x_\nu \nu.$$

Soit ν un entier, $1 \leq \nu \leq p-2$. On a

$$(\nu - \sigma_\nu)\vartheta = \sum_{\mu=1}^{p-1} \left(\frac{\mu\nu}{p} - \frac{\mu\sigma_\nu}{p} \right) \sigma_\mu^{-1}.$$

Mais

$$\sum_{\mu=1}^{p-1} \left(\frac{\mu\nu}{p} - \left[\frac{\mu\nu}{p} \right] \right) \sigma_{\mu^{-1}} = \sum_{l=1}^{p-1} \left\{ \frac{l}{p} \right\} \sigma_{l\nu^{-1}}^{-1} = \sigma_\nu \sum_{l=1}^{p-1} \frac{l}{p} \sigma_l^{-1}.$$

On en déduit donc

$$(\nu - \sigma_\nu)\vartheta = \sum_{\mu=1}^{p-1} \left[\frac{\mu\nu}{p} \right] \sigma_\mu^{-1} = \psi_{\nu-1},$$

où $\psi_0 = 0$ par définition. Par définition de $\mathcal{I}$, on en déduit que $(\nu - \sigma_\nu)\vartheta = \psi_{\nu-1} \in \mathcal{I}$. Par conséquent, $x\vartheta \in \mathcal{I}$ si et seulement si $y\vartheta \in \mathcal{I}$. Comme y est un entier, $y\vartheta$ est un élément de $\mathcal{I}$ si et seulement si $p|y$. L'idéal $\mathcal{I}$ est donc engendré par $p\vartheta$ et ψ_d, $\quad 1 \leq d \leq p-2$. Par définition de ψ_{d-2}, on a

$$\psi_{d-2} = \sum_{\mu=1}^{p-1} \left[\frac{\mu(p-1)}{p} \right] \sigma_\mu^{-1} = \sum_{\mu=1}^{p-1} (\mu - 1)\, \sigma_\mu^{-1} \tag{4.5}$$

$$= \sum_{\mu=1}^{p-1} \mu\sigma_\mu^{-1} - \mathcal{N} = p\vartheta - \mathcal{N}. \tag{4.6}$$

$$\tag{4.7}$$

L'idéal $\mathcal{I}$ est donc engendré sur $\mathbb{Z}$ par la norme et la famille $\{\psi_1, \ldots, \psi_{d-2}\}$.On a donc bien $\mathcal{I} = \mathcal{L}$. ■

Remarque 4.2.9 *Au cours de la démonstration, on a montré que si n est un entier, $1 \leq n \leq p-2$, alors $\Theta_n = \sum_{c=1}^{p-1} \left[\frac{nc}{p} \right] \sigma_c^{-1} \in \mathcal{I}_{st}$. Les élments Θ_n, $1 \leq n \leq p-2$, sont les éléments Fuchsiens de $\mathcal{I}_{st}$.*

4.3 Irrégularité et l'idéal de Stickelberger.

4.3.1 Idempotents orthogonaux de $\mathbb{F}_p[G]$.

Soit $\tau : \mathbb{Z}[G] \twoheadrightarrow \mathbb{F}_p[G]$ la surjection canonique. On pose

$$\mathcal{A} = \mathbb{F}_p[G] = \tau(\mathbb{Z}[G]), \quad \mathcal{A}^- = (1-J)\mathcal{A}.$$

On vérifie que

$$\mathcal{A}^- = \{x \in \mathcal{A} : \quad (1+J)x = 0\}.$$

Proposition 4.3.1 *On a la relation suivante :*

$$\tau(\mathcal{I}^-) = \mathcal{A}^- \cap \tau(\mathcal{I}).$$

Preuve L'idéal de Stickelberger $\mathcal{I}$ est engendré par la norme $\mathcal{N}$ et les éléments $\phi_1, \ldots, \phi_\pi$. En particulier, cet idéal est aussi engendré par $\mathcal{N}, \phi_1, \phi_2 - \phi_1, \ldots, \phi_\pi - \phi_1$. Comme $\mathcal{N} = (1+J)\phi_1$ et que 2 est inversible modulo p, on en déduit que $\tau(\mathcal{I})$ est engendré par

$$\tau((1+J)\mathcal{N}), \tau((1-J)\mathcal{N}), \tau(\phi_2 - \phi_1), \ldots, \tau(\phi_\pi - \phi_1).$$

Parmi les générateurs précédents, tous sont des éléments de $\tau(\mathcal{I}^-)$, sauf $\tau(\mathcal{N})$. Donc, si x est un élément de $\tau(\mathcal{I})$, il existe un élément y de $\tau(\mathcal{I}^-)$ et $a \in \mathbb{F}_p$ tels que

$$x = a\tau(\mathcal{N}) + y.$$

Supposons que $x \in \mathcal{A}^-$. Alors, on a $(1+j)x = 0$. Mais $(1+j)x = 2a\tau(\mathcal{N})$. Donc $a = 0$ et $x \in \tau(\mathcal{N})^-$. On a donc montré l'inclusion

$$\mathcal{A}^- \cap \tau(\mathcal{I}) \subset \tau(\mathcal{I}^-).$$

Inversement, comme $\mathcal{I}^- = \mathbb{Z}[G]^- \cap \mathcal{I}$:

$$\tau(\mathcal{I}^-) \subset \tau(\mathbb{Z}[G]^-) \cap \tau(\mathcal{I}) = \mathcal{A}^- \cap \tau(\mathcal{I}).$$

■

Rappelons la définition suivante :

Definition 4.3.2 *La suite $(\boldsymbol{B}_n)_n$ des polynômes de Bernoulli est définie par :*

$$\begin{cases} \boldsymbol{B}_0(X) = 1, \\ \boldsymbol{B}'_{n+1}(X) = (n+1)\boldsymbol{B}_n(X), \\ \int_0^1 \boldsymbol{B}_n(X)dX = 0 \end{cases} \qquad si\ n \geq 1.$$

On appelle alors n-ième nombre de Bernoulli, que l'on note B_n, le nombre rationnel défini par $B_n = \mathbf{B}_n(0)$.

Lemme 4.3.3 *Soit m un entier pair tel que $2 \leq m \leq p-1$. Soit a un entier premier à p. On a alors*

$$a^m \sum_{j=1}^{p-1} \left[\frac{aj}{p}\right] j^{m-1} \equiv \frac{(a^{m+1} - a^m)B_m}{m} \bmod p.$$

Sur le $\mathbb{F}_p$-module $\mathbb{F}_p[G]$, on définit la forme bilinéaire symétrique non dégénérée suivante :

$$\left(\sum_{\sigma\in G} x_\sigma \sigma, \sum_{\sigma\in G} y_\sigma \sigma\right) = \sum_{\sigma\in G} x_\sigma y_{\sigma^{-1}}.$$

Dans la suite du chapitre, toute notion d'orthogonalité dans $\mathbb{F}_p[G]$ sera relative à celle-ci.

Proposition-définition 4.3.4 *Soit i un entier, $1 \leq i \leq p-1$. Notons ω le caracère cyclotomique de G, qui à $\sigma_t : \zeta \to \zeta^t$ associe $t \bmod p$ et posons*

$$\epsilon_i = -\sum_{\sigma\in G} \omega(\sigma)^i \sigma^{-1} \in \mathbb{F}_p[G].$$

Les éléments ϵ_i vérifient les propriétés

$$(\epsilon_i, \epsilon_j) = -\delta_{i,j}, \quad \epsilon_i\epsilon_j = \delta_{i,j}.$$

On les appelle idempotents orthogonaux de $\mathbb{F}_p[G]$, dont ils forment une $\mathbb{F}_p$-base.

Proposition 4.3.5 *L'élément ϵ_1 est un élément de $\tau(\mathcal{I}^-)$. De plus, si n est un entier impair tel que $3 \leq n \leq p-2$, les conditions suivantes sont équivalentes :*

1. *l'entier n est un élément de $\mathcal{B}$;*
2. *L'élément ϵ_n est orthogonal à l'idéal $\tau(\mathcal{I})$;*
3. *L'élément ϵ_n est orthogonal à l'idéal $\tau(\mathcal{I}^-)$;*

Preuve Comme $p\vartheta$ est un élément de $\mathcal{I}_{st}$ et que $\epsilon_1 = -\tau(p\vartheta)$, on en déduit que $\epsilon_1 \in \tau(\mathcal{I}_{st})$. De plus,

$$J\epsilon_\nu = (-1)^\nu \epsilon_\nu. \tag{4.8}$$

En effet :

$$\begin{aligned} J\epsilon_\nu &= \sum_{t=1}^{p-1} \omega(\sigma_t)^\nu \sigma_{-1}\sigma_t^{-1} = \sum_{t=1}^{p-1} \omega(\sigma_t)^\nu \sigma_{-t}^{-1} \\ &= \sum_{t=1}^{p-1} \omega(\sigma_{-t})^\nu \sigma_t^{-1} = \sum_{t=1}^{p-1} \omega(\sigma_{-1})^\nu \omega(\sigma_t)^\nu \sigma_t^{-1} \\ &= (-1)^\nu \sum_{t=1}^{p-1} \omega(\sigma_t)^\nu \sigma_t^{-1} = (-1)^\nu \epsilon_\nu. \end{aligned}$$

Si ν est un entier impair il vient, $(1+J)\epsilon_\nu = 0$, c'est à dire $\epsilon_\nu \in \mathcal{A}^-$. L'idempotent ϵ_1 est donc un élément de $\mathcal{A}^- \cap \tau(\mathcal{I}_{st})$, donc un élément de $\tau(\mathcal{I}^-)$ par la proposition (4.3.1).

Montrons maintenant les équivalences annoncées. Soit n un entier impair tel que $3 \leq n \leq p-2$. On vient de voir que $\epsilon_n \in \mathcal{A}^-$. De plus, ϵ_{p-1} est orthogonal à $\mathcal{A}^-$. En effet, par (4.8)

$$\mathcal{A}^- = \bigoplus_{2\nmid i} \mathbb{F}_p \epsilon_i.$$

d'où le résultat car $p-1$ est pair. La proposition (4.3.1) montre donc que ϵ_n est orthogonal à $\tau(\mathcal{I})$ si et seulement si ϵ_n est orthogonal à $\tau(\mathcal{I}^-)$, c'est à dire (2) $\Leftrightarrow$ (3). Lors de la preuve de la proposition (4.2.8), on a montré que $\mathcal{I}_{st}$ est engendré sur $\mathbb{Z}$ par la norme $\mathcal{N}$ et ψ_d, $1 \leq d \leq p-2$. En particulier, $\tau(\mathcal{I})$ est engendré sur $\mathbb{F}_p$ par $\tau(\mathcal{N})$ et $\tau(\psi_d)$, $1 \leq d \leq p-2$. Comme $(\epsilon_n, \tau(\mathcal{N})) = 0$, car $\tau(\mathcal{N}) = -\epsilon_{p-1}$, ϵ_n est orthogonal à $\tau(\mathcal{I})$ si et seulement si $(\epsilon_n, \tau(\psi_d)) = 0$, $1 \leq d \leq p-2$. Or, par le lemme (4.3.3) appliqué avec $m = p-n$, on obtient :

$$\begin{aligned} -(\epsilon_n, \psi_d) &= \sum_{j=1}^{p-1} \left[\frac{(d+1)j}{p}\right] j^{p-1-n} \\ &\equiv \frac{(d+1)^{p-1-n} - d - 1}{(d+1)^{p-n}} \frac{B_{p-n}}{p-n} \bmod p. \end{aligned}$$

Donc ϵ_n est orthogonal à ψ_d pour tout entier d tel que $1 \leq d \leq p-2$ si et seulement si $B_{p-n} \equiv 0 \bmod p$. Ainsi (1) $\Leftrightarrow$ (2). ■

4.3.2 Indice d'irrégularité.

Definition 4.3.6 *Soit* $P = \{1, \ldots, p-1\}$ *et*

$$\mathcal{B} = \{i \in P; p | B_{p-i}, \quad i \equiv 1 \bmod 2\}.$$

On appelle indice d'irrégularité du nombre premier p, que l'on note $\iota(p)$, l'entier défini par

$$\iota(p) = |\mathcal{B}|\,.$$

Théorème 4.3.7 *Soit p un nombre premier impair. L'indice d'irrégularité de p vérifie*

$$i(p) = dim_{\mathbb{F}_p}(\tau(\mathcal{R}^-)/\tau(\mathcal{I}^-)).$$

Preuve La dimension sur $\mathbb{F}_p$ de $\tau(\mathcal{R}^-)/\tau(\mathcal{I}^-)$ est celle de l'orthogonal de $\tau(\mathcal{I}^-)$. Or $\epsilon_1 \in \tau(\mathcal{I}^-)$ par la proposition (4.3.5). Par cette même proposition, pour n entier, $3 \leq n \leq p-2$, ϵ_n est dans l'orthogonal de $\tau(\mathcal{I}^-)$ si et seulement si $B_{p-n} \equiv 0 \bmod p$, d'où le résultat par définition de $\iota(p)$. ■

Corollaire 4.3.8 *On a $p^{\iota(p)}|h_p^-$. En particulier, le p-rang r_p du groupe des classes relatives du p-ième corps cyclotomique vérifie $\iota(p) \leq r_p$.*

Preuve Le p-rang du quotient $\mathcal{R}^-/\mathcal{I}^-$ est la dimension sur $\mathbb{F}_p$ de $\left(\mathcal{R}^-/\mathcal{I}^-\right)/p\left(\mathcal{R}^-/\mathcal{I}^-\right)$. Or

$$\begin{aligned}\left(\mathcal{R}^-/\mathcal{I}^-\right)/p\left(\mathcal{R}^-/\mathcal{I}^-\right) &\simeq \mathcal{R}^-/\left(p\mathcal{R}^- + \mathcal{I}^-\right)\\ &\simeq \left(\mathcal{R}^-/p\mathcal{R}^-\right)/\left(\left(p\mathcal{R}^- + \mathcal{I}^-\right)/p\mathcal{R}^-\right)\\ &\simeq \tau\left(\mathcal{R}^-\right)/\tau\left(\mathcal{I}^-\right).\end{aligned}$$

Par le théorème précédent, la dimension sur $\mathbb{F}_p$ du quotient précédent est $iota(p)$. Donc, le p-rang de $\mathcal{R}^-/\mathcal{I}^-$ est $\iota(p)$. Or ce quotient a pour ordre h_p^- (résultat d'Iwasawa, [77]). On en déduit donc bien que $p^{\iota(p)}|h_p^-$. ■

Corollaire 4.3.9 *Soit p premier impair. Alors $\iota(p) \leq \frac{p+1}{4}$.*

Preuve Si $p = 3$, $\iota(p) = 0$ et il n'y a rien à faire. Supposons $p \geq 5$. Par le corollaire précédent, il suffit de montrer que $h_p^- \leq p^{\frac{p+1}{4}}$. C'est une conséquence par exemple des majorations de Keqin Feng données dans [33]. Dans le cas où $p \equiv 3 \bmod 4$, donnons en une nouvelle preuve : on montrera au chapitre 6, l'inégalité

$$h_p^- \leq 6h(-p)\sqrt{p}\left(\frac{p-1}{24}\right)^{\frac{p-1}{4}},$$

$h(-p)$ étant le nombre de classes de $\mathbb{Q}(\sqrt{-p})$; l'entier $h(-p)$ étant majoré par $\frac{1}{\pi}\sqrt{p}\log(p)$ (voir [32]), il vient alors

$$h_p^- \leq \frac{6}{\pi}p\log(p)\left(\frac{p-1}{24}\right)^{\frac{p-1}{4}} \leq p^{\frac{p+1}{4}},$$

si $p \geq 5$, ce qu'on voulait. ■

4.4 Entiers de Jacobi, relation d'Iwasawa.

Dans la suite, on se fixe un nombre entier $m > 2$. Soit I le groupe multiplicatif des idéaux de $\mathbb{Q}(\zeta_m)$ qui sont premiers à m. Soit $\mathfrak{p}$ un premier de I. On note $\chi_{\mathfrak{p}} = \left(\frac{\cdot}{\mathfrak{p}}\right)_m$ le symbole de la m-ième puissance résiduelle dans le corps $\mathbb{Q}(\zeta_m)$. Soit $a = (a_1, \ldots, a_r) \in \mathbb{Z}^r$ de sorte que $\sum_{i=1}^r a_i \neq 0 \bmod m$. On pose alors

$$J_a(\mathfrak{p}) = (-1)^{r+1} \sum_{x_i} \prod_{i=1}^{r} \chi_{\mathfrak{p}}(x_i)^{a_i},$$

où $x_1, \ldots, x_r$ parcourent un système de représentants de l'anneau $\mathbb{Z}[\zeta_m]$ pris modulo $\mathfrak{p}$, tels que $x_1 + \ldots + x_r \equiv -1 \bmod \mathfrak{p}$, $x_i \neq 0 \bmod \mathfrak{p}$. Dans la suite, on notera pour simplifier par $s(a) = a_1 + \ldots a_r$ la somme des composantes de a.

Remarque 4.4.1 *Si $a_r = 0$, alors*

$$J_a(\mathfrak{p}) = J_{(a_1,\ldots,a_{r-1})}(\mathfrak{p}).$$

En effet, on a

$$(-1)^{r+1} J_a(\mathfrak{p}) = \sum_{x_1+\ldots+x_r \equiv -1 \bmod \mathfrak{p}} \prod_{i=1}^{r-1} \chi_{\mathfrak{p}}(x_i)^{a_i} = \sum_{x_r \neq 0,-1} \sum_{\frac{x_1}{1+x_r}+\ldots+\frac{x_{r-1}}{1+x_r} \equiv -1 \bmod \mathfrak{p}} \prod_{i=1}^{r-1} \chi_{\mathfrak{p}}(x_i)^{a_i}$$
$$+ \sum_{x_1+\ldots+x_{r-1} \equiv 0 \bmod \mathfrak{p}} \prod_{i=1}^{r-1} \chi_{\mathfrak{p}}(x_i)^{a_i}.$$

Or

$$\sum_{x_1+\ldots+x_{r-1} \equiv 0 \bmod \mathfrak{p}} \prod_{i=1}^{r-1} \chi_{\mathfrak{p}}(x_i)^{a_i} = \sum_{x_{r-1} \neq 0} \sum_{\frac{x_1}{x_{r-1}}+\ldots+\frac{x_{r-2}}{x_{r-1}} \equiv -1 \bmod \mathfrak{p}} \prod_{i=1}^{r-1} \chi_{\mathfrak{p}}(x_i)^{a_i}$$
$$= \sum_{x_{r-1} \neq 0} \sum_{y_1+\ldots+y_{r-2} \equiv -1 \bmod \mathfrak{p}} \chi_{\mathfrak{p}}(x_{r-1})^{s(a)} \prod_{i=1}^{r-2} \chi_{\mathfrak{p}}(y_i)^{a_i}$$
$$= \left(\sum_{x_{r-1} \neq 0} \chi_{\mathfrak{p}}(x_{r-1})^{s(a)} \right) \left(\sum_{y_1+\ldots+y_{r-2} \equiv -1 \bmod \mathfrak{p}} \prod_{i=1}^{r-1} \chi_{\mathfrak{p}}(y_i)^{a_i} \right).$$

Comme $s(a) \neq 0 \bmod m$, $\chi_{\mathfrak{p}}^{s(a)}$ *est non trivial, d'où* $\sum_{x_{r-1}\neq 0} \chi_{\mathfrak{p}}(x_{r-1})^{s(a)} = 0$. *De plus*

$$\sum_{x_r\neq 0,-1} \sum_{\frac{x_1}{1+x_r}+\ldots+\frac{x_{r-1}}{1+x_r}\equiv -1 \bmod \mathfrak{p}} \prod_{i=1}^{r-1} \chi_{\mathfrak{p}}(x_i)^{a_i} = \sum_{x_r\neq 0,-1} \chi_{\mathfrak{p}}(1+x_r)^{s(a)} \sum_{\frac{x_1}{1+x_r}+\ldots+\frac{x_{r-1}}{1+x_r}\equiv -1 \bmod \mathfrak{p}} \prod_{i=1}^{r-1} \chi_{\mathfrak{p}}\left(\frac{x_i}{1+x_r}\right)^{a_i}$$
$$= \left(\sum_{x_r\neq 0,-1} \chi_{\mathfrak{p}}(1+x_r)^{s(a)}\right) \left(\sum_{y_1+\ldots+y_{r-1}\equiv -1 \bmod \mathfrak{p}} \prod_{i=1}^{r-1} \chi_{\mathfrak{p}}(y_i)^{a_i}\right)$$

Comme $s(a) \neq 0 \bmod m$, *on a* $\sum_{x_r\neq 0,-1} \chi_{\mathfrak{p}}(1+x_r)^{s(a)} = \sum_{x_r\neq -1} \chi_{\mathfrak{p}}(1+x_r)^{s(a)} - \chi_{\mathfrak{p}}(1) = -1$, *d'où*

$$\sum_{x_r\neq 0,-1} \sum_{\frac{x_1}{1+x_r}+\ldots+\frac{x_{r-1}}{1+x_r}\equiv -1 \bmod \mathfrak{p}} \prod_{i=1}^{r-1} \chi_{\mathfrak{p}}(x_i)^{a_i} = - \sum_{y_1+\ldots+y_{r-1}\equiv -1 \bmod \mathfrak{p}} \prod_{i=1}^{r-1} \chi_{\mathfrak{p}}(y_i)^{a_i}.$$

On obtient finalement

$$(-1)^{r+1} J_a(\mathfrak{p}) = - \sum_{y_1+\ldots+y_{r-1}\equiv -1 \bmod \mathfrak{p}} \prod_{i=1}^{r-1} \chi_{\mathfrak{p}}(y_i)^{a_i},$$

c'est à dire $J_a(\mathfrak{p}) = (-1)^{r-1} \sum_{y_1+\ldots+y_{r-1}\equiv -1 \bmod \mathfrak{p}} \prod_{i=1}^{r-1} \chi_{\mathfrak{p}}(y_i)^{a_i} = J_{(a_1,\ldots,a_{r-1})}(\mathfrak{p})$, *ce qu'on voulait. Par exemple, si* $m > 2$, *alors* $J_{(2,0)}(\mathfrak{p}) = J_2(\mathfrak{p}) = \chi_{\mathfrak{p}}(-1)^2 = 1$.

Par multiplicativité, on définit une application $J_a : I \to \mathbb{Q}(\zeta_m)^\times$.

Definition 4.4.2 *Soit* $G = \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. *Le groupe* G *agit sur* I *et* $\mathbb{Q}(\zeta_m)^\times$. *Cela munit* J_a *d'une structure de* G*-module. On note* $\boldsymbol{J}$ *le sous-groupe de* $Hom_G(I, \mathbb{Q}(\zeta_m)^\times)$ *engendré par les* J_a.

Le sous-groupe de $\mathbb{Q}(\zeta_m)^\times$ *engendré par les images des* J_a, *avec* a r*-uplet comme avant,* r *décrivant* $\mathbb{N}^*$, *définit l'ensemble des fractions de Jacobi de* $\mathbb{Q}(\zeta_m)$. *Si on se restreint aux images des idéaux entiers premiers à* m, *cela définit les entiers de Jacobi de l'anneau* $\mathbb{Z}[\zeta_m]$.

Dans la suite, on montre le théorème suivant du à Kenkichi Iwasawa :

Théorème 4.4.3 *Si* $m = p$, p *nombre premier impair, et si* $\mathfrak{p}$ *est l'unique premier de* $\mathbb{Q}(\zeta_p)$ *au-dessus de* p, *alors pour tout entier de Jacobi* β, *on a la relation*

$$\beta \equiv 1 \bmod \mathfrak{p}^2. \tag{4.9}$$

Remarque 4.4.4 Iwasawa montre même dans [39] que $\beta \equiv 1 \bmod \mathfrak{p}^3$ si $p > 3$, mais le résultat précédent nous suffit.

4.4.1 Relations de Weil.

Pour chaque premier $\mathfrak{p}$ de I, on se fixe un caractère $\psi_{\mathfrak{p}}$ additif sur le corps fini $\frac{\mathbb{Z}[\zeta_m]}{\mathfrak{p}}$. On pose

$$g_a(\mathfrak{p}) = \sum_{x \neq 0[\mathfrak{p}]} \chi_{\mathfrak{p}}(x)\psi_{\mathfrak{p}}(x),$$

ainsi que $\tau_a(\mathfrak{p}) = -g_a(\mathfrak{p})$. On note $\mathcal{J}_a(\mathfrak{p})$ la somme de Jacobi associée aux caractères $\chi_{\mathfrak{p}}^{a_1}, \ldots, \chi_{\mathfrak{p}}^{a_t}$, ie

$$\mathcal{J}_a(\mathfrak{p}) = \sum_{x_i} \prod_{i=1}^{r} \chi_{\mathfrak{p}}(x_i)^{a_i}$$

où $x_1, \ldots, x_r$ parcourent les représentants de l'anneau des entiers de $\mathbb{Q}(\zeta_m)$ pris modulo $\mathfrak{p}$ tels que $x_1 + \ldots + x_r \equiv 1 \bmod \mathfrak{p}$, $x_i \neq 0 \bmod \mathfrak{p}$. Rappelons que la somme de Jacobi précédente, et les sommes de Gauss $g_{a_i}(\mathfrak{p}), i = 1, \ldots, r$ pour $a = (a_1, \ldots, a_r)$ sont liées par la proposition suivante :

Proposition 4.4.5 *Si $s(a) \neq 0 \bmod m$, on a*

$$\mathcal{J}_a(\mathfrak{p}) = \frac{g_{a_1}(\mathfrak{p}) \ldots g_{a_r}(\mathfrak{p})}{g_{a_1+\ldots+a_r}(\mathfrak{p})}. \tag{4.10}$$

Preuve Calculons le produit $g_{a_1}(\mathfrak{p}) \ldots g_{a_r}(\mathfrak{p})$. On a

$$\begin{aligned} g_{a_1}(\mathfrak{p}) \ldots g_{a_r}(\mathfrak{p}) &= \sum_{x_i \neq 0 \bmod \mathfrak{p}} \psi_{\mathfrak{p}}(x_1 + \ldots x_r) \prod_{i=1}^{r} \chi_{\mathfrak{p}}(x_i)^{a_i} \\ &= \sum_{a \neq 0 \bmod \mathfrak{p}} \sum_{x_1+\ldots+x_r = a \bmod \mathfrak{p}} \psi_{\mathfrak{p}}(x_1 + \ldots x_r) \prod_{i=1}^{r} \chi_{\mathfrak{p}}(x_i)^{a_i} \\ &+ \sum_{x_1+\ldots+x_r \equiv 0 \bmod \mathfrak{p}} \prod_{i=1}^{r} \chi_{\mathfrak{p}}(x_i)^{a_i}. \end{aligned}$$

Comme $s(a) \neq 0 \bmod m$, la démonstration de la remarque (4.4.1) montre en particulier que $\sum_{x_1+\ldots+x_r\equiv 0 \bmod \mathfrak{p}} \prod_{i=1}^r \chi_{\mathfrak{p}}(x_i)^{a_i} = 0$. On obtient

$$\begin{aligned} g_{a_1}(\mathfrak{p}) \ldots g_{a_r}(\mathfrak{p}) &= \sum_{a\neq 0 \bmod \mathfrak{p}} \sum_{\frac{x_1}{a}+\ldots+\frac{x_r}{a}\equiv 1 \bmod \mathfrak{p}} \psi_{\mathfrak{p}}(a)\chi_{\mathfrak{p}}(a)^{s(a)} \prod_{i=1}^r \chi_{\mathfrak{p}}\left(\frac{x_i}{a}\right)^{a_i} \\ &= \left(\sum_{a\neq 0 \bmod \mathfrak{p}} \psi_{\mathfrak{p}}(a)\chi_{\mathfrak{p}}(a)^{s(a)}\right)\left(\sum_{\frac{x_1}{a}+\ldots+\frac{x_r}{a}\equiv 1 \bmod \mathfrak{p}} \prod_{i=1}^r \chi_{\mathfrak{p}}\left(\frac{x_i}{a}\right)^{a_i}\right) \\ &= g_{s(a)}(\mathfrak{p})\mathcal{J}_a(\mathfrak{p}), \end{aligned}$$

ce qui était à démontrer. ■

On peut reformuler cette proposition comme suit, en notant $\mathcal{N}(\mathfrak{p})$ la norme du premier $\mathfrak{p}$, norme relative à $\mathbb{Q}(\zeta_m)/\mathbb{Q}$:

Proposition 4.4.6 *Soit $a \in \mathbb{Z}^r$ tel que $s(a) \neq 0 \bmod m$. On a*

$$\mathcal{J}_a(\mathfrak{p}) = \chi_{\mathfrak{p}}(-1)^{s(a)} \frac{g_{a_1}(\mathfrak{p}) \ldots g_{a_r}(\mathfrak{p}) g_{-s(a)}(\mathfrak{p})}{\mathcal{N}(\mathfrak{p})} \tag{4.11}$$

Preuve En effet, on dispose de

$$\overline{g_{s(a)}(\mathfrak{p})} = \sum_{x\neq 0 \bmod \mathfrak{p}} \chi_{\mathfrak{p}}(x)^{-s(a)}\psi_{\mathfrak{p}}(-x) = \chi_{\mathfrak{p}}(-1)^{s(a)} g_{-s(a)},$$

et de la relation classique $g_{s(a)}(\mathfrak{p})\overline{g_{s(a)}(\mathfrak{p})} = \mathcal{N}(\mathfrak{p})$. La proposition découle de la précédente. ■

On en déduit les relations de Weil suivantes :

Proposition 4.4.7 *Soit $\mathfrak{p}$ un premier de I, $r \geq 3$ un entier, $a = (a_1, \ldots a_r) \in \mathbb{Z}^r$ tel que $s(a) \neq 0 \bmod m$. On a*

1. $J_a(\mathfrak{p}) = \frac{\tau_{a_1}(\mathfrak{p})\ldots\tau_{a_r}(\mathfrak{p})\tau_{-s(a)}(\mathfrak{p})}{\mathcal{N}(\mathfrak{p})}$.
2. *Si $a_1 + a_2 \equiv 0 \bmod m$, alors*

$$J_a(\mathfrak{p}) = J_{a_2}(\mathfrak{p})J_{a_3,\ldots,a_r}(\mathfrak{p})\mathcal{N}(\mathfrak{p}).$$

3. *Si $a_1 + a_2 \neq 0 \bmod m$, alors*

$$J_a(\mathfrak{p}) = J_{a_1+a_2}(\mathfrak{p})J_{a_1,a_2}(\mathfrak{p})J_{a_1+a_2,a_3\ldots,a_r}(\mathfrak{p}).$$

Preuve Commençons par montrer l'assertion (1). Par définition de $J_a(\mathfrak{p})$ et la proposition précédente, on a

$$\begin{aligned} J_a(\mathfrak{p}) &= (-1)^{r+1}\chi_{\mathfrak{p}}(-1)^{s(a)}\mathcal{J}_a(\mathfrak{p}) \\ &= (-1)^{r+1}\chi_{\mathfrak{p}}(-1)^{2s(a)}\frac{g_{a_1}(\mathfrak{p})\dots g_{a_r}(\mathfrak{p})g_{-s(a)}(\mathfrak{p})}{\mathcal{N}(\mathfrak{p})} \\ &= (-1)^{r+1}\frac{g_{a_1}(\mathfrak{p})\dots g_{a_r}(\mathfrak{p})g_{-s(a)}(\mathfrak{p})}{\mathcal{N}(\mathfrak{p})} \\ &= \frac{\tau_{a_1}(\mathfrak{p})\dots\tau_{a_r}(\mathfrak{p})\tau_{-s(a)}(\mathfrak{p})}{\mathcal{N}(\mathfrak{p})}. \end{aligned}$$

Prouvons l'assertion (2). On pose $s'(a) = a_3 + \ldots + a_r$. On a par (1)

$$\begin{aligned} J_a(\mathfrak{p}) &= \frac{\tau_{a_1}(\mathfrak{p})\dots\tau_{a_r}(\mathfrak{p})\tau_{-s(a)}(\mathfrak{p})}{\mathcal{N}(\mathfrak{p})} \\ &= \frac{\tau_{-a_2}(\mathfrak{p})\tau_{a_2}(\mathfrak{p})\tau_{a_3}(\mathfrak{p})\dots\tau_{a_r}(\mathfrak{p})\tau_{-s'(a)}(\mathfrak{p})}{\mathcal{N}(\mathfrak{p})} \\ &= \chi_{\mathfrak{p}}(-1)^{a_2}\frac{|\tau_{a_2}(\mathfrak{p})|^2\,\tau_{a_3}(\mathfrak{p})\dots\tau_{a_r}(\mathfrak{p})\tau_{-s'(a)}(\mathfrak{p})}{\mathcal{N}(\mathfrak{p})} \\ &= J_{a_2}(\mathfrak{p})J_{a_3,\dots a_r}(\mathfrak{p})\mathcal{N}(\mathfrak{p}). \end{aligned} \tag{4.12}$$

Prouvons l'assertion (3). On a par l'assertion (1) :

$$\begin{aligned} J_{a_1+a_2}(\mathfrak{p})J_{a_1,a_2}(\mathfrak{p})J_{a_1+a_2,a_3,\dots,a_r}(\mathfrak{p}) &= \chi_{\mathfrak{p}}(-1)^{a_1+a_2}\frac{\tau_{a_1}(\mathfrak{p})\tau_{a_2}(\mathfrak{p})\tau_{-a_1-a_2}(\mathfrak{p})}{\mathcal{N}(\mathfrak{p})}\frac{\tau_{a_1+a_2}(\mathfrak{p})\tau_{a_3}(\mathfrak{p})\dots\tau_{a_r}(\mathfrak{p})\tau_{-s(a)}(\mathfrak{p})}{\mathcal{N}(\mathfrak{p})} \\ &= \frac{\chi_{\mathfrak{p}}(-1)^{a_1+a_2}\tau_{-a_1-a_2}(\mathfrak{p})\tau_{a_1+a_2}(\mathfrak{p})}{\mathcal{N}(\mathfrak{p})}J_a(\mathfrak{p}) \\ &= J_a(\mathfrak{p}). \end{aligned} \tag{4.13}$$

■

Remarque 4.4.8 *L'assertion (1) montre en particulier que J_a est invariant par permutation des composantes de a.*

4.4.2 Quelques lemmes.

Lemme 4.4.9 *Soit $m > 2$ un entier. Le groupe $\boldsymbol{J}$ est engendré par les $J_{(u,v)}$.*

Preuve Par la proposition (4.4.7), on a pour $\mathfrak{a} \in I$:

$$J_{(1,-1,1)}(\mathfrak{a}) = J_{-1}(\mathfrak{a})J_1(\mathfrak{a})\mathcal{N}(\mathfrak{a}).$$

En particulier, $\mathcal{N} \in \mathbf{J}$. Soit $\mathbf{J}'$ le sous-groupe de $\mathbf{J}$ engendré par les $J_{(u,v)}$, $(u+v) \neq 0 \bmod m, (u,v) \neq (0,0)$. On a pour $u \neq 0 \bmod m$, $J_u = J_{u,0} \in \mathbf{J}'$. De plus, via les relations de Weil, on vérifie par récurrence sur $r \geq 3$, que tout J_a pour a ayant r composantes, est dans le groupe engendré, par $\mathbf{J}'$ et $\mathcal{N}$. Par la remarque (4.4.8), on a

$$J_{(1,1,-1)} = J_{(1,-1,1)},$$

de sorte que par les relations de Weil

$$J_2 J_{(1,1)} J_{(2,-1)} = J_{-1} J_1 \mathcal{N},$$

ie $\mathcal{N} \in \mathbf{J}'$, donc $\mathbf{J} = \mathbf{J}'$.□

Lemme 4.4.10 *Soit $m > 2$. Alors $\boldsymbol{J}$ est engendré par part $\tau_{-r}\tau_1^r, 1 \leq r \leq m$.*

Preuve Si $r \in \mathbb{N}^*$, on note $r \times 1$ le r-uplet $(1, \ldots, 1)$. Par la proposition (4.4.7), on a

$$J_{r\times 1} = \tau_{-r}\tau_1^r \mathcal{N}^{-1},$$

de sorte que $\tau_{-r}\tau_1^r \in \mathbf{J}$. Soit $\mathbf{J}''$ le sous-groupe de $\mathbf{J}$ engendré par les $\tau_{-r}\tau_1^r, 1 \leq r \leq m$. Comme $\tau_{-m} = 1$, $\tau_1^m \in \mathbf{J}''$. On en déduit que pour tout entier r, $\tau_{-r}\tau_1^r \in \mathbf{J}''$. Soit $(u,v) \neq (0,0)$ tel que $u + v \neq 0[m]$. Comme

$$\begin{aligned} J_{(u,v)} &= \mathcal{N}^{-1}\tau_{-u-v}\tau_u\tau_v \\ &= \mathcal{N}^{-1}\left(\tau_{-u-v}\tau_1^{u+v}\right)\left(\tau_u\tau_1^{-u}\right)\left(\tau_v\tau_1^{-v}\right), \end{aligned} \tag{4.14}$$

on déduit du lemme (4.4.9), que $\mathbf{J}$ est engendré par $\mathcal{N}$ et par $\mathbf{J}''$. Comme $m > 2$, on a $(2,0) \neq (0,0) \bmod m$. Le calcul précédent montre en particulier que $J_{(2,0)} \equiv \mathcal{N}^{-1} \bmod \mathbf{J}''$. Mais si $\mathfrak{p}$ est un premier de I, on a

$$J_{(2,0)}(\mathfrak{p}) = J_2(\mathfrak{p}) = \chi_{\mathfrak{p}}(-1)^2 = 1,$$

ie $J_{(2,0)} = 1$, et donc $\mathcal{N} \in \mathbf{J}''$.□

4.4.3 Preuve du théorème d'Iwasawa

Supposons que $m = l$, l nombre premier impair. Soit ζ_l une racine primitive l-ième de l'unité. Le nombre premier l est totalement ramifié dans l'extension $\mathbb{Q}(\zeta_l)/\mathbb{Q}$. On note $\mathfrak{l}$ l'unique premier de $\mathbb{Z}[\zeta_l]$ au-dessus de l. Il est principal, engendré par $1-\zeta_l$. Soit $\mathfrak{p}$ un premier de I (en particulier $\mathfrak{l} \neq \mathfrak{p}$). Soit p le nombre premier en-dessous de $\mathfrak{p}$. Soit ζ_{p^f} une racine primitive p^f-ième de l'unité, f étant l'inertie de $\mathfrak{p}$ sur $\mathbb{Q}$. Les sommes de Gauss $\tau_u(\mathfrak{p})$ appartiennent à $\mathbb{Q}(\zeta_l, \zeta_{p^f})$. On pose $\tau := \tau_1$. Les éléments de $\mathrm{Gal}(\mathbb{Q}(\zeta_l)/\mathbb{Q})$ seront notés σ_t, σ_t étant défini par $\sigma_t(\zeta_l) = \zeta_l^t$, $(t,l) = 1$. On note encore de cette façon les éléments de $\mathrm{Gal}\big(\mathbb{Q}(\zeta_l, \zeta_{p^f})/\mathbb{Q}(\zeta_{p^f})\big)$. En particulier

$$\psi_{\mathfrak{p}}(x)^{\sigma_t} = \psi_{\mathfrak{p}}(x), \quad \tau^{t+\sigma_{-t}} = \tau_{-t}\tau^t.$$

De plus, $\tau_{-l}\tau^l = \tau^l = \tau^{l+1-\sigma_{l+1}}$. Par le lemme (4.4.10), le groupe $\mathbf{J}$ étant engendré par les homomorphismes $\tau_{-r}\tau^r$, $1 \leq r \leq l$, pour montrer la relation d'Iwasawa, il suffit de montrer les congruences

$$\tau^{t+\sigma_{-t}}(\mathfrak{p}) \equiv 1 \bmod \mathfrak{l}^2, \quad \tau^{l+1-\sigma_{l+1}}(\mathfrak{p}) \equiv 1 \bmod \mathfrak{l}^2,$$

où t est un entier premier à l. Montrons d'abord la première congruence. Soit $\mathcal{L}$ un premier de $\mathbb{Q}(\zeta_l, \zeta_{p^f})$ au-dessus de $\mathfrak{l}$. Comme $\mathfrak{l}$ est principal engendré par $\zeta_l - 1$, il vient pour a entier

$$\zeta_l^a = (1 + \zeta_l - 1)^a \equiv 1 + a(\zeta_l - 1) \bmod \mathcal{L}^2.$$

Comme $\chi_{\mathfrak{p}}(x)$ est une racine l-ième de l'unité pour tout élément $x \in \mathbb{Z}[\zeta_l]$ premier à l, il existe donc un entier a_x tel que $\chi_{\mathfrak{p}}(x) = \zeta_l^{a_x}$. En particulier

$$\frac{\chi_{\mathfrak{p}}(x) - 1}{\zeta_l - 1} \equiv a_x \bmod \mathcal{L}^2.$$

Il vient alors

$$\begin{aligned}
\tau(\mathfrak{p}) &= -\sum_{x \neq 0 \bmod \mathfrak{p}} \chi_{\mathfrak{p}}(x)\psi_{\mathfrak{p}}(x) \\
&= -\sum_{x \neq 0 \bmod \mathfrak{p}} \psi_{\mathfrak{p}}(x) - \sum_{x \neq 0 \bmod \mathfrak{p}} (\chi_{\mathfrak{p}}(x) - 1)\psi_{\mathfrak{p}}(x) \\
&= 1 - (\zeta_l - 1) \sum_{x \neq 0 \bmod \mathfrak{p}} \psi_{\mathfrak{p}}(x) \frac{\chi_{\mathfrak{p}}(x) - 1}{\zeta_l - 1} \\
&\equiv 1 - (\zeta_l - 1) \sum_{x \neq 0 \bmod \mathfrak{p}} a_x \psi_{\mathfrak{p}}(x) \bmod \mathcal{L}^2 \\
&\equiv 1 + (\zeta_l - 1)y \bmod \mathcal{L}^2
\end{aligned}$$

avec $y \in \mathbb{Q}(\zeta_{p^f})$. Comme le premier de $\mathbb{Q}(\zeta_{p^f})$ en dessous de $\mathcal{L}$ se ramifie totalement dans $\mathbb{Q}(\zeta_l, \zeta_{p^f})/\mathbb{Q}(\zeta_{p^f})$, on en déduit pour t entier premier à l :

$$\tau(\mathfrak{p})^{\sigma_{-t}} \equiv 1 + (\zeta_l^{-t} - 1)y \equiv 1 - t(\zeta_l - 1)y \bmod \mathcal{L}^2.$$

De même, de $\tau(\mathfrak{p}) \equiv 1 + (\zeta_l - 1)y \bmod \mathcal{L}^2$, il vient

$$\tau(\mathfrak{p})^t \equiv 1 + t(\zeta_l - 1)y \bmod \mathcal{L}^2,$$

d'où

$$\tau(\mathfrak{p})^{t+\sigma_{-t}} \equiv 1 \bmod \mathcal{L}^2.$$

Le premier $\mathcal{L}$ de $\mathbb{Q}(\zeta_{p^f}, \zeta_l)$ étant fixé quelconque et $\mathfrak{l}$ étant non ramifié dans $\mathbb{Q}(\zeta_{p^f}, \zeta_l)/\mathbb{Q}(\zeta_l)$, on obtient

$$\tau(\mathfrak{p})^{t+\sigma_{-t}} \equiv 1 \bmod \mathfrak{l}^2.$$

On montre de même que $\tau(\mathfrak{p})^{l+1-\sigma_{l+1}} \equiv 1 \bmod \mathfrak{l}^2$, ce qui clôt la démonstration.■

4.4.4 Les fractions de Jacobi.

Definition 4.4.11 *Les fractions de Jacobi, sont définies comme le sous-groupe des fractions d'Iwasawa, engendré par les $J_{u,v}(\mathfrak{a})$ qui vérifient en plus la condition $uv \neq 0[m]$. Si une fraction de Jacobi est un entier algébrique, on dira que c'est un entier de Jacobi.*

En particulier, les fractions, et donc les entiers de Jacobi, vérifient la relation d'Iwasawa.

4.4.5 Une application de la relation d'Iwasawa.

Rappelons le lemme suivant :

Lemme 4.4.12 *Soient $p > 2$ un nombre premier, ζ une racine primitive p-ième de l'unité, b un entier et $\epsilon = \pm 1$. Si $\epsilon\zeta^b \equiv 1 \bmod (1-\zeta)^2$, alors $\epsilon = \zeta^b = 1$.*

En ce qui concerne la génération d'un idéal principal de l'anneau $\mathbb{Z}[\zeta]$, par un entier Jacobi, on obtient alors la proposition suivante :

Proposition 4.4.13 *([41]) Soit $\alpha \in \mathbb{Z}[\zeta]$ tel que $\alpha\overline{\alpha} \in \mathbb{Z}$. Si l'idéal (α) est engendré par un entier de Jacobi β, alors il existe un entier naturel n tel que*

$$\alpha = \pm\zeta^n \cdot \beta. \tag{4.15}$$

En particulier, l'entier algébrique β est unique.

Preuve Soit donc $\alpha \in \mathbb{Z}[\zeta]$ tel que $\alpha\overline{\alpha} \in \mathbb{Z}$. Supposons qu'il existe un entier de Jacobi β tel que $(\alpha) = (\beta)$. Il existe donc une unité u de $\mathbb{Z}[\zeta]$ telle que $\alpha = u \cdot \beta$. Comme β peut s'écrire comme produit de puissances entières positives de sommes de Gauss (voir [39]), en particulier $\beta\overline{\beta} \in \mathbb{N}$. L'unité u est donc telle que $u\overline{u} \in \mathbb{Q}$. Comme $u\overline{u}$ est un entier algébrique, on a donc $u\overline{u} \in \mathbb{N}$, d'où $u\overline{u} = 1$ car u est une unité. Le théorème de Kronecker montre alors que u est nécesairement une racine de l'unité de $\mathbb{Q}(\zeta)$. Les seules racines de l'unité de ce corps étant les racines $2p$-ième de l'unité (voir [28]), il existe donc $\epsilon = \pm 1$ et un entier n tel que $u = \epsilon\zeta^n$, d'où (4.15).

Montrons l'unicité de β. Supposons qu'il existe deux entiers de Jacobi β_1, β_2 engendrant le même idéal de l'anneau $\mathbb{Z}[\zeta]$. Par la seconde assertion, il existe donc $\epsilon = \pm 1$ et un entier n tel que $\beta_1 = \epsilon\zeta^n \cdot \beta_2$. La relation d'Iwasawa montre alors $1 \equiv \epsilon\zeta^n \bmod \mathfrak{p}^2$. Par le lemme (4.4.12), $\epsilon = \zeta^n = 1$. On a donc $\beta_1 = \beta_2$.□

4.5 Annihilation du groupe des classes et des racines p-ième de l'unité.

On va démontrer que l'idéal de Stickelberger annihile le groupe des classes de $\mathbb{Q}(\zeta)$ (théorème de Stickelberger). On montrera également que si $\mathfrak{l}$ est un idéal premier de degrés relatif un sur $\mathbb{Q}$ et $\theta \in \mathcal{I}_{st}$, $\theta \geq 0$, alors $\mathfrak{l}^\theta$ est principal, engendré par un entier de Jacobi.

4.5.1 Décomposition primaire des sommes de Gauss.

Soit l un nombre premier tel que $p|l-1$.

Proposition 4.5.1 *Il y a une correspondance entre les caractères d'ordre p de $\mathbb{F}_l^\times$ et les idéaux premiers de $\mathbb{Q}(\zeta)$ au-dessus de l : si χ est le caractère associé à $\mathfrak{l}$, il est caractérisé par*

$$\forall x \in \mathbb{Z}, \quad \chi(x) \equiv x^{\frac{l-1}{p}} \bmod \mathfrak{l}. \tag{4.16}$$

Preuve Soit $\mathfrak{l}$ un idéal premier de $\mathbb{Q}(\zeta)$ au-dessus de l. Comme $l \equiv 1 \bmod p$, $\mathfrak{l}$ est de degrés relatif 1 sur $\mathbb{Q}$. Il existe donc $r \in \mathbb{Z}$ tel que $\zeta \equiv r \bmod \mathfrak{l}$. En prenant la puissance p-ième, il vient $r^p \equiv 1 \bmod \mathfrak{l}$, d'où $r^p \equiv 1 \bmod l$. Il existe donc un générateur s de $\mathbb{F}_l^\times$ tel que $r \equiv s^{\frac{l-1}{p}} \bmod l$. Comme s engendre $\mathbb{F}_l^\times$, il existe un unique caractère $\chi_\mathfrak{l}$ de $\mathbb{F}_l^\times$ tel que $\chi_\mathfrak{l}(s) = \zeta$. Un tel caractère vérifie (4.16). Ainsi, pour tout idéal premier $\mathfrak{l}$ de $\mathbb{Q}(\zeta)$ au-dessus de l, il existe bien $\chi_\mathfrak{l} \in \hat{\mathbb{F}_l^\times}$ vérifiant (4.16). Cette dernière propriété caractérise $\chi_\mathfrak{l}$. En effet, si χ' convient également, alors $\chi_\mathfrak{l}(s) \equiv \chi'(s) \bmod \mathfrak{l}$. Comme $\chi_\mathfrak{l}(s)$, $\chi'(s)$ sont des racines

p-ième de l'unité, et que $l \neq p$, on doit avoir $\chi_{\mathfrak{l}}(s) = \chi'(s)$, donc $\chi_{\mathfrak{l}} = \chi'$ (car s est un générateur de $\mathbb{F}_l^\times$).

On peut donc définir une application C des idéaux premiers de $\mathbb{Q}(\zeta)$ au-dessus de l vers les éléments d'ordre p de $\hat{\mathbb{F}_l^\times}$ en posant

$$C(\mathfrak{l}) = \chi_{\mathfrak{l}}.$$

Une telle application est injective. En effet, supposons qu'il existe deux idéaux premiers $\mathfrak{l}$ et $\mathfrak{l}'$ tels que $C(\mathfrak{l}) = C(\mathfrak{l}') = \chi \in \hat{\mathbb{F}_l^\times}$. Il existe un entier a tel que $\mathfrak{l}' = \mathfrak{l}^{\sigma_a}$. Par définition de $\chi = \chi_{\mathfrak{l}}$, on a alors

$$\chi(s) \equiv \chi(s)^a \bmod \mathfrak{l}'.$$

Si $a \neq 1$, comme $\chi(s)$ est une racine primitive p-ième de l'unité, on aurait $\mathfrak{l}' | \chi(s) - \chi(s)^a$, ie $\mathfrak{l} = \mathfrak{p}$ l'unique premier de $\mathbb{Q}(\zeta)$ au-dessus de p, d'où $l = p$, ce qui n'est pas. On a donc $a = 1$, ie $\mathfrak{l}' = \mathfrak{l}$: l'application C est bien injective. Comme il y a $p-1$ premiers de $\mathbb{Z}[\zeta]$ au-dessus de l (car $l \equiv 1 \bmod p$) et $p-1$ caractères de $\mathbb{F}_l^\times$ qui sont d'ordre p, l'application C est bijective (car injective entre deux ensembles de même ordre). ■

Fixons un caractère χ de $\mathbb{F}_l^\times$, caractère d'ordre p. Soit $a \in \{1, \ldots, p-1\}$. Soit b l'inverse de $a \bmod p$ et $\mathfrak{l}_a$ l'idéal premier associé à $\overline{\chi}^b$ par la proposition (4.5.1). L'idéal premier $\mathfrak{l}_1$ associé à $\overline{\chi}$ sera simplement noté $\mathfrak{l}$. Par définition

$$\overline{\chi}(x) \equiv x^{\frac{l-1}{p}} \bmod \mathfrak{l}, \quad x \in \mathbb{Z}.$$

On a

Lemme 4.5.2

$$\mathfrak{l}_a^{\sigma_a} = \mathfrak{l}.$$

Preuve En effet, on a

$$\overline{\chi}^b(x) \equiv x^{\frac{l-1}{p}} \bmod \mathfrak{l}_a, \quad x \in \mathbb{Z},$$

d'où

$$\overline{\chi}(x) \equiv x^{\frac{l-1}{p}} \bmod \mathfrak{l}_a^{\sigma_a}, \quad x \in \mathbb{Z},$$

c'est à dire $C(\mathfrak{l}) = C(\mathfrak{l}_a^\sigma)$, d'où le résultat par injectivité de C.□

Soit ξ une racine primitive l-ième de l'unité. Le premier $\mathfrak{l}_a$ est totalement ramifié dans $\mathbb{Q}(\zeta, \xi)$: il existe un unique premier $\mathcal{L}_a$ de $\mathbb{Z}[\zeta, \xi]$ tel que $\mathfrak{l}_a = \mathcal{L}_a^{l-1}$. En particulier

$$(l) = \mathcal{L}_1^{l-1} \ldots \mathcal{L}_{p-1}^{l-1}.$$

Posons $\mathcal{L} = \mathcal{L}_1$. Soit $a \in \{1, \ldots, p-1\}$. Si $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\zeta, \xi)/\mathbb{Q})$ est défini par $\zeta^{\sigma_a} = \zeta^a$ et $\xi^{\sigma_a} = \xi$, alors par le lemme précédent

$$\mathcal{L}_a^{\sigma_a} = \mathcal{L}.$$

Théorème 4.5.3 *(Kummer) Notons $g(\chi, \psi)$ la somme de Gauss associée :*

$$g(\psi, \chi) = \sum_{x=1}^{l-1} \psi(x)\chi(x).$$

La décomposition de l'idéal $(g(\psi, \chi))$ de $\mathbb{Z}[\zeta, \xi]$ est

$$(g(\psi, \chi)) = \left(\mathcal{L}_1 \mathcal{L}_2^2 \ldots \mathcal{L}_{p-1}^{p-1}\right)^{\frac{l-1}{p}}. \tag{4.17}$$

Preuve χ étant un caractère multiplicatif non trivial $g(\chi)\overline{g(\chi)} = l$. Les seuls facteurs premiers de $\mathbb{Z}[\zeta, \xi]$ divisant $g(\chi)$ se situent donc parmi $\mathcal{L}_1, \ldots, \mathcal{L}_{p-1}$, la multiplicité de chacun n'excèdant pas $l-1$:

$$g(\chi) = \mathcal{L}_1^{s_1} \cdots \mathcal{L}_{p-1}^{s_{p-1}}, \quad 0 \leq s_i \leq l-1.$$

Comme $\mathcal{L}_a^{\sigma_a} = \mathcal{L}$ et $\chi^{\sigma_a} = \chi^a$, on a

$$s_a = \nu_{\mathcal{L}_a}(g(\chi)) = \nu_{\mathcal{L}}(g(\chi^a)).$$

Par conséquent, le nombre algébrique

$$\beta = \frac{(1-\xi)^{s_a}}{g(\chi^a)}$$

est une $\mathcal{L}$-unité. Soit b un entier premier à l. Soit $\tau_b \in \mathrm{Gal}(\mathbb{Q}(\zeta, \xi)/\mathbb{Q})$ défini par

$$\zeta^{\tau_b} = \zeta, \quad \xi^{\tau_b} = \xi^b.$$

Comme $\frac{\xi^b - 1}{\xi - 1} \equiv b \bmod \mathcal{L}$ et $g(\chi)^{\tau_b} = \overline{\chi}(b) g(\chi)$, il vient

$$\beta^{\tau_b} = \frac{(1-\xi^b)^{s_a}}{\overline{\chi}(b)^a g(\chi^a)} = \frac{\beta}{\overline{\chi}(b)^a} \left(\frac{1-\xi^b}{1-\xi}\right)^{s_a} \equiv \frac{b^{s_a}}{\overline{\chi}(b)^a} \beta \bmod \mathcal{L}.$$

Comme $\mathfrak{l}$ est totalement ramifié dans l'extension $\mathbb{Q}(\zeta, \xi)/\mathbb{Q}(\zeta)$, on a $\beta^{\tau_b} \equiv \beta \bmod \mathcal{L}$, d'où

$$b^{s_a} \equiv \overline{\chi}(b)^a \bmod \mathcal{L}.$$

Or $\overline{\chi}(b)^a \equiv b^{a\frac{l-1}{p}} \bmod \mathcal{L}$, d'où

$$b^{s_a} \equiv b^{a\frac{l-1}{p}} \bmod l,$$

pour tout entier b. Il vient

$$s_a \equiv a\frac{l-1}{p} \bmod l - 1.$$

Comme $s_a \leq l-1$, on donc $s_a = a\frac{l-1}{p}$. ■

4.5.2 Théorème de densité de Frobenius.

Il nous reste à montrer que toute classe d'idéaux, contient un idéal de degrés un sur $\mathbb{Q}$.

On commence par rappeler quelques résultats généraux, sur la théorie de Galois des corps de nombres. Soit E/K une extension de corps de nombres et soit L la clôture galoisienne de E. Soit $H = \mathrm{Gal}(L/E)$ et soit $G = \mathrm{Gal}(L/K)$. On pose :

$$G = \bigcup_{i=1}^{t} H\sigma_i.$$

Un élément σ de G permute les ensembles $H\sigma_i$ par multiplication à droite.

Definition 4.5.4 *Si les ensembles $H\sigma_i, \ldots, H\sigma_i\sigma^{l-1}$ sont deux à deux distincts, et si $H\sigma_i = H\sigma_i\sigma^l$, on dit que la suite $\left(H\sigma_i, \ldots, H\sigma_i\sigma^{l-1}\right)$ est un cycle de longueur l pour σ.*

Tout élément de G admet une unique décomposition en produits de cycles disjoints.

Proposition 4.5.5 *Soit $\mathfrak{p}$ un idéal premier de K non ramifié dans L/K. Soit $\mathfrak{b}$ un premier de L au-dessus de $\mathfrak{p}$. Soit σ son automorphisme de Frobenius. On suppose que la longueur des cycles qui composent σ est $t_1, \ldots, t_s$. Le premier $\mathfrak{p}$ se décompose alors dans E en produit de s premiers de L, de degrés respectifs $t_1, \ldots, t_s$.*

Preuve L'automorphisme σ se décompose en produit de cycles à supports disjoints. Soit $H\tau$ un représentant d'un cycle de longueur l pour σ. On pose $\mathfrak{p}_0 = \tau(\mathfrak{b}) \cap E$, premier de E qui divise $\mathfrak{p}$. Calculons le degrés relatif $f(\mathfrak{p}_0|\mathfrak{p})$. Soit $H(\tau(\mathfrak{b}))$ (respectivement $G(\tau(\mathfrak{b}))$) le groupe de décomposition de $\tau(\mathfrak{b})$ dans L/E (respectivement L/K). On a

$$H(\tau(\mathfrak{b})) = H \cap G(\tau(\mathfrak{b})).$$

Mais

$$G(\tau(\mathfrak{b})) = \tau \cdot G(\mathfrak{b}) \cdot \tau^{-1} = < \tau \cdot \sigma \cdot \tau^{-1} > .$$

L'entier l est le plus petit entier strictement positif tel que $H\tau = H\tau\sigma^l$. On a alors :

$$H \cap < \tau \cdot \sigma \cdot \tau^{-1} > = < \tau \cdot \sigma^l \cdot \tau^{-1} > .$$

On a donc $H(\tau(\mathfrak{b})) = < \tau \cdot \sigma^l \cdot \tau^{-1} >$. Il vient alors

$$f(\mathfrak{p}_0|\mathfrak{p}) = \frac{f(\tau(\mathfrak{b})|\mathfrak{p})}{f(\tau(\mathfrak{b})|\mathfrak{p}_0)} = \frac{|G(\tau(\mathfrak{b}))|}{|H(\tau(\mathfrak{b}))|} = \frac{| < \tau \cdot \sigma \cdot \tau^{-1} > |}{| < \tau \cdot \sigma^l \cdot \tau^{-1} > |} = l.$$

Définissons une application C d'un système de représentants $\mathcal{R}$ des cycles intervenant dans la décomposition de σ en produits de cycles disjoints, vers les premiers de L au-dessus de $\mathfrak{p}$: à un cycle de longueur l de σ représenté par $H\tau$, on lui associe le premier $\mathfrak{p}_0 = \tau(\mathfrak{b}) \cap E$ de E, qui est de degrés relatif l sur K. Montrons que cette application est biunivoque. Soient donc deux représentants $H\tau$ et $H\lambda$ tels que

$$\mathfrak{p}_0 = \lambda(\mathfrak{b}) \cap E = \tau(\mathfrak{b}) \cap E.$$

Les premiers $\lambda(\mathfrak{b})$ et $\tau(\mathfrak{b})$ sont donc deux premiers de L au-dessus de $\mathfrak{p}_0$. Par transitivité de l'action de H sur de tels premiers, il existe un élément γ de H, tel que

$$\gamma\lambda(\mathfrak{b}) = \tau(\mathfrak{b}).$$

L'élément $\tau^{-1}\gamma\lambda$ est un élément de $G(\mathfrak{b})$ engendré par σ. Il existe donc un entier i tel que

$$\gamma\lambda = \tau\sigma^i.$$

On a alors

$$H\tau\sigma^i = H\gamma\lambda = H\lambda.$$

$H\tau$ et $H\lambda$ représentent donc le même cycle, et sont donc égaux car éléments de $\mathcal{R}$. L'application C est donc injective.

De plus, C est surjective. En effet

$$\sum_{H\tau\in\mathcal{R}} f\left(\tau(\mathfrak{b}) \cap E|\mathfrak{p}\right) = \sum_i t_i = [G:H] = [E:K].$$

Mais $\mathfrak{p}$ étant non ramifié dans E/K : $\sum_{\mathfrak{p}_0|\mathfrak{p}} f\left(\mathfrak{p}_0|\mathfrak{p}\right) = [E:K]$. On a donc

$$\sum_{H\tau\in\mathcal{R}} f\left(\tau(\mathfrak{b}) \cap E|\mathfrak{p}\right) = \sum_{\mathfrak{p}_0|\mathfrak{p}} f\left(\mathfrak{p}_0|\mathfrak{p}\right). \tag{4.18}$$

Comme C est injective, (4.18) montre qu'elle est surjective, donc bijective. ■

Corollaire 4.5.6 *Le nombre de premiers de E au-dessus de $\mathfrak{p}$ de degrés relatif 1 sur K est égal au nombre d'entiers i tels que $\sigma_i G(\mathfrak{b})\sigma_i^{-1} \subset H$.*

Preuve Soit $\mathfrak{b}$ un premier de L au-dessus de $\mathfrak{p}$. Soit σ un générateur de $G(\mathfrak{b})$. Par la proposition précédente, le nombre des premiers de E au-dessus de $\mathfrak{p}$ et de degrés 1 sur ce premier, est égal au nombre d'entiers i tels que $H\sigma_i\sigma = H\sigma_i$, d'où le résultat. ■

Dans la suite, on adopte la notation suivante : si f_1 et f_2 sont deux fonctions définies sur $\{s : \quad Re(s) > 1\}$; on pose $f_1 \sim f_2$ si et seulement si $f_1 - f_2$ a une limite finie en 1^+.

Definition 4.5.7 *Soit G un groupe fini et $\sigma \in G$ un élément d'ordre n. On appelle division de σ, l'ensemble des éléments de G qui sont conjugués à un certain σ^m, $(m,n)=1$.*

On peut maintenant démontrer le théorème de densité de Frobenius :

Théorème 4.5.8 *(Théorème de densité de Frobenius.) Soit σ un élément de $G = \mathrm{Gal}(L/K)$, ayant t éléments dans sa division. Soit S_1 le nombre de premiers de K qui sont divisibles par un premier de L dont le Frobenius est dans la division de σ. Cet ensemble possède une densité $d(S_1)$ au sens de Dirichlet. Cette densité vaut $d(S_1) = \frac{t}{|G|}$.*

Preuve La preuve se fait par récurrence sur l'ordre de σ, que l'on note dorénavant n. Supposons d'abord que $n=1$. S_1 est donc l'ensemble des premiers de K qui se décomposent totalement dans L. Soit S^* l'ensemble des premiers de L qui divise un premier de S_1. Pour chaque premier $\mathfrak{p}$ de S_1, il y a exactement $|G|$ premiers distincts de S^* qui divisent $\mathfrak{p}$, et ces éléments de S^* sont de norme $\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{p})$, vu qu'ils sont de degrés relatif 1 sur K. On a donc :

$$\sum_{\mathfrak{b}\in S^*} \mathcal{N}_{L/\mathbb{Q}}(\mathfrak{b})^{-s} = |G| \sum_{\mathfrak{p}\in S_1} \mathcal{N}_{K/\mathbb{Q}}(\mathfrak{p})^{-s}$$

Soit T l'ensemble des premiers de L qui sont de degrés relatif 1 sur $\mathbb{Q}$. On a $T \subset S^*$. Un premier qui est dans S^* mais pas dans T est de degrés relatif au moins 2 sur $\mathbb{Q}$. Sa norme sur $\mathbb{Q}$ est donc au moins le carré d'un nombre premier. En particulier, la série $\sum_{\mathfrak{b}\in S^*-T} \mathcal{N}_{L/\mathbb{Q}}(\mathfrak{b})^{-s}$ est convergente au voisinage de 1 :

$$\sum_{\mathfrak{b}\in S^*-T} \mathcal{N}_{L/\mathbb{Q}}(\mathfrak{b})^{-s} \sim 0.$$

Comme T admet une densité $d(T)$ au sens de Dirichlet, avec $d(T)=1$, il en va de même pour S^* et $d(S^*)=1$. On a donc

$$\sum_{\mathfrak{p}\in S_1} \mathcal{N}_{K/\mathbb{Q}}(\mathfrak{b})^{-s} \sim -\frac{1}{|G|} log(s-1).$$

L'ensemble S_1 admet donc une densité de Dirichlet, et celle-ci vaut $\frac{1}{|G|}$. L'assertion est prouvée dans le cas $n=1$.

Supposons maintenant que $n>1$. Soit d un diviseur de n. Soit t_d le nombre d'éléments dans la division de σ^d. Soit S_d le nombre de premiers de K divisibles par un premier de L, dont le Frobenius est dans la division de σ^d. Par hypothèse de récurrence, si $d \neq 1$, on a $d(S_d) = \frac{t_d}{|G|}$.

Soit E le sous-corps de L, qui est invariant sous $H =< \sigma >$, le sous-groupe de G engendré par σ. Les premiers de K qui ont au moins un facteur premier dans E qui est de degrés relatif 1 sur K, sont exactement les premiers de K, qui sont divisibles par un premier $\mathfrak{b}$ de L, dont le Frobenius τ, a un cycle de logueur 1, dans son action sur les co-ensembles de H dans G (par la proposition 4.5.5). Par le corollaire (4.5.6), cela arrive quand il existe un entier i tel que $\sigma_i \tau \sigma_i^{-1} \in H$, c'est à dire que τ est conjugué à une puissance de σ, et donc que $\mathfrak{p}$ est un élément de S_d pour un certain d, diviseur de n.

Soit S_E l'ensemble des premiers de E de degrés relatif 1 sur K. Si $\mathfrak{p}$ est un élément de S_d, on note $n(\mathfrak{p})$ le nombre de premiers de E divisant $\mathfrak{p}$ et de degrés relatif 1 sur K. Si $\mathfrak{p}$ est un élément de S_d, il est la norme de $n(\mathfrak{p})$ premiers de S_E. Comme S_E contient tous les premiers de E de degrés relatif 1 sur $\mathbb{Q}$, comme avant S_E admet une densité au sens de Dirichlet, et celle-ci vaut 1. On a donc

$$-log(1-s) \sim \sum_{\mathfrak{b} \in S_E} \mathcal{N}_{K/\mathbb{Q}} \left(\mathcal{N}_{E/K} (\mathfrak{b}) \right)^{-s} \sim \sum_{d|n} \sum_{\mathfrak{p} \in S_d} n(\mathfrak{p}) \mathcal{N}_{K/\mathbb{Q}} (\mathfrak{p})^{-s}. \tag{4.19}$$

Calculons $n(\mathfrak{p})$. Soit donc $\mathfrak{p} \in S_d$. Par le corollaire (4.5.6), $n(\mathfrak{p})$ est égal au nombre de co-ensembles $H\sigma_i$ tels que $\sigma_i \sigma^d \sigma_i^{-1} \in H$. Comme H est cyclique, engendré par σ, c'est équivalent à $\sigma_i \in N_G(< \sigma^d >)$. Donc, on a

$$n(\mathfrak{p}) = \left[N_G(< \sigma^d >) : H \right].$$

En appliquant l'hypothèse de récurrence à (4.19), on obtient :

$$[N_G(H) : H] \sum_{\mathfrak{p} \in S_1} \mathcal{N}(\mathfrak{b})^{-s} \sim \left(-1 + \sum_{d|n, d \neq n} \frac{\left[N_G \left(< \sigma^d > \right) : H \right] t_d}{|G|} \right) log(s-1) \tag{4.20}$$

Lemme 4.5.9 *Soit σ un élément d'ordre n d'un groupe G. Soit H le sous-groupe de G engendré par σ. Soit t le nombre d'éléments dans la division de σ. On a alors :*

$$t = \varphi(n)[G : N_G(H)].$$

Preuve Pour deux éléments a et b de G, on pose $a \sim b$ si et seulement s'ils sont conjugués (dans G). Soient $\mathcal{C} = \{\sigma^i | 1 \leq i \leq n-1, \quad (i,n) = 1\}$ et Q le quotient de $\mathcal{C}$ par cette relation d'équivalence, dont on note S un système de représentants. Soit $Int(H)$ le groupe des automorphsimes de H de la forme $\phi(\sigma) = g^{-1}\sigma g$, où $g \in G$. Ce groupe s'identifie à $\frac{N_G(H)}{C_G(\sigma)}$. En notant φ la fonction d'Euler, on a

$$\left| \frac{Aut(H)}{Int(H)} \right| = \frac{\varphi(n) \left| C_G(\sigma) \right|}{|N_G(H)|}.$$

Le groupe $\frac{Aut(H)}{Int(H)}$ est en bijection avec Q. En particulier, $|S| = \frac{\varphi(n)|C_G(\sigma)|}{|N_G(H)|}$. Soit $\mathcal{D}$ la division de σ. On a

$$\mathcal{D} = \bigcup_{s \in S} \{g \in G | g \sim s\}.$$

Soit m un entier premier à n ; alors l'ensemble des conjugués de $C_G(\sigma)$ est aussi $C_G(\sigma^m)$. Or, il y a $[G : C_G(s)]$ éléments dans $\{g \in G | g \sim s\}$. On en déduit donc

$$|\mathcal{D}| = |S| \cdot \frac{|G|}{|C_G(\sigma)|} = \frac{\varphi(n)|G|}{|N_G(H)|} = \varphi(n)[G : N_G(H)].$$

□

Ce lemme montre que $t_d = \phi\left(\frac{n}{d}\right)\left[G : N_G\left(< \sigma^d >\right)\right]$. Le coefficient du $log(s-1)$ de l'égalité précédente devient :

$$-1 + \sum_{d|n, d \neq n} \frac{1}{n}\phi\left(\frac{n}{d}\right) = -1 - \frac{\phi(n)}{n} + \sum_{d|n} \frac{1}{n}\phi\left(\frac{n}{d}\right) = -\frac{\phi(n)}{n}.$$

Toujours en utilisant le lemme, on obtient :

$$\sum_{\mathfrak{p} \in S_1} \mathcal{N}_{K/\mathbb{Q}}(\mathfrak{p})^{-s} \sim \frac{-t}{|G|} log(s-1).$$

■

Proposition 4.5.10 *Soit K un corps de nombres. Alors, toute classe d'idéaux de K contient une infinité de puissances entières de premiers de degrés relatif 1 sur $\mathbb{Q}$.*

Preuve Soit en effet C une classe d'idéaux de K. Soit L le corps de classes de K. Soit $\sigma \in \mathrm{Gal}(L/K)$, associé à C via l'aplication d'Artin. On a

$$\mathfrak{a} \in C \Longleftrightarrow \left[\frac{\mathfrak{a}}{L/K}\right] = \sigma.$$

Comme l'extension L/K est abélienne, la division S de σ est réduite aux puissances entières premières à l'ordre de σ. Par le théorème de densité de Frobenius, l'ensemble des premiers de K qui admettent pour Frobenius un élément de S, admet une densité au sens de Dirichlet valant $\frac{|S|}{|G|}$. Comme les idéaux premiers de K ayant un degrés relatif valant 1 sur $\mathbb{Q}$ ont pour densité de Dirichlet 1, on en déduit qu'il existe un entier l premier à l'ordre de σ, pour lequel il existe une infinité de premiers premier de K de degrés 1 sur $\mathbb{Q}$, disons $\mathfrak{p}_i$, ayant pour Frobenius σ^l, où l est premier à l'ordre de σ. Il existe donc une puissance entière de $\mathfrak{p}_i$ qui admet σ pour Frobenius. ■

En particulier, pour démontrer que l'idéal de Stickelberger annihile le groupe des classes de $K = \mathbb{Q}(\zeta)$, il suffit de le démontrer pour les idéaux premiers de K qui sont de degrés relatif 1 sur $\mathbb{Q}$.

4.5.3 Annihilation des idéaux de degrés un et les fractions de Jacobi.

Proposition 4.5.11 *Soit $\mathfrak{l}$ un idéal premier de degrés relatif 1 sur $\mathbb{Q}$. Pour tout élément Θ positif de l'idéal de Stickelberger, l'idéal $\mathfrak{l}^{\Theta}$ est principal, engendré par un entier de Jacobi.*

Preuve Soit l le nombre premier en dessous de $\mathfrak{l}$. Comme $\mathfrak{l}$ est d'inertie 1 sur $\mathbb{Q}$, on a $l \equiv 1 \bmod p$. Soit χ le caractère associé à $\mathfrak{l}$ par la proposition (4.5.1). Comme

$$\mathfrak{l}_a = \mathfrak{l}^{\sigma_a^{-1}}, \quad \mathcal{L}_a = \mathcal{L}^{\sigma_a^{-1}},$$

la décomposition (4.17) s'écrit

$$(g(\chi)) = \mathcal{L}^{\frac{l-1}{p}\left(\sigma_1^{-1}+\ldots+(p-1)\sigma_{p-1}^{-1}\right)},$$

c'est à dire

$$\mathcal{L}^{(l-1)\vartheta} = (g(\chi)).$$

Comme $\psi_{b-1} = (b - \sigma_b)\vartheta$, il vient

$$\mathcal{L}^{(l-1)\psi_{b-1}} = \left(g(\chi)^{b-\sigma_b}\right).$$

L'idéal $\mathfrak{l}^{\Theta_b}$ est donc bien principal. Montrons maintenant que si θ est un élément de l'idéal de Stickelberger de $\mathbb{Q}(\zeta)$, et si $\mathfrak{l}$ est un idéal de degrés relatif 1 sur $\mathbb{Q}$ alors $\mathfrak{l}^{\theta}$ est engendré par une fraction de Jacobi. Si s et t sont deux entiers tels que $rs(r+s) \neq 0 \bmod p$, alors on pose

$$\varphi_{r,s} = \sum_{t=1}^{p-1} \varphi_{r,s}(t)\sigma_t^{-1},$$

où $\varphi_{r,s}(t) = \left[\frac{(r+s)t}{p}\right] - \left[\frac{rt}{p}\right] - \left[\frac{st}{p}\right]$.

On vérife que $\mathcal{N} = \varphi_{p-1,p-1}$ et $\varphi_i = \varphi_{1,i}$. Donc, il suffit de montrer que $\mathfrak{l}^{\varphi_{r,s}} \in \mathcal{J}$. On a

$$\varphi_{r,s} = \theta_{r+s} - \theta_r - \theta_s.$$

Posons aussi $g_r = g^{\sigma_r}$. On a

$$\mathfrak{l}^{\varphi_{r,s}} = \left(\frac{g_r g_s}{g_{r+s}}\right) = (\mathcal{J}_{r,s}(\mathfrak{l})) \in \mathcal{J}.$$

■

Corollaire 4.5.12 *En particulier, soit $\mathfrak{a}$ un idéal entier de $\mathbb{Q}(\zeta)$, tel que si l est un nombre premier qui divise $\mathcal{N}(\mathfrak{a})$, alors $l \equiv 1 \bmod p$. Soit θ un élément positif de l'idéal de Stickelberger de $\mathbb{Q}(\zeta)$. L'idéal $\mathfrak{a}^{\theta}$ est engendré par un entier de Jacobi.*

Preuve Soit $\mathfrak{l}$ un facteur premier de $\mathfrak{a}$. L'idéal $\mathfrak{l}$ est totalament décomposé dans le corps $\mathbb{Q}(\zeta)$, car le Frobenius de $\mathfrak{l}$ est trivial vu que $l \equiv 1 \bmod p$. Le degrés relatif de $\mathfrak{l}$ sur $\mathbb{Q}$ vaut donc 1. La proposition précédente montre donc que $\mathfrak{l}^\theta$ est engendré par un entier de Jacobi ($\theta \geq 0$). ■

4.5.4 Annihilation des racines p-ième de l'unité.

On peut également considérer l'action additive de $\mathcal{I}_{st}$ sur le groupe des racines p-ième de l'unité :

Definition 4.5.13 *On appelle quotient de Fermat, l'application $\phi : \mathcal{I} \to \mathbb{F}_p$ définie par :*

$$\zeta^\Theta = \zeta^{\phi(\Theta)}.$$

Lemme 4.5.14 *(Clausen-Von Staudt.) Soit k un entier divisible par $p-1$. Alors*

$$pB_k \equiv -1 \bmod p.$$

Preuve Soit $\alpha \neq 1$ un entier premier à p. Considérons la distribution de Bernoulli régularisée $\mu_{k,\alpha}$ sur $\mathbb{Z}_p$. Rappelons qu'elle est définie pour U compact ouvert de $\mathbb{Z}_p$ par

$$\mu_{k,\alpha}(U) = \mu_{B,k}(U) - \frac{1}{\alpha^k}\mu_{B,k}(\alpha U),$$

où $\alpha U = \left\{x \in \mathbb{Q}_p | \frac{x}{\alpha} \in U\right\}$ et où $\mu_{B,k}$ est l'unique distribution sur $\mathbb{Z}_p$ vérifiant

$$\mu_{B,k}\left(a + (p^N)\right) = p^{N(k-1)}\mathbf{B}_k\left(\frac{a}{p^N}\right).$$

A partir de l'égalité classique

$$\frac{te^{tx}}{e^t - 1} = \sum_{k=0}^{\infty} \mathbf{B}_k(x)\frac{t^k}{k!},$$

on déduit que

$$\sum_{i=0}^{p-1} \mathbf{B}_k\left(\frac{i}{p}\right) = B_k.$$

Il vient alors $\mu_{B,k} = (\mathbb{Z}_p)$, donc $\mu_{B,k}\left(\mathbb{Z}_p^\times\right) = B_k - \mu_{B,k}(0 + (p)) = B_k(1 - p^{k-1})$. On a donc $\mu_{k,\alpha}\left(\mathbb{Z}_p^\times\right) = (1 - \frac{1}{\alpha^k})(1 - p^{k-1})B_k$. Cela s'écrit aussi

$$(1 - \frac{1}{\alpha^k})(1 - p^{k-1})B_k = \int_{\mathbb{Z}_p^\times} d\mu_{k,\alpha}.$$

En écrivant cette dernière intégrale comme limite de sommes de Riemann, on obtient

$$(1-\frac{1}{\alpha^k})(1-p^{k-1})B_k = \int_{\mathbb{Z}_p^\times} d\mu_{k,\alpha} = k\int_{\mathbb{Z}_p^\times} f d\mu_{1,\alpha}, \tag{4.21}$$

où $f(x) = x^{p-1}$. Prenons maintenant plus précisément $\alpha = 1+p$. Alors, en notant $d = \nu_p(k)$, il vient

$$\frac{1}{\alpha^k} - 1 = (1+p)^{-k} - 1 \equiv -kp \bmod p^{d+2},$$

d'où $\frac{-kp}{\alpha^{-k}-1} \equiv 1 \bmod p$. On en déduit

$$pB_k = -kp\frac{-B_k}{k} \equiv \frac{B_k}{k}(1-\alpha^{-k}) \equiv \frac{B_k}{k}(1-\alpha^{-k})(1-p^{k-1}) \equiv \int_{\mathbb{Z}_p^\times} f d\mu_{1,\alpha} \bmod p.$$

Comme $p-1|k$, on a pour $x \in \mathbb{Z}_p^\times$ $f(x) \equiv x^{-1} \bmod p$, ie

$$pB_k \equiv \int_{\mathbb{Z}_p^\times} x^{-1} d\mu_{1,\alpha}(x) \bmod p \equiv -1 \bmod p.$$

Pour montrer cette dernière congruence, on pose pour $x \in \mathbb{Z}_p^\times$ $g(x) = \frac{1}{a_0(x)}$, $a_0(x) \in \{1,\dots,p-1\}$ tel que $x \equiv a_0(x) \bmod p$. La fonction g est localement constante et vérifie $g(x) \equiv x^{-1} \bmod p$. En particulier

$$\int_{\mathbb{Z}_p^\times} x^{-1} d\mu_{1,\alpha}(x) \equiv \int_{\mathbb{Z}_p^\times} g d\mu_{1,\alpha} \equiv \sum_{i=1}^{p-1} \frac{1}{i}\mu_{1,\alpha}\left(i+(p)\right) \bmod p.$$

Comme

$$\begin{aligned}\mu_{1,\alpha}\left(a+(p^N)\right) &= \frac{a}{p^N} - \frac{1}{2} - \frac{1}{\alpha}\left(\frac{\{\alpha a\}}{p^N} - \frac{1}{2}\right) \\ &= \frac{1}{\alpha}\left[\frac{\alpha a}{p^N}\right] + \frac{1/\alpha - 1}{2},\end{aligned}$$

il vient $\sum_{i=1}^{p-1} \frac{1}{i}\mu_{1,\alpha}\left(i+(p)\right) \equiv -1 \bmod p$. ■

En particulier, le lemme précédent et le lemme (4.3.3) appliqué avec $m = p-1$ montrent que

$$\sum_{j=1}^{p-1}\left[\frac{aj}{p}\right] j^{p-2} \equiv (a^p-a)\frac{B_{p-1}}{p-1} \equiv \frac{a^p-a}{p}\frac{pB_{p-1}}{p-1} \equiv \frac{(a^p-a)}{p} \bmod p.$$

On en déduit immédiatement la proposition suivante, qui explique le nom donné à l'application ϕ :

Proposition 4.5.15

$$\phi\left(\Theta_n\right) \equiv \frac{n^p - n}{p} \bmod p.$$

De cette proposition, découle le théorème suivant du à Mihăilescu :

Théorème 4.5.16 *Il existe au moins un élément Fuchsien $\theta \in \mathcal{I}_{st}$ tel que $\phi(\theta) \neq 0$.*

Preuve Raisonnons par l'absurde et supposons que pour tout élément Fuchsien Θ_n, $1 \leq n \leq p-2$ on ait $\phi\left(\Theta_n\right) = 0$. Soit $f(X) \in \mathbb{F}_p[X]$ le polynôme de degrés $p-1$ défini par

$$f(X) = \frac{(X+1)^p - X^p - 1}{p} \equiv \sum_{k=1}^{p-1} \frac{1}{k}(-X)^k \bmod p.$$

Par hypothèse, $1 = \zeta^{\Theta_n} = \zeta^{\Theta_{n+1}}$. De plus, par la proposition (4.5.15)

$$\zeta^{\Theta_n} = \zeta^{\varphi(\Theta_n)} = \zeta^{\frac{n^p-n}{p}}, \quad \zeta^{\Theta_{n+1}} = \zeta^{\varphi(\Theta_{n+1})} = \zeta^{\frac{(n+1)^p-n-1}{p}},$$

d'où

$$\zeta^{f(n)} = \zeta^{\frac{(n+1)^p-n-1}{p} - \frac{n^p-n}{p}} = 1.$$

Le polynôme f a donc pour racine au moins dans $\mathbb{F}_p$, $1, \ldots, p-2$. Comme p est impair, on a également $f(p-1) \equiv 0 \bmod p$. Enfin, $f(0) \equiv 0 \bmod p$. Ainsi f admet au moins p racines distinctes alors qu'il est de degrés $p-1$: contradiction. ■

Chapitre 5

Arithmétique de l'équation $X^p + Y_0^p = BZ^p$

5.1 Introduction

Soit p un nombre premier impair. On appelle équation diagonale générale de Nagell-Ljunggren, l'équation diophantienne suivante[1] :

$$\frac{x^p + y^p}{x + y} = p^e z^p, \quad x, y, z \in \mathbb{Z}, \quad (x, y, z) = 1. \tag{5.1}$$

On dit qu'une solution éventuelle x, y, z de (5.1) se situe dans le premier cas si $xy(x^2 - y^2) \neq 0 \bmod p$. On dit qu'une solution éventuelle de (5.1) se situe dans le second cas, si elle ne se situe pas dans le premier.

Rappelons que si ζ désigne une racine primitive p-ième de l'unité, alors on note par h_p^+ (respectivement par h_p^-) le nombre de classes de $\mathbb{Q}(\zeta) \cap \mathbb{R}$ (respectivement le nombre de classes relatif de $\mathbb{Q}(\zeta)$), et par r_p, le p-rang du groupe des classes relatif de $\mathbb{Q}(\zeta)$.

Pour l'étude des solutions de (5.1) se situant dans le second cas, Mihăilescu se fixe $y = -1$ et obtient le théorème suivant (théorème 4 de [53]) :

Théorème 5.1.1 *Soit $p > 17$ un nombre premier. S'il existe des entiers x, z vérifiant*

$$\frac{x^p - 1}{x - 1} = z^p, \quad p|x,$$

alors $|x| \leq (16p)^{\frac{p-1}{2}}$. De plus, si $p^3|x$, alors p divise h_p^+.

En fait, Mihăilescu énonce un résultat plus général, mais sa démonstration dans le cas $p|x^2 - 1$ est éronnée. De plus, sa démonstration dans le cas $p|x$ nécessite en fait $p^3|x$: on

[1] Rappelons que $e \in \{0; 1\}$, avec $e = 1$ si et seulement si $p|x + y$.

peut montrer que si $p|x$, alors $p^2|x$. Par contre, de $p^2|x$ on ne peut déduire en général que $p^3|x$. En effet, on a par exemple $\frac{18^3-1}{18-1} = 7^3$ (seule solution non triviale de $\frac{x^3-1}{x-1} = y^3$). On montrera néanmoins que c'est vrai sous certaines conditions portant sur les facteurs premiers de z : voir la démonstration du corollaire (5.1.6).

Dans ce chapitre, on se propose de développer l'étude d'un certain $\mathbb{F}_p$-module (plus précisément celle de $\mathbf{A}_1$; voir le paragraphe 5.2), et d'étendre les arguments de [53] au cas $|y| \geq 1$. On obtient sur l'équation (5.1) le nouveau théorème suivant :

Théorème 5.1.2 *Soient $p \geq 3$ un nombre premier, y_0 un entier fixé premier à p. S'il existe des entiers x, z qui vérifient*

$$\frac{x^p + y_0^p}{x + y_0} = p^e z^p, \quad (x, y_0, z) = 1, \tag{5.2}$$

alors soit $y_0 = \pm 1$, soit pour tout facteur premier r de y_0, on a $r^{p-1} \equiv 1 \bmod p^2$. En particulier, $y_0^{p-1} \equiv 1 \bmod p^2$. De même, si $p \nmid x$, alors pour tout facteur premier r de x, on a $r^{p-1} \equiv 1 \bmod p^2$.

Supposons $p > 3$ et qu'il existe des entiers x, z tels que

$$\frac{x^p + y_0^p}{x + y_0} = z^p, \quad (x, y_0, z) = 1. \tag{5.3}$$

Si $p|x$ on a alors $|x| < (16p)^{\frac{p-1}{2}} |y_0|^{\frac{p+1}{2}}$. De plus, si $p^3|x$ et[2] $|y_0| \leq \frac{p}{19}$, alors p divise h_p^+.

Du théorème précédent, on déduit immédiatement le

Corollaire 5.1.3 *Soient $p \geq 19$ un nombre premier, y_0 un entier impair fixé premier à p, $|y_0| \leq \frac{p}{19}$, $a \geq 3$ un entier. Supposons qu'il existe des entiers x, z tels que*

$$\frac{x^{ap} + y_0^p}{x^a + y_0} = z^p, \quad (x, y_0, z) = 1, \quad 2|x. \tag{5.4}$$

Alors de deux choses l'une, soit $2^{p-1} \equiv 1 \bmod p^2$, soit $p|h_p^+$.

[En effet, comme x est pair, si $p \nmid \frac{2^{p-1}-1}{p}$, la première partie du théorème (5.1.2) montre que $p|x^a$, donc $p^3|x^a$ car $a \geq 3$. Comme $|y_0| \leq \frac{p}{19}$, la deuxième partie de ce même théorème montre alors que $p|h_p^+$.]

Rappelons que si n est un entier non nul, $|n| > 1$, on appelle radical de n, noté $Rad(n)$, le produit de ses facteurs premiers. On pose également $Rad(n) = 1$ si $n = \pm 1$. Soit φ la fonction d'Euler. Si n est un entier, on définit alors $\Psi(n)$ par

$$\Psi(n) = \varphi(Rad(n)).$$

[2]En fait, on montrera que la condition légèrement plus faible $|y_0| \leq \frac{p}{\left(2(p-1)16^{\frac{p-1}{2}}\right)^{\frac{2}{p+1}}}$ suffit.

On adopte la terminologie suivante : nous dirons qu'un triplet d'entiers (A, B, C) est **primitif** si $C = 0$ et $AB \neq 0$, ou bien $C \neq 0$ et $(A, B, C) = 1$.

Pour la suite, **on se fixe un nombre premier $p > 3$ et un entier Y_0 non nul tel que** $|Y_0| \leq \frac{p}{19}$. On note B_k le k-ième nombre de Bernoulli. Du théorème (5.1.2), on obtient les nouveaux résultats suivant sur les équations diophantiennes de la forme $X^p + Y_0^p = BZ^q$:

Corollaire 5.1.4 *Soit B un entier tel que $(Y_0\Psi(B), p) = 1$. On se fixe également un entier $a > 0$ et $q > 2$ un nombre premier. Si $q \neq p$, on suppose que a est pair, $q \nmid h_p^-$ et $Y_0 = -1$. Si $q = p$, on suppose $a \geq 3$ et que les conditions suivantes sont satisfaites :*

1. $\left(\frac{B}{2}\right)^{p-1} \neq 1 \bmod p^2$,
2. $p \nmid B \cdot h_p^+$,
3. $p^3 \nmid B_{pi}$, $i = 2, 4, \ldots, p-3$,
4. $r_p \leq \sqrt{p} - 1$ *ou bien parmi les entiers* $2^{p-1} - 1$, $3^{p-1} - 1$, *l'un des deux n'est pas divisible par* p^2, *ou bien il existe un facteur premier r de B tel que* $r^{p-1} \neq 1 \bmod p^2$.

Supposons qu'il existe des entiers X, Z tels que (X, Y_0, Z) soit une solution primitive de l'équation diophantienne

$$X^{ap} + Y_0^p = BZ^q. \tag{5.5}$$

Si $q \neq p$, alors $X = \pm 1$, $Z = 0$. Si $q = p$, on a au plus comme solution $X^a = -Y_0$, $Z = 0$.

Remarque 5.1.5 *Les conditions 2, 3 et 4 du corollaire sont des conditions particulièrement faibles : il a été vérifié récemment que h_p^+ est premier à p si $p < 7.10^6$; on conjecture (conjecture de Vandiver) que h_p^+ est en fait premier à p pour tout nombre premier p.*

Si $p < 4.10^6$,la simultanéité des congruences $2^{p-1} \equiv 1 \bmod p^2$, $3^{p-1} \equiv 1 \bmod p^2$ n'a pas lieu. Notons que les entiers 1093 et 3511 sont les seuls nombres premiers plus petits que 125.10^{13} et solutions de la congruence $2^{p-1} \equiv 1 \bmod p^2$.

Enfin, si $p < 12.10^6$, aucun des nombres de Bernoulli d'indice pair compris entre 2 et $p - 3$ n'a un numérateur divisible par p^3.

On montrera à la fin de la preuve du corollaire, que la condition $p \nmid h_p^+$ et celle portant sur les nombres de Bernoulli peuvent être remplacées par la seule condition $\iota(p) = 0$, $\iota(p)$ étant l'indice d'irrégularité de p.

Corollaire 5.1.6 *Soit B un entier tel que $(Y_0\Psi(B), p) = 1$. Soient $s, t \geq 1$ deux entiers. On considère deux suites de nombres premiers fixés distincts de p : $l_1, \ldots, l_s$, et $l'_1, \ldots, l'_t$. On pose $L = l_1 \ldots l_s$. On suppose que pour tout i, on a $l'_i \neq 1 \bmod p$, et que l'ordre de p modulo L est premier à p. Supposons que les conditions suivantes soient satisfaites :*

1. $\left(\frac{B}{2}\right)^{p-1} \neq 1 \bmod p^2$,
2. $p \nmid B \cdot h_p^+$,
3. $r_p \leq \sqrt{p} - 1$ *ou bien parmi les entiers* $2^{p-1} - 1$, $3^{p-1} - 1$, *l'un des deux n'est pas divisible par* p^2.

Il n'existe pas d'entiers $X, a_1, \ldots, a_s, a'_1, \ldots, a'_t$ *tels que* $\left(X, Y_0, l_1^{a_1} \ldots l_s^{a_s} l_1^{'a'_1} \ldots l_t^{'a'_t}\right)$ *soit une solution primitive de*

$$X^p + Y_0^p = B l_1^{pa_1} \ldots l_s^{pa_s} l_1^{'pa'_1} \ldots l_t^{'pa'_t}. \tag{5.6}$$

Enfin, la démonstration du corollaire précédent, permettra de montrer le corollaire suivant :

Corollaire 5.1.7 *Soit* $p > 3$ *un nombre premier,* y_0 *un entier impair premier à* p *tel que* $|y_0| \leq \frac{p}{19}$. *Supposons qu'il existe des entiers* x, z *tels que*

$$\frac{x^p + y_0^p}{x + y_0} = z^{p^2}, \quad (x, y_0, z) = 1, \quad 2|x. \tag{5.7}$$

Alors, pour tout facteur premier r *de* y_0, *on a* $r^{p-1} \equiv 1 \bmod p^3$. *De plus, de deux choses l'une, soit* $2^{p-1} \equiv 1 \bmod p^3$, *soit* $p|h_p^+$. *En particulier,* $p > 7.10^6$.

Comme application, on donne l'exemple suivant, dans lequel on applique le corollaire (5.1.4) à une classe de nombres premiers distincts p, q vérifiant toujours la condition $q \nmid h_p^-$:

Exemple 5.1.8 *Rappelons que l'on désigne par* $\wp$ *l'ensemble des nombres premiers et par* $\wp'$ *l'ensemble des nombres premiers qui sont congrus à* 3 *modulo* 4. *On a adopté les notations suivantes* ($A > 0$ *entier) :*

$$\Pi_t = \left\{ p \in \wp : \quad \frac{p-1}{2^t} \in \wp' \right\}, \quad \Pi_t(A) = \{ p \in \Pi_t : p \geq A \}.$$

Si un nombre premier p *est un élément de* Π_t *pour un certain* $t \geq 1$, *on pose* $\tilde{p} = \frac{p-1}{2^t}$, *qui est donc un nombre premier. On a montré au paragraphe 2.2.2 la proposition*

Proposition 5.1.9 *Soit* $t \geq 1$ *un entier. Il existe une constante effective* $C(t)$ *ne dépendant que de* t *(avec* $C(1) = C(2) = 7$*), telle que si* $p \in \Pi_t(C(t))$, *alors,* $\tilde{p} \nmid h_p^-$.

Fixons deux entiers t, B *tels que* $t \geq 1$. *Soit* p *un nombre premier tel que* $p \in \Pi_t(C(t))$ *et* $(\Psi(B), p) = 1$. *L'équation diophantienne*

$$X^{2p} - 1 = B Z^{\tilde{p}}, \tag{5.8}$$

admet pour seules solutions entières $X = \pm 1$, $Z = 0$.

Autre exemple :

Exemple 5.1.10 *Soient $l, p > 3$ deux nombres premiers impairs tels que p soit une racine primitive modulo l, $a \geq 3$ un entier, y_0 un entier impair premier à p tel que $|y_0| \leq \frac{p}{19}$. Supposons qu'il existe des entiers x, v tels que*

$$\frac{x^{ap} + y_0^p}{x^a + y_0} = l^v, \quad (x, y_0, l) = 1, \quad p|x. \tag{5.9}$$

Alors $p|v$. En particulier, $p|h_p^+$, donc $p > 7.10^6$.

Pour la suite, on se fixe un nombre premier impair p ainsi que ζ une racine primitive p-ième de l'unité. Rappelons que p est totalement ramifié dans l'extension $\mathbb{Q}(\zeta)/\mathbb{Q}$. L'unique premier de $\mathbb{Z}[\zeta]$ au-dessus de p est principal, engendré par $1 - \zeta$.

5.2 Sur l'anneau $\mathbb{F}_p[G]$.

Le groupe des classes de $\mathbb{Q}(\zeta)$ est noté $\mathcal{C}_p$. L'ensemble des éléments d'ordre divisant p de $\mathcal{C}_p$ est noté $\mathcal{A}$. **On suppose à partir de maintenant que $p > 3$.** On a déjà posé au chapitre 4

$$P = \{1, \ldots, p-1\}, \quad \mathcal{B} = \{i \in P; p|B_{p-i}, \quad i \equiv 1 \bmod 2\}.$$

L'ordre de $\mathcal{B}$ est l'indice d'irrégularité du nombre premier p, c'est à dire $\iota(p)$. Posons

$$\mathcal{B}' = \{i \in P; i \in \mathcal{B} \quad ou \quad p - i \in \mathcal{B}\},$$

puis

$$\mathbf{A}_1 = \sum_{i \in P - \mathcal{B}'} \epsilon_i \mathbb{F}_p[G],$$

où $\epsilon_i = -\sum_{\sigma \in G} \omega(\sigma)^i \sigma^{-1} \in \mathbb{F}_p[G]$, ω étant le caractère cyclotomique de $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$.

Montrons que $\mathbf{A}_1$ contient au moins un élément de la forme ϵ_{p-l} où l est un entier impair, $l \neq 1$. Soit P' les entiers impairs contenus dans P. Comme $\iota(p) \leq \frac{p+1}{4}$ (corollaire (4.3.9)), on a $|P' - \mathcal{B}| \geq \frac{p-1}{2} - \frac{p+1}{4} = \frac{p-3}{4} \geq 2$ si $p \geq 11$, c'est à dire $|P' - \mathcal{B}| \geq 2$ si $p > 7$. Il existe donc au moins un entier impair $l \neq 1$ tel que $l \in P' - \mathcal{B}$ si $p > 7$. L'idempotent ϵ_{p-l} est alors un élément de $\mathbf{A}_1$.

En effet, l'entier $p - l$ n'est pas un élément de $\mathcal{B}'$: $p - l$ est pair, donc n'est pas un élément de $\mathcal{B}$, et l'entier $p - (p - l) = l$ n'est pas un élément de $\mathcal{B}$ par construction. Ainsi, l'idempotent ϵ_{p-l} est bien un élément de $\mathbf{A}_1$. Si $p = 5$ ou $p = 7$, alors $\mathcal{B}$ est l'ensemble

vide. Comme P contient alors un entier impair $l \neq 1$, il existe donc encore dans ces cas, un entier l impair, $l \neq 1$ tel que ϵ_{p-l} soit un élément de $\mathbf{A}_1$.

De plus, remarquons, j étant la conjugaison complexe, que $j\epsilon_{p-l} = \epsilon_{p-l}$. En effet, on a

$$\begin{aligned} j\epsilon_{p-l} &= -\sum_{t=1}^{p-1} \omega(\sigma_t)^{p-l} j\sigma_t^{-1} = -\sum_{t=1}^{p-1} \omega(\sigma_t)^{p-l}\sigma_{-t}^{-1} \\ &= -\omega(j)^{p-l}\sum_{t=1}^{p-1} \omega(\sigma_{-t})^{p-l}\sigma_{-t}^{-1} = (-1)^{p-l}\epsilon_{p-l} = \epsilon_{p-l}, \end{aligned}$$

$p-l$ étant pair. Ainsi, il existe un élément $\theta_0 = \epsilon_{p-l}$ de $\mathbf{A}_1$, tel que $j\theta_0 = \theta_0$, et qui n'est pas de la forme $a\mathcal{N}$, $a \in \mathbb{F}_p$ (en effet $\mathcal{N} = -\epsilon_{p-1}$ tandis que $l \neq 1$). De plus, la norme $\mathcal{N}$ relative à l'extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ est un élément de $\mathbf{A}_1$. En effet, si ce n'était pas le cas, comme $\mathcal{N} = -\epsilon_{p-1}$, l'entier $p-1$ serait un élément de $\mathcal{B}'$, c'est à dire $1 \in \mathcal{B}$, c'est à dire

$$p|B_{p-1}.$$

Or cette dernière propriété n'a pas lieu par le lemme suivant due à Clausen et Von Staudt :

Lemme 5.2.1 *Soit p un nombre premier impair et k un entier divisible par $p-1$. On a alors*

$$pB_k \equiv -1 \bmod p.$$

Enfin, remarquons que l'élément ϵ_{p-l} annihile le groupe des racines p-ième de l'unité. En effet, comme $j\epsilon_{p-l} = \epsilon_{p-l}$, on a

$$\zeta^{-\epsilon_{p-l}} = \overline{\zeta}^{\epsilon_{p-l}} = \zeta^{j\epsilon_{p-l}} = \zeta^{\epsilon_{p-l}},$$

d'où $\zeta^{2\epsilon_{p-l}} = 1$, c'est à dire $\zeta^{\epsilon_{p-l}} = 1$.

Pour la suite, on adopte la notation suivante : si $\theta = \sum_{k=1}^{p-1} c_k\sigma_k \in \mathbb{F}_p[G]$, on pose

$$l(\theta) = \sum_{k=1}^{p-1} c_k \in \mathbb{F}_p.$$

Le groupe $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times$ étant cyclique, il vient

$$l(\theta_0) \equiv \sum_{t=1}^{p-1} t^{p-l} \equiv 0 \bmod p.$$

On a ainsi démontré le lemme suivant :

Lemme 5.2.2 *Il existe un élément θ_0 de $\boldsymbol{A}_1 - \{0\}$ tel que $j\theta_0 = \theta_0$, $\zeta^{\theta_0} = 1$ et $l(\theta_0) \equiv 0 \bmod p$. La norme $\mathcal{N}$ est également un élément de $\boldsymbol{A}_1$. De plus, la famille $(\mathcal{N}, \theta_0)$ est $\mathbb{F}_p$-libre.*

Soit s la surjection canonique $s : \mathbb{Z}[G] \twoheadrightarrow \mathbb{F}_p[G]$ qui consiste à réduire modulo p les coefficients des éléments de $\mathbb{Z}[G]$.

Lemme 5.2.3 *Il existe un élément $\Theta = \sum_{c=1}^{p-1} n_c\sigma_c$ de $\mathbb{N}[G] - \{0\}$ tel que $n_c < p$ pour tout c, $s(\Theta) \in \boldsymbol{A}_1 - \{0\}$, dont le poids $W(\Theta)$ est divisible par p et majoré par $\frac{p(p-1)}{2}$. De plus, Θ n'est pas un multiple entier de la norme $\mathcal{N}$ et il vérifie les propriétés*

$$j\Theta = \Theta, \quad \zeta^{\Theta} = 1.$$

Preuve Fixons un élément $\theta_0 \in \mathbb{F}_p[G]$ donné par le lemme (5.2.2). Soit $\Theta_1 = \sum_c n_c\sigma_c \in \mathbb{N}[G]$ l'unique relèvement[3] de θ_0 par s tel que $n_c < p$, pour tout c. Comme $s(\Theta_1)$ est invariant par multiplication par j, on a en particulier

$$n_c \equiv n_{p-c} \bmod p.$$

Comme $0 \leq n_c, n_{p-c} < p$, on a $n_c = n_{p-c}$, c'est à dire $j\Theta_1 = \Theta_1$.

Par construction, le poids de Θ_1 est divisible par p, puisque sa réduction modulo p, c'est à dire $\theta_0 = s(\Theta_1)$ vérifie $l(\theta_0) \equiv 0 \bmod p$. Soit $\Theta_1' = p\mathcal{N} - \Theta_1$. Comme les coefficients n_c de Θ_1 sont compris (au sens large) entre 0 et $p-1$, on a $\Theta_1' \in \mathbb{N}[G] - \{0\}$. De plus $s(\Theta_1') = -\theta_0 \in \mathbf{A}_1 - \{0\}$. Par construction, le poids de Θ_1' est divisible par p, Θ_1' étant somme de deux éléments de poids divisible par p. La somme de Θ_1 et de Θ_1' vaut $p\mathcal{N}$, de poids $p(p-1)$. Ainsi, les éléments Θ_1 et Θ_1' ont des poids dont la somme vaut $p(p-1)$. Nécessairement, l'un des deux est de poids au plus $\frac{p(p-1)}{2}$: on note cet élément $\Theta \in \mathbb{N}[G] - \{0\}$. Cet élément est de poids divisible par p (car les poids de Θ_1 et Θ_1' le sont). Comme $j\Theta_1 = \Theta_1$ et $j\Theta_1' = \Theta_1'$, on a aussi $j\Theta = \Theta$. Si Θ était un multiple entier de la norme, il existerait un entier m tel que $\Theta = m\mathcal{N}$. En appliquant s à cette relation on obtiendrait que θ_0 serait de la forme $a\mathcal{N}$, $a \in \mathbb{F}_p$, ce qui n'est pas. Il reste à montrer que $\zeta^{\Theta} = 1$. Or, $\zeta^{\theta_0} = 1$. Par construction, on a donc encore $\zeta^{\Theta} = 1$. Enfin, comme $s(\Theta_1), s(\Theta_1') \in \mathbf{A}_1 - \{0\}$, on a bien $s(\Theta) \in \mathbf{A}_1 - \{0\}$.□

5.2.1 Nombres p-primaires et ramification.

Théorème 5.2.4 *Soit K un corps de nombres et soit μ_p le groupe des racines p-ième de l'unité. On se fixe $\alpha \in K^\times - (K^\times)^p$ premier à p et on pose $L = K(\alpha^{1/p})$. Soit v une place*

[3] c'est à dire $s(\Theta_1) = \theta_0$

finie de K au-dessus de p, et soit e_v l'indice de ramification de v dans $K/\mathbb{Q}(\mu_p)$. On a alors les assertions suivantes :

1. *La place v est ramifiée dans L/K si et seulement si la congruence*

$$\frac{\alpha}{x^p} \equiv 1 \bmod \Pi^{pe_v}$$

   n'a aucune solution en $x \in K_v^\times$, Π paramètre local de K_v.

2. *Si v est non ramifiée, alors, elle se décompose totalement si et seulement si $\overline{\alpha} \in K_v^{\times p}$.*

3. *La condition précédente peut aussi se vérifier comme suit : posons*

$$\frac{\alpha}{x^p} = 1 + p(1-\zeta)y$$

   avec $y \in K^\times$. Alors $\overline{\alpha} \in K_v^{\times p}$ si et seulement si $\boldsymbol{Tr}_{F_v/\mathbb{F}_p}(\overline{y}) = 0$.

Preuve Le corps local K_v a une unique extension non ramifiée de degrés p, qui s'obtient naturellement de manière cyclotomique comme relèvement de corps résiduel. En fait, on peut aussi la réaliser comme extension de type Kummer. Plus précisément, on a le lemme suivant :

Lemme 5.2.5 *Soit $\kappa = 1 + p(1-\zeta)\eta$ où η est un entier de K_v. Alors $K_v(\kappa^{1/p})/K_v$ est non ramifiée. Elle est de degrés p, si et seulement si $\boldsymbol{Tr}_{F_v/\mathbb{F}_p}(\overline{\eta}) \neq 0$.*

Preuve (du lemme) : Posons $x = \kappa^{1/p} - 1$, et soit $y = \frac{x}{1-\zeta}$, racine d'un polynôme P de la forme :

$$P = Y^p + \sum_{i=2}^{p-1} \pi_i Y^i + \frac{p}{(1-\zeta)^{p-1}} Y - \frac{p\eta}{(1-\zeta)^{p-1}}$$

où les π_i sont des multiples de $1-\zeta$ dans $\mathbb{Z}[\zeta]$. En écrivant p sous la forme $p = \prod_{i=1}^{p-1}(1-\zeta^i)$, on en déduit, en appliquant le théorème de Wilson, que l'on a :

$$\frac{p}{(1-\zeta)^{p-1}} \equiv -1 \bmod (1-\zeta).$$

Donc, en tant qu'élément de $F_v[Y]$, F_v corps résiduel de K_v , on a $\overline{P} = Y^p - Y + \overline{\eta}$. C'est donc un polynôme d'Artin-Schreier. En particulier, si a est une racine de $\overline{P}$ dans $\overline{\mathbb{F}_p}$, les racines de $\overline{P}$ valent $a + b$, $b \in \mathbb{F}_p$. En effet, on a

$$\begin{aligned} \overline{P}\,(a+b) &= (a+b)^p - (a+b) + \overline{\eta} \\ &= a^p - a + \overline{\eta} + b^p - b = 0, \end{aligned}$$

d'où le résultat vu que $\overline{P}$ a au plus p racines. Le lemme de Hensel montre donc que soit le polynôme P est irréductible dans $K_v[Y]$, soit il y est scindé, cette dernière condition ayant lieu si et seulement si $\overline{P}$ admet une racine dans F_v, c'est à dire $\overline{\eta} \in \{t^p - t, t \in F_v\}$. Or

$$Ker(\mathbf{Tr}_{F_v/\mathbb{F}_p}) = \{t^p - t, t \in F_v\}.$$

En effet, $\mathbf{Tr}_{F_v/\mathbb{F}_p}$ étant surjective, $Ker(\mathbf{Tr}_{F_v/\mathbb{F}_p})$ est de dimension $d-1$ sur $\mathbb{F}_p$, avec d degrés de $F_v/\mathbb{F}_p$. Soit $\wp = Id - \mathcal{F}$, $\mathcal{F}$ Frobenius de $F_v/\mathbb{F}_p$. Le $\mathbb{F}_p$-espace vectoriel $\wp(F_v)$ a pour dimension $d-1$, le noyau de $\wp$ étant $\mathbb{F}_p$. Comme $\wp(F_v) \subset Ker(\mathbf{Tr}_{F_v/\mathbb{F}_p})$, ils sont donc égaux, ayant même dimension sur $\mathbb{F}_p$. Ainsi, P est scindé dans $K_v[Y]$ ssi $\mathbf{Tr}_{F_v/\mathbb{F}_p}(\overline{\eta}) = 0$. Si ce n'est pas le cas, P est irréductible dans $K_v[Y]$ et l'extension $K_v(\kappa^{1/p})/K_v$ est de degrés p, qui est aussi le degrés de l'extension de leurs corps résiduels ; l'extension $K_v(\kappa^{1/p})/K_v$ est alors de degrés p non ramifiée.□ Donc, connaissant le corps résiduel $F_v/\mathbb{F}_p$, pour définir l'extension non ramifiée de degrés p, il suffit de poser $\kappa_0 = 1 + p(1-\zeta)\eta_v^0$, avec $\mathbf{Tr}(\overline{\eta_v^0}) = 1$. Rappelons qu'un tel élément existe car la trace est surjective, pour une extension de corps finis. Revenons maintenant à l'extension $K_v(\alpha^{1/p})/K_v$. Par unicité, si cette extension est non ramifiée de degrés p, alors les extensions $K_v(\alpha^{1/p})/K_v$ et $K_v(\kappa_0^{1/p})/K_v$ sont Kummer équivalentes, c'est à dire qu'il existe $x \in K_v^\times$, tel que $\alpha = x^p \kappa_0^n$ avec $n \in \mathbb{Z}$, ce qui implique que la congruence suivante :

$$\frac{\alpha}{x^p} \equiv 1 \bmod p\pi$$

avec $\pi = 1 - \zeta$, a une solution dans le corps K_v. Il n'y a rien à faire si $K_v(\alpha^{1/p})/K_v$ est triviale. Inversement, si une telle solution x existe, alors, $\frac{\alpha}{x^p} = 1 + p\pi\eta$, avec η entier de K_v et le lemme nous dit que l'extension $K(\alpha^{1/p})/K$ est non ramifiée. Le théorème est prouvé. (Comme $p = \pi^{p-1}$ à unité près, on a $p\pi = \Pi^{pe_v}$ à unité près).□

Definition 5.2.6 *Soit p un nombre premier impair, et soit K un corps de nombre, contenant ζ, avec ζ racine primitive p-ième de l'unité. On pose $\pi = 1 - \zeta$. Soit aussi $\alpha \in K^* - K^p$, qui est premier à p. On dit que α est un nombre p-primaire si et seulement si l'équation $x^p \equiv \alpha \bmod p\pi$ admet une solution dans K^*.*

En particulier

Corollaire 5.2.7 *Soient K un corps de nombres et p un nombre premier. Supposons que K contienne le groupe des racines p-ième de l'unité. Soit $\alpha \in K$ un nombre p-primaire. Alors l'extension $K(\alpha^{1/p})/K$ est non ramifiée en p.*

Proposition 5.2.8 *Soit p un nombre premier, $\mathcal{K}$ une extension finie de $\mathbb{Q}_p$, n un entier premier à p et $x \in \mathcal{K}^*$. Alors, l'extension $\mathcal{K}(x^{1/n})/\mathcal{K}$ est non ramifiée si et seulement si $x \in U_{\mathcal{K}}\mathcal{K}^{*n}$, $U_{\mathcal{K}}$ étant le groupe des unités de $\mathcal{K}$.*

Preuve Supposons que $x = uy^n$, avec u unité de K. On a $\mathcal{K}(x^{1/n}) = \mathcal{K}(u^{1/n})$. Soit κ', le corps de décomposition du polynôme $X^n - u$ sur le corps résiduel κ de $\mathcal{K}$. Soit $\mathcal{K}'$ l'extension (à isomorphisme près) non ramifiée de $\mathcal{K}$ de corps résiduel κ'. Comme $(n, p) = 1$, par le lemme de Hensel, le corps $\mathcal{K}'$ contient $K(u^{1/n})$, qui est donc non ramifiée. Réciproquement, supposons que l'extension $\mathcal{K}(x^{1/n})/\mathcal{K}$ soit non ramifiée. Soit $\mathcal{L} = \mathcal{K}(x^{1/n})$. Soit π un paramètre local de $\mathcal{K}$. On pose $x = u\pi^r$. On a

$$\nu_{\mathcal{L}}(x^{1/n}) = \frac{1}{n}\nu_{\mathcal{K}}(x) = \frac{r}{n} \in \mathbb{Z},$$

c'est à dire $n|r$, c'est à dire $x = uy^n$, $u \in U_{\mathcal{K}}$.□ En particulier, si K est un corps de nombres et $a \in K$ tel que $(a) = I^n$, pour un certain idéal de K, alors l'extension $K(a^{1/n})/K$ est au plus ramifiée en les diviseurs premiers de n.

Definition 5.2.9 *Soient K un corps de nombres et p un nombre premier. Supposons que K contienne le groupe des racines p-ième de l'unité. Soit $\alpha \in K$. On dit que α est un nombre p-primaire singulier ssi α est p-primaire et si l'idéal (α) est la puissance p-ième d'un autre idéal de K.*

Ce qui précède montre

Corollaire 5.2.10 *Soient K un corps de nombres et p un nombre premier. Supposons que K contienne le groupe des racines p-ième de l'unité. Soit $\alpha \in K$ un nombre p-primaire singulier. Alors l'extension $K(\alpha^{1/p})/K$ est non ramifiée.*

En particulier

Corollaire 5.2.11 *Soient K un corps de nombres et p un nombre premier. Supposons que K contienne le groupe des racines p-ième de l'unité. Soit $\alpha \in K$ une unité p-primaire. Alors l'extension $K(\alpha^{1/p})/K$ est non ramifiée.*

Tous ces résultats seront utilisés sans référence particulière dans la suite.

5.2.2 Notion de support.

Rappelons que $\mathcal{A}$ est l'ensemble des classes du groupe $\mathcal{C}_p$ qui sont d'ordre 1 ou p. Le $\mathbb{F}_p$-module $\mathbb{F}_p[G]$ agit naturellement sur $\mathcal{A}$. On pose :

$$Supp\,(\mathcal{A}) = \{i \in P : \mathcal{A}^{\epsilon_i} \neq \{1\}\}.$$

Soient E_p le groupe des unités p-primaires de $\mathbb{Z}[\zeta]$, et E'_p le sous-groupe formé des unités p-primaires qui sont des puissances p-ième dans $\mathbb{Z}[\zeta]$. De même, le $\mathbb{F}_p$-module $\mathbb{F}_p[G]$ agit naturellement sur le groupe quotient E_p/E'_p. On pose :

$$Supp\,(E_p) = \left\{i \in P : \left(E_p/E'_p\right)^{\epsilon_i} \neq \{1\}\right\}.$$

Proposition 5.2.12 *(Mihăilescu, [53]) On a*

$$Supp\,(\mathcal{A}) \cup Supp\,(E_p) \subseteq \mathcal{B}'.$$

Preuve Commençons par montrer que $Supp\,(\mathcal{A}) \subseteq \mathcal{B}'$. Soit donc $i \in P$ tel que $\mathcal{A}^{\epsilon_i} \neq \{1\}$. Si i est impair, par le théorème d'Herbrand (voir [77]) p divise B_{p-i}, c'est à dire $i \in \mathcal{B} \subseteq \mathcal{B}'$. Supposons i pair. Soit $j = p - i$. Comme $\mathcal{A}^{\epsilon_i} \neq \{1\}$, le p-rang de $\mathcal{A}^{\epsilon_i}$ vaut au moins 1. Par le théorème 10.9 de [77], il en est de même pour $\mathcal{A}^{\epsilon_j}$. Le théorème d'Herbrand montre donc que $p|B_{p-j}$, c'est à dire $p - i = j \in \mathcal{B}$, c'est à dire $i \in \mathcal{B}'$. On a bien montré que $Supp\,(\mathcal{A}) \subseteq \mathcal{B}'$.

Montrons que $Supp\,(E_p) \subseteq \mathcal{B}'$. Soit $i \in Supp\,(E_p)$. Par définition, il existe une unité p-primaire u de l'anneau $\mathbb{Z}[\zeta]$ telle que u^{ϵ_i} n'est pas une puissance p-ième dans $\mathbb{Z}[\zeta]$: en particulier u non plus n'est pas une puissance p-ième. Soit $\mathbb{L} = \mathbb{Q}(\zeta, u^{\frac{1}{p}})$. Comme u est une unité p-primaire, c'est en particulier un nombre p-primaire singulier. L'extension $\mathbb{L}/\mathbb{Q}(\zeta)$ est donc non ramifiée en toute place. L'extension $\mathbb{L}/\mathbb{Q}(\zeta)$ est donc une extension abélienne non ramifiée, de degrés p, car u n'est pas une puissance p-ième dans l'anneau $\mathbb{Z}[\zeta]$. Soit $\mathbb{L}'$ l'extension maximale non ramifiée p-élémentaire de $\mathbb{Q}(\zeta)$. C'est une extension de type Kummer car son groupe de Galois est d'exposant p. Il existe donc un sous-groupe fini B de $\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta)^{\times p}$ contenant la classe de u, tel que $\mathbb{L}' = \mathbb{Q}(\zeta, B^{\frac{1}{p}})$. La notation précédente signifie que $\mathbb{L}'$ s'obtient en adjoingnant au corps $\mathbb{Q}(\zeta)$, les racines p-ième d'un système de représentants de B, système auquel u appartient.

Lemme 5.2.13 *(voir [77], preuve du théorème* 10.9*.) Soient i_0, j_0 des entiers tels que $i_0 + j_0 \equiv 1 \bmod (p-1)$. On a l'isomorphisme de groupes suivant :*

$$B^{\epsilon_{i_0}} \simeq \left(\frac{A}{A^p}\right)^{\epsilon_{j_0}}, \tag{5.10}$$

où A est le p-sous groupe de Sylow de $\mathcal{C}_p$.

Supposons d'abord que i soit pair. Comme u^{ϵ_i} n'est pas une puissance p-ième de l'anneau $\mathbb{Z}[\zeta]$ et vu que u est un élément du système de représentants de B, le groupe B^{ϵ_i} est donc non trivial. L'isomorphisme (5.10) appliqué avec $i_0 = i$ et $j_0 = p - i$ montre donc en particulier que $A^{\epsilon_{j_0}}$ est non trivial. Comme $j_0 = p - i$ est impair car i pair, le théorème d'Herbrand montre alors $p|B_{p-j_0}$, c'est à dire $j_0 \in \mathcal{B}$, c'est à dire $p - i \in \mathcal{B}$, autrement dit $i \in \mathcal{B}'$.

Supposons maintenant que i soit impair. Comme avant, le groupe $A^{\epsilon_{p-i}}$ est non trivial. Comme c'est un p-groupe, il est donc de p-rang au moins 1. L'entier $p - i$ étant pair, le théorème 10.9 de [77] montre alors que le p-rang de A^{ϵ_i} vaut au moins 1 : le groupe A^{ϵ_i}

est donc non trivial lui aussi. L'entier i étant impair, le théorème d'Herbrand montre que $p|B_{p-i}$, c'est à dire $i \in \mathcal{B} \subset \mathcal{B}'$. ■

5.2.3 Action de $\mathbf{A}_1$ sur $\mathcal{A}$.

Rappelons que $\mathfrak{p} = (1-\zeta)$ est l'unique premier de $\mathbb{Q}(\zeta)$ au-dessus de p. On démontre la proposition suivante, qui servira lors de la preuve du théorème (5.1.2) :

Proposition 5.2.14 *Soit $\mathfrak{a}$ un idéal de l'anneau $\mathbb{Z}[\zeta]$, premier à $\mathfrak{p}$. On suppose qu'il existe $\alpha \in \mathbb{Z}[\zeta]$ vérifiant $\mathfrak{a}^p = (\alpha)$. Soit $\Theta = \sum_c n_c\sigma_c \in \mathbb{N}[G]$ un relèvement quelconque par l'application s d'un élément $\theta \in \boldsymbol{A}_1$. Il existe alors une unité $\epsilon \in \mathbb{Z}[\zeta]^\times$ et $\nu \in \mathbb{Z}[\zeta]$ tels que*

$$\alpha^\Theta = \epsilon\nu^p.$$

De plus, si α est p-primaire, il existe un unique $\nu[\Theta] \in \mathbb{Z}[\zeta]$ tel que

$$\begin{cases} \alpha^\Theta = \nu[\Theta]^p, \\ \nu[\Theta] \equiv \alpha^\Theta \bmod (1-\zeta)^2. \end{cases}$$

Preuve Supposons d'abord que $\theta = \epsilon_k$, $\Theta = \epsilon'_k \in \mathbb{N}[G]$ avec $k \in P - \mathcal{B}'$ et $s(\epsilon'_k) = \epsilon_k$. L'idéal $\mathfrak{a}$ est d'ordre 1 ou p. Par la proposition (5.2.12), ϵ_k annihile les éléments d'ordre 1 ou p de $\mathcal{C}_p$. Par définition de l'action de ϵ_k sur $\mathcal{C}_p$, cela signifie qu'il existe[4] $\nu \in \mathbb{Z}[\zeta]$ tel que $\mathfrak{a}^{\epsilon'_k} = (\nu)$. En prenant la puissance p-ième de l'égalité précédente, on déduit qu'il existe une unité $\epsilon \in \mathbb{Z}[\zeta]$ telle que $\alpha^{\epsilon'_k} = \epsilon\nu^p$. Le cas général s'en déduit par linéarité : en effet, comme $\theta \in \mathbf{A}_1$, c'est une combinaison linéaire de ϵ_k, k parcourant $P - \mathcal{B}'$.

Supposons que α soit un nombre p-primaire. Soient $k \in P - \mathcal{B}'$ et $\epsilon'_k \in \mathbb{N}[G]$ tels que $s(\epsilon'_k) = \epsilon_k$. Par ce qui précède, il existe $\nu \in \mathbb{Z}[\zeta]$ et $\epsilon \in \mathbb{Z}[\zeta]^\times$ tels que

$$\alpha^{\epsilon'_k} = \epsilon\nu^p. \tag{5.11}$$

Appliquons ϵ'_k à l'identité (5.11) : comme $\epsilon_k^2 = \epsilon_k$, on a $\epsilon_k'^2 \equiv \epsilon'_k \bmod p$, d'où l'existence de $\nu_1 \in \mathbb{Z}[\zeta]$ tel que

$$\alpha^{\epsilon'_k} = \epsilon^{\epsilon'_k}\nu_1^p. \tag{5.12}$$

Comme α est un nombre p-primaire, il en est de même pour $\alpha^{\epsilon'_k}$. L'unité ϵ, par (5.11) est donc p-primaire. Par la proposition (5.2.12), $\epsilon^{\epsilon'_k}$ est donc une puissance p-ième. La relation (5.12) montre donc que $\alpha^{\epsilon'_k}$ est une puissance p-ième : il existe $\nu_2 \in \mathbb{Z}[\zeta]$ tel que $\alpha^{\epsilon'_k} = \nu_2^p$. Par linéarité, on a donc montré qu'il existe un entier algébrique ν tel que

$$\alpha^\Theta = \nu^p.$$

[4] ν est un entier algébrique et pas seulement un nombre algébrique car ϵ'_k est à coefficients positifs.

Comme α est p-primaire et p totalement ramifié dans $\mathbb{Q}(\zeta)/\mathbb{Q}$, il existe en particulier $\alpha_0 \in \mathbb{Z}$ premier à p tel que $\alpha^\Theta \equiv \alpha_0^p \bmod p(1-\zeta)$, donc un entier α_0 premier à p tel que $\alpha^\Theta \equiv \alpha_0 \bmod (1-\zeta)^2$. Soit $\nu_0 \in \mathbb{Z}$ tel que $\nu \equiv \nu_0 \bmod (1-\zeta)$. On a alors

$$\alpha^\Theta \equiv \nu_0^p \equiv \nu_0 \bmod (1-\zeta).$$

Comme $\alpha^\Theta \equiv \alpha_0 \bmod (1-\zeta)$, et vu que α_0, ν_0 sont des entiers, il vient $\alpha_0 \equiv \nu_0 \bmod p$, donc $\alpha_0 \equiv \nu_0 \bmod (1-\zeta)^2$.

Il existe un entier l tel que $\zeta^l \nu \equiv \alpha_0 \bmod (1-\zeta)^2$. En effet, on a le lemme suivant :

Lemme 5.2.15 *Soit $\alpha \in \mathbb{Z}[\zeta]$, α_0 un entier premier à p, $\alpha \equiv \alpha_0 \bmod (1-\zeta)$. Il existe une racine de l'unité u, telle que $u\alpha \equiv \alpha_0 \bmod (1-\zeta)^2$.*

Preuve Soit α_1 un entier tel que $\alpha \equiv \alpha_0 + \alpha_1(1-\zeta) \bmod (1-\zeta)^2$. L'entier α_0 etant premier à p, soit c un entier fixé tel que $c \equiv \frac{\alpha_1}{\alpha_0} \bmod p$.

$$\zeta^c = (1-(1-\zeta))^c \equiv 1 - c(1-\zeta) \bmod (1-\zeta)^2.$$

On a alors

$$\zeta^c\alpha \equiv (1-c(1-\zeta))(\alpha_0 + \alpha_1(1-\zeta)) \equiv \alpha_0 + (\alpha_1 - c\alpha_0)(1-\zeta) \bmod (1-\zeta)^2 \equiv \alpha_0 \bmod (1-\zeta)^2,$$

par choix de c, ce qu'on voulait.□

Comme $\nu \equiv \nu_0 \bmod (1-\zeta)$, le lemme précédent montre qu'il existe un entier l tel que $\zeta^l\nu \equiv \nu_0 \bmod (1-\zeta)^2$. Comme $\alpha_0 \equiv \nu_0 \bmod (1-\zeta)^2$, il existe bien un entier l tel que $\zeta^l\nu \equiv \alpha_0 \bmod (1-\zeta)^2$.

Soit $\nu' = \zeta^l\nu$. L'entier algébrique ν' vérifie, comme ν, l'égalité $\nu'^p = \alpha^\Theta$, mais vérifie en plus la congruence

$$\nu' \equiv \alpha_0 \equiv \alpha^\Theta \bmod (1-\zeta)^2.$$

Ainsi, si $\alpha \in \mathbb{Z}[\zeta]$ est un nombre p-primaire premier à p, il existe bien un entier algébrique $\nu_1 \in \mathbb{Z}[\zeta]$ tel que

$$\begin{cases} \alpha^\Theta = \nu_1^p, \\ \nu_1 \equiv \alpha^\Theta \bmod (1-\zeta)^2. \end{cases}$$

Un tel entier algébrique ν_1 est unique. En effet, s'il existe un deuxième entier algébrique ν_2 tel que

$$\begin{cases} \alpha^\Theta = \nu_2^p, \\ \nu_2 \equiv \alpha^\Theta \bmod (1-\zeta)^2, \end{cases}$$

il existerait en particulier un entier a tel que

$$\nu_1 = \zeta^a \nu_2.$$

Comme $\nu_1 \equiv \nu_2 \bmod (1-\zeta)^2$, on obtientrait $(\zeta^a - 1)\,\nu_2 \equiv 0 \bmod (1-\zeta)^2$, d'où $\zeta^a \equiv 1 \bmod (1-\zeta)^2$ car α donc ν_2 est premier à p. Le lemme (4.4.12) montre alors que $\zeta^a = 1$, donc que $\nu_1 = \nu_2$. ■

5.3 Equation de Nagell-Ljunggren diagonale générale.

Soit y_0 un entier fixé premier à p. Soient x, z deux entiers fixés tels que (x, z) soit solution de

$$\frac{x^p + y_0^p}{x + y_0} = p^e z^p, \quad (x, y_0, z) = 1.$$

Rappelons qu'alors $e \in \{0; 1\}$ avec $e = 1$ si et seulement si $p | x + y_0$. Supposons que l'entier $xy_0(x^2 - y_0^2)$ soit premier à p. Alors, la proposition 1 de [53] montre que $r^{p-1} \equiv 1 \bmod p^2$, pour tout facteur premier r de y_0 si $y_0 \neq \pm 1$. Il reste à étudier les trois cas $p|x$, $p|x - y_0$ et $p|x + y_0$.

Supposons d'abord que $p|x$. Soit $\alpha = \zeta x + y_0$. Soit θ un élément positif (définition (4.1.1)) de l'idéal de Stickelberger de $\mathbb{Q}(\zeta)$ tel que $\zeta^\theta \neq 1$. Un tel élément θ existe par le théorème (4.5.16). Comme le poids de θ est un multiple entier de $\frac{p-1}{2}$ (voir la proposition (4.1.6)), quitte à multiplier θ par 2, on peut supposer que son poids est divisible par $p-1$. Comme $p|x$, il vient alors

$$\alpha^\theta = (\zeta x + y_0)^\theta \equiv y_0^{W(\theta)} \bmod (1-\zeta)^2,$$

d'où $(\zeta x + y_0)^\theta \equiv 1 \bmod (1-\zeta)^2$ car $p - 1 | W(\theta)$.

D'un autre côté, par l'équation (5.2), il existe un idéal entier $\mathfrak{a}$ de $\mathbb{Z}[\zeta]$ tel que $(\zeta x + y_0) = \mathfrak{a}^p$. Le lemme (5.3.13) montre que les facteurs premiers de $\mathfrak{a}$ sont tous d'inertie 1 sur $\mathbb{Q}$. De plus, $(1 + j)\theta$ est un multiple entier positif de la norme relative à $\mathbb{Q}(\zeta)/\mathbb{Q}$: en particulier, $\alpha^\theta \alpha^{j\theta} \in \mathbb{Z}$. On peut donc appliquer la proposition (4.5.11) : il existe un entier de Jacobi β, un entier n et $\epsilon = \pm 1$ tels que

$$\alpha^\theta = \epsilon \zeta^n \beta^p.$$

Mais $\alpha^\theta \equiv 1 \bmod (1-\zeta)^2$, et par la relation d'Iwasawa (voir (4.9)) $\beta \equiv 1 \bmod (1-\zeta)^2$, d'où

$$\epsilon \zeta^n \equiv 1 \bmod (1-\zeta)^2.$$

Par le lemme (4.4.12), on doit donc avoir $\epsilon\zeta^n = 1$: il existe ainsi un entier de Jacobi β tel que

$$(\zeta x + y_0)^\theta = \beta^p.$$

Soit $r \in \mathbb{N}$ un facteur premier de y_0 si $y_0 \neq \pm 1$. Soit $\mathcal{R}$ un idéal premier de l'anneau $\mathbb{Z}[\zeta]$ au-dessus de r. Modulo $\mathcal{R}$, l'égalité précédente devient

$$(\zeta x)^\theta \equiv \beta^p \bmod \mathcal{R}.$$

De même, en travaillant avec l'idéal premier $\overline{\mathcal{R}}$ (conjugué complexe de $\mathcal{R}$), on a

$$(\zeta x)^\theta \equiv \beta^p \bmod \overline{\mathcal{R}},$$

d'où

$$\left(\overline{\zeta} x\right)^\theta \equiv \overline{\beta}^p \bmod \mathcal{R}.$$

On en déduit donc

$$\zeta^{2\theta} \equiv \left(\frac{\beta}{\overline{\beta}}\right)^p \bmod \mathcal{R}. \tag{5.13}$$

Or on dispose du lemme suivant :

Lemme 5.3.1 *([53]) Soit $r \neq p$ un nombre premier, $\mathcal{R}$ un idéal premier de $\mathbb{Z}[\zeta]$ au-dessus de r. Supposons qu'il existe un entier algébrique $\beta \in \mathbb{Z}[\zeta]$ tel que*

$$\zeta \equiv \beta^p \bmod \mathcal{R}.$$

On a alors $r^{p-1} \equiv 1 \bmod p^2$.

Preuve Comme $r \neq p$, on a $\beta^p \neq 1 \bmod \mathcal{R}$. En effet, sinon, on aurait $\zeta - 1 \equiv 0 \bmod \mathcal{R}$. Comme $\zeta - 1$ engendre l'unique premier de $\mathbb{Z}[\zeta]$ au-dessus de p, on aurait donc $(1-\zeta) = \mathcal{R}$, d'où $r = p$: contradiction. De plus, $\beta^{p^2} \equiv 1 \bmod \mathcal{R}$, car $\zeta^p = 1$. Par le théorème de Lagrange, p^2 divise donc $r^f - 1$, où f est l'inertie de r dans l'extension $\mathbb{Q}(\zeta)/\mathbb{Q}$. Comme $f|p-1$, on en déduit que $p^2|r^{p-1} - 1$.□ Comme $\zeta^{2\theta} \neq 1$, le lemme précédent appliqué à (5.13) montre que $r^{p-1} \equiv 1 \bmod p^2$.

Les cas où $p|x - y$ et $p|x + y$ se traitent de la même façon.

On vient donc de montrer que si $y_0 \neq \pm 1$, alors pour tout facteur premier r de y_0, on a $r^{p-1} \equiv 1 \bmod p^2$. En particulier,

$$y_0^{p-1} \equiv 1 \bmod p^2. \tag{5.14}$$

Supposons que $p \nmid x$ et montrons que $r^{p-1} \equiv 1 \bmod p^2$ pour tout facteur premier r de x. Si $p \nmid x^2 - y_0^2$, c'est une conséquence de la proposition 1 de [53]. Supposons que $p|x - y_0$. Soit θ un élément positif de poids divisible par $p-1$ de l'idéal de Stickelberger, tel que $\zeta^\theta \neq 1$. Soit $\alpha = \frac{x+\zeta y_0}{1+\zeta}$. Par l'équation (5.2), il existe un idéal $\mathfrak{a}$ de $\mathbb{Z}[\zeta]$ tel que

$$(x + \zeta y_0) = \mathfrak{a}^p.$$

Comme $1 + \zeta$ est une unité de $\mathbb{Z}[\zeta]$,

$$\left(\frac{x + \zeta y_0}{1 + \zeta}\right) = \mathfrak{a}^p.$$

Comme avant, il existe un entier de Jacobi β, $\epsilon = \pm 1$ et un entier l tels que

$$\frac{x + \zeta y_0}{1 + \zeta} = \epsilon \zeta^l \beta^p.$$

Comme $p|x - y_0$, $y_0^{p-1} \equiv 1 \bmod p^2$, et que le poids de θ est divisible par $p-1$, il vient modulo $(1-\zeta)^2$:

$$\left(\frac{x + \zeta y_0}{1 + \zeta}\right)^\theta \equiv \left(\frac{y_0 + \zeta y_0}{1 + \zeta}\right)^\theta \equiv y_0^\theta \equiv y_0^{W(\theta)} \equiv 1 \bmod (1-\zeta)^2.$$

La relation d'Iwasawa montre alors que $\left(\frac{x+\zeta y_0}{1+\zeta}\right)^\theta = \beta^p$. On termine la démonstration comme lors de l'étude précédente.

Supposons que $p|x + y_0$. De l'équation (5.2), il existe un idéal $\mathfrak{a}$ de $\mathbb{Z}[\zeta]$ tel que

$$\left(\frac{x + \zeta y_0}{\zeta - 1}\right) = \mathfrak{a}^p.$$

Soit θ comme avant. L'entier p divisant $x + y_0$, il vient modulo $(1-\zeta)^2$:

$$\left(\frac{x + \zeta y_0}{\zeta - 1}\right)^\theta \equiv y_0^\theta \equiv 1 \bmod (1-\zeta)^2.$$

Il existe donc un entier de Jacobi β tel que $\left(\frac{x+\zeta y_0}{\zeta-1}\right)^\theta = \beta^p$. La preuve se termine comme précédemment.

On se fixe pour la suite des entiers x, z qui constituent une solution de (5.3), avec $p|x$.

5.3.1 Séries de Mihăilescu.

Definition 5.3.2 *Soit $\Theta = \sum_{c=1}^{p-1} n_c \sigma_c$ un élément de $\mathbb{Z}[G]$. On appelle série de Mihăilescu associée à Θ, la série formelle notée $f[\Theta, T] \in \mathbb{C}[[T]]$ et définie par*

$$f[\Theta, T] = (1 + T\zeta)^{\Theta/p} = \prod_{c=1}^{p-1} (1 + T\zeta^c)^{n_c/p},$$

où $(1 + T\zeta^c)^{n_c/p} = \sum_{k=0}^{+\infty} \binom{n_c/p}{k} (T\zeta^c)^k$.

Soit $m \geq 0$ un entier. La m-ième somme partielle de $f[\Theta, T]$, sera notée $S_m(\Theta, T) \in \mathbb{C}[T]$.

Definition 5.3.3 *Soit $\Theta \in \mathbb{Z}[G]$. On appelle reste d'ordre m, la série formelle notée $R_m(\Theta, T)$, et définie par*

$$R_m(\Theta, T) = f[\Theta, T] - S_m(\Theta, T).$$

Si $\Theta \in \mathbb{Z}[G]$ et $z \in \mathbb{C}$, $|z| < 1$, la série $f[\Theta, z]$ est convergente dans $\mathbb{C}$. De plus :

Lemme 5.3.4 *On a l'inégalité suivante :*

$$|R_m(\Theta, z)| \leq \left| \binom{-|\Theta|/p}{m+1} \right| \frac{|z|^{m+1}}{(1-|z|)^{m+1+|\Theta|/p}}, \tag{5.15}$$

où $|\Theta| = \sum_{c=1}^{p-1} |n_c|$.

Preuve Rappelons que si $\sum_k A_k T^k$ (repectivement $\sum_k a_k T^k$) est une série à coefficients complexes (respectivement réels positifs), on dit que $\sum_k A_k T^k$ est dominée par $\sum_k a_k T^k$ et on écrit $\sum_k A_k T^k << \sum_k a_k T^k$ ssi pour tout entier k, on a $|A_k| \leq a_k$. Soient $s \in \mathbb{C}$, $|s| \leq 1$, et $r \in \mathbb{R}$. Comme $\left|\binom{r}{k}\right| \leq (-1)^k \binom{-|r|}{k}$ on a

$$(1+sT)^r = \sum_{k=0}^{\infty} \binom{r}{k} s^k T^k << \sum_{k=0}^{\infty} (-1)^k \binom{-|r|}{k} T^k = (1-T)^{-|r|}.$$

On en déduit que

$$f[\Theta, z] << (1-T)^{-\frac{|\Theta|}{p}}.$$

En particulier,

$$|f[\Theta, z] - S_m(\Theta, z)| \leq \left| (1-|z|)^{-\frac{|\Theta|}{p}} - S_m(|z|) \right|,$$

$S_m(|z|)$ étant la m-ième somme partielle de $(1-|z|)^{-\frac{|\Theta|}{p}}$. L'inégalité de Taylor-Lagrange montre alors

$$\begin{aligned} |f[\Theta, z] - S_m(\Theta, z)| &\leq Sup_{|\xi| \leq |z|} \left| \frac{d^{m+1}(1-T)^{-\frac{|\Theta|}{p}}}{dT^{m+1}} \right|_{T=\xi} \frac{|z|^{m+1}}{(m+1)!} \\ &\leq \left| \binom{-|\Theta|/p}{m+1} \right| \frac{|z|^{m+1}}{(1-|z|)^{m+1+|\Theta|/p}}. \end{aligned}$$

□

Soit $\Theta = \sum_{c=1}^{p-1} n_c \sigma_c \in \mathbb{Z}[G]$. On pose alors

$$\rho(\Theta) = \sum_{c=1}^{p-1} n_c \zeta^c \in \mathbb{Z}[\zeta].$$

On pose également

$$f[\Theta, T] = \sum_{k=0}^{+\infty} a_k[\Theta] T^k,$$

et

$$b_k[\Theta] = p^k \cdot k! \cdot a_k[\Theta].$$

Les propriétés arithmétiques des coefficients a_k et b_k sont rappelées dans la proposition suivante :

Proposition 5.3.5 *1. Si $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, alors $a_k[\Theta]^\sigma = a_k[\sigma\Theta]$;*

2. $a_k[\Theta] \in \mathbb{Z}\left[\zeta, \frac{1}{p}\right]$; de plus, $p^{E(k)} a_k[\Theta] \in \mathbb{Z}[\zeta]$, où on a posé $E(k) = k + \nu_p(k!)$, ν_p étant la valuation p-adique ;

3. $b_k[\Theta] \in \mathbb{Z}[\zeta]$ et

$$b_k[\Theta] \equiv \rho(\Theta)^k \bmod p\mathbb{Z}[\zeta].$$

Preuve

– preuve de la première assertion : cela résulte du fait que σ agit seulement sur ζ, pas sur T.

– preuve de la seconde assertion : on fait une récurrence sur le nombre de $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ intervenant dans l'écriture de Θ en tant qu'élément de $\mathbb{Z}[G]$. S'il n'y en a qu'un seul, on peut écrire $\Theta = \eta\sigma$. Alors

$$a_k[\Theta] = \frac{\eta(\eta-1)\cdots(\eta-p(k-1))}{k!p^k}\zeta^{k\sigma},$$

d'où $p^{E(k)} a_k[\Theta] \in \mathbb{Z}[\zeta]$. Soit maintenant $\Theta \in \mathbb{Z}[G]$ quelconque. Ecrivons le sous la forme $\Theta = \Theta_1 + \Theta_2$, le nombre de $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ intervenant dans l'écriture des Θ_i étant strictement plus petit que pour Θ. En particulier, si l est un entier, $0 \leq l \leq k$, on a

$$\nu_p(a_l[\Theta_1]\, a_{k-l}[\Theta_2]) \geq -(E(l) + E(k-l)) = -E(k) + \nu_p\left(\binom{k}{l}\right) \geq -E(k).$$

Or

$$a_k\left[\Theta\right] = \sum_{l=0}^{k} a_l\left[\Theta_1\right] a_{k-l}\left[\Theta_2\right],$$

d'où l'assertion.

– preuve de la troisième assertion : supposons d'abord que $\Theta = \eta\sigma$. On a alors

$$\begin{aligned} b_k\left[\Theta\right] = p^k k! a_k\left[\Theta\right] &= p^k \cdot \frac{\eta}{p}\left(\frac{\eta}{p} - 1\right)\cdots\left(\frac{\eta}{p} - (k-1)\right)\zeta^{k\sigma} \equiv \eta^k \zeta^{k\sigma} \\ &\equiv \rho\left(\eta\sigma\right)^k \bmod p\mathbb{Z}[\zeta]. \end{aligned}$$

Comme pour la preuve précédente, si maintenant $\Theta = \Theta_1 + \Theta_2$, le nombre de $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ intervenant dans l'écriture des Θ_i étant strictement plus petit que pour Θ, on a, pour l entier

$$b_l\left[\Theta_i\right] \equiv \rho\left(\Theta\right)^l \bmod p\mathbb{Z}[\zeta], \quad i = 1, 2.$$

Or

$$\begin{aligned} b_k\left[\Theta\right] &= b_k\left[\Theta_1 + \Theta_2\right] \\ &= p^k k! a_k\left[\Theta_1 + \Theta_2\right] \\ &= p^k k! \sum_{l=0}^{k} a_l\left[\Theta_1\right] a_{k-l}\left[\Theta_2\right] \\ &= p^k k! \sum_{l=0}^{k} p^{-l} \cdot \frac{1}{l!} \cdot b_l\left[\Theta_1\right] \cdot p^{-(k-l)} \cdot \frac{1}{(k-l)!} b_{k-l}\left[\Theta_2\right] \\ &= \sum_{l=0}^{k} \binom{k}{l} b_l\left[\Theta_1\right] \cdot b_{k-l}\left[\Theta_2\right] \\ &\equiv \sum_{l=0}^{k} \binom{k}{l} \rho\left(\Theta_1\right)^l \rho\left(\Theta_2\right)^{k-l} \bmod p\mathbb{Z}[\zeta] \\ &\equiv \left(\rho\left(\Theta_1\right) + \rho\left(\Theta_2\right)\right)^k \equiv \left(\rho\left(\Theta\right)\right)^k \bmod p\mathbb{Z}[\zeta], \end{aligned}$$

ce qu'on voulait montrer.

□

Rappelons que l'application E définie dans la proposition précédente vérifie le lemme suivant :

Lemme 5.3.6 *L'application E est strictement croissante et vérifie $E(k) < k \cdot \frac{p}{p-1}$.*

Preuve Pour la stricte croissance de E, il n'y a rien à faire. De plus, par le théorème de Legendre, on a $\nu_p(k!) < \frac{k}{p-1}$, d'où $E(k) < k + \frac{k}{p-1} = \frac{kp}{p-1}$.□

5.3.2 Majoration de $|x|$ en fonction de y_0 et p.

On peut supposer dans ce paragraphe que $|x| \geq 2|y_0|$. En effet, dans le cas contraire, la majoration donnée dans l'énoncé du théorème (5.1.2) est immédiate.

De l'équation (5.3) on déduit qu'il existe un idéal $\mathfrak{a}$ de l'anneau $\mathbb{Z}[\zeta]$, premier à $\mathfrak{p}$, tel que

$$\left(\overline{\zeta}x + y_0\right) = \mathfrak{a}^p. \tag{5.16}$$

Soit $\alpha = \overline{\zeta}x + y_0$.

Proposition 5.3.7 *Soit $\Theta \in \mathbb{N}[G]$ de poids divisible par p tel que $s(\Theta) \in \boldsymbol{A}_1$. Il existe un unique $\nu[\Theta] \in \mathbb{Z}[\zeta]$ tel que*

$$\alpha^{\Theta} = \nu[\Theta]^p, \quad \nu[\Theta] \equiv y_0^{W(\Theta)} \bmod (1-\zeta)^2.$$

Preuve L'idéal $\mathfrak{a}$ est d'ordre 1 ou p. Soit $\Theta \in \mathbb{N}[G]$ de poids divisible par p tel que $s(\Theta) \in \mathbf{A}_1$. Par hypothèse, $p|x$. Admettons momentanément le fait que cela entraîne $p^2|x$. Il vient alors

$$\alpha^{\Theta} \equiv y_0^{W(\Theta)} \bmod p^2.$$

Comme $p|W(\Theta)$, l'entier algébrique α est donc un nombre p-primaire de $\mathbb{Q}(\zeta)$. La proposition (5.2.14) montre qu'il existe un unique entier algébrique $\nu[\Theta]$ tel que

$$\begin{cases} \alpha^{\Theta} = \nu[\Theta]^p, \\ \nu[\Theta] \equiv y_0^{W(\Theta)} \bmod (1-\zeta)^2. \end{cases}$$

Il reste à démontrer le fait admis que $p^2|x$. Comme $p|x$ et y_0 premier à p, on a

$$z^p = \frac{x^p + y_0^p}{x + y_0} \equiv y_0^{p-1} \equiv 1 \bmod p.$$

La congruence $z^p \equiv 1 \bmod p$ implique $z^p \equiv 1 \bmod p^2$, d'où $\frac{x^p+y_0^p}{x+y_0} \equiv 1 \bmod p^2$. Comme $\frac{x^p+y_0^p}{x+y_0} = \sum_{k=0}^{p-1}(-x)^k y_0^{p-1-k}$ et $p|x$, on obtient donc

$$-xy_0^{p-2} + y_0^{p-1} \equiv 1 \bmod p^2.$$

Or d'après (5.14) : $y_0^{p-1} \equiv 1 \bmod p^2$. On doit donc avoir $xy_0^{p-2} \equiv 0 \bmod p^2$, c'est à dire $p^2|x$.□

Fixons pour la suite $\Theta \in \mathbb{N}[G]$ donné par le lemme (5.2.3). Soit $\nu[\Theta]$ l'entier algébrique donné par la proposition (5.3.7). Comme $j\Theta = \Theta$, on a

$$\begin{aligned}
\alpha^{\Theta} &= \nu[\Theta]^p, \\
\alpha^{\Theta} &= \alpha^{j\Theta} = \left(\nu[\Theta]^j\right)^p, \\
\nu[\Theta] &\equiv \nu[\Theta]^j \equiv y_0^{W(\Theta)} \bmod (1-\zeta)^2.
\end{aligned}$$

Par unicité, on a donc $\nu[\Theta] = \nu[\Theta]^j$, c'est à dire $\nu[\Theta] \in \mathbb{R}$. Posons $\Theta = \sum_{c=1}^{p-1} n_c\sigma_c$. Comme $\Theta = j\Theta$, on a $n_c = n_{p-c}$. Soit $\Theta_0 = \sum_{c=1}^{\frac{p-1}{2}} n_c\sigma_c$. Comme $n_c = n_{p-c}$, on a

$$\begin{aligned}
(1+j)\Theta_0 &= \sum_{c=1}^{\frac{p-1}{2}} n_c\sigma_c + \sum_{c=1}^{\frac{p-1}{2}} n_c j\sigma_c = \sum_{c=1}^{\frac{p-1}{2}} n_c\sigma_c + \sum_{c=1}^{\frac{p-1}{2}} n_c\sigma_{p-c} \\
&= \sum_{c=1}^{\frac{p-1}{2}} n_c\sigma_c + \sum_{c=\frac{p+1}{2}}^{p-1} n_{p-c}\sigma_c = \sum_{c=1}^{\frac{p-1}{2}} n_c\sigma_c + \sum_{c=\frac{p+1}{2}}^{p-1} n_c\sigma_c = \Theta
\end{aligned}$$

Comme $|x| \geq 2|y_0|$, la série $f\left[\Theta, \frac{y_0}{x}\right]$ est convergente dans $\mathbb{C}$. L'égalité $\Theta = (1+j)\Theta_0$ montre que le nombre complexe $f\left[\Theta, \frac{y_0}{x}\right]$ est en fait réel (voir [28]). Le poids de Θ étant un entier positif non nul, divisible par p et majoré par $\frac{p(p-1)}{2}$, il existe un entier h, $1 \leq h \leq \frac{p-1}{2}$ tel que $W(\Theta) = p \cdot h$. L'égalité $\alpha^{\Theta} = \nu[\Theta]^p$ s'écrit alors

$$\nu[\Theta]^p = \overline{\zeta}^{\Theta} \cdot x^{p\cdot h} \cdot \left(1 + \frac{\zeta y_0}{x}\right)^{\Theta},$$

c'est à dire

$$\nu[\Theta]^p = x^{p\cdot h} \cdot f\left[\Theta, \frac{y_0}{x}\right]^p,$$

car $\zeta^{\Theta} = 1$. Il existe donc un entier a tel que

$$\nu[\Theta] = \zeta^a \cdot x^h \cdot f\left[\Theta, \frac{y_0}{x}\right].$$

Or on a montré précédemment que $f\left[\Theta, \frac{y_0}{x}\right]$ et $\nu[\Theta]$ sont des nombres réels. On a donc $\zeta^a = 1$, c'est à dire

$$\nu[\Theta] = x^h \cdot f\left[\Theta, \frac{y_0}{x}\right].$$

Soit $\beta[\Theta] = p^h\nu[\Theta] \in \mathbb{Z}[\zeta + \overline{\zeta}]$. Soit $S'_h(\Theta)$ la somme définie par

$$S'_h(\Theta) = p^h x^h S_h\left(\Theta, \frac{y_0}{x}\right) = \sum_{i=0}^{h} x^{h-i} \cdot y_0^i \cdot p^h \cdot a_i[\Theta],$$

et $R'_h(\Theta)$ définie par

$$R'_h(\Theta) = \beta[\Theta] - S'_h(\Theta) = R_h\left(\Theta, \frac{y_0}{x}\right) \cdot x^h \cdot p^h.$$

Par la proposition (5.3.5), on a $p^h a_i[\Theta] \in \mathbb{Z}[\zeta]$ si $i \leq h$. En effet, si $i \leq h$, comme $h \leq \frac{p-1}{2}$, en particulier $E(i) = i$. Par la proposition (5.3.5), on a donc $p^i a_i[\Theta] \in \mathbb{Z}[\zeta]$. En particulier, on a pour i entier, $i \leq h$ le fait que $p^h a_i[\Theta] \in \mathbb{Z}[\zeta]$. La somme $S'_h(\Theta)$ est donc un élément de l'anneau $\mathbb{Z}[\zeta]$. Il en est donc de même pour $R'_h(\Theta)$. L'inégalité (5.15) permet de majorer ce dernier élément comme suit :

$$|R'_h(\Theta)| \leq |x|^h \cdot p^h \left|\binom{-h}{h+1}\right| \frac{|y_0|^{h+1}}{|x|^{h+1}\left(1 - \left|\frac{y_0}{x}\right|\right)^{2h+1}}.$$

On a $\left|\binom{-h}{h+1}\right| = \binom{2h}{h+1} < 2^{2h-1}$. Comme $|x| \geq 2|y_0|$, on a aussi $\left(1 - \left|\frac{y_0}{x}\right|\right)^{-2h-1} \leq 2^{2h+1}$. On obtient :

$$|R'_h(\Theta)| < \frac{(16p)^h |y_0|^{h+1}}{|x|}.$$

Lemme 5.3.8 *Pour tout élément $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, on a*

$$R'_h(\Theta)^\sigma = R'_h(\sigma\Theta). \tag{5.17}$$

Preuve On a $\nu[\Theta]^\sigma = \nu[\sigma\Theta]$: en vertu de la proposition (5.3.7), pour le montrer, il suffit de prouver que

$$(\nu[\Theta]^\sigma)^p = \alpha^{\sigma\Theta}, \quad \nu[\Theta]^\sigma \equiv y_0^{W(\sigma\Theta)} \bmod (1-\zeta)^2.$$

Or par définition de $\nu[\Theta]$:

$$(\nu[\Theta]^\sigma)^p = \nu[\Theta]^{p\sigma} = (\nu[\Theta]^p)^\sigma = \alpha^{\sigma\Theta}.$$

Encore par définition de $\nu[\Theta]$:

$$\nu[\Theta] \equiv y_0^{W(\Theta)} \bmod (1-\zeta)^2,$$

d'où

$$\nu[\Theta]^\sigma \equiv y_0^{\sigma W(\Theta)} \bmod (1-\zeta^\sigma)^2 \equiv y_0^{W(\Theta)} \bmod (1-\zeta)^2.$$

Comme $W(\Theta) = W(\sigma\Theta)$, on a bien $\nu[\Theta]^\sigma \equiv y_0^{W(\sigma\Theta)} \bmod (1-\zeta)^2$.

Par la proposition (5.3.5), pour tout entier k positif, $a_k[\Theta]^\sigma = a_k[\sigma\Theta]$. En particulier, on a $S'_h(\Theta)^\sigma = S'_h(\sigma\Theta)$. Des égalités

$$\nu[\Theta]^\sigma = \nu[\sigma\Theta], \quad S'_h(\Theta)^\sigma = S'_h(\sigma\Theta),$$

on déduit que $R'_h(\Theta)^\sigma = R'_h(\sigma\Theta)$.□

Soit $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Par (5.17), on peut donc majorer $|R'_h(\Theta)^\sigma| = |R'_h(\sigma\Theta)|$ en appliquant également la majoration (5.15). Une telle majoration ne dépend que de $|\sigma\Theta|$. Comme $|\Theta| = |\sigma\Theta|$, on obtient la même majoration que pour $|R_h(\Theta)|$:

$$\forall \sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}), \quad |R'_h(\Theta)^\sigma| < \frac{(16p)^h |y_0|^{h+1}}{|x|}. \tag{5.18}$$

Supposons que $\frac{(16p)^h|y_0|^{h+1}}{|x|} \leq 1$. Les inégalités (5.18) montrent en particulier que l'entier algèbrique $R'_h(\Theta)$ est donc de norme (sur $\mathbb{Q}$) strictement moindre que 1, d'où $R'_h(\Theta) = 0$. On obtient $\beta[\Theta] = S'_h(\Theta)$. On en déduit que $\frac{S'_h(\Theta)}{p} = \frac{\beta[\Theta]}{p} = p^{h-1}\nu[\Theta] \in \mathbb{Z}[\zeta]$ (car $h \geq 1$), c'est à dire

$$\sum_{i=0}^{h} x^{h-i} \cdot y_0^i \cdot p^{h-1} \cdot a_i[\Theta] \in \mathbb{Z}[\zeta]. \tag{5.19}$$

Si $i < h$, $p^{h-1} \cdot a_i[\Theta] \in \mathbb{Z}[\zeta]$. En effet, soit i un entier positif, $i < h$. Comme $i < p$ (car $h < p$) la proposition (5.3.5) montre

$$p^{E(i)} a_i[\Theta] = p^i a_i[\Theta] \in \mathbb{Z}[\zeta].$$

Comme $i \leq h-1$, en particulier

$$p^{h-1} \cdot a_i[\Theta] \in \mathbb{Z}[\zeta].$$

Par (5.19), on doit donc avoir $y_0^h \cdot p^{h-1} \cdot a_h[\Theta] \in \mathbb{Z}[\zeta]$. Par définition de $b_h[\Theta]$, on a

$$y_0^h \cdot h! \cdot p^h \cdot a_h[\Theta] = y_0^h \cdot b_h[\Theta].$$

Comme $y_0^h \cdot p^{h-1} \cdot a_h[\Theta] \in \mathbb{Z}[\zeta]$, en particulier, on a

$$y_0^h \cdot b_h[\Theta] \equiv 0 \bmod p\mathbb{Z}[\zeta].$$

Or, par la proposition (5.3.5), $y_0^h \cdot b_h[\Theta] \equiv y_0^h \cdot \rho(\Theta)^h \bmod p\mathbb{Z}[\zeta]$. L'entier y_0 étant premier à p, on doit donc avoir

$$\rho(\Theta) \equiv 0 \bmod p\mathbb{Z}[\zeta].$$

Le lemme 1.9 de [77] montre alors que $s(\Theta) = 0$ en contradiction avec le fait que $s(\Theta) \neq 0$.

On a donc bien

$$|x| < (16p)^h |y_0|^{h+1} \leq (16p)^{\frac{p-1}{2}} |y_0|^{\frac{p+1}{2}}. \tag{5.20}$$

Remarque sur les calculs précédents : Pour obtenir la majoration précédente, il est vain d'espérer utiliser un élément Θ positif non nul de $\mathcal{I}_{st}$ tel que $j\Theta = \Theta$, $p|W(\Theta)$, $W(\Theta) \leq \frac{p(p-1)}{2}$ et $\rho(\Theta) \neq 0 \bmod p\mathbb{Z}[\zeta]$: aucun élément de $\mathcal{I}_{st}$ ne vérifie ces propriétés. En effet, on peut montrer (voir [28]) pour $\Theta \in \mathcal{I}_{st}$ que l'égalité $j\Theta = \Theta$ implique qu'il existe un entier a tel que $\Theta = a\mathcal{N}$. Pour avoir $p|W(\Theta)$, l'entier a est nécessairement divisible par p. On a alors $\rho(\Theta) \equiv 0 \bmod p\mathbb{Z}[\zeta]$.

5.3.3 Minoration de $|x|$ en fonction de p.

Dans ce paragraphe, on suppose que $p^3|x$, et que l'entier $|y_0|$ est majoré au sens large par $\frac{p}{\left(4(p-1)(16)^{\frac{p-1}{2}}\right)^{\frac{2}{p+1}}}$. On va alors montrer que le nombre premier p est un diviseur de h_p^+. L'idée de la démonstration sera de raisonner par l'absurde : on supposera que $p \nmid h_p^+$; on montrera alors que l'entier $|x|$ est minoré par une constante trop grande pour que l'hypothèse de majoration faite sur $|y_0|$ soit satisfaite.

Lemme 5.3.9 *Soit p un nombre premier impair tel que $p \nmid h_p^+$. Supposons qu'il existe des entiers A, B, C premiers entre eux dans leur ensemble tels que*

$$\frac{A^p + B^p}{A + B} = C^p, \quad p^2|B.$$

Il existe alors un (unique) $\gamma \in \mathbb{Q}(\zeta)$ tel que

$$\frac{A + B\zeta}{A + B\overline{\zeta}} = \gamma^p, \quad \gamma \equiv 1 \bmod (1-\zeta)^2.$$

Preuve Soient $\alpha = \frac{A+B\zeta}{A+B\overline{\zeta}}$ et $\mathbb{L} = \mathbb{Q}(\zeta, \alpha^{\frac{1}{p}})$. L'entier B étant divisible par p^2, en particulier on a $\alpha \equiv 1 \bmod p(1-\zeta)$. Comme $(A, B, C) = 1$, il existe un idéal entier $\mathfrak{a}$ de $\mathbb{Z}[\zeta]$ tel que $(A + B\zeta) = \mathfrak{a}^p$. Le nombre algébrique α est donc un nombre algébrique primaire singulier : l'extension $\mathbb{L}/\mathbb{Q}(\zeta)$ est non ramifiée.

Comme $p \nmid h_p^+$ et $\overline{\alpha} = \alpha^{-1}$, le lemme 9.2 de [77] montre qu'il existe $\gamma_1 \in \mathbb{Q}(\zeta)$, tel que $\frac{A+B\zeta}{A+B\overline{\zeta}} = \gamma_1^p$. Le nombre algébrique γ_1 vérifie en particulier $\gamma_1^p \equiv 1 \bmod (1-\zeta)$, c'est à dire $\gamma_1 \equiv 1 \bmod (1-\zeta)$. Par le lemme (5.2.15), il existe donc un entier a tel que

$$\gamma_1 \zeta^a \equiv 1 \bmod (1-\zeta)^2.$$

Comme $(\zeta^a\gamma_1)^p = \gamma_1^p$, il suffit donc de poser $\gamma = \zeta^a\gamma_1$.□

En particulier, il existe alors un (unique) $\gamma \in \mathbb{Q}(\zeta)$ tel que

$$\frac{x\zeta + y_0}{x\overline{\zeta} + y_0} = \gamma^p, \quad \gamma \equiv 1 \bmod (1-\zeta)^2.$$

Soit $\mathbb{Z}_p$ l'anneau des entiers p-adiques. Comme $p^2|x$, la série $f(x) = \left(1+\frac{\zeta x}{y_0}\right)^{\frac{1}{p}}\left(1+\frac{\overline{\zeta} x}{y_0}\right)^{-\frac{1}{p}}$ converge dans $\mathbb{Z}_p[\zeta]$. On a

$$\gamma^p = \frac{1+\frac{x\zeta}{y_0}}{1+\frac{x\overline{\zeta}}{y_0}} = f(x)^p.$$

Il existe donc un entier a tel que $\zeta^a\gamma = f(x)$. Comme $p^2|x$, on a $f(x) \equiv 1 \bmod (1-\zeta)^2$. Comme $\gamma \equiv 1 \bmod (1-\zeta)^2$, on a $\zeta^a \equiv 1 \bmod (1-\zeta)^2$ donc $\zeta^a = 1$, c'est à dire

$$\gamma = \left(\sum_{k=0}^{+\infty}\binom{1/p}{k}\left(\frac{\zeta x}{y_0}\right)^k\right)\left(\sum_{k=0}^{+\infty}\binom{-1/p}{k}\left(\frac{\overline{\zeta} x}{y_0}\right)^k\right) = \sum_{n=0}^{+\infty} b_n(\zeta)\frac{x^n}{y_0^n},$$

où

$$b_n(\zeta) = \sum_{k=0}^{n}\binom{-1/p}{k}\binom{1/p}{n-k}\zeta^{n-2k}.$$

Soit $d = \frac{p-1}{2}$. Pour la suite, on note par **Tr** l'application trace relative à $\mathbb{Q}(\zeta)/\mathbb{Q}$.

Lemme 5.3.10 *Soit n un entier, $0 \leq n < d$. On a* $\boldsymbol{Tr}\left((\zeta^{d+1}-\zeta^d)b_n(\zeta)\right) = 0$.

Preuve Soit k un entier, $0 \leq k \leq n$. Comme $n < d$, on a $|n-2k| \leq n < d$, d'où $0 < d+1+n-2k, d+n-2k < p$, d'où

$$\mathbf{Tr}\left(\zeta^{d+1+n-2k} - \zeta^{d+n-2k}\right) = (-1) - (-1) = 0,$$

et le lemme.□

Soit alors

$$\Delta = \mathbf{Tr}\left((\zeta^{d+1}-\zeta^d)\gamma z\right).$$

C'est un entier relatif. En effet, on a

$$(\gamma z)^p = \frac{x\zeta + y_0}{x\overline{\zeta} + y_0} z^p,$$

et $x\overline{\zeta} + y_0$ divise z^p dans $\mathbb{Z}[\zeta]$, car

$$(x\zeta + y_0)\ldots\left(x\overline{\zeta} + y_0\right) = z^p.$$

Ainsi $(\zeta^{d+1}-\zeta^d)\gamma z \in \mathbb{Z}[\zeta]$, donc $\Delta \in \mathbb{Z}$. De plus, $\Delta \equiv 0 \bmod p^p$. En effet, rappelons que $p^3|x$ par hypothèse. Notons ν_π la valuation usuelle sur $\mathbb{Q}_p(\zeta)$ (en particulier $\nu_\pi(p) = p-1, \nu_\pi(\zeta^a-\zeta^b) = 1$ si $a \neq b \bmod p$). Soit $k \geq d$ un entier. Si $k < p$, on a alors

$$\nu_\pi\left((\zeta^{d+1}-\zeta^d)b_k(\zeta)\,x^k\right) > 2k(p-1) \geq 2d(p-1).$$

Si $k \geq p$, on a, en utilisant le fait que pour l entier, $\nu_p(l!) < \frac{l}{p-1}$:

$$\nu_\pi\left((\zeta^{d+1}-\zeta^d)b_k(\zeta)\,x^k\right) > (3k-k-\frac{k}{p-1})(p-1) > k(p-1) \geq p(p-1) > 2d(p-1).$$

On a donc $\nu_p(\Delta) \geq p$. Admettons momentanément que $\Delta \neq 0$. Comme $\Delta \equiv 0 \bmod p^p$, on a $p^p \leq |\Delta|$. De plus, comme $|\gamma| = 1$, il vient

$$|\Delta| \leq 2(p-1)|z|.$$

Comme $p|x$, par le paragraphe (5.3.2) on a $|x| < (16p)^{\frac{p-1}{2}}\,|y_0|^{\frac{p+1}{2}}$. Comme $p|x$ et $|y_0| < p$, en particulier $|x| > |y_0|$ et il vient de l'équation (5.3) que $|z| < |x|$, d'où

$$p^p \leq |\Delta| \leq 2(p-1)|z| < 2(p-1)\,(16p)^{\frac{p-1}{2}}\,|y_0|^{\frac{p+1}{2}},$$

d'où

$$\frac{p}{\left(2(p-1)\,(16)^{\frac{p-1}{2}}\right)^{\frac{2}{p+1}}} < |y_0|,$$

en contradiction avec les hypothèses. On a donc bien $p|h_p^+$. Pour terminer la démonstration, il reste à démontrer la proposition fondamentale suivante admise plus haut :

Proposition 5.3.11 *On a $\Delta \neq 0$.*

Preuve Définissons une suite d'entiers a_l, $l \geq 2$:

$$\begin{cases} a_2 = 3, \\ a_{l+1} = a_l + l + 1. \end{cases}$$

On vérifie que $a_l = \frac{l(l+1)}{2}$. De plus, par définition, on a

$$(1-p)(1-2p)\ldots(1-(d-1)p) \equiv 1 - a_{d-1}p \bmod p^2,$$

où $d = \frac{p-1}{2}$. En effet $(1-p)(1-2p) \equiv 1 - a_2 p \bmod p^2$. De plus

$$(1-a_l p)(1-(l+1)p) \equiv 1 - (a_l + l + 1)p \equiv 1 - a_{l+1}p \bmod p^2.$$

De la même façon, on a

$$(1+p)(1+2p)\ldots(1+(d-1)p) \equiv 1 + a_{d-1}p \bmod p^2.$$

Lemme 5.3.12 *Soit $T := \boldsymbol{Tr}\left(\left(\zeta^{d+1}-\zeta^d\right) b_d(\zeta)\frac{x^d}{y_0^d}z\right)$. On a*

$$T = p\frac{x^d}{y_0^d}z\left(\binom{1/p}{d} - \binom{-1/p}{d}\right).$$

Preuve Soit k un entier, $0 \leq k \leq d$. On a alors $0 \leq 2d-2k < p$ avec $2d-2k=0$ si et seulement si $k=d$. De même $1 \leq 2d-2k+1 \leq p$ avec $2d-2k+1=p$ si et seulement si $k=0$. Ainsi :

$$\mathbf{Tr}\left(\zeta^{2d+1-2k}-\zeta^{2d-2k}\right)=\begin{cases}\mathbf{Tr}\left(1-\zeta^{2d}\right)=p & \text{si } k=0,\\ (-1)-(-1)=0 & \text{si } 0<k<d,\\ \mathbf{Tr}\left(\zeta-1\right)=-p & \text{si } k=d.\end{cases}$$

Par définition de $b_d(\zeta)$, on obtient :

$$\begin{aligned}T :&= \mathbf{Tr}\left(\left(\zeta^{d+1}-\zeta^d\right)b_d(\zeta)\frac{x^d}{y_0^d}z\right)=\frac{x^d}{y_0^d}z\sum_{k=0}^{d}\binom{-1/p}{k}\binom{1/p}{d-k}\mathbf{Tr}\left(\zeta^{2d+1-2k}-\zeta^{2d-2k}\right)\\ &=\frac{x^d}{y_0^d}z\left(\binom{1/p}{d}p+\binom{-1/p}{d}(-p)\right),\end{aligned}$$

d'où le lemme. □ On peut donc écrire

$$T=\frac{x^d}{y_0^d d! p^{d-1}}z\left((1-p)(1-2p)\dots(1-(d-1)p)-(-1)^d(1+p)(1+2p)\dots(1+(d-1)p)\right),$$

où

$$(1-p)\dots(1-(d-1)p)-(-1)^d(1+p)\dots(1+(d-1)p)\equiv 1-a_{d-1}p-(-1)^d\left(1+a_{d-1}p\right) \bmod p^2.$$

Soit $v=\nu_p(x)$. Si $(-1)^d=-1$, c'est à dire $p\equiv 3 \bmod 4$, alors $\nu_p\left(T\right)=dv+1-d$, et si $p\equiv 1 \bmod 4$, alors

$$(1-p)\dots(1-(d-1)p)-(-1)^d(1+p)\dots(1+(d-1)p)\equiv -2a_{d-1}p\equiv -p(d-1)d \bmod p^2,$$

d'où $\nu_p\left(T\right)=dv+2-d$. Raisonnons par l'absurde et supposons que $\Delta=0$. On a alors

$$\mathbf{Tr}\left(\left(\zeta^{d+1}-\zeta^d\right)b_d(\zeta)\frac{x^d}{y_0^d}z\right)=-\mathbf{Tr}\left(\left(\zeta^{d+1}-\zeta^d\right)\sum_{k=d+1}^{+\infty}b_k(\zeta)\frac{x^k}{y_0^k}z\right). \tag{5.21}$$

Supposons d'abord que $p\equiv 3 \bmod 4$, donc que $\nu_{1-\zeta}\left(T\right)=(dv+1-d)(p-1)$. De (5.21), en comparant les valuations $(1-\zeta)$-adiques, on obtient

$$(dv+1-d)(p-1)\geq 1+((d+1)v-d-1)(p-1),$$

d'où

$$dv+1-d>(d+1)v-d-1,$$

d'où $v<2$. Or par hypothèse, $p^3|x$, donc $v>2$. Si $p\equiv 1 \bmod 4$, on trouve $v<3$, or $v\geq 3$. On a donc bien $\Delta\neq 0$.□ Le théorème (5.1.2) est prouvé.

■

5.3.4 Démonstration du corollaire (5.1.4).

Supposons d'abord que $q = p$. Soit X, Z une solution entière de (5.5), autre que la solution éventuelle $X^a = -Y_0$, $Z = 0$. Comme $X^a \neq -Y_0$, on peut mettre l'équation (5.5) sous la forme

$$\frac{X^{ap} + Y_0^p}{X^a + Y_0} (X^a + Y_0) = BZ^p,$$

avec $(B, p) = 1$ par hypothèse. **On suppose dans un premier temps que Z est premier à p.** On a donc $(BZ, p) = 1$. Rappelons que si a, b sont des entiers premiers entre eux, alors

$$\left(\frac{a^p - b^p}{a - b}, a - b \right) = (a - b, p)\,.$$

Autrement dit, p divisera $\frac{a^p - b^p}{a-b}$ si et seulement si p divise $a - b$, et alors[5] $p || \frac{a^p - b^p}{a-b}$. Comme BZ est premier à p

$$\left(\frac{X^{ap} + Y_0^p}{X^a + Y_0}, X^a + Y_0 \right) = 1.$$

La condition $(\Psi(B), p) = 1$ est équivalente au fait qu'aucun des facteurs premiers l de B ne vérifie $l \equiv 1 \bmod p$.

Lemme 5.3.13 *Soient C, D deux entiers premiers entre eux. Soit $l \neq p$ un facteur premier de $\frac{C^p + D^p}{C+D}$. Alors $l \equiv 1 \bmod p$.*

Preuve En effet, comme $(A, B, C) = 1$, nécessairement les idéaux $(A + B\zeta^i)$ de $\mathbb{Z}[\zeta]$, $i = 1, \ldots, p-1$ sont deux à deux premiers entre eux. On en déduit que le nombre premier l se décompose totalement dans l'extension $\mathbb{Q}(\zeta)/\mathbb{Q}$. Comme de façon générale, le groupe de décomposition de l dans cette extension est engendré par sa classe modulo p, on doit donc avoir $l \equiv 1 \bmod p$.□

Par le lemme (5.3.13), l'entier B est donc un diviseur de $X^a + Y_0$, et on a donc dans $\mathbb{Z}$:

$$\frac{X^a + Y_0}{B} \frac{X^{ap} + Y_0^p}{X^a + Y_0} = Z^p, \quad \left(\frac{X^{ap} + Y_0^p}{X^a + Y_0}, X^a + Y_0 \right) = 1.$$

Il existe donc des entiers Z_1, Z_2 tels que

$$\frac{X^{ap} + Y_0^p}{X^a + Y_0} = Z_1^p, \quad X^a + Y_0 = BZ_2^p.$$

[5] c'est à dire p divise $\frac{a^p - b^p}{a-b}$ mais pas p^2.

Si $X(X^{2a}-Y_0^2)$ est premier à p, les théorèmes 1, 3 et la proposition 1 de [53] montrent que $r_p > \sqrt{p}-1$, $2^{p-1} \equiv 3^{p-1} \equiv 1 \bmod p^2$ et que $r^{p-1} \equiv 1 \bmod p^2$ pour tout facteur premier r de B. Les hypothèses faites montrent donc que l'on est nécessairement dans le cas $p|X(X^{2a}-Y_0^2)$. Comme $p \nmid X^a+Y_0$ (car $p \nmid Z$), on a donc $p|X$ ou $p|X^a-Y_0$.

Supposons d'abord que $p|X$. Comme $a \geq 3$, $p^3|X^a$. La deuxième partie du théorème (5.1.2) appliquée à l'équation $\frac{X^{ap}+Y_0^p}{X^a+Y_0} = Z_1^p$ (il est licite de l'appliquer car on a supposé $|Y_0| \leq \frac{p}{19}$) montre alors que $p|h_p^+$, ce qui n'a pas lieu par hypothèse. On est donc dans le cas $p|X^a-Y_0$.

Lemme 5.3.14 *Si $p|X^a-Y_0$, alors $p^2|X^a-Y_0$.*

Preuve Comme $p|X^a-Y_0$, il vient

$$\begin{aligned}
\frac{X^{ap}+Y_0^p}{X^a+Y_0} &= \sum_{k=0}^{p-1}(-Y_0)^{p-1-k}X^{ak} = Y_0^{p-1} - Y_0^{p-2}X^a + \sum_{k=2}^{p-1}(-Y_0)^{p-1-k}\left(Y_0+X^a-Y_0\right)^k \\
&\equiv Y_0^{p-1} - Y_0^{p-2}X^a + \sum_{k=2}^{p-1}(-Y_0)^{p-1-k}\left(Y_0^k + kY_0^{k-1}\left(X^a-Y_0\right)\right) \bmod p^2 \\
&\equiv 2Y_0^{p-1} - Y_0^{p-2}X^a + Y_0^{p-2}\left(X^a-Y_0\right)\sum_{k=2}^{p-1}(-1)^k k \bmod p^2 \\
&\equiv 2Y_0^{p-1} - Y_0^{p-2}X^a + Y_0^{p-2}\left(X^a-Y_0\right)\frac{p+1}{2} \bmod p^2 \\
&\equiv Y_0^{p-1} + Y_0^{p-2}\left(X^a-Y_0\right)\frac{p-1}{2} \bmod p^2.
\end{aligned}$$

Comme $Z^p = \frac{X^{ap}+Y_0^p}{X^a+Y_0} \equiv 1 \bmod p$, il vient $\frac{X^{ap}+Y_0^p}{X^a+Y_0} \equiv 1 \bmod p^2$, d'où

$$Y_0^{p-1} + Y_0^{p-2}\left(X^a-Y_0\right)\frac{p-1}{2} \equiv 1 \bmod p^2.$$

Or, par le theorème (5.1.2), $Y_0^{p-1} \equiv 1 \bmod p^2$. On a donc bien $p^2|X^a-Y_0$.□ Comme $X^a+Y_0 = BZ_2^p$, la congruence $X^a \equiv Y_0 \bmod p^2$ montre

$$2Y_0 \equiv X^a+Y_0 \equiv BZ_2^p \bmod p^2.$$

Comme $Y_0^{p-1} \equiv 1 \bmod p^2$,

$$2^{p-1} \equiv (2Y_0)^{p-1} \equiv (BZ_2^p)^{p-1} \equiv B^{p-1} \bmod p^2,$$

d'où $\left(\frac{B}{2}\right)^{p-1} \equiv 1 \bmod p^2$, en contradiction avec les hypothèses.

Il nous reste à étudier le cas dans lequel la solution (X, Z) de l'équation (5.5) vérifie $p|Z$. Posons $Z = p^v Z_1$, avec $p \nmid Z_1$. L'équation (5.5) s'écrit

$$X^p + Y_0^p = Bp^{pv} Z_1^p.$$

Soit $\lambda = (1-\zeta)(1-\overline{\zeta})$. L'équation précédente s'écrit aussi

$$X^p + Y_0^p = B\frac{p^{pv}}{\lambda^{pv\frac{p-1}{2}}} \lambda^{pv\frac{p-1}{2}} Z_1^p.$$

Le quotient $\eta = \frac{p^{pv}}{\lambda^{pv\frac{p-1}{2}}}$ est une unité de l'anneau $\mathbb{Z}[\lambda]$. Posons $m = pv\frac{p-1}{2} \geq p$. On vient donc de montrer qu'il existe $\eta \in \mathbb{Z}[\lambda]^\times$ (unités de $\mathbb{Z}[\lambda]$) et un entier $m \geq p$ tels que

$$X^p + Y_0^p = \eta B \lambda^m Z_1^p, \tag{5.22}$$

où X, Y_0, λ et Z_1 sont premiers entre eux deux à deux.

Proposition 5.3.15 *Supposons qu'il existe des entiers algébriques x, y, z de l'anneau $\mathbb{Z}[\lambda]$, un entier $m \geq p$, et une unité η de l'anneau $\mathbb{Z}[\lambda]$ tels que x, y, z et λ soient premiers entre eux deux à deux et vérifient*

$$x^p + y^p = \eta \lambda^m B_1 z^p, \quad B|B_1|B^N, \tag{5.23}$$

avec B_1, $N \in \mathbb{Z}$, $N \geq 1$. Alors z n'est pas une unité de $\mathbb{Z}[\lambda]$. De plus, il existe des entiers algébriques x', y', z' de l'anneau $\mathbb{Z}[\lambda]$, un entier $m' \geq p$, et une unité η' de l'anneau $\mathbb{Z}[\lambda]$ tels que x', y', z', λ' et η' vérifient les mêmes propriétés. L'entier algébrique z' divise z dans $\mathbb{Z}[\zeta]$. Le nombre d'idéaux premiers de $\mathbb{Z}[\zeta]$ divisant z' est strictement plus petit que celui de z.

Preuve L'équation (5.23) s'écrit

$$(x+y)\prod_{a=1}^{p-1}(x+\zeta^a y) = \eta \lambda^m B_1 z^p.$$

Comme B_1 a les mêmes facteurs premiers que B, on a comme avant $B|x+y$ dans $\mathbb{Z}$, ce qui donne dans $\mathbb{Z}[\zeta]$:

$$\frac{x+y}{B_1}\prod_{a=1}^{p-1}(x+\zeta^a y) = \eta \lambda^m z^p.$$

En raisonnant alors comme dans le paragraphe 9.1 du chapitre 9 de [77], on en déduit qu'il existe des unités **réelles** $\eta_0, \eta_1, \ldots, \eta_{p-1} \in \mathbb{Z}[\lambda]^\times$ et des entiers algébriques $\rho_0 \in \mathbb{Z}[\lambda]$, $\rho_1, \ldots, \rho_{p-1} \in \mathbb{Z}[\zeta]$ tels que

$$x + y = \eta_0 B_1 \lambda^{m-\frac{p-1}{2}} \rho_0^p, \quad \frac{x + \zeta^a y}{1 - \zeta^a} = \eta_a \rho_a^p, \quad a = 1, \ldots, p-1. \tag{5.24}$$

Montrons que z n'est pas une unité. Comme ρ_1 divise z dans $\mathbb{Z}[\zeta]$, il suffit donc de montrer que ρ_1 n'en est pas une, ce que l'on va faire. Posons $\alpha = \frac{x+\zeta y}{1-\zeta}$. On a

$$\alpha = -y + \frac{x+y}{1-\zeta} \equiv -y \bmod (1-\zeta)^2.$$

En particulier $\frac{\overline{\alpha}}{\alpha} \equiv 1 \bmod (1-\zeta)^2$. Raisonnons par l'absurde et supposons que ρ_1 soit une unité. Alors, le quotient $\frac{\overline{\rho_1}^p}{\rho_1^p}$ est une unité de module 1 de l'anneau $\mathbb{Z}[\zeta]$, donc une racine de l'unité de cet anneau par le théorème de Kronecker. Or, les seules racines de l'unité de $\mathbb{Z}[\zeta]$ sont les racines $2p$-ième de l'unité (voir [77]). Comme l'unité η_1 est réelle, il existe donc un entier l et $\epsilon = \pm 1$ tels que $\frac{\overline{\eta_1}\cdot\overline{\rho_1}^p}{\eta_1 \cdot \rho_1^p} = \frac{\overline{\rho_1}^p}{\rho_1^p} = \epsilon\zeta^l$. Il vient alors

$$\frac{\overline{\alpha}}{\alpha} = \epsilon\zeta^l.$$

Comme $\frac{\overline{\alpha}}{\alpha} \equiv 1 \bmod (1-\zeta)^2$, on a donc $\epsilon\zeta^l \equiv 1 \bmod (1-\zeta)^2$, d'où $\epsilon\zeta^l = 1$, ie $\frac{\overline{\alpha}}{\alpha} = 1$, ie

$$\frac{x+\zeta y}{1-\zeta} = \frac{x+\overline{\zeta} y}{1-\overline{\zeta}},$$

car x et y sont réels. Cette dernière équation conduit à $\zeta^2 = 1$ ce qui est faux. L'entier algébrique ρ_1 (et donc z) n'est pas une unité. La première partie de la proposition est prouvée.

Montrons maintenant l'existence de x', y', z', η' et m'. C'est juste une adaptation des calculs développés dans le paragraphe 9.1 au chapitre 9 de [77] dans le cadre du second cas de l'équation de Fermat. Par souci du détail, on préfère redonner les grandes lignes. Soit $a \in \{1, \ldots, p-1\}$. On pose $\lambda_a = (1-\zeta^a)(1-\zeta^{-a})$. Par (5.24), il existe une unité **réelle** η_a et $\rho_a \in \mathbb{Z}[\zeta]$ tels que

$$\frac{x+\zeta^a y}{1-\zeta^a} = \eta_a \rho_a^p,$$

et en conjuguant (rappelons que $x, y \in \mathbb{R}$) :

$$\frac{x+\zeta^{-a} y}{1-\zeta^{-a}} = \eta_a \overline{\rho_a}^p.$$

Ainsi

$$x+\zeta^a y=(1-\zeta^a)\eta_a\rho_a^p,$$
$$x+\zeta^{-a} y=(1-\zeta^{-a})\eta_a\overline{\rho_a}^p.$$

En multipliant les égalités précédentes, il vient

$$x^2+y^2+\left(\zeta^a+\zeta^{-a}\right)xy=\lambda_a\eta_a^2\left(\rho_a\overline{\rho_a}\right)^p. \tag{5.25}$$

L'élévation au carré de $x+y=\eta_0 B_1\lambda^{m-\frac{p-1}{2}}\rho_0^p$ donne

$$x^2+y^2+2xy=\eta_0^2 B_1^2\lambda^{2m-p+1}\rho_0^{2p}. \tag{5.26}$$

La différence de (5.26) par (5.25) et la division par λ_a donne

$$-xy=\eta_a^2\left(\rho_a\overline{\rho_a}\right)^p-\eta_0^2 B_1^2\lambda^{2m-p+1}\rho_0^{2p}\lambda_a^{-1}. \tag{5.27}$$

Comme $p>3$, il existe un entier $b\in\{1,\ldots,p-1\}$ tel que $b\neq\pm a \bmod p$. Pour cet entier b, il vient de même

$$-xy=\eta_b^2\left(\rho_b\overline{\rho_b}\right)^p-\eta_0^2 B_1^2\lambda^{2m-p+1}\rho_0^{2p}\lambda_b^{-1}. \tag{5.28}$$

La différence de (5.28) par (5.27) donne après simplification

$$\eta_a^2\left(\rho_a\overline{\rho_a}\right)^p-\eta_b^2\left(\rho_b\overline{\rho_b}\right)^p=\eta_0^2 B_1^2\lambda^{2m-p+1}\rho_0^{2p}\left(\lambda_a^{-1}-\lambda_b^{-1}\right).$$

Or, comme $b\neq\pm a \bmod p$, on a $\lambda_a^{-1}-\lambda_b^{-1}=\frac{\left(\zeta^{-b}-\zeta^{-a}\right)\left(\zeta^{a+b}-1\right)}{\lambda_a\lambda_b}=\frac{\delta'}{\lambda}$, où δ' est une unité. Comme λ_a, λ_b et λ sont réels, l'unité δ' l'est aussi. Il existe donc une unité réelle η' telle que

$$\left(\frac{\eta_a}{\eta_b}\right)^2\left(\rho_a\overline{\rho_a}\right)^p+\left(-\rho_b\overline{\rho_b}\right)^p=\eta' B_1^2\lambda^{2m-p}\left(\rho_0^2\right)^p, \tag{5.29}$$

où δ est une unité réelle. La condition imposée aux nombres de Bernoulli implique que $\frac{\eta_a}{\eta_b}$ est une puissance p-ième dans $\mathbb{Z}[\lambda]$ (voir [77]) : $\frac{\eta_a}{\eta_b}=\xi^p$. Posons

$$x'=\xi^2\rho_a\overline{\rho_a},\quad y'=-\rho_b\overline{\rho_b},\quad z'=\rho_0^2,\quad m'=2m-p.$$

Ils vérifient bien

$$x'^p+y'^p=\eta' B_1^2\lambda^{m'}z'^p.$$

L'entier B_1 divise B^{2N}. De plus, on a vu que l'entier algébrique ρ_1 n'est pas une unité de $\mathbb{Z}[\zeta]$. Comme $\rho_0\rho_1$ divise z dans $\mathbb{Z}[\zeta]$, le nombre d'idéaux premiers divisant z' dans $\mathbb{Z}[\zeta]$ est donc bien strictement plus petit que celui de z. Enfin, $m'=2m-p\geq 2p-p=p$. La proposition est prouvée.□

Appliquons la proposition (5.3.15) à l'équation (5.22). Par récurrence, elle montre l'existence d'une suite d'entiers algébriques Z_i telle que $Z_{i+1}|Z_i$ dans $\mathbb{Z}[\zeta]$ et dont le nombre de facteurs premiers dans $\mathbb{Z}[\zeta]$ est strictement décroissant. Il existe donc un rang n tel que Z_n soit une unité. Or la proposition (5.3.15) nous assure que chacun des Z_i n'en est pas une : contradiction. La partie $p = q$ du corollaire est prouvée.

Remarque 5.3.16 *Si $\iota(p) = 0$ (p est dit régulier), alors tout unité de $\mathbb{Z}[\zeta]$ congrue à un rationnel modulo p, est une puissance p-ième dans ce même anneau (théorème* 5.36 *de [77]). De plus, l'entier h_p^+ est alors premier à p (théorème* 5.34 *de [77]). Ainsi l'hypothèse portant sur les nombres de Bernoulli et $p \nmid h_p^+$ peuvent être remplacées par la seule condition $\iota(p) = 0$.*

Etudions maintenant le cas $q \neq p$. Alors par hypothèse $Y_0 = -1$ et a est pair. Si (5.5) admet une solution entière X, Z, autre que $X = \pm 1$, $Z = 0$, alors il existe un entier $e \in \{0; 1\}$ et un entier Z_1 divisant Z tel que

$$\frac{X^{ap} - 1}{X^a - 1} = p^e Z_1^q. \tag{5.30}$$

Comme $q \nmid h_p^-$, le théorème (1.1.1) du chapitre 1 montre que $e = 0$. Comme a est pair, le théorème principal de [50] montre alors que l'équation (5.30) est sans solution entière. On a donc bien $X = \pm 1$, $Z = 0$. ■

5.3.5 Démonstration du corollaire (5.1.6).

Comme lors de la démonstration du corollaire (5.1.4), il existe un entier Z tel que

$$\frac{X^p + Y_0^p}{X + Y_0} = Z^p. \tag{5.31}$$

Le lemme (5.3.13) montre qu'aucun des nombres premiers l_i' ne peut diviser Z. On a $|Z| \neq 1$ sauf si $X = Y_0 = \pm 1$, auquel cas on a $B = \pm 2$ ce qui est exclus. Il existe donc un produit de puissances entières de certains l_i qui divise Z. Quitte à changer les notations, on peut supposer que $Z = l_1^{a_1} \dots l_n^{a_n}$, pour un certain entier $n \geq 1$.

Supposons d'abord que $p|X$. Soit $\alpha = X\zeta + Y_0$. Par le lemme (5.3.13), chacun des $l_i, i = 1, \dots, n$ est totalement décomposé dans $\mathbb{Q}(\zeta)$. Pour chaque entier $i = 1, \dots, n$, il existe donc un unique premier $\mathcal{L}_i$ de $\mathbb{Q}(\zeta)$ au dessus de l_i, tels que

$$(\alpha) = \mathcal{L}_1^{pa_1} \dots \mathcal{L}_n^{pa_n}.$$

Soit ζ' une racine primitive L-ième de l'unité. D'après le chapitre 4, il existe des sommes de Gauss $g_1, \ldots, g_n$ contenues dans le corps $\mathbb{Q}(\zeta, \zeta')$ telles que $g_i^p \in \mathbb{Z}[\zeta]$ et

$$\mathcal{L}_i^{2p\vartheta} = \left(g_i^{2p}\right),$$

ϑ étant, rappelons le, l'élément de Stickelberger. Il existe donc une unité u de $\mathbb{Z}[\zeta]$ telle que

$$\alpha^{2p\vartheta} = u g_1^{2a_1 p^2} \ldots g_n^{2a_n p^2}. \tag{5.32}$$

L'entier algébrique $\alpha^{2p\vartheta}$ est un entier de Jacobi. En effet, par (5.31), il existe un idéal $\mathfrak{a}$ de l'anneau $\mathbb{Z}[\zeta]$ tel que $(\alpha) = \mathfrak{a}^p$. Comme tous les facteurs premiers de (α) sont de degrés relatif 1 sur $\mathbb{Q}$, la proposition (4.5.11) montre qu'il existe un entier de Jacobi β et $v \in \mathbb{Z}[\zeta]^\times$ tels que

$$\alpha^{2p\vartheta} = v\beta^p.$$

Comme $(1+j)p\vartheta$ est un multiple entier et positif de la norme (c'est une conséquence de (4.1), chapitre 4) on a $\alpha^{2p\vartheta}\overline{\alpha^{2p\vartheta}} \in \mathbb{Z}$. La proposition (4.4.13) montre alors que $v = \pm\zeta^b$ pour un certain entier b. Le poids de $2p\vartheta$ vaut $p(p-1)$. Comme $Y_0^{p-1} \equiv 1 \bmod (1-\zeta)^2$ et $p|X$ on a

$$\alpha^{2p\vartheta} = (X\zeta + Y_0)^{2p\vartheta} \equiv Y_0^{p(p-1)} \equiv 1 \bmod (1-\zeta)^2,$$

d'où $\pm\zeta^b \equiv 1 \bmod (1-\zeta)^2$. L'unité v vaut donc en fait 1, d'où $\alpha^{2p\vartheta} = \beta^p$. L'entier algébrique $\alpha^{2p\vartheta}$ est donc bien un entier de Jacobi. Comme g_i est une somme de Gauss, $g_i\overline{g_i} \in \mathbb{N}$. On peut donc appliquer la proposition (4.4.13) à (5.32) : elle montre qu'il existe un entier b et $\epsilon = \pm 1$ tel que $u = \epsilon\zeta^b$. Le nombre premier p étant totalement ramifié dans $\mathbb{Q}(\zeta)$ et ayant $g_i^p \in \mathbb{Z}[\zeta]$, il existe un entier a premier à p (car α l'est) tel que

$$g_1^{2a_1 p} \ldots g_n^{2a_n p} \equiv a \bmod (1-\zeta),$$

d'où

$$\alpha^{2p\vartheta} \equiv \epsilon\zeta^b a^p \equiv \epsilon\zeta^b a \bmod (1-\zeta)^2.$$

Comme $\alpha^{p\vartheta} \equiv 1 \bmod (1-\zeta)^2$, on a donc

$$\epsilon\zeta^b a \equiv 1 \bmod (1-\zeta)^2. \tag{5.33}$$

Soit **Tr** la trace relative à l'extension $\mathbb{Q}(\zeta)/\mathbb{Q}$. Par (5.33), on a $p|\mathbf{Tr}\left(\epsilon\zeta^b a - 1\right)$. Si $\zeta^b \neq 1$, il vient $-\epsilon a \equiv -1 \bmod p$, donc $\zeta^b \equiv 1 \bmod (1-\zeta)^2$ par (5.33), ce qui est impossible avec

$\zeta^b \neq 1$. Donc $\zeta^b = 1$. Posons $\Pi = \epsilon g_1^{2a_1} \dots g_n^{2a_n} \in \mathbb{Q}(\zeta, \zeta')$. Par définition des g_i, Π^p est un élément de l'anneau $\mathbb{Z}[\zeta]$. On a

$$\alpha^{2p\vartheta} = \Pi^{p^2}. \tag{5.34}$$

Soit d le degrés de l'extension $\mathbb{Q}_p(\zeta, \Pi)/\mathbb{Q}_p(\zeta)$. Comme Π^p est un élément de l'anneau $\mathbb{Z}[\zeta]$, en particulier, $\Pi^p \in \mathbb{Q}_p(\zeta)$, et l'entier d vaut donc 1 ou p. Comme Π est un élément du corps $\mathbb{Q}(\zeta, \zeta')$, en particulier il se situe dans $\mathbb{Q}_p(\zeta, \zeta')$. Le degrés de l'extension $\mathbb{Q}_p(\zeta, \zeta')/\mathbb{Q}_p(\zeta)$ est donc divisible par d. Or, $\mathbb{Q}_p(\zeta, \zeta')/\mathbb{Q}_p(\zeta)$ a pour degrés l'ordre de $p \bmod L$, qui est premier à p par hypothèse. Il en va donc de même pour d. Comme $d|p$, on doit donc avoir $d = 1$, c'est à dire $\Pi \in \mathbb{Z}_p[\zeta]$. L'égalité (5.34) montre donc que l'entier algébrique $\alpha^{2p\vartheta}$ est une puissance p^2-ième dans $\mathbb{Z}_p[\zeta]$.

Lemme 5.3.17 *Soit $\alpha \in \mathbb{Z}[\zeta]$ premier à p, tel que $\alpha = \beta^{p^k}$, $\beta \in \mathbb{Z}_p[\zeta]$, $k \geq 1$. Il existe alors un entier a, $1 \leq a \leq p-1$ tel que*

$$\alpha \equiv a^{p^k} + \mathrm{mod} p^k (1-\zeta)^2.$$

L'entier a est le premier terme dans le développement de Hensel de β.

Preuve Comme dans la démonstration du lemme (5.2.5), on a, en utilisant le théorème de Wilson :

$$\frac{(1-\zeta)^{p-1}}{p} = -1 + \mathcal{O}(\pi)$$

et donc $\pi^{p-1} = -p + \mathcal{O}(p\pi)$. Soit maintenant $\beta \in \mathbb{Z}[\zeta]$, et écrivons β sous la forme $\beta = a_0 + \pi\gamma$, avec $\gamma \in \mathbb{Z}[\zeta]$, et $a_0 \in \mathbb{Z}$. Supposons que z soit une puissance p-ième locale de $\mathbb{Q}(\zeta)$, ie $z = \beta^p$, avec $\beta \in \mathbb{Q}_p(\zeta)$. Soit a_0 le premier terme dans le développement de Hensel de β. On pose aussi $\beta = a_0 + \pi\gamma$. On désigne également par c le premier terme dans le développement de Hensel de γ. On a alors, modulo un $\mathcal{O}(p\pi^2)$, en utilisant la remarque initiale :

$$\begin{aligned} z = (a_0 + \pi\gamma)^p &\equiv a_0^p + a_0^{p-1} p\pi\gamma + \pi^p \gamma^p \\ &\equiv a_0^p + pc\pi + c\pi^{p-1}\pi \equiv a_0^p + pc\pi - pc\pi \equiv a_0^p \end{aligned} \tag{5.35}$$

ce qui prouve l'assertion pour $k = 1$. Soit maintenant $k > 1$ un entier. Supposons maintenant que z soit une p^k-ième puissance locale de $\mathbb{Q}(\zeta)$. En utilisant les mêmes notations que précédemment, on a $z = (a_0 + \pi\gamma)^{p^k}$. Rappelons que si v_p désigne la valuation p-adique usuelle, on a

$$v_p\left(\binom{p^k}{n}\right) = k - v_p(n).$$

En effet :

$$\begin{aligned} v_p(n!\binom{p^k}{n}) &= k + v_p(p^k-1) + \ldots + v_p(p^k-(n-1)) \\ &= k + v_p((n-1)!) \end{aligned} \tag{5.36}$$

On a donc $v_p\left(\binom{p^k}{n}\right) = k + v_p((n-1)!) - v_p(n!) = k - v_p(n)$. On en déduit que si on développe $(a_0+\pi\gamma)^{p^k}$, les seuls termes qui ne s'annulent pas modulo $p^k\pi^2$, est celui d'indice $0, 1$ et p. En effet, on a :

$$v_{\mathfrak{p}} = \nu_{\mathfrak{p}}\left(\binom{p^k}{j} a_0^{p^k-j}(\pi\gamma)^j\right) \geq (p-1)(k-v_p(j)) + j \geq k(p-1)+2 \tag{5.37}$$

si $j \geq 2$ et $(p,j)=1$. Si $p^2|j$, on a $v_{\mathfrak{p}} \geq p^2 + (p-1)(k-2) \geq k(p-1)+2$, car $p \geq 3$. Si $j=p$, on a $v_{\mathfrak{p}} = p + (p-1)(k-1) = 1 + k(p-1) < 2 + k(p-1)$. Donc, seuls les termes d'indice $j = 0, 1$ et p, sont non nuls modulo $p^k\pi^2$. On a donc, à l'ordre $p^k\pi^2$:

$$z \equiv a_0^{p^k} + a_0^{p^k-1}c\pi + \binom{p^k}{p} a_0^{p^k-p}(c\pi)^p \equiv a_0^{p^k} + c\pi - c\pi \equiv a_0^{p^k} \bmod p^k\pi^2.$$

□

Il existe donc un entier a, $1 \leq a < p$ tel que

$$\alpha^{2p\vartheta} \equiv a^{p^2} \bmod p^2(1-\zeta)^2.$$

L'entier a est le premier terme du developpement de Hensel de $\Pi \in \mathbb{Z}_p[\zeta]$. Soit U (respectivement U_1) les unités (respectivement les unités principales) de $\mathbb{Z}_p[\zeta]$. Le groupe U_1 est d'indice $p-1$ dans U (voir [28]) et $\Pi \in U$ car α est premier à p. Comme $\Pi^{p^2} = \alpha^{2p\vartheta} \equiv 1 \bmod (1-\zeta)$, on a donc $\Pi \equiv 1 \bmod (1-\zeta)$, d'où $a = 1$ et

$$(X\zeta + Y_0)^{2p\vartheta} \equiv 1 \bmod p^2(1-\zeta)^2. \tag{5.38}$$

Lors de la démonstration de la proposition (5.3.7), on a vu que $p|X$ implique $p^2|X$. On obtient alors en développant

$$\alpha^{2p\vartheta} \equiv Y_0^{p(p-1)} + Y_0^{p(p-1)-1} X \sum_{t=1}^{p-1} 2t\zeta^{t^{p-2}} \bmod p^2(1-\zeta)^2, \tag{5.39}$$

Comme $2p\vartheta$ est de poids $p(p-1)$ et $Y_0^{p-1} \equiv 1 \bmod p^2$, on a donc $Y_0^{2p\vartheta} \equiv 1 \bmod p^3$. Des congruences (5.38) et (5.39), il vient alors

$$Y_0^{p(p-1)-1} X \sum_{t=1}^{p-1} 2t\zeta^{t^{p-2}} \equiv 0 \bmod p^2(1-\zeta)^2.$$

Comme $\zeta^{t^{p-2}} \equiv 1 - t^{p-2}(1-\zeta) \bmod (1-\zeta)^2$, il vient

$$\sum_{t=1}^{p-1} t\zeta^{t^{p-2}} \equiv (1-\zeta) \bmod (1-\zeta)^2 \neq 0 \bmod (1-\zeta)^2.$$

On a donc $X \equiv 0 \bmod p^2(1-\zeta)$, d'où $p^3|X$. La deuxième partie du théorème (5.1.2) appliquée à (5.31) montre[6] alors que $p|h_p^+$, ce qui n'a pas lieu par hypothèse. Les autres cas, c'est à dire $p \nmid X$, se traitent comme dans la démonstration du corollaire (5.1.4). Comme on ne peut avoir $X^a = -Y_0$, l'équation (5.6) n'admet donc aucune solution entière primitive. ■

5.3.6 Démonstration du corollaire (5.1.7).

La démonstration du fait que $r^{p-1} \equiv 1 \bmod p^3$ pour tout facteur premier r de y_0 (si $y_0 \neq \pm 1$) est semblable à celle éffectuée lors de la preuve du théorème (5.1.2). Néanmoins, comme l'exposant de z dans l'équation (5.7) est p^2, au lieu de travailler avec des puissances p-ième d'entiers de Jacobi, on travaille avec des puissances p^2-ième, d'où le terme plus précis de p^3. De même, si $p \nmid x$, $r^{p-1} \equiv 1 \bmod p^3$ pour tout facteur premier r de x. En particulier, comme x est pair, si $2^{p-1} \neq 1 \bmod p^3$, alors $p|x$. Comme l'exposant de z dans l'équation (5.7) est p^2, avec les notations de la preuve précédente, on a

$$\alpha^{2p\vartheta} = \Pi^{p^3}, \quad \Pi^p \in \mathbb{Z}[\zeta].$$

L'entier algébrique $\alpha^{2p\vartheta}$ est donc une puissance p^2-ième dans $\mathbb{Z}[\zeta]$. La preuve précédente montre alors que $p^3|x$. Ainsi, les entiers x, y_0 et z vérifient

$$\frac{x^p + y_0^p}{x + y_0} = (z^p)^p, \quad (x, y_0, z) = 1, \quad p^3|x, \quad |y_0| \leq \frac{p}{19}.$$

La seconde partie du théorème (5.1.2) montre alors que $p|h_p^+$. ■

5.3.7 Exemple (5.1.10) détaillé.

Soit $\alpha = \zeta x^a + y_0$. Comme $p|x$, la preuve du corollaire (5.1.6) montre qu'il existe un caractère mutiplicatif χ d'ordre p, un caractère additif ψ d'ordre l, $\epsilon = \pm 1$ tels que

$$\alpha^{2p\vartheta} = \epsilon g\left(\chi, \psi\right)^{2vp^2}. \tag{5.40}$$

En fait, comme

$$g\left(\chi, \psi\right) = -1 + \sum_{x=1}^{l-1} \left(\chi(x) - 1\right) \psi(x)$$

[6] Rappelons que l'on a posé $|Y_0| \leq \frac{p}{19}$.

et $\alpha^{2p\vartheta} \equiv 1 \bmod (1-\zeta)$, on a $\epsilon = 1$. Posons

$$\alpha^{2\vartheta} = \sum_{k=0}^{\infty} \binom{1/p}{k} \left(\alpha^{2p\vartheta} - 1\right)^k \in \mathbb{Z}_p[\zeta],$$

cette série étant bien convergente car $p^3 | x^a$. Par (5.40), il existe donc un entier n tel que

$$\zeta^n \alpha^{2\vartheta} = g(\chi, \psi)^{2vp}$$

Comme $\alpha^{2\vartheta} \equiv g(\chi, \psi)^{2vp} \equiv 1 \bmod (1-\zeta)^2$, on a $\zeta^n = 1$. Posons alors

$$\alpha^{\frac{2\vartheta}{p}} = \sum_{k=0}^{\infty} \binom{1/p}{k} \left(\alpha^{2\vartheta} - 1\right)^k \in \mathbb{Z}_p[\zeta],$$

cette série étant bien convergente car $p^3 | x^a$. Par (5.40), il existe donc un entier n' tel que

$$\zeta^{n'} \alpha^{\frac{2\vartheta}{p}} = g(\chi, \psi)^{2v}.$$

En particulier, $g(\chi, \psi)^{2v} \in \mathbb{Z}_p[\zeta]$. D'un autre côté, $g(\chi, \psi) \in \mathbb{Q}_p(\zeta, \zeta_l)$, où ζ_l est une racine primitive l-ième de l'unité. Soit τ le générateur de $\mathrm{Gal}(\mathbb{Q}_p(\zeta, \zeta_l)/\mathbb{Q}_p(\zeta))$ défini par $\zeta_l^\tau = \zeta_l^p$. On a

$$g(\chi, \psi)^{2v\tau} = \overline{\chi(p)}^{2v} g(\chi, \psi)^{2v}.$$

Comme on vient de montrer que $g(\chi, \psi)^{2v} \in \mathbb{Z}_p[\zeta]$, on doit avoir

$$\overline{\chi(p)}^{2v} = 1,$$

donc $p | v$ car χ est d'ordre p et p racine primitive modulo l. Ainsi $p | v$ et les entiers x^a, $l^{v/p}$ constituent une solution de l'équation diagonale. Comme $p^3 | x^a$, le théorème (5.1.2) montre que $p | h_p^+$.

Chapitre 6

Arithmétique de l'équation $X^p + Y^p = BZ^q$.

6.1 Introduction

Sur l'équation de Nagell-Ljunggren générale $\frac{x^p+y^p}{x+y} = p^e z^q$, p, q premiers impairs distincts, on commence par montrer le théorème suivant :

Théorème 6.1.1 *Soient p, q deux nombres premiers impairs distincts. Soit $e \in \{0, 1\}$. Supposons qu'il existe des entiers x, y, z premiers entre eux dans leur ensemble tels que*

$$\frac{x^p + y^p}{x + y} = p^e z^q, \quad q \nmid y. \tag{6.1}$$

On a les assertions suivantes :

1. *Si $q|x$, alors $q^2|x$.*
2. *Si q ne divise pas h_p^- et si $q < Sup\left(p, \frac{p(p-20)}{16}\right)$, alors il existe un entier $f \in \{-1, 0, 1\}$ tel que*

$$q^2|x + fy.$$

3. *Supposons que $p \equiv 3 \bmod 4$ et que q ne divise pas h_p^-. Si $q|x+y$, alors en fait $q^2|x+y$.*
4. *Soient m l'ordre de 2 modulo p et $\epsilon = (-1)^{\frac{p^2-1}{8}}$. Supposons que q ne divise ni h_p^-, ni $\left(2^{m/2^{\frac{1-\epsilon}{2}}} - \epsilon\right)$. Si $q|x - y$, alors en fait $q^2|x - y$.*

Nous rappelons la définition suivante :

Definition 6.1.2 *On appelle fonction de Moebius, la fonction notée μ et définie sur $\mathbb{N}^*$ par*

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1, \\ 0 & \text{si } n > 1 \text{ et divisible par le carré d'un premier,} \\ (-1)^r & \text{si } n \text{ est le produit de } r \text{ premiers.} \end{cases}$$

La démonstration du théorème précédent, nous amènera à démontrer la proposition suivante,

Proposition 6.1.3 *Soit $p > 2$ un nombre premier. Soit $\zeta_0 = e^{\frac{2i\pi}{p}}$, $a \in \mathbb{F}_p^\times$ et b un nombre rationnel. Soit g une racine primitive modulo p, et soit $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ défini par $\zeta^\sigma = \zeta^g$. Soit $\mathcal{E}(p,a,b)$ le determinant circulant gauche, dont la première ligne est donnée par*

$$\frac{1}{b-\zeta_0^a} - \frac{1}{b-\zeta_0^{-a}} \quad \frac{1}{b-\zeta_0^{a\sigma}} - \frac{1}{b-\zeta_0^{-a\sigma}} \cdots \frac{1}{b-\zeta_0^{a\sigma^{\frac{p-3}{2}}}} - \frac{1}{b-\zeta_0^{-a\sigma^{\frac{p-3}{2}}}}.$$

Le nombre algébrique $\mathcal{E}(p,a,b)$ est un nombre algébrique de Gauss. Plus précisément, il existe un nombre rationnel $E(p,a,b)$ tel que $\mathcal{E}(p,a,b) = E(p,a,b)\sqrt{-p}$ et $E(p,a,b) = 0$ si $p \equiv 1 \bmod 4$. Si $b = 0$ ou si $b = \pm 1$, $E(p,a,b)$ est en fait un entier. On a les valeurs explicites suivantes :

$$E(p,a,b) = \begin{cases} 2^{\frac{p-3}{4}} p^{\frac{p-7}{4}} h_p^- \left(\frac{a}{p}\right) & \text{si } b = 1, \\ -(-1)^{\frac{p-1}{m}} 2^{\frac{p-3}{2}} p^{\frac{p-7}{4}} h_p^- \left(2^{m/2^{\frac{1-\epsilon}{2}}} - \epsilon\right)^{\frac{p-1}{2^{\frac{1+\epsilon}{2}} m}} \left(\frac{a}{p}\right), & \text{si } b = -1, \\ \left(\frac{a}{p}\right) p^{\frac{p-3}{4}} & \text{si } b = 0. \end{cases}$$

où m est l'ordre de 2 modulo p, et $\epsilon = (-1)^{\frac{p^2-1}{8}}$. De plus, s'il existe un nombre premier impair q tel que $p = 1 + 2q$, ou bien si $p \equiv 3 \bmod 4$ et

$$\sum_{k=1}^{\frac{p-3}{2}} \frac{\mu\left(\frac{p-1}{2gcd(\frac{p-1}{2},k)}\right)}{\varphi\left(\frac{p-1}{2gcd(\frac{p-1}{2},k)}\right)} \neq -1, \tag{6.2}$$

alors $E(p,a,b) \neq 0$ pour tout entier b.

Remarque 6.1.4
- $-\sum_{k=1}^{\frac{p-3}{2}} \frac{\mu\left(\frac{p-1}{2gcd(\frac{p-1}{2},k)}\right)}{\varphi\left(\frac{p-1}{2gcd(\frac{p-1}{2},k)}\right)} = -1$ *si $p = 1 + 2q$, q nombre premier.*
- *En complément, on montrera (voir le paragraphe (6.3.8)), que si $b \neq 1$ est un nombre rationnel, on a*

$$E(p,a,b) = -\frac{1}{p^{\frac{p+1}{4}}} \prod_{\chi \in \hat{G}^-} \left(\sum_{z=1}^{p-1} \overline{\chi}(z) \left(-b^{z-1} \left(p - 1 - \frac{z-1}{b} \right) + b^z \tau(0,b) \right) \right).$$

où φ_p désigne le p-ième polynôme cyclotomique et $\tau(0,b) = \frac{1+b^{p-1}(bp-b-p)}{\varphi_p(b)(1-b)^2}$ (voir le lemme (6.3.13)).

Cette proposition admet le corollaire suivant :

Corollaire 6.1.5 *Soit $\mathcal{C}(p,a)$ le determinant circulant gauche, dont la première ligne est donnée par*

$$\frac{1}{1-\zeta_0^a} \quad \frac{1}{1-\zeta_0^{a\sigma}} \cdots \frac{1}{1-\zeta_0^{a\sigma^{\frac{p-3}{2}}}}.$$

On a alors

$$\mathcal{C}(p,a) = p^{\frac{p-7}{4}} h_p^- \left(\frac{a}{p}\right) \left(\frac{p-1}{4h(-p)} + \frac{\sqrt{-p}}{2}\right).$$

On en déduit en particulier

$$h_p^- \leq 6h(-p)\sqrt{p}\left(\frac{p-1}{24}\right)^{\frac{p-1}{4}}. \tag{6.3}$$

Remarque 6.1.6 *On conjecture que*

$$h_p^- \sim 2p\left(\frac{p-1}{4\pi^2}\right)^{\frac{p-1}{4}} = 2p\left(\frac{p-1}{39.4784...}\right)^{\frac{p-1}{4}}.$$

En lien avec la proposition (6.1.3), on donne la définition suivante, qui nous sera utile lors de l'énoncé du corollaire (6.1.20) :

Definition 6.1.7 *Soient $p,q > 2$ deux nombres premiers, $p \equiv 3 \bmod 4$. Soit $b > 0$ un entier.*

- *On dit que le couple (p,q) est b-convenable si le nombre rationnel $E(p,a,b)$ est non nul et a un numérateur premier à q.*
- *On dit que le couple (p,q) est convenable, s'il est b-convenable pour tout entier b tel que $0 < b < q$.*

On donne également la définition suivante :

Definition 6.1.8 *Soient $p,q > 2$ deux nombres premiers impairs, $p \equiv 3 \bmod 4$. Soit C (respectivement N) l'ensemble des carrés modulo p (respectivement l'ensemble des non-carrés modulo p). Soit $b > 1$ un entier, $b < q$.*

– *On dit que le couple (p,q) est b-sous-convenable, si l'entier*[1] Q_b, *défini par*

$$Q_b = \sum_{c\in C} b^{q-1-c} - \sum_{n\in N} b^{q-1-n},$$

est premier à q.

– *On dit que le couple (p,q) est sous-convenable, s'il est b-sous-convenable pour tout entier b tel que $0 < b < q$.*

Remarque 6.1.9 *Si p, q sont deux nombres premiers impairs distincts, vu la proposition (6.1.3), supposer que le couple (p,q) est 1-convenable, revient à supposer que $q \nmid h_p^-$. On montrera au lemme (6.10.1), que si x_1 et x_2 sont dans la même classe modulo q, et si $q \neq 1 \bmod p$, alors $E(p,1,x_1) \equiv E(p,1,x_2) \bmod q$. En particulier, si $q \neq 1 \bmod p$, vu la proposition (6.1.3), supposer que le couple (p,q) est $(q-1)$-convenable, revient à supposer qu'il est (-1)-convenable, c'est à dire $q \nmid h_p^- \left(2^{m/2^{\frac{1-\epsilon}{2}}} - \epsilon\right)$.*

Ces deux notions sont liées par la proposition suivante (voir le paragraphe (6.3.9) :

Proposition 6.1.10 *Un couple de nombres premiers (p,q) convenable et vérifiant $q \neq 1 \bmod p$, est toujours sous-convenable, la réciproque étant généralement fausse. Néamoins, si $p - 1 = 2q$, il y a équivalence entre ces deux notions.*

Ainsi, si $p - 1 = 2q$, on pourra remplacer la condition de convenabilité par la condition moins forte de sous-convenabilité (voir par exemple le corollaire (6.1.20)).

Donnons maintenant quelques corollaires, que l'on déduit du théorème (6.1.1) lui-même. On les énonce les uns à la suite des autres. On les illustre par quelques exemples. Les derniers résultats que l'on obtiendra à partir du théorème (6.1.1), auront pour objet l'étude de l'existence de solutions de deux équations diophantiennes simultanées de la forme de celle du titre (voir théorème (6.1.18) et corollaire (6.1.20)).

Corollaire 6.1.11 *Soient p, q deux nombres premiers impairs distincts, tels que $p \equiv 3 \bmod 4$ et $(q, h_p^-) = 1$, ou $p \equiv 1 \bmod 4$, $(q, h_p^-) = 1$ et $p > 181$. Supposons qu'il existe deux entiers x, y tels que*

$$\frac{x^p - 1}{x - 1} = y^q, \quad q | x - 1. \tag{6.4}$$

On a alors $q^2 | x - 1$.

Si (p,q) est un couple de nombres premiers impairs, on introduit les ensembles $\mathcal{F}_{p,q}$ suivants :

[1] Un tel entier est non nul car $p \equiv 3 \bmod 4$: voir le paragraphe (6.3.5).

Definition 6.1.12 *L'ensemble $\mathcal{F}_{p,q}$, est l'ensemble des entiers $F \neq 0$, premiers à p, tels que $|F| > 1$, et si $|F| = L_1^{e_1} \dots L_t^{e_t}$ est sa décomposition en produits de facteurs premiers, alors pour tout entier i tel que $1 \leq i \leq t$, on a $L_i^{e_i f_i} \neq 1 \bmod q$, f_i étant l'ordre de L_i modulo p.*

Definition 6.1.13 *L'ensemble $\mathcal{G}_{p,q}$, est l'ensemble des entiers F tels que $F^{q-1} \neq 1 \bmod q^{q+1}$.*

Rappelons que si $n > 1$ est un entier, on appelle radical de n, que l'on note $Rad(n)$, le produit des facteurs premiers de n. Par convention, on posera $Rad(1) = 1$. Afin de simplifier les notations, φ étant l'indicatrice d'Euler, on pose pour la suite :

$$\Psi(B) = \varphi\left(Rad(B)\right).$$

Enfin, si $B > 0$ est un entier, on note B^* l'unique entier libre de carré tel qu'il existe un entier C vérifiant $B = B^* C^2$.

Corollaire 6.1.14 *Soient p, q deux nombres premiers distincts, avec $p > 2$. On suppose que $q \neq 1 \bmod p$. Soit $B > 0$ un entier. On se fixe également un nombre entier Y_0 premier à p si $q > 2$, et un entier $l \geq 0$. On notera r, le reste de la division euclidienne de l par 2. Suivant les valeurs de p et q, nous faisons les hypothèses supplémentaires suivantes :*

1. *si $q = 2$ et $p \geq 7$, on suppose :*
   - $Y_0 = 1$ *ou* Y_0 *premier ;*
   - $Y_0 \neq \left(\frac{-B^*}{Y_0}\right) \bmod p$ *si* $Y_0 > 2$ *et l pair ;*
   - $Y_0 \neq 3$ *si l est impair ;*
2. *si $q = 2$, $p = 3$ et $B^* = 1$, on suppose :*
   - $Y_0 = 1$ *ou* Y_0 *premier ;*
   - $Y_0 \neq \left(\frac{-1}{Y_0}\right) \bmod 3$ *si* $Y_0 > 2$ *et l pair ;*
   - $Y_0 \neq 3$ *;*
   - $Y_0^l \neq 2, 4$ *;*
   - $Y_0 \neq 3 \bmod 4$ *si l est impair ;*
   - $l \neq 2$ *si* $Y_0 > 2$ *;*
   - *si* $(l, 6) = 1$ *et* $Y_0 > 2$*, il n'exite pas d'entier* A_0 *tel que* $Y_0^l = 3A_0^2 - 1$.
3. *Si $q = 2$, $p = 3$ et $B^* > 1$ on fera les hypothèses suivantes :*
   - $Y_0 = 1$ *ou* Y_0 *premier ;*
   - $Y_0 \neq \left(\frac{-B^*}{Y_0}\right) \bmod 3$ *si* $Y_0 > 2$ *et l pair ;*
   - $Y_0 \neq 3$ *si l est impair ;*

- *si* $Y_0 = 2$ *et* $2|l$, $l > 0$, *il n'existe pas d'entier* b *tel que* $B^*b^2 = \frac{1+2^{\frac{l}{2}+3}}{3}$ *si* $4|l$ *et il n'existe pas d'entier* b *tel que* $B^*b^2 = \frac{2^l-1}{3}$;
- *si* $Y_0 = 2$ *et* $2 \nmid l$, *il n'existe pas d'entier* b *tel que* $B^*b^2 = \frac{2^l+1}{3}$;
- $B^*Y_0^r \neq 3 \bmod 4$ *si* $Y_0 \neq 2$;
- *il n'existe pas d'entier* A *et* $\epsilon_0 = \pm 1$, *tels que* $A^2B^* = 3^{l-3+r} + \epsilon_0$ *si* $Y_0 = 3$;
- *il n'existe pas d'entier* A *et* $\epsilon_0 = \pm 1$, *tels que* $3A^2B^* = Y_0^l + \epsilon_0$;
- *il n'existe pas d'entier* A *et* k *tels que* $8Y_0^r = sY_0^{\frac{l-r}{2}} + 3^{k+1}\epsilon_0$, *ou bien tels que* $A^2B^* = 3Y_0^r - 3^k\epsilon_0$, $\epsilon_0 = \pm 1$, $s = \pm 1$, *si* $Y_0 \neq 2$;
- *il n'existe pas d'entier* A *et* k *tels que* $8Y_0^l = s + 3^{k+1}$, $s = \pm 1$ *ou bien tels que* $A^2B^* = 3Y_0^l - 3^k$, *si* $Y_0 \neq 2$;

4. *Si* $q = 2$, $p = 5$, $B^* > 1$, *on fera les hypothèses suivantes :*
   - Y_0 *premier ;*
   - $Y_0 \neq \left(\frac{-B^*}{Y_0}\right) \bmod 5$ *si* $Y_0 > 2$, l *pair*, $l > 0$;
   - $B^*Y_0^r \neq 7 \bmod 8$;
   - *si* $2|l$, $\nexists B|Y_0^l$, $\quad E \in \mathbb{N}$ *tels que* $\frac{Y_0^{\frac{l}{2}}}{B} + 4B^4 = 5E^2$;
   - *si* $2 \nmid l$, $\nexists B|Y_0^l$, $\quad E \in \mathbb{N}$ *tels que* $\frac{Y_0^{\frac{l-1}{2}}}{B} + 4B^4Y_0^2 = 5E^2$;

5. *Si* $q > 2$, *on suppose que l'on est dans l'une des situations suivantes, dans lesquelles les entiers* B *et* l *vérifieront toujours les conditions* $(\Psi(B), p) = 1$ *et* $l = p$:
   (a) *soit* $p|B$, $Y_0 = 1$;
   (b) *soit* $p|B$, $q||B$, $Y_0 \in \mathcal{F}_{p,q}$, Y_0 *est un élément de* $\mathcal{G}_{p,q}$, $p \equiv 3 \bmod 4$, *ou bien* $p \equiv 1 \bmod 4$ *et* $q < Sup\left(p, \frac{p(p-20)}{16}\right)$;
   (c) *soit* $q||B$, $Y_0 = 1$, $p \in \mathcal{G}_{p,q}$, $p \equiv 3 \bmod 4$, *ou bien* $p \equiv 1 \bmod 4$ *et* $p > 181$,
   (d) *soit* $q||B$, $pY_0^{(p-1)} \in \mathcal{G}_{p,q}$, $Y_0 \in \mathcal{G}_{p,q}$, $p \neq 1 \bmod q$ *si* $Y_0 \neq \pm 1$, $p \equiv 1 \bmod 4$ *et* $q < Sup\left(p, \frac{p(p-20)}{16}\right)$, *ou bien* $p \equiv 3 \bmod 4$,

   Supposons que l'équation diophantienne

$$X^p = Y_0^l + BZ^q, \quad X \neq \pm 1, \quad (X, Y_0, Z) = 1, \tag{6.5}$$

   admette une solution en nombres entiers X, Z. *Alors, soit* $q = 2$, *et on a* $p|h(-B^*Y_0^r)$, *soit* $q > 2$, *et on a* $q|h_p^-$.

Remarque 6.1.15 – *Si* $q = 2$, $p = 3$, $B^* = 1$, $Y_0^l = 4$, *l'équation (6.5) admet* $X = \pm 11$, $Z = 5$ *comme solution, tandis que* $h(-1) = 1$. *On est alors dans le cas particulier des équations d'Aigner.*

– *Si* $q = 2$, $p = 3$, $B^* = 1$, $Y_0^l = 2$, *l'équation (6.5) admet* $X = \pm 5$, $Z = 3$ *comme solution, tandis que* $h(-2) = 1$. *On est alors dans le cas particulier des équations de Muriefah.*
– *Si* $q = 2$, $p = 5$, $B = B^* = 2$ *et* $Y_0 = 1$, *l'équation (6.5) a pour solution* $Z = 11$, $X = 3$, *tandis que* $h(-2) = 1$ *est premier à* 3.

Le corollaire suivant étend le théorème 4 de [54] :

Corollaire 6.1.16 *Soient* p, q *deux nombres premiers impairs distincts tels que* $q < Sup\left(p, \frac{p(p-20)}{16}\right)$ *et soit* $e \in \{0; 1\}$. *Soit* $y_0 = \pm 1$ *ou bien* $y_0 \in \mathcal{F}_{p,q}$ *un entier fixé, premier à* q. *On fait les hypothèses suivantes :*

1. *si* $y_0 = \pm 1$ *on suppose que* $p^{q-1} \neq 1 \bmod q^2$, *et* $q \nmid \boldsymbol{Tr}\left(\frac{1-\zeta^{1-q}}{(1+\zeta^{-q})(1-\zeta)}\right)$,
2. *si* $y_0 \neq \pm 1$, *et* $e = 0$, *on suppose que* $y_0^{(p-1)(q-1)} \neq 1 \bmod q^2$ *et* $y_0^{(p-1)(q-1)} p^{q-1} \neq 1 \bmod q^2$,
3. *si* $y_0 \neq \pm 1$, *et* $e = 1$, *on suppose que* $y_0^{(p-1)(q-1)} \neq 1 \bmod q^2$ *et* $y_0^{(p-1)(q-1)} \neq p^{q-1} \bmod q^2$.

S'il existe des entiers x, z *tels que*

$$\frac{x^p + y_0^p}{x + y_0} = p^e z^q, \quad x \neq \pm 1, \quad (x, y_0, z) = 1,$$

alors le nombre premier q *divise* h_p^-.

En guise d'application à la théorie des groupes du corollaire précédent, on donne la proposition suivante :

Proposition 6.1.17 *Soit* $n \geq 3$ *un entier,* p *un nombre premier, et* q *une puissance d'un nombre premier. Soit* $G = PSL_n(q)$. *Supposons qu'il existe un sous-groupe* H *de* G *et un entier* $a \geq 3$ *tel que* $[G : H] = p^a$. *Alors* n *est premier,* $(a, n) = 1$ *et* h_p^- *est divisible par le produit des facteurs premiers impairs de* a.

Du théorème (6.1.1) et de son corollaire précédent, on déduit le théorème suivant :

Théorème 6.1.18 *Soient* p, q *deux nombres premiers impairs distincts,* $q \neq 1 \bmod p$ *si* $p \equiv 3 \bmod 4$. *Soit* $Y_0 = \pm 1$ *ou* $Y_0 \in \mathcal{F}_{p,q}$ *un entier fixé. On supposera toujours* $q < Sup\left(p, \frac{p(p-20)}{16}\right)$ *si* $p \equiv 1 \bmod 4$. *Soient* B_1, B_2 *deux entiers premiers à* p, *tels que* $(\Psi(B_1), p) = (\Psi(B_2), p) = 1$, *et tels que* $q || B_1 + Y_0 B_2$. *Soit* $\mathcal{S}$ *l'ensemble des entiers valant*

0 *ou non nuls et ayant au plus un facteur premier valant* $1 \bmod p$. *Supposons qu'il existe des entiers* X, A, Z *tels que*

$$\begin{cases} X^p = Y_0^p + B_1 Z^q, \quad Z \geq 0, \quad X \geq 0, \\ A^p = -1 + B_2 Z^q, \\ Z \in \mathcal{S}, Z = 0, ou \quad (X, Y_0, Z) = 1. \end{cases} \tag{6.6}$$

Si $Z \neq 0$ *et* $X \neq 1$, *alors on est dans l'un des cas suivants :*

1. *soit* $Y_0 = \pm 1$, $p \equiv 1 \bmod 4$, *et alors le nombre premier* q *divise au moins l'un des trois entiers suivants :*

$$h_p^-, \quad \frac{p^{q-1}-1}{q}, \quad \boldsymbol{Tr}\left(\frac{1-\zeta^{1-q}}{(1+\zeta^{-q})(1-\zeta)}\right);$$

2. *soit* $Y_0 \neq \pm 1$, $p \equiv 1 \bmod 4$, *et alors le nombre premier* q *divise au moins l'un des quatres entiers suivants :*

$$h_p^-, \quad \frac{\left(Y_0^{(q-1)(p-1)}-1\right)}{q}, \quad \frac{\left(\left(pY_0^{p-1}\right)^{q-1}-1\right)}{q}, \quad \frac{\left(Y_0^{q-1}-p^{q-1}\right)}{q};$$

3. *soit* $p \equiv 3 \bmod 4$, *et alors le couple* (p, q) *n'est pas convenable au sens de la définition (6.1.7) ; autrement dit le nombre premier* q *divise* h_p^-, *ou bien* $2^{\frac{m}{2^{\frac{1-\epsilon}{2}}}} - \epsilon$ *(*m *étant l'ordre de* $2 \bmod p$, $\epsilon = (-1)^{\frac{p^2-1}{8}}$*) ou bien le numérateur de l'un des* $E(p, 1, c)$, *avec* $2 \leq c \leq q-2$,
4. *soit* $p \equiv 3 \bmod 4$, $Y_0 = \pm 1$, *et alors* q^q *divise* $p^{q-1} - 1$;
5. *soit* $p \equiv 3 \bmod 4$, $Y_0 \neq \pm 1$ *et alors* q^q *divise au moins l'un des trois entiers suivants :*

$$Y_0^{(q-1)(p-1)} - 1, \quad \left(pY_0^{p-1}\right)^{q-1} - 1, \quad Y_0^{q-1} - p^{q-1};$$

Exemple 6.1.19 *Prenons* $p = 7$ *(donc* $h_p^- = 1$*) et* $q = 5$. *On vérifie que*

$$E(7, 1, c) = \begin{cases} \frac{7 \cdot 41 \cdot 919}{(2^7-1)^3} & si\ c = 2, \\ \frac{2^5 \cdot 7^2 \cdot 151 \cdot 463}{(3^7-1)^3} & si\ c = 3, \end{cases}$$

ainsi que $m = 3$, $\epsilon = 1$, *soit* $2^{\frac{m}{2^{\frac{1-\epsilon}{2}}}} - \epsilon = 7$. *Fixons deux entier* B_1, B_2 *premiers à* 7, *tels que* $(\Psi(B_i), 7) = 1$, $i = 1, 2$. *Fixons également un entier* Y_0 *premier à* 5 *tel que* $Y_0 = \pm 1$ *ou* $Y_0 \in \mathcal{F}_{7,5}$. *Si* $Y_0 \neq \pm 1$, *supposons également que parmi les entiers suivants*

$$Y_0^{24} - 1, \quad \left(7Y_0^6\right)^4 - 1, \quad Y_0^4 - 7^4,$$

aucun ne soit divisible par 5^5. *Le théorème (6.1.18) montre que le système*

$$\begin{cases} X^7 = Y_0^7 + B_1 Z^5, \quad Z \geq 0, \quad X \geq 0, \\ A^7 = -1 + B_2 Z^5, \\ Z \in \mathcal{S}, Z = 0, ou \quad (X, Y_0, Z) = 1. \end{cases}$$

a pour seule solution entière $X = Y_0, Z = 0, A = -1$.

Dans le cas où $p = 1 + 2q$, le corollaire précédent et la proposition (6.1.10) montrent en particulier, que l'on a

Corollaire 6.1.20 *Soient* p, q *deux nombres premiers impairs distincts,* $q \neq 1 \bmod p$ *si* $p \equiv 3 \bmod 4$. *Soit* $Y_0 = \pm 1$ *ou* $Y_0 \in \mathcal{F}_{p,q}$ *un entier fixé premier à* q. *On supposera toujours* $q < Sup\left(p, \frac{p(p-20)}{16}\right)$ *si* $p \equiv 1 \bmod 4$. *Soient* B_1, B_2 *deux entiers premiers à* p *tels que* $(\Psi(B_1), p) = (\Psi(B_2), p) = 1$, *et tels que* $q || B_1 + Y_0 B_2$. *Soit* $\mathcal{S}$ *l'ensemble des entiers valant* 0 *ou non nuls et ayant au plus un facteur premier valant* $1 \bmod p$. *Supposons qu'il existe des entiers* X, A, Z *tels que*

$$\begin{cases} X^p = Y_0^p + B_1 Z^q, \quad Z \geq 0, \quad X \geq 0, \\ A^p = -1 + B_2 Z^q, \\ Z \in \mathcal{S}, Z = 0, ou \quad (X, Y_0, Z) = 1. \end{cases} \tag{6.7}$$

Si $Z \neq 0$ *et* $X \neq \pm 1$, *alors on est dans l'un des cas suivants :*

1. *soit* $Y_0 = \pm 1$, $p \equiv 1 \bmod 4$, *et alors le nombre premier* q *divise l'un des deux entiers suivants*

$$\frac{p^{q-1} - 1}{q}, \quad \boldsymbol{Tr}\left(\frac{1 - \zeta^{1-q}}{(1 + \zeta^{-q})(1 - \zeta)}\right);$$

2. *soit* $Y_0 \neq \pm 1$, $p \equiv 1 \bmod 4$, *et alors* q^2 *divise l'un des trois entiers suivants*

$$Y_0^{(q-1)(p-1)} - 1, \quad \left(pY_0^{p-1}\right)^{q-1} - 1, \quad Y_0^{q-1} - p^{q-1};$$

3. *soit* $p \equiv 3 \bmod 4$, *et alors le nombre premier* q *divise l'un des entiers* Q_b, b *entier,* $1 < b < q - 1$ *(rappelons que les entiers* Q_b *sont définis en 6.1.8),*
4. *soit* $p \equiv 3 \bmod 4$, *et alors le nombre premier* q *divise* $\left(2^{m/2^{\frac{1-\epsilon}{2}}} - \epsilon\right)$, *où* m *est l'ordre de* $2 \bmod p$, $\epsilon = (-1)^{\frac{p^2-1}{8}}$;
5. *soit* $p \equiv 3 \bmod 4$, $Y_0 = \pm 1$, *et alors* q^q *divise* $p^{q-1} - 1$;
6. *soit* $p \equiv 3 \bmod 4$, $Y_0 \neq \pm 1$ *et* q^q *divise l'un des trois entiers suivants :*

$$Y_0^{(q-1)(p-1)} - 1, \quad \left(pY_0^{p-1}\right)^{q-1} - 1, \quad Y_0^{q-1} - p^{q-1};$$

Exemple 6.1.21 *Fixons $p = 11$, $q = 5$, ainsi que deux entiers B_1, B_2 premiers à 11, tels que $(\Psi(B_i, 11) = 1$. Pour un tel p, $m = 10$, $\epsilon = 1$, d'où $2^{m/2^{\frac{1-\epsilon}{2}}} - \epsilon = 7$. On se fixe un entier $Y_0 \in \mathcal{F}_{11,5}$. Si $Y_0 \neq \pm 1$, on suppose que les entiers*

$$Y_0^{40} - 1, \quad \left(11 Y_0^{10}\right)^4 - 1, \quad Y_0^{10} - 11^4,$$

ne sont pas divisibles par 5^5. Les résidus quadratiques modulo 11, parmi les entiers $\{1, \ldots, 10\}$ étant $1, 3, 4, 5, 9$ on a

$$Q_b = b + b^5 + b^6 + b^7 + b^9 - 1 - b^2 - b^3 - b^4 - b^8.$$

On vérifie que $Q_2 = 453$ et $Q_3 = 16166$ qui sont premiers à 5. Enfin, on a $5^5 \nmid 11^4 - 1$. Le corollaire (6.1.20) montre que le système

$$\begin{cases} X^{11} = 1 + B_1 Z^5, \quad Z \geq 0, \quad X \geq 0, \\ A^{11} = -1 + B_2 Z^5, \\ Z \in \mathcal{S}, \end{cases}$$

a alors pour seule solution entière $X = 1, A = -1, Z = 0$.

Dans l'énoncé du corollaire (6.1.14), aux assertions (5c) et (5d), nous faisons l'hypothèse que l'entier B est strictement divisible par q. Dans la suite, on s'intéresse à l'équation (6.5), dans laquelle l'entier B est divisible par q^2 : on obtiendra le corollaire (6.1.23). On commence par démontrer le théorème suivant, dont la démonstration nécessitera une extension d'un théorème de Bugeaud et Hanrot sur les idéaux de Mihăilescu (voir le théorème (6.2.3)) :

Théorème 6.1.22 *Soient p, q deux nombres premiers impairs distincts tels que $3 < p < q$ et $q \nmid h_{pq}^+$. Soient $Y_0 \in \mathbb{Z}^*$, et B un entier divisible par q^2, tel que $p \nmid \Psi(B)$. Supposons qu'il existe des entiers relatifs X, Z tels que*

$$X^p = Y_0^p + BZ^q, \quad (X, Y_0, Z) = 1.$$

On a alors

$$|X| \leq 8 |Y_0| \left(\frac{2}{5} |Y_0| \, q p^{\frac{1}{p-1} + v} \right)^q,$$

où v est la valuation p-adique de Y_0.

Corollaire 6.1.23 *Soient p, q deux nombres premiers impairs, $3 < p < q$. Soient $Y_0 \in \mathbb{Z}^*$, et B, C deux entiers tels que $q^2 | B$, $p \nmid BC\Psi(BC)$, et*

$$BC^q > 8 |Y_0| \left(\frac{2}{5} |Y_0| \, q p^{\frac{1}{p-1} + v} \right)^q,$$

où v est la valuation p-adique de Y_0. Supposons qu'il existe des entiers relatifs X, Z tels que

$$X^p = Y_0^p + BZ^q, \quad (X, Y_0, Z) = 1.$$

Le nombre premier q est alors un diviseur de h_{pq}^+. En particulier, c'est un diviseur de h_{pq}^-.

De la démonstration du théorème (6.1.22), on déduit le résultat complémentaire suivant sur l'équation de Catalan :

Corollaire 6.1.24 *Soient $p < q$ deux nombres premiers impairs. S'il existe des entiers non nuls x, y tels que $x^p - y^q = 1$, alors q divise h_{pq}^+.*

Un autre cas particulier intéressant de (6.5), est celui où B vaut 1 : on obtient l'équation dite de Catalan-Fermat. Pour cette équation, on obtient le nouveau résultat suivant :

Théorème 6.1.25 *Soient p, q deux nombres premiers impairs distincts tels que $3 < p < q < \frac{p(p-20)}{16}$ et soit y_0 un entier fixé, tel que*

$$|y_0| \leq \left(Inf\left(\frac{2}{p^{m+1}}, \frac{1}{2p^{q-m}} \right) \cdot \frac{5^q}{2^{q(p-1)+3}(p-1)^q p^{\frac{q}{p-1}}} q^{\frac{q(q-2)(p-2)}{p-1}} \right)^{\frac{1}{2q+1}}. \tag{6.8}$$

Supposons qu'il existe des entiers relatifs x, z tels que

$$x^p + y_0^p = z^q, \quad (x, y_0, z) = 1, \quad |x| \geq |y_0|.$$

Le nombre premier q est alors un diviseur de h_{pq}^-.

Dans l'énoncé précédent, la condition $q < \frac{p(p-20)}{16}$ pouvant paraître restrictive, on donne une version bis du corollaire (6.1.25), où la condition $q < \frac{p(p-20)}{16}$ est remplacée par deux conditions portant sur p et y_0 :

Corollaire 6.1.26 *Soient p, q deux nombres premiers impairs distincts tels que $3 < p < q$, $p \neq 1 \bmod 8$ et $p \geq 358747$. Soit y_0 un entier fixé, tel que*

$$|y_0| < inf\left(\frac{1}{2p^{\frac{p}{p-1}}} (2p+1)^{\sqrt{5}\left(\frac{p^2(p-20)^2)}{256(p-1)} - 167c_0\left(\frac{1}{2} + \frac{11\pi}{log(2p+1)}\right)\right)}, \left(\frac{5^q}{2^{pq-q+4}(p-1)^q p^{\frac{pq}{p-1}}} q^{\frac{q(pq-2p-3q+5)}{q-1}} \right)^{\frac{1}{q+2}} \right). \tag{6.9}$$

Supposons qu'il existe des entiers relatifs x, z tels que

$$x^p + y_0^p = z^q, \quad (x, y_0, z) = 1, \quad |x| \geq |y_0|.$$

Alors on a

$$q | h_{pq}^-.$$

Afin d'illustrer les résultats précédents, nous donnons trois exemples :

Exemple 6.1.27 *Soient p, q deux nombres premiers tels que $q > 2$. Considérons l'équation en entiers positifs x, y, m :*

$$x^p + 3^{mp} = y^q, \quad (x, y) = 1.$$

On sait déjà (voir le chapitre 3) que dans le cas $p = 2$, cette equation admet des solutions seulement si $q = 3$, et celles-ci sont données par $x = \pm 46, \quad y = 13, \quad m = 2$.

Supposons $p > 2$, $q < Sup\left(p, \frac{p(p-20)}{16}\right)$ et que 3^m vérifie (6.8).

Le corollaire (6.1.25) montre que sous la condition $(q, h_{pq}^-) = 1$, l'entier x est borné strictement par 3^m. En particulier, si on se fixe $m = 1$, comme (6.8) est valide en remplaçant y_0 par 3, l'entier x vaut donc 2, le cas $x = 1$ étant exclus par le théorème de Mihăilescu (anciennement problème de Catalan, voir [28]). On a alors l'équation diophantienne suivante :

$$2^p + 3^p = y^q,$$

ie

$$(y - 3)\frac{y^q - 3^q}{y - 3} = 2^p.$$

Comme $\frac{y^q - 3^q}{y-3} > 1$, c'est donc une puissance de deux. Or, c'est un entier impair. On peut donc énoncer :

Proposition 6.1.28 *Soient p, q deux nombres premiers tels que*

$$2 < q < Sup\left(p, \frac{p(p-20)}{16}\right)$$

Si l'équation

$$x^p + 3^p = y^q, \quad (x, y) = 1.$$

admet une solution en entiers positifs (x, y), alors q divise h_{pq}^-.

Exemple 6.1.29 *(une version faible d'un théorème de Bugeaud et Hanrot) Le corollaire (6.1.24) donne une version faible d'un théorème de Bugeaud-Hanrot sur l'équation de catalan (voir [8]) : soient p, q deux nombres premiers impairs distincts tels que $q > p$. S'il existe*

des entiers non nuls x, y tels que $x^p - y^q = 1$, alors $q|h^+_{pq}$ et donc $q|h^-_{pq}$ par la proposition (6.16.2).

Le théorème de Bugeaud-Hanrot qui étudie uniquement le cas $y_0 = 1$ montre plus précisément que s'il existe des entiers non nuls x, y tels que $x^p - y^q = 1$, alors $q|h^-_p$ si $q > p$. Ce résultat est plus précis que la condition $q|h^-_{pq}$ par le critère de Masley-Montgomery.

On donne maintenant un autre exemple. Le résultat qui y est énoncé **généralise le théorème principal de [76]** :

Exemple 6.1.30 *Soient p, p', q trois nombres premiers impairs tels que $q^2 + 1 = 2p$. Soit m un entier fixé tel que q^m vérifie (6.8). On pose :*

$$e = \begin{cases} 1 & si\ p' = 2, \\ p' & sinon. \end{cases}$$

Considérons l'équation diophantienne suivante, en nombres entiers positifs x, n :

$$\begin{cases} x^{p'} + q^{em} = p^n & n > 1, \\ Rad(n) \nmid q - 1 & si\ p' = 2,\ 2 \nmid n. \end{cases} \tag{6.10}$$

- *Si $p' = 2$, alors elle admet une solution si et seulement si $m = 1$, et celle-ci est alors $x = p - 1, n = 2$.*
- *Si $p' > 2$, et si elle admet une solution (x, n) telle que $x \geq q^m$, alors soit n est une puissance de 2, soit $Rad\left(\frac{n}{2_2^v(n)}\right)$ divise $h^-_{p' \frac{Rad(n)}{2_2^v(n)}}$.*

On termine ce paragraphe, en montrant que la condition $q < \frac{p(p-20)}{16}$ n'est pas si restrictive :

Théorème 6.1.31 *Soient p, q deux nombres premiers impairs distincts, $e \in \{0; 1\}$ et $|y_0|$ un entier tel que $|y_0| < \frac{\left(p+\frac{1}{2}\right)^{\frac{p-1}{2}}}{2}$. Supposons que l'équation*

$$\frac{x^p + y_0^p}{x + y_0} = p^e z^q, \quad (x, y_0, z) = 1, \quad |x| \geq 2|y_0|, \tag{6.11}$$

admette une solution non triviale. Il existe une constante effective C_0 telle que si $p \geq C_0$, alors

$$q \leq 2p(p-1).$$

Dans le cas où $q \nmid h^-_p$, on obtient :

Théorème 6.1.32 *Soient p, q deux nombres premiers impairs distincts tels que $p \geq C_0$, $q \nmid h_p^-$, y_0 un entier tel que $|y_0| < \frac{\left(p+\frac{1}{2}\right)^{\frac{p-1}{2}}}{2}$ et $e \in \{0;1\}$. Supposons que l'équation*

$$\frac{x^p + y_0^p}{x + y_0} = p^e z^q, \quad (x, y_0, z) = 1, \quad |x| \geq 2|y_0|,$$

admette une solution non triviale. Alors

$$q < \left(\frac{\log|y_0| + 3\log(2)}{\log(2p+1)} + 6 + \frac{6\log(p)}{\log(3)} \right) p.$$

6.2 Idéaux de Mihăilescu généralisés.

Dans ce paragraphe on se fixe deux entiers relatifs non nuls x, y et p, q deux nombres premiers impairs distincts.

Definition 6.2.1 *On appelle idéal de Mihăilescu associé au quadruplet (x, y, p, q), et que l'on note $\mathcal{I}_M(x, y, p, q)$, l'idéal de $\mathbb{Z}[G]$, défini par*

$$\mathcal{I}_M(x, y, p, q) = \left\{ \theta \in \mathbb{Z}[G]; \quad (x + y\zeta)^\theta \in \mathbb{Q}(\zeta)^{*q} \right\}.$$

Remarque 6.2.2 *Si le contexe est suffisamment clair, on notera $\mathcal{I}_M$, au lieu de $\mathcal{I}_M(x, y, p, q)$.*

On pose également

$$\mathcal{I}_M^{aug} = \{\theta \in \mathcal{I}_M; \quad W(\theta) = 0\}, \quad \mathcal{I}_M(r) = \{\theta \in \mathcal{I}_M; \quad ||\theta|| \leq r\};$$

Ainsi, si $\theta \in \mathcal{I}_M$, il existe un nombre algébrique unique $\alpha = \alpha(\theta, x, y, p, q) \in \mathbb{Q}(\zeta)^*$ tel que $(x+y\zeta)^\theta = \alpha^q$. L'unicité découle du fait que $(q, 2p) = 1$. En effet, si α et β conviennent, alors $\left(\frac{\alpha}{\beta}\right)^q = 1$. Les seules racines de l'unité de $\mathbb{Q}(\zeta)$ étant les racines $2p$-ième de l'unité et vu que $(2p, q) = 1$, on en déduit que $\alpha = \beta$. On énonce maintenant une version étendue du théorème 4.2 de [8]. La démonstration s'inspire de celle du théorème de Bugeaud-Hanrot donnée dans [8].

Théorème 6.2.3 *Soit $\epsilon \in]0;1]$. Soient p, q deux nombres premiers impairs tels que $p \leq (2-\epsilon)q + 1$ et $q \geq 5$. Soient x, y des entiers premiers entre eux. On définit $e \in \{0;1\}$ comme suit*

$$e = \begin{cases} 0 & si\ p \nmid x + y \\ 1 & si\ p | x + y. \end{cases}$$

Soient $c = \frac{e^2-1}{2}$ *et* v *la valuation p-adique de* y*. Si les entiers* x *et* y *vérifient*

$$\left|\frac{x}{y}\right| \geq \sup\left(\left(\frac{64c^2.2^{p-1}|y|^2}{(p-1)^2}\right)^{1/\epsilon}, 8\left(\frac{2}{5}qp^{\frac{1-e}{p-1}+v}|y|\right)^q\right), \tag{6.12}$$

alors $\mathcal{I}_M(x,y,p,q)(2) = \{0\}$*.*

Avant de démontrer ce théorème, énonçons d'abord un corollaire que l'on démontre ensuite :

Corollaire 6.2.4 *Soient* p, q *deux nombres premiers impairs tels que* $3 < p < q$ *et soient* x, y *deux entiers premiers entre eux. Si les entiers* x *et* y *vérifient*

$$|x| \geq 8|y|\left(\frac{2}{5}qp^{\frac{1-e}{p-1}+v}|y|\right)^q, \tag{6.13}$$

alors $\mathcal{I}_M(x,y,p,q)(2) = \{0\}$*.*

Preuve Comme $p < q$, avec les notations de l'énoncé du théorème (6.2.3), on peut prendre $\epsilon = 1$. Pour avoir le résultat escompté, il suffit donc de montrer que si $3 < p < q$, alors

$$\frac{64c^2.2^{p-1}|y|^2}{(p-1)^2} \leq 8\left(\frac{2}{5}q|y|\right)^q.$$

Or, on a

$$\begin{aligned} 8\left(\frac{2}{5}q|y|\right)^q &\geq 8\left(\frac{2}{5}q\right)^{q-p+1}\left(\frac{2}{5}q\right)^{p-1}|y|^2 \\ &\geq 8\left(\frac{2}{5}q\right)^3 2^{p-1}|y|^2, \end{aligned}$$

cette dernière inégalité étant due au fait que $q \geq p+2$. Il vient alors ($q \geq 7$) :

$$\begin{aligned} 8\left(\frac{2}{5}q|y|\right)^q &\geq 8\left(\frac{2}{5}7\right)^3 2^{p-1}|y|^2 \geq \frac{64c^2.2^{p-1}|y|^2}{4^2} \\ &\geq \frac{64c^2.2^{p-1}|y|^2}{(p-1)^2} \end{aligned}$$

■

Preuve (du théorème (6.2.3))

On commence par prouver quelques lemmes.

Lemme 6.2.5 *Soient* $\Theta \in \mathbb{Z}[G]$ *et* $h((x+y\zeta)^\Theta)$ *le poids de Weil de* $(x+y\zeta)^\Theta$*. On a*

$$h((x+y\zeta)^\Theta) \leq \frac{||\Theta|| + W(\Theta)}{2} log(|x|+|y|).$$

Preuve Posons $\Theta = \Theta_+ - \Theta_-$, avec $\Theta_+, \Theta_- \geq 0$. On a

$$\begin{aligned} h((x+y\zeta)^{\Theta}) = h\left(\frac{(x+y\zeta)^{\Theta_+}}{(x+y\zeta)^{\Theta_-}}\right) &\leq \frac{1}{p-1}\sum_{\sigma\in G} log\left(Sup\left(\left|(x+y\zeta)^{\Theta_+}\right|, \left|(x+y\zeta)^{\Theta_-}\right|\right)\right) \\ &\leq \frac{1}{p-1}\sum_{\sigma\in G} Sup\left(W(\theta_+), W(\theta_-)\right) log(|x|+|y|) \\ &\leq \frac{||\Theta|| + W(\Theta)}{2} log(|x|+|y|). \end{aligned}$$

□

En particulier, si $\theta \in \mathbb{Z}[G]$ est tel que $(x+y\zeta)^{\theta} = \alpha^q$, $\alpha \in \mathbb{Q}(\zeta)^*$, on déduit

$$h(\alpha) \leq \frac{||\Theta|| + W(\Theta)}{2q} log(|x|+|y|). \tag{6.14}$$

Lemme 6.2.6 *Si $|x| > |y|$ et $W(\Theta) = 0$, alors*

$$\left|log((x+y\zeta)^{\Theta})\right| \leq \frac{||\Theta||}{\left|\frac{x}{y}\right| - 1}.$$

Preuve Comme $W(\Theta) = 0$, il vient :

$$log((x+y\zeta)^{\Theta}) = log\left(\left(1+\frac{y\zeta}{x}\right)^{\Theta}\right).$$

Le résultat découle alors de la majoration $|log(1+z)| \leq \frac{|z|}{1-|z|}$, pour z complexe, $|z| < 1$.□

Proposition 6.2.7 *Si $(x,y) = 1$, $|x| > |y|$ avec $|x| > 2$ si $p = 3$, alors $(x+y\zeta)^{\Theta} \neq \pm 1$, sauf si $\Theta = 0$.*

Preuve Soit $\mathfrak{p}$ l'unique premier de $\mathbb{Q}(\zeta)$ au-dessus de p. Supposons que $x+y\zeta$ ait au plus comme facteur premier $\mathfrak{p}$. Comme $(x,y) = 1$ et que $\mathfrak{p}$ est engendré par $\zeta^a - \zeta^b$ si $a \neq b$, on a

$$(x+y\zeta^a, x+y\zeta^b) | \mathfrak{p}, \tag{6.15}$$

d'où $(x+y\zeta) = \mathfrak{p}^k$, $k \leq 1$. En passant à la norme, on obtient

$$\frac{x^p + y^p}{x+y} \in \{\pm 1, \pm p\}. \tag{6.16}$$

Lemme 6.2.8 *Soient $X > Y > 0$ des entiers premiers entre eux.*

1. *On a l'inégalité $\frac{X^p+Y^p}{X+Y} \geq p$, avec égalité si et seulement si $p = 3, X = 2, Y = 1$.*
2. *On a $\frac{X^p-Y^p}{X-Y} > p$.*

Preuve Comme $X \geq 2$ et $p \geq 3$, il vient

$$\begin{aligned}\frac{X^p+Y^p}{X+Y} &= \left(X^{p-1}-X^{p-2}Y\right)+\ldots+\left(X^2Y^{p-3}-XY^{p-2}\right)+Y^{p-1}\\ &\geq X^{p-2}\left(X-Y\right)+Y^{p-1}\geq 2^{p-2}+1\geq p.\end{aligned}$$

Si $\frac{X^p+Y^p}{X+Y}=p$, les égalités précédentes sont toutes des égalités, d'où $2^{p-2}+1=p$, soit $p=3, x=2$ et $y=1$, ce qui prouve la première assertion. De plus, on a

$$\frac{X^p-Y^p}{X-Y}=X^{p-1}+X^{p-2}Y+\ldots+XY^{p-2}+Y^{p-1}\geq 2^{p-1}>p,$$

ce qui prouve la deuxième assertion.□

A partir du lemme précédent, on va montrer que l'égalité (6.16) est impossible, ce qui montrera que le nombre algébrique $x+y\zeta$ a au moins un facteur premier $\mathfrak{q}\neq\mathfrak{p}$. Distinguons les quatres cas suivants :

1. $x, y>0$,
2. $x>0, y<0$,
3. $x<0, y<0$,
4. $x<0, y>0$.

Comme $|x|>2$ si $p=3$, dans le premier cas, le lemme (6.2.8) s'applique directement et montre donc que (6.16) n'a pas lieu. Dans le second cas, on peut écrire

$$\frac{x^p+y^p}{x+y}=\frac{x^p-|y|^p}{x-|y|}>p,$$

par le lemme (6.2.8). Dans le troisième cas, on a

$$\frac{x^p+y^p}{x+y}=\frac{-|x|^p-|y|^p}{-|x|-|y|}=\frac{|x|^p+|y|^p}{|x|+|y|}>p,$$

car $|x|>2$ si $p=3$. Enfin, dans le quatrième cas, on a

$$\frac{x^p+y^p}{x+y}=\frac{-|x|^p+|y|^p}{|x|+|y|}=\frac{|x|^p-|y|^p}{|x|-|y|}>p,$$

toujours par le lemme (6.2.8). On a donc bien montré que (6.16) est impossible. Le nombre algébrique $x+y\zeta$ a donc au moins un facteur premier $\mathfrak{q}\neq\mathfrak{p}$. Soit $l=\nu_{\mathfrak{q}}\left(x+y\zeta\right)>0$. Posons $\Theta=\sum_{\sigma\in G}a_\sigma\sigma$. D'après (6.15), on a

$$\begin{cases}\nu_{\mathfrak{q}^\sigma}\left(x+y\zeta^\tau\right)=l & \text{si } \sigma=\tau\,;\\ \nu_{\mathfrak{q}^\sigma}\left(x+y\zeta^\tau\right)=0 & \text{si } \sigma\neq\tau\,;\end{cases}$$

On en déduit que $\nu_{\mathfrak{q}^\sigma}\left((x+y\zeta)^\Theta\right) = la_\sigma$. Si $(x+y\zeta)^\Theta = \pm 1$, on en déduit que

$$\forall \sigma \in G, \quad la_\sigma = 0,$$

d'où $\Theta = 0$, car $l \neq 0$.□

Definition 6.2.9 *Soit $z \in \mathbb{C}^*$. Il existe une unique racine q-ième de l'unité ξ telle que*

$$-\frac{\pi}{q} < arg(z\xi^{-1}) \leq \frac{\pi}{q}.$$

Un tel nombre complexe ξ est appelé plus proche racine q-ième de l'unité de z.

On a la proposition suivante (voir [10]) :

Proposition 6.2.10 *Soit $z \in \mathbb{C}^*$ et ξ sa plus proche racine q-ième de l'unité. On a l'assertion suivante :*

$$log\left(z\xi^{-1}\right) = \frac{1}{q} log\left(z^q\right).$$

On en déduit en particulier le corollaire suivant :

Corollaire 6.2.11 *Soient $|x| > |y|$ deux entiers. Soit $\Theta \in \mathcal{I}_M^{aug}$ et soit $\xi(\Theta)$ la plus proche racine q-ième de $\alpha(\Theta)$ (notation que l'on garde dans la suite). On a alors :*

$$\left|log\left(\alpha(\Theta)\xi(\Theta)^{-1}\right)\right| \leq \frac{||\Theta||}{q\left(\frac{|x|}{|y|}-1\right)}.$$

Preuve Par la proposition (6.2.10), et par définition de $\alpha(\Theta)$, on a

$$log\left(\alpha(\Theta)\xi(\Theta)^{-1}\right) = \frac{1}{q} log\left(\alpha(\Theta)^q\right) = \frac{1}{q} log\left((x+y\zeta)^\Theta\right).$$

La minoration annoncée se déduit donc du lemme (6.2.6).□

Avant de pouvoir enfin passer à la démonstration du théorème (6.2.3), il nous reste à prouver la proposition suivante :

Proposition 6.2.12 *Soit $r > 0$ tel que $r = (2-\epsilon)\frac{q}{p-1}$. Soit $\Theta \in \mathcal{I}_M^{aug}(2r)$, tel que $\xi(\Theta) = 1$. On a alors $\Theta = 0$.*

Preuve Raisonnons par l'absurde et supposons que Θ soit non nul. Soit $\alpha = \alpha(\Theta)$. Par propriété du poids logarithmique d'un nombre algébrique :

$$h(\alpha - 1) \leq h(\alpha) + log(2).$$

Par la relation (6.14), on a donc

$$h(\alpha - 1) \leq \frac{||\Theta||}{2q} log(|x| + |y|) + log(2).$$

Comme $\xi(\Theta) = 1$, le corollaire (6.2.11), montre

$$|log(\alpha)| \leq \frac{||\Theta||}{q\left(\frac{|x|}{|y|} - 1\right)} \leq 2.$$

On déduit de l'inégalité précédente :

$$|\alpha - 1| \leq \frac{e^2 - 1}{2} \frac{||\Theta||}{q\left(\frac{|x|}{|y|} - 1\right)},$$

Pour celle-ci, on a besoin de la version suivante du lemme de Schwarz :

Lemme 6.2.13 *Soit $r > 0$ un nombre réel, et soit z un nombre complexe, $|z| \leq r$. On a*

$$|e^z - 1| \leq \frac{e^r - 1}{r} |z|.$$

Preuve On se ramène au lemme de Schwarz "classique". Soit D l'ensemble des nombres complexes de module au plus 1. Soit φ la fonction holomorphe définie sur D par

$$\varphi(Z) = \frac{e^{rZ} - 1}{e^r - 1}.$$

Comme cette fonction est holomorphe sur D et vérifie $\varphi(0) = 0$, $|\varphi(Z)| \leq 1$, le lemme de Schwarz "classique" montre que

$$|\varphi(Z)| \leq |Z|.$$

Comme $\frac{z}{r} \in D$, on a en particulier :

$$\left|\varphi\left(\frac{z}{r}\right)\right| \leq \frac{|z|}{r},$$

qui est l'inégalité à montrer.□ L'application de ce lemme, avec $z = log(\alpha)$ et $r = 2$ montre

$$|\alpha - 1| \leq \frac{e^2 - 1}{2} |log(\alpha)|.$$

On en déduit l'inégalité escomptée

$$|\alpha - 1| \leq c \frac{||\Theta||}{q\left(\frac{|x|}{|y|} - 1\right)},$$

où $c = \frac{e^2-1}{2}$.

Rappelons le lemme suivant dont le résultat est classiquement nommé inégalité de Liouville :

Lemme 6.2.14 *Soient K un corps de nombres, V un ensemble de places non équivalentes de ce corps et $\alpha \in K$. On a alors l'inégalité suivante :*

$$\prod_{v \in V} |\alpha|_v^{[K_v:\mathbb{Q}_v]} \geq e^{-[K:\mathbb{Q}]h(\alpha)}.$$

L'inégalité de Liouville appliquée à $K = \mathbb{Q}(\zeta)$, $\alpha \in \mathbb{Q}(\zeta)$ et $V = \{j\}$, montre

$$|\alpha - 1|^2 \geq e^{-(p-1)h(\alpha-1)}.$$

De cette inégalité, on déduit :

$$2log\left(\left|\frac{x}{y}\right| - 1\right) \leq 2log\left(\frac{c||\Theta||}{q}\right) + (p-1)\frac{||\Theta||}{2q} log\left(|x| + |y|\right) + (p-1)log(2),$$

d'où

$$\left(2 - \frac{(p-1)||\Theta||}{2q}\right) log\left|\frac{x}{y}\right| \leq 2log\left(\frac{|x/y|}{|x/y| - 1}\right) + \frac{(p-1)||\Theta||}{2q} log\left(\frac{|x| + |y|}{|x/y|}\right) + (p-1)log(2) + 2log\left(\frac{c||\Theta||}{q}\right).$$

Par hypothèse, $||\Theta|| \leq 2r$, avec $r = (2-\epsilon)\frac{q}{p-1}$, d'où $||\Theta||\frac{p-1}{2q} \leq 2 - \epsilon$ et

$$\begin{aligned}\epsilon log\left|\frac{x}{y}\right| &\leq 2log\left(\frac{|x/y|}{|x/y| - 1}\right) + \frac{(p-1)||\Theta||}{2q} log\left(\frac{|x| + |y|}{|x/y|}\right) + (p-1)log(2) \\ &\quad + 2log\left(\frac{c||\Theta||}{q}\right) \\ &\leq 2log\left(\frac{|x/y| + 1}{|x/y| - 1}\right) + 2log|y| + (p-1)log(2) + 2log\left(\frac{4c}{p-1}\right).\end{aligned}$$

Comme $|x/y| \geq 8 \cdot 2^5$, on a

$$log\left(\frac{|x/y| + 1}{|x/y| - 1}\right) = log\left(\frac{1 + |x/y|^{-1}}{1 - |x/y|^{-1}}\right) \leq log\left(\frac{1 + 2^{-8}}{1 - 2^{-8}}\right) \leq log(2).$$

On obtient donc

$$\begin{aligned}\epsilon log\,|x/y| &\leq 2log(2) + 2log|y| + (p-1)log(2) + 2log\left(\frac{4c}{p-1}\right)\\ &\leq \left(64c^2\frac{2^{p-1}|y|^2}{(p-1)^2}\right)^{1/\epsilon},\end{aligned}$$

en contradiction avec (6.12). On a donc bien $\xi(\Theta) = 1$.□ Nous passons maintenant à la dernière étape de la preuve. On se donne donc $\Theta \in \mathcal{I}_M^{aug}$ tel que $||\Theta|| \leq 2$, $\Theta \neq 0$, donc tel que $||\Theta|| = 2$. Soit $\alpha = \alpha(\Theta)$. Par hypothèse

$$p \leq (2-\epsilon)q + 1.$$

Posons $r = \frac{(2-\epsilon)q}{p-1} \geq 1$. On a donc $\Theta \in \mathcal{I}_M^{aug}(2r)$, et même

$$\sigma\Theta \in \mathcal{I}_M^{aug}(2r), \quad \sigma \in G.$$

Autrement dit, comme $\sigma\Theta \neq 0$, pour σ fixé dans G, on a $\xi(\sigma\Theta) \neq 1$ par la proposition (6.2.12).

Lemme 6.2.15 *Soit α un nombre complexe non nul, et soit ξ une racine q-ième de l'unité distincte de* 1. *Supposons que*

$$\left|log\left(\alpha\xi^{-1}\right)\right| \leq \frac{1}{10q}.$$

On a alors $|\alpha - 1| \geq \frac{5}{q}$.

Preuve Comme $\xi \neq 1$, on a $\xi = e^{\frac{2i\pi k}{q}}$, $k \in \{1, 2, \ldots, q-1\}$. On a donc

$$|\xi - 1| = 2\left|sin\left(\frac{\pi k}{q}\right)\right| \geq 2sin\left(\frac{\pi}{q}\right).$$

La fonction $x \to \frac{sin(x)}{x}$ étant décroissante sur $\left[0; \frac{\pi}{2}\right]$ on a

$$\frac{sin(\pi/q)}{\pi/q} \geq \frac{sin(\pi/3)}{\pi/3},$$

d'où

$$|\xi - 1| \geq 2sin(\pi/q) \geq 2\frac{sin(\pi/3)}{\pi/3}\frac{\pi}{q} \geq \frac{5.19}{q}. \tag{6.17}$$

Par le lemme (6.2.13),

$$|\alpha - \xi| = \left|\alpha\xi^{-1} - 1\right| \leq \frac{e^{0.1} - 1}{0.1}\frac{0.1}{q} \leq \frac{0.11}{q}. \tag{6.18}$$

De (6.17) et (6.18), il vient

$$|\alpha - 1| \geq \frac{5.19}{q} - \frac{0.11}{q} > 5/q.$$

□ Par le corollaire (6.2.11), on a

$$log\left(\alpha(\Theta)\xi(\Theta)^{-1}\right)\frac{||\Theta||}{q\left(\frac{|x|}{|y|}-1\right)} \leq \frac{1}{10q},$$

car $\left|\frac{x}{y}\right| - 1 \geq 20$. On a donc par le lemme précédent

$$|\alpha^\sigma - 1| > \frac{5}{q}, \quad \forall \sigma \in G. \tag{6.19}$$

Comme Θ vérifie $||\Theta|| = 2$ et $W(\Theta) = 0$, il existe σ_1, σ_2 éléments de G distincts tels que

$$\Theta = \sigma_1 - \sigma_2.$$

Posons $\zeta_i = \zeta^{\sigma_i}$. Par définition de α

$$\alpha^q - 1 = \frac{\zeta_2 - \zeta_1}{x + \zeta_2 y} y$$

Soit $\mathfrak{q}$ un facteur premier de $\mathbb{Q}(\zeta)$. Si $\mathfrak{q} = \mathfrak{p}$ le seul premier de $\mathbb{Q}(\zeta)$ au-dessus de p, on a

$$\nu_{\mathfrak{q}}\left(\alpha^q - 1\right) = \begin{cases} 1 + (p-1)\nu_p(y) & \text{si } e = 0, \\ (p-1)\nu_p(y) & \text{si } e = 1. \end{cases} \tag{6.20}$$

En effet, si $e = 0$, $(p, x + y) = 1$. Comme

$$x + \zeta y = x + y + (\zeta - 1)y \equiv x + y \bmod \mathfrak{p} \neq 0 \bmod \mathfrak{p},$$

on a dans ce cas (rappelons que $v = \nu_p(y)$) :

$$\nu_{\mathfrak{p}}\left(\frac{\zeta_2 - \zeta_1}{x + \zeta_2 y} y\right) = \nu_{\mathfrak{p}}\left(\zeta_2 - \zeta_1\right) + \nu_{\mathfrak{p}}\left(y\right) = 1 + (p-1)v.$$

Si $e = 1$, $p|x + y$. Comme $(x, y) = 1$, on a $(p, y) = 1$, d'où

$$\mathfrak{p}||(x + y\zeta).$$

Par conséquent, si $e = 1$, on a

$$\nu_{\mathfrak{p}}\left(\frac{\zeta_2 - \zeta_1}{x + \zeta_2 y} y\right) = 1 + (p-1)v - 1 = (p-1)v.$$

On a donc bien

$$\nu_{\mathfrak{p}}\left(\alpha^q-1\right)=1-e+(p-1)v. \tag{6.21}$$

On a également

$$\left|\alpha^q-1\right|_{\mathfrak{q}}=\frac{1}{\mathcal{N}(\mathfrak{q})^{\nu_{\mathfrak{q}}(\alpha^\sigma-1)}}\geq\frac{1}{\mathcal{N}\left(\mathfrak{q}\right)^{\nu_{\mathfrak{q}}(y)}}\geq\frac{1}{|y|^{p-1}}, \tag{6.22}$$

car $|y|^{p-1}=\prod_{\mathfrak{q}}\mathcal{N}\left(\mathfrak{q}\right)^{\nu_{\mathfrak{q}}(y)}$. Si $\left|\alpha-1\right|_{\mathfrak{q}}<1$, alors on a l'inégalité

$$\left|\alpha-1\right|_{\mathfrak{q}}^{-1}\leq\left|\alpha^q-1\right|_{\mathfrak{q}}^{-1}.$$

Comme

$$\begin{aligned}
h\left((\alpha-1)^{-1}\right)&=\frac{1}{p-1}\sum_{\sigma\in G}logSup\left(1,\left|\alpha^\sigma-1\right|\right)+\frac{1}{p-1}\sum_{\mathfrak{q}}logSup\left(1,\left|(\alpha-1)^{-1}\right|_{\mathfrak{q}}\right)\\
&\leq\frac{1}{p-1}\sum_{\sigma\in G}logSup\left(1,\left|\alpha^\sigma-1\right|\right)+\frac{1}{p-1}\sum_{\left|\alpha-1\right|_{\mathfrak{q}}<1}logSup\left(1,\left|(\alpha-1)^{-1}\right|_{\mathfrak{q}}\right)\\
&\leq\frac{1}{p-1}\sum_{\sigma\in G}logSup\left(1,\left|\alpha^\sigma-1\right|\right)+\frac{1}{p-1}\sum_{\left|\alpha-1\right|_{\mathfrak{q}}<1}logSup\left(1,\left|(\alpha^q-1)^{-1}\right|_{\mathfrak{q}}\right)
\end{aligned}$$

On déduit de (6.21) et (6.22)

$$\left|\alpha-1\right|_{\mathfrak{q}}^{-1}\leq\begin{cases}|y|^{p-1} & \text{si } \mathfrak{q}\neq\mathfrak{p},\\ p^{1-e+v(p-1)} & \text{si } \mathfrak{q}=\mathfrak{p}.\end{cases} \tag{6.23}$$

De (6.19) et (6.23), il vient alors

$$h\left((\alpha-1)^{-1}\right)\leq log\left(\frac{q}{5}\right)+log|y|+\frac{1-e+v(p-1)}{p-1}log(p).$$

On en déduit

$$\begin{aligned}
log\left|\frac{x}{y}\right|=h\left(\frac{x}{y}\right)&=h\left(\frac{\zeta_2-\zeta_1}{\alpha^q-1}+\zeta_2\right)\\
&\leq 3log(2)+qh\left(\alpha\right)\\
&\leq 3log(2)+qh\left(\alpha-1\right)+qlog(2)\\
&\leq 3log(2)+qh\left((\alpha-1)^{-1}\right)+qlog(2)\\
&\leq log(8)+q\left(log\left(\frac{2q}{5}\right)+log|y|+\frac{1-e+v(p-1)}{p-1}log(p)\right).
\end{aligned}$$

On a ainsi obtenu

$$log\left|\frac{x}{y}\right|\leq log(8)+q\left(log\left(\frac{2q}{5}\right)+log|y|+\frac{1-e+v(p-1)}{p-1}log(p)\right),$$

en contradiction avec les hypothèses (6.12). ■

6.3 Sur les déterminants $\mathcal{E}(p,a,b)$.

6.3.1 Forme générale de $\mathcal{E}(p,a,b)$.

On se fixe ξ une racine primitive $\frac{p-1}{2}$-ième de l'unité. On pose

$$Z_{b,a} = \frac{1}{b-\zeta_0^a} - \frac{1}{b-\zeta_0^{-a}}.$$

On considère alors le polynôme $P_{b,a}(X) \in \mathbb{C}[X]$ défini par

$$P_{b,a}(X) = \sum_{k=0}^{\frac{p-3}{2}} Z_{b,a}^{\sigma^k} X^k.$$

Le determinant $\mathcal{E}(p,a,b)$ étant circulant gauche, on a

$$\mathcal{E}(p,a,b) = (-1)^{\frac{p-3}{4}} P_{b,a}(1) P_{b,a}(\xi) \dots P_{b,a}(\xi^{\frac{p-3}{2}}). \tag{6.24}$$

En particulier, si $p \equiv 1 \bmod 4$, on a $\mathcal{E}(p,a,b) = 0$. En effet, dans un tel cas, -1 est un résidu quadratique modulo p. En notant C l'ensemble des résidus quadratiques modulo p, il vient alors

$$\begin{aligned} P_{b,a}(1) &= \sum_{k=0}^{\frac{p-3}{2}} \frac{1}{b-\zeta_0^a} - \frac{1}{b-\zeta_0^{-a}} \\ &= \sum_{c\in C} \frac{1}{b-\zeta_0^c} - \sum_{c\in C} \frac{1}{b-\zeta_0^{-c}} = 0. \end{aligned}$$

Plaçons nous dans le cas où $p \equiv 3 \bmod 4$. Le determinant $\mathcal{E}(p,a,b)$ est invariant sous les éléments de $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ de la forme σ_c, c carré modulo p. En effet, rappelons que g désigne une racine primitive modulo p, que $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ est défini par $\zeta^\sigma = \zeta^{g^2}$. Par définition, la ligne d'indice i de $\mathcal{E}(p,a,b)$ est alors

$$\left(Z_{b,a}^{\sigma^{i-1}} \dots Z_{b,a}^{\sigma^{i-1+\frac{p-3}{2}}} \right) = L^{\sigma^{i-1}},$$

où L est la première ligne de $\mathcal{E}(p,a,b)$. L'action de σ sur $\mathcal{E}(p,a,b)$ revient donc à multiplier ce determinant par la signature de la permutation circulaire

$$\begin{pmatrix} 2 & 3 \dots \frac{p-1}{2} & 1 \end{pmatrix},$$

c'est à dire 1. C'est donc bien un nombre algébrique de Gauss car il est σ-invariant. De plus, comme $Z_{b,a}^j = -Z_{b,a}$, et $(-1)^{\frac{p-1}{2}} = -1$, il existe donc un nombre rationnel $E(p,a,b)$ tel que

$$\mathcal{E}(p,a,b) = E(p,a,b)\sqrt{-p}.$$

Dans le cas où $p > 3$, et $b = \pm 1$, on peut même montrer à partir de (6.24), que $E(p,a,b)$ est entier, si $b = \pm 1$, et divisible par $h(-p)$ si $b = 1$. En effet, supposons d'abord que $b = 1$. Comme $\sum_{k=0}^{\frac{p-3}{2}} \xi^k = 0$, il vient

$$\begin{aligned}\mathcal{E}(p,a,1) &= P_{1,a}(1) \prod_{l=1}^{\frac{p-3}{2}} \sum_{k=0}^{\frac{p-3}{2}} \xi^{kl} \left(\frac{1}{1-\zeta_0^{a\sigma^k}} - \frac{1}{1-\zeta_0^{-a\sigma^k}} \right) \\ &= P_{1,a}(1) \prod_{l=1}^{\frac{p-3}{2}} \sum_{k=0}^{\frac{p-3}{2}} \xi^{kl} \frac{1+\zeta_0^{a\sigma^k}}{1-\zeta_0^{a\sigma^k}}.\end{aligned}$$

Par le lemme (6.3.2) (voir paragraphe suivant) appliqué au symbole de Legendre $\left(\frac{\cdot}{p}\right)$, il vient

$$P_{1,a}(1) = \sum_{x=1}^{p-1} \frac{\left(\frac{x}{p}\right)}{1-\zeta_0^{ax}} = \left(\frac{a}{p}\right)\sqrt{-p}h(-p),$$

c'est à dire

$$P_{1,a}(1) = \left(\frac{a}{p}\right) h(-p) \prod_{l=0}^{\frac{p-3}{2}} \left(1-\zeta_0^{\sigma^l}\right).$$

On obtient donc

$$\mathcal{E}(p,a,1) = \left(\frac{a}{p}\right) h(-p)(1-\zeta_0) \prod_{l=1}^{\frac{p-3}{2}} \sum_{k=0}^{\frac{p-3}{2}} \xi^{kl} \frac{\left(1+\zeta_0^{a\sigma^k}\right)\left(1-\zeta_0^{\sigma^l}\right)}{1-\zeta_0^{a\sigma^k}}.$$

Le quotient $\frac{1-\zeta_0^{\sigma^l}}{1-\zeta_0^{a\sigma^k}}$ étant une unité de l'anneau $\mathbb{Z}[\zeta]$, $\frac{\mathcal{E}(p,a,1)}{h(-p)}$ est donc un entier algébrique du corps $\mathbb{Q}(\sqrt{-p})$. Comme $p \equiv 3 \bmod 4$, il existe donc deux entiers A, B de même parité tels que $\mathcal{E}(p,a,1) = \frac{A+B\sqrt{-p}}{2}h(-p)$. Comme $\mathcal{E}(p,a,1)^j = -\mathcal{E}(p,a,1)$, on a $A = 0$. L'entier B est donc pair, et $\mathcal{E}(p,a,1) = \frac{B}{2}h(-p)\sqrt{-p}$. Le nombre rationnel $E(p,a,b)$ est donc bien un entier si $b = 1$, divisible par $h(-p)$.

L'étude du cas $b = -1$ se fait de même, mais est plus simple, car $1+\zeta$ est une unité de $\mathbb{Z}[\zeta]$.

Les paragraphes suivants sont dédiés au calcul explicite du nombre entier $E(p,a,\pm 1)$, et de $E(p,a,0)$.

6.3.2 Calcul de $E(p,a,1)$.

On commence par prouver le lemme suivant :

Lemme 6.3.1 *Soit $x \neq 0$ la classe d'un entier modulo p. On a $\sum_{j=1}^{p-1} j\zeta^{jx} = -\frac{p}{1-\zeta^x}$.*

Preuve On a

$$\begin{aligned}(1-\zeta^x)\sum_{j=1}^{p-1} j\zeta^{jx} &= \sum_{j=1}^{p-1} j\zeta^{jx} - \sum_{j=1}^{p-1} j\zeta^{(j+1)x} \\ &= \sum_{j=1}^{p-1} j\zeta^{jx} - \sum_{j=2}^{p} (j-1)\zeta^{jx} = -p.\end{aligned}$$

□

Lemme 6.3.2 *Soit p un nombre premier impair. Soit χ un caractère du groupe $\mathbb{F}_p^\times$. Soit $\mathcal{S}(\chi)$ la somme suivante :*

$$\mathcal{S}(\chi) = \sum_{x=1}^{p-1} \frac{\chi(x)}{1-\zeta^x}.$$

On a $\mathcal{S}(\chi) = -B_{1,\overline{\chi}}\tau(\chi)$, où $\tau(\chi) = \sum_{x=1}^{p-1}\chi(x)\zeta^x$ et $B_{1,\overline{\chi}}$ est le nombre de Bernoulli généralisé associé au caractère $\overline{\chi}$.

Preuve On a

$$\begin{aligned}-p\mathcal{S}(\chi) &= \sum_{x=1}^{p-1} -\chi(x)\frac{p}{1-\zeta^x} = \sum_{j=1}^{p-1} j\sum_{x=1}^{p-1}\chi(x)\zeta^{jx} = \sum_{j=1}^{p-1} j\overline{\chi}(j)\sum_{x=1}^{p-1}\chi(jx)\zeta^{jx} \\ &= pB_{1,\overline{\chi}}\tau(\chi),\end{aligned}$$

d'où le lemme.□ Fixons un nombre premier p tel que $p \equiv 3 \bmod 4$. Montrons dans un premier temps que

$$\mathcal{E}(p,1,1) = 2^{\frac{p-3}{4}} p^{\frac{p-7}{4}} h_p^- \sqrt{-p}.$$

Soit $\hat{G}^-$ le groupe de caractères impairs de G. Comme $p \equiv 3 \bmod 4$, il vient

$$\mathcal{E}(p,1,1) = (-1)^{\frac{p-3}{4}} \prod_{\chi\in\hat{G}^-} \mathcal{S}(\chi).$$

Le lemme (6.3.2) montre donc

$$\mathcal{E}(p,1,1) = (-1)^{\frac{p-3}{4}} \prod_{\chi\in\hat{G}^-} -B_{1,\overline{\chi}}\tau(\chi) = (-1)^{\frac{p-3}{4}} 2^{\frac{p-1}{2}} \prod_{\chi\in\hat{G}^-} -\frac{1}{2}B_{1,\overline{\chi}} \prod_{\chi\in\hat{G}^-} \tau(\chi).$$

On a $\prod_{\chi\in\hat{G}^-}\tau(\chi) = \frac{\prod_{\chi\in\hat{G}}\tau(\chi)}{\prod_{\chi\in\hat{G}^+}\tau(\chi)}$. Par le théorème 11.7.16 de [28], il vient :

$$\prod_{\chi\in\hat{G}} \tau(\chi) = \left(\frac{-2}{p}\right) ip^{\frac{p-2}{2}}, \quad \prod_{\chi\in\hat{G}^+} \tau(\chi) = \left(\frac{p}{\frac{p-1}{2}}\right) p^{\frac{p-3}{4}},$$

d'où

$$\prod_{\chi\in\hat{G}^-} \tau(\chi) = \left(\frac{-2}{p}\right)\left(\frac{p}{\frac{p-1}{2}}\right) ip^{\frac{p+1}{4}} = (-1)^{\frac{p-3}{4}}\, ip^{\frac{p-1}{4}}.$$

Par [77], on sait que $\prod_{\chi\in\hat{G}^-} -\frac{1}{2}B_{1,\overline{\chi}} = \frac{h_p^-}{2p}$. On a donc

$$\mathcal{E}(p,1,1) = (-1)^{\frac{p-3}{4}} 2^{\frac{p-1}{2}} \frac{h_p^-}{2p} (-1)^{\frac{p-3}{4}} p^{\frac{p-3}{4}} \sqrt{-p} = 2^{\frac{p-3}{2}} p^{\frac{p-7}{4}} h_p^- \sqrt{-p}.$$

Comme $\mathcal{E}(p,1,1) \in \mathbb{Q}(\sqrt{-p})$, si a est un carré modulo p, on a $\mathcal{E}(p,1,1) = \mathcal{E}(p,a,1)$. Comme $\frac{p-1}{2}$ est impair, $\mathcal{E}(p,-1,1) = \mathcal{E}(p,1,1)^j = -\mathcal{E}(p,1,1)$, d'où la valeur de $\mathcal{E}(p,a,1)$ dans le cas général.

6.3.3 Calcul de $E(p,a,-1)$.

Le calcul de $E(p,a,-1)$ est similaire à celui de $E(p,a,1)$. On commence par rappeler successivement les trois lemmes suivants :

Lemme 6.3.3 *(voir [47]) Soit χ un caractère impair de conducteur $f_\chi \neq 2 \bmod 4$, et soit S_χ la somme définie par*

$$S_\chi = \sum_{1\leq x\leq f_\chi/2} \chi(x).$$

On a alors

$$\mathcal{B}_{1,\chi} = -\frac{1}{2-\overline{\chi}(2)} S_\chi.$$

Lemme 6.3.4 *Soit $\boldsymbol{Tr}$ la trace relative à l'extension $\mathbb{Q}(\zeta)/\mathbb{Q}$. Soit n un entier, $0 \leq n \leq p-1$. On pose*

$$\tau_n = \boldsymbol{Tr}\left(\frac{\zeta^n}{1+\zeta}\right).$$

On a alors

$$\tau_n = \begin{cases} \frac{p-1}{2} - p & \text{si } n > 0, \quad 2|n, \\ \frac{p-1}{2} & \text{sinon.} \end{cases}$$

Preuve Si $n = 0$, on a $\tau_n = \mathbf{Tr}\left(\frac{1}{1+\zeta}\right) = \frac{p-1}{2}$ à partir du polynôme minimal de $\frac{1}{1+\zeta}$ (voir pour plus de détails la preuve du lemme (6.34)). Pour le calcul de τ_1 et τ_2, on a

$$\tau_1 = \mathbf{Tr}\left(\frac{\zeta}{1+\zeta}\right) = \mathbf{Tr}\left(1 - \frac{1}{1+\zeta}\right) = p - 1 - \tau_0 = \frac{p-1}{2}.$$

et

$$\begin{aligned}\tau_2 &= \mathbf{Tr}\left(\frac{\zeta^2}{1+\zeta}\right) = \mathbf{Tr}\left(\frac{\zeta^2 - 1 + 1}{1+\zeta}\right) \\ &= \mathbf{Tr}\left(\zeta - 1 + \frac{1}{1+\zeta}\right) = -p + \tau_0 = \frac{p-1}{2} - p.\end{aligned}$$

Soit maintenant un entier $m > 0$. On a

$$\begin{aligned}\tau_{m+2} &= \mathbf{Tr}\left(\frac{\zeta^{m+2}}{1+\zeta}\right) = \mathbf{Tr}\left(\frac{\zeta^{m+2} - \zeta^m + \zeta^m}{1+\zeta}\right) \\ &= \mathbf{Tr}\left(\zeta^m(\zeta - 1) + \frac{\zeta^m}{1+\zeta}\right) = \tau_m,\end{aligned}$$

car $m > 0$. On déduit donc la valeur de τ_m, $m > 0$, de celle de τ_1 et τ_2.□

Lemme 6.3.5 *Soit $p \equiv 3 \bmod 4$ un nombre premier, et soit m l'ordre de 2 modulo p. Soit également $\epsilon = \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. On a alors*

$$\prod_{\chi \in \hat{\mathbb{F}_p^\times}^-} (2 - \chi(2)) = \left(2^{m/2^{\frac{1-\epsilon}{2}}} - \epsilon\right)^{2^{\frac{1+\epsilon}{2}} m}.$$

Preuve Rappelons le lemme 6, page 119 de [71][2] : si G est un groupe abélien, et si g est un élément de G d'ordre m, alors

$$\prod_{\chi \in \hat{G}} (1 - \chi(g)T) = (1 - T^m)^{\frac{|G|}{m}}.$$

On obtient en appliquant ce lemme à $T = \frac{1}{2}$ et $G = \mathbb{F}_p^\times$:

$$\prod_{\chi \in \hat{\mathbb{F}_p^\times}} (2 - \chi(2)) = 2^{p-1} \prod_{\chi \in \hat{\mathbb{F}_p^\times}} \left(1 - \chi(2)\frac{1}{2}\right) = 2^{p-1}\left(1 - \frac{1}{2^m}\right)^{\frac{p-1}{m}}.$$

[2]En fait, ce lemme est énoncé pour un groupe G de la forme $(\mathbb{Z}/M\mathbb{Z})^\times$, mais la démonstration de [71] est valable plus généralement pour un groupe abélien.

Comme $\frac{p-1}{2}$ est impair, si on désigne par m' l'ordre de 2ϵ modulo p, on a

$$m = \begin{cases} m' & \text{si } \epsilon = 1 \\ 2m' & \text{si } \epsilon = -1 \end{cases}$$

Supposons d'abord que $\epsilon = 1$. Toujours par le lemme 6 de [71], on a, en notant C les résidus quadratiques modulo p :

$$\prod_{\chi \in \hat{C}} (2 - \chi(2)) = 2^{\frac{p-1}{2}} \left(1 - \frac{1}{2^m}\right)^{\frac{p-1}{2m}}.$$

On a donc si $\epsilon = 1$

$$\begin{aligned} \prod_{\chi \in \hat{\mathbb{F}_p^\times}^-} (2 - \chi(2)) &= \frac{\prod_{\chi \in \hat{\mathbb{F}_p^\times}} (2 - \chi(2))}{\prod_{\chi \in \hat{\mathbb{F}_p^\times}^+} (2 - \chi(2))} = \frac{\prod_{\chi \in \hat{\mathbb{F}_p^\times}} (2 - \chi(2))}{\prod_{\chi \in \hat{C}} (2 - \chi(2))} \\ &= \frac{2^{p-1} \left(1 - \frac{1}{2^m}\right)^{\frac{p-1}{m}}}{2^{\frac{p-1}{2}} \left(1 - \frac{1}{2^m}\right)^{\frac{p-1}{2m}}} = (2^m - 1)^{\frac{p-1}{2m}} \end{aligned}$$

Supposons maintenant que $\epsilon = -1$. Il vient alors

$$\begin{aligned} \prod_{\chi \in \hat{\mathbb{F}_p^\times}^+} (2 - \chi(2)) &= \prod_{\chi \in \hat{\mathbb{F}_p^\times}^+} (2 - \chi(-2)) = \prod_{\chi \in \hat{C}} (2 - \chi(-2)) \\ &= 2^{\frac{p-1}{2}} \left(1 - \frac{1}{2^{\frac{m}{2}}}\right)^{\frac{p-1}{m}} = \left(2^{\frac{m}{2}} - 1\right)^{\frac{p-1}{m}}. \end{aligned}$$

On a alors

$$\prod_{\chi \in \hat{\mathbb{F}_p^\times}^-} (2 - \chi(2)) = \frac{2^{p-1} \left(1 - \frac{1}{2^m}\right)^{\frac{p-1}{m}}}{\left(2^{\frac{m}{2}} - 1\right)^{\frac{p-1}{m}}} = \left(2^{\frac{m}{2}} + 1\right)^{\frac{p-1}{m}},$$

ce qui conclut la preuve du lemme.□

A partir de ces trois lemmes, on obtient le lemme suivant :

Lemme 6.3.6 *Soit $p > 2$ un nombre premier et soit $\chi \in \hat{\mathbb{F}_p^\times}$. On a alors*

$$\tau(\overline{\chi}) \sum_{x=1}^{p-1} \frac{\chi(x)}{1 + \zeta^x} = p\overline{\chi}(2) (2 - \chi(2)) \mathcal{B}_{1,\overline{\chi}}.$$

Preuve En effet, on a

$$\tau(\overline{\chi})\sum_{x=1}^{p-1}\frac{\chi(x)}{1+\zeta^x}=\sum_{x,y}\frac{\chi(x)\overline{\chi}(y)}{1+\zeta^x}\zeta^y=\sum_{x,y}\frac{\chi\left(\frac{x}{y}\right)}{1+\zeta^x}$$
$$=\sum_{x,z}\frac{\chi(z)\zeta^y}{1+\zeta^{yz}}=\sum_z\chi(z)\mathbf{Tr}\left(\frac{\zeta^{z^{-1}}}{1+\zeta}\right),$$

où z^{-1} est l'inverse de z mod p. Comme

$$\sum_z\chi(z)\mathbf{Tr}\left(\frac{\zeta^{z^{-1}}}{1+\zeta}\right)=\sum_z\overline{\chi}(z)\mathbf{Tr}\left(\frac{\zeta^z}{1+\zeta}\right),$$

l'application du lemme (6.3.4), et le fait que $\sum_z\overline{\chi}(z)=0$ montrent

$$\tau(\overline{\chi})\sum_{x=1}^{p-1}\frac{\chi(x)}{1+\zeta^x}=-p\sum_{2|z}\overline{\chi}(z)=-p\overline{\chi}(2)\mathcal{S}_{\overline{\chi}},$$

où $\mathcal{S}_{\overline{\chi}}$ est définie au lemme (6.3.3). L'application de ce même lemme à la dernière égalité obtenue, termine la démonstration.□

On peut alors, grâce au lemme précédent, refaire le même type de calculs que ceux qui ont permis de calculer $\mathcal{E}(p,a,1)$. En effet, par le lemme précédent, on a

$$\mathcal{E}(p,1,-1)\prod_{\chi\in\hat{G}^-}\tau(\chi)=(-1)^{\frac{p-1}{2}+\frac{p-3}{4}}\prod_{\chi\in\hat{G}^-}\tau(\overline{\chi})\sum_{x=1}^{p-1}\frac{\chi(x)}{1+\zeta_0^x}$$
$$=(-1)^{\frac{p-1}{2}+\frac{p-3}{4}}p^{\frac{p-1}{2}}\prod_{\chi\in\hat{G}^-}\chi(2)\prod_{\chi\in\hat{G}^-}(2-\chi(2))\prod_{\chi\in\hat{G}^-}\mathcal{B}_{1,\chi}$$
$$=(-1)^{\frac{p-1}{2}+\frac{p-3}{4}}p^{\frac{p-1}{2}}(-2)^{\frac{p-1}{2}}\prod_{\chi\in\hat{G}^-}\chi(2)\prod_{\chi\in\hat{G}^-}(2-\chi(2))\prod_{\chi\in\hat{G}^-}-\frac{1}{2}\mathcal{B}_{1,\chi}.$$

Remarquons que $\prod_{\chi\in\hat{G}^-}\chi(2)=(-1)^{\frac{p-1}{m}}$ (rappelons que m est l'ordre de 2 modulo p). On a alors, en utilisant le lemme (6.3.5) :

$$(-1)^{\frac{p-3}{4}}ip^{\frac{p-1}{4}}\mathcal{E}(p,1,-1)=(-1)^{\frac{p-3}{4}}(2p)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{m}}\cdot\left(2^{m/2^{\frac{1-\epsilon}{2}}}-\epsilon\right)^{\frac{p-1}{2^{\frac{1+\epsilon}{2}}m}}\cdot\frac{h_p^-}{2p},$$

où $\epsilon=(-1)^{\frac{p^2-1}{8}}$. On a donc finalement

$$\mathcal{E}(p,1,-1)=-(-1)^{\frac{p-1}{m}}2^{\frac{p-3}{2}}p^{\frac{p-7}{4}}h_p^-\left(2^{m/2^{\frac{1-\epsilon}{2}}}-\epsilon\right)^{\frac{p-1}{2^{\frac{1+\epsilon}{2}}m}}\sqrt{-p}.$$

Pour le cas général où a n'est plus égal à 1, on procède comme lors du calcul de $\mathcal{E}(p,a,b)$. La proposition (6.1.3) est démontrée.

6.3.4 Calcul de $E(p,a,0)$.

Comme avant, il suffit de traiter le cas $a=1$. Soit $\zeta_0 = e^{\frac{2i\pi}{p}}$. On a

$$\begin{aligned}\mathcal{E}(p,1,0) &= (-1)^{\frac{p-3}{4}+\frac{p-1}{2}} \prod_{\chi\in\hat{G}^-} \sum_{x=1}^{p-1} \chi(x)\zeta_0^{-x} = (-1)^{\frac{p-3}{4}+\frac{p-1}{2}} \prod_{\chi\in\hat{G}^-} \chi(-1) \prod_{\chi\in\hat{G}^-} \tau(\chi) \\ &= (-1)^{\frac{p-3}{4}+\frac{p-1}{2}}(-1)^{\frac{p-1}{2}} \prod_{\chi\in\hat{G}^-} \tau(\chi) = (-1)^{\frac{p-3}{4}}(-1)^{\frac{p-3}{4}} i p^{\frac{p-1}{4}} \\ &= p^{\frac{p-3}{4}}\sqrt{-p}.\end{aligned}$$

6.3.5 $E(p,a,b) \neq 0$ si $p = 1+2q$, q premier.

Dans ce paragraphe, on montre que si $p = 1+2q$, q nombre premier impair, alors $E(p,a,b) \neq 0$ pour tout entier b. Raisonnons par l'absurde et supposons que $E(p,a,b) = 0$, donc que $E(p,1,b) = 0$, pour un certain entier b. Vu les valeurs explicites de $E(p,a,0)$ et $E(p,a,\pm 1)$, on doit avoir $|b| > 1$. Il existe un entier k parmi les entiers $0,\ldots,\frac{p-3}{2}$, tel que

$$P_{1,b}\left(\xi^k\right) = 0,$$

c'est à dire

$$Z + \sum_{k=1}^{\frac{p-3}{2}} \xi^k Z^{\sigma^k} = 0, \quad Z = \frac{1}{b-\zeta_0} - \frac{1}{b-\zeta_0^{-1}}, \tag{6.25}$$

où $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ est défini par $\zeta^\sigma = \zeta^{g^2}$, g racine primitive de l'unité.

Si $k=0$, l'égalité (6.25) s'écrit

$$\sum_{x=1}^{p-1} \frac{\left(\frac{x}{p}\right)}{b-\zeta_0^x} = 0. \tag{6.26}$$

Comme $|b| > 1$, en développant en série entière les quotients $\frac{1}{b-\zeta_0}$, on vérifie que

$$\sum_{x=1}^{p-1} \frac{\left(\frac{x}{p}\right)}{b-\zeta_0^x} = \left(\sum_{c\in C} \frac{1}{b^c} - \sum_{n\in N} \frac{1}{b^n}\right) \frac{b^{p-1}}{b^p-1}\sqrt{-p}, \tag{6.27}$$

où C (respectivement N) désigne les résidus quadratiques modulo p parmi les entiers $1,\ldots,p-1$ (respectivement les non résidus quadratiques modulo p parmi les entiers $1,\ldots,p-1$). De (6.26) et (6.27), on obtient

$$\sum_{c\in C} \frac{1}{b^c} = \sum_{n\in N} \frac{1}{b^n}.$$

Montrons que cette égalité est impossible. En effet, si elle était possible, on pourrait écrire

$$\begin{aligned}\sum_{b=1}^{p-1}\frac{1}{b^i} &= \sum_{c\in C}\frac{1}{b^c}+\sum_{n\in N}\frac{1}{b^n}\\ &= 2\sum_{c\in C}\frac{1}{b^c},\end{aligned}$$

d'où

$$b^{p-1}-1 = 2\sum_{c\in C} b^{p-c}-b^{p-1-c}. \tag{6.28}$$

Comme $c<p$, $b|b^{p-c}$. Comme $p\equiv 3 \bmod 4$, -1 n'est pas résidu quadratique modulo p, d'où $p-1-c>0 \quad (1\leq c\leq p-1)$, c'est à dire $b|b^{p-1-c}$. Finalement le terme de droite de (6.28) est divisible par b, et (6.28) est donc fausse. On a ainsi montré que (6.25) était impossible si $k=0$. Supposons maintenant que $k\in\{1,\ldots,\frac{p-3}{2}\}$. En appliquant la trace $\mathbf{Tr}_{\mathbb{Q}(\zeta,\xi)/\mathbb{Q}(\zeta)}$ à l'égalité (6.25), on obtient ($\mathbf{Tr}_{\mathbb{Q}(\zeta,\xi)/\mathbb{Q}(\zeta)}(\xi)=-1$ car q premier) :

$$(q-1)Z-\sum_{k=1}^{\frac{p-3}{2}} Z^{\sigma^k}=0,$$

c'est à dire

$$q\left(\frac{1}{b-\zeta_0}-\frac{1}{b-\zeta_0^{-1}}\right)=\left(\sum_{c\in C}\frac{1}{b^c}-\sum_{n\in N}\frac{1}{b^n}\right)\frac{b^{p-1}}{b^p-1}\sqrt{-p}. \tag{6.29}$$

On vérifie que l'application de $\mathcal{N}$, norme relative à l'extension $\mathbb{Q}(\zeta)/\mathbb{Q}$, à (6.29) donne

$$q^{p-1}\left(\frac{b^p-1}{b-1}\right)^{p-3}(b-1)^{p-1}=p^{\frac{p-3}{2}}\left(b^{p-1}Q_b\right)^{p-1} \tag{6.30}$$

où $b^{p-1}Q_b=\sum_{c\in C}b^{p-1-c}-\sum_{n\in N}b^{p-1-n}$. Rappelons le lemme suivant :

Lemme 6.3.7 *Soient a,b des entiers non nuls tels que $a-b\neq 0$, et n un entier impair. Alors*

$$\left(\frac{a^n-b^n}{a-b},a-b\right)=\left(n(a,b)^{n-1},a-b\right).$$

En particulier, si a et b sont premiers entre eux et $n=p$ nombre premier impair, alors p divise l'entier $a-b$ si et seulement si p divise l'entier $\frac{a^p-b^p}{a-b}$, et alors $p||\frac{a^p-b^p}{a-b}$.

Preuve En écrivant $a^n = (a-b+b)^n$, la formule du binôme montre qu'il existe un entier K tel que

$$\frac{a^n - b^n}{a-b} = nb^{n-1} + K(a-b),$$

d'où

$$\left(\frac{a^n - b^n}{a-b}, a-b\right) = \left(a-b, nb^{n-1}\right).$$

De même, il existe un entier L tel que

$$\frac{a^n - b^n}{a-b} = na^{n-1} + L(a-b),$$

d'où

$$\left(\frac{a^n - b^n}{a-b}, a-b\right) = \left(a-b, na^{n-1}\right).$$

Soit $d = (na^{n-1}, a-b) = (nb^{n-1}, a-b)$ et soit $g = (n(a,b)^{n-1}, a-b)$. On a $g = d$. En effet comme $d|na^{n-1}$ et $d|nb^{n-1}$, on a

$$d|\left(na^{n-1}, nb^{n-1}\right) = n\left(a^{n-1}, b^{n-1}\right) = n(a,b)^{n-1}.$$

Comme $d|a-b$, $d|g$. Inversement, puisque $g|n\,(a,b)^{n-1}$, $g|na^{n-1}$, et vu que $g|a-b$, il vient $g|\,(na^{n-1}, a-b) = d$. On a donc bien $d = g$. En particulier, si $(a,b) = 1$, $n = p$ premier et $p|a-b$, de l'égalité

$$\left(\frac{a^p - b^p}{a-b}, a-b\right) = (a-b, p)\,,$$

on déduit que $p||\frac{a^p-b^p}{a-b}$. Inversement, si $p|\frac{a^p-b^p}{a-b}$, on obtient $a^p \equiv b^p \bmod p$, donc $a \equiv b \bmod p$.□

En particulier, dans notre cas, comme p divise l'entier à droite de (6.30), et vu que $q \neq p$, le lemme précédent montre donc que p divise $b-1$ et $p||\frac{b^p-1}{b-1}$. Posons

$$v = \nu_p\,(b-1)\,, \quad w = \nu_p\left(b^{p-1}Q_b\right).$$

De (6.30), il vient en égalisant les valuations p-adiques

$$(p-3) + (p-1)v = (p-1)w + \frac{p-3}{2},$$

c'est à dire

$$(p-1)(w-v) = \frac{p-3}{2},$$

ce qui est absurde. L'égalité (6.25) est donc impossible, ce qui montre que $E(p,a,b) \neq 0$ si $p = 1+2q$, q premier impair.

6.3.6 $E(p,a,b) \neq 0$ sous la condition (6.2).

En effet, supposons $E(p,a,b)=0$, $p \equiv 3 \bmod 4$ (donc $|b|>1$). En appliquant la trace $\mathbf{Tr}_{\mathbb{Q}(\zeta,\xi)/\mathbb{Q}(\zeta)}$ à l'égalité (6.25), on obtient :

$$\varphi(q)\, Z + \sum_{k=1}^{\frac{p-3}{2}} t_k Z^{\sigma^k} = 0,$$

où on a posé $t_k = \mathbf{Tr}_{\mathbb{Q}(\zeta,\xi)/\mathbb{Q}(\zeta)}(\xi^k)$.

Théorème 6.3.8 *(Ramanujan) Soient $n>1$ et $k>0$ deux entiers. Posons $d=(n,k)$ et $e=\frac{n}{d}$. Soit ξ_0 une racine primitive n-ième de l'unité. Alors*

$$\boldsymbol{Tr}_{\mathbb{Q}(\xi_0)/\mathbb{Q}}(\xi_0^k) = \frac{\mu(e)\varphi(n)}{\varphi(e)}.$$

Preuve Soit $\wp_n$ (respectivement $\wp_d$) l'ensemble des racines primitives n-ième (respectivement d-ième de l'unité).

Lemme 6.3.9 *Soit f l'application définie sur $\wp_n$ par $f(z)=z^k$. L'application f réalise une surjection de $\wp_n$ vers $\wp_e$. De plus, pour $\theta \in \wp_e$, les ensembles $f^{-1}(\theta)$ ont tous $\frac{\varphi(n)}{\varphi(e)}$ pour ordre.*

Preuve Soit $z \in \wp_n$. Comme $n|ke$, $z^{ke}=1$ et $f(z) \in \wp_e$: f est bien à valeurs dans $\wp_e$. Montrons que f est surjective. Il suffit de montrer que pour $\xi \in \wp_n$ et l entier premier à e, il existe un entier l' premier à n tel que $f(\xi^{l'}) = f(\xi)^l$. Or on vérifie qu'à l fixé, l'entier $l' = l + e \times \prod_{p|d, p\nmid l} p$ convient (le produit portant sur p premier). Enfin, si $\theta \in \wp_e$, l'ensemble $f^{-1}(\theta)$ est constitué des $z \cdot u$, avec $f(z)=\theta$ et u racine k-ième de l'unité. En particulier, les ensembles $f^{-1}(\theta)$ ont tous même ordre, disons N. Comme ils réalisent une partition de $\wp_n$, on a $\varphi(n) = N\varphi(e)$, d'où le lemme.□

Considérons le polynôme $\Psi(X) = \prod_{\xi \in \wp_n} \left(X - \xi^k\right)$. Notons $\Phi_e(X)$ le e-ième polynôme cyclotomique. Par le lemme précédent

$$\Psi(X) = \prod_{\theta \in \wp_e} \prod_{\xi \in f^{-1}(\theta)} (X-\theta) = \left(\Phi_e(X)\right)^{\frac{\varphi(n)}{\varphi(e)}}.$$

Soit $a(n)$ le coefficient de $X^{\varphi(n)-1}$ du n-ième polynôme cyclotomique, $n \geq 1$.

Lemme 6.3.10 *On a $a(n) = -\mu(n)$.*

Preuve En effet, $a(1) = -1$ car $\Phi_1(X) = X - 1$. Si $n > 1$, comme $X^n - 1 = \prod_{d|n} \Phi_d(X)$, le coefficient de X^{n-1} dans $\prod_{d|n} \Phi_d(X)$ est nul. Mais ce coefficient vaut aussi $\sum_{d|n} a(d)$, donc $\sum_{d|n} a(d) = 0$. Définissons l'application $e : \mathbb{N}^* \to \mathbb{N}$ par

$$e(m) = \begin{cases} 1 & \text{si } m = 1, \\ 0 & \text{s } m > 1. \end{cases}$$

Ce qui précède montre que $\sum_{d|n} a(d) = -e(n)$. Par la formule d'inversion de Möebius, il vient

$$a(n) = \sum_{d|n} (-e(d))\mu\left(\frac{n}{d}\right) = -e(1)\mu(n) = -\mu(n),$$

d'où le lemme.□ Le lemme précédent montre que le coefficient de $X^{\varphi(n)-1}$ dans $(\Phi_e(X))^{\frac{\varphi(n)}{\varphi(e)}}$ est $-a(1)\frac{\varphi(n)}{\varphi(e)} = -\mu(e)\frac{\varphi(n)}{\varphi(e)}$. D'un autre côté, ce coefficient est celui de $X^{\varphi(n)-1}$ dans dans $\Psi(X)$, c'est à dire est $-\sum_{\xi \in \wp_n} \xi^k$. On a donc

$$-\sum_{\xi \in \wp_n} \xi^k = -\mu(e)\frac{\varphi(n)}{\varphi(e)},$$

d'où le théorème de Ramanujan.□ En particulier, on obtient

$$\varphi(q)\, Z + \sum_{k=1}^{\frac{p-3}{2}} \frac{\mu\left(\frac{p-1}{2gcd(\frac{p-1}{2},k)}\right)\varphi(q)}{\varphi\left(\frac{p-1}{2gcd(\frac{p-1}{2},k)}\right)} Z^{\sigma^k} = 0. \tag{6.31}$$

Appliquons maintenant à (6.31), σ^i, $i \in \{1, \ldots, \frac{p-3}{2}\}$ et sommons les égalités obtenues. On obtient :

$$\varphi(q)\, \mathbf{Tr}\left(\frac{1}{b-\zeta_0}\right) + \sum_{k=1}^{\frac{p-3}{2}} \frac{\mu\left(\frac{p-1}{2gcd(\frac{p-1}{2},k)}\right)\varphi(q)}{\varphi\left(\frac{p-1}{2gcd(\frac{p-1}{2},k)}\right)} \mathbf{Tr}\left(\frac{1}{b-\zeta_0}\right) = 0. \tag{6.32}$$

On calculera au lemme (6.3.13) la trace sur $\mathbb{Q}$ de $\frac{\zeta_0^n}{b-\zeta_0}$, notée $\tau(n, b)$. En particulier, on a $\tau(0, b) \neq 0$. L'égalité (6.32) montre donc

$$\sum_{k=1}^{\frac{p-3}{2}} \frac{\mu\left(\frac{p-1}{2gcd(\frac{p-1}{2},k)}\right)}{\varphi\left(\frac{p-1}{2gcd(\frac{p-1}{2},k)}\right)} = -1.$$

La dernière assertion de la proposition (6.1.3) est donc démontrée.

6.3.7 Démonstration du corollaire (6.1.5).

Le calcul de $\mathcal{C}(p,a)$ est une conséquence directe de celui de $\mathcal{C}(p,a)$. Calculons plutôt $\mathcal{C}(p,1)$. Posons

$$Q(X)=\sum_{k=0}^{\frac{p-3}{2}}\frac{1}{1-\zeta_0^{\sigma^k}}X^k.$$

On a par définition de $\mathcal{C}(p,1)$:

$$\mathcal{C}(p,1)=\prod_{k=0}^{\frac{p-3}{2}}Q(\xi^k).$$

Comme $\sum_{k=0}^{\frac{p-3}{2}}\xi^k=0$, on a si $0<k\leq\frac{p-3}{2}$:

$$Q(\xi^k)=\frac{1}{2}P(\xi^k),$$

d'où

$$\mathcal{C}(p,1)=2^{-\frac{p-3}{2}}\frac{Q(1)}{P(1)}\prod_{k=0}^{\frac{p-3}{2}}P(\xi^k).$$

On a $Q(1)=\sum_c\frac{1}{1-\zeta_0^c}$, où c décrit les carrés modulo p. Comme $\mathbf{Tr}\left(\frac{p-1}{2}\right)$ (voir la relation 6.34), et comme

$$\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\frac{1}{1-\zeta_0^x}=\sqrt{-p}h(-p),$$

on a

$$\sum_c\frac{1}{1-\zeta_0^c}=\frac{p-1}{4}+\frac{h(-p)\sqrt{-p}}{2}.$$

De plus, $P(1)=h(-p)\sqrt{-p}$. On a donc

$$\begin{aligned}\mathcal{C}(p,1)&=2^{-\frac{p-3}{2}}\left(\frac{p-1}{4}+\frac{h(-p)\sqrt{-p}}{2}\right)\frac{1}{h(-p)\sqrt{-p}}2^{\frac{p-3}{2}}h_p^-p^{\frac{p-7}{4}}\sqrt{-p}\\&=p^{\frac{p-7}{4}}h_p^-\left(\frac{p-1}{4h(-p)}+\frac{\sqrt{-p}}{2}\right).\end{aligned}$$

Le traitement pour a quelconque est identique à celui de $\mathcal{D}(p,a)$.

Montrons maintenant l'inégalité (6.3). Pour démontrer l'inégalité, on va appliquer l'inégalité de Hadamard à la matrice $\mathcal{M}(p,1)$. Pour ce faire, on va d'abord calculer la somme $\sum_c\frac{1}{|1-\zeta|^2}$, où c parcourt les carrés modulo p. On a la proposiion suivante :

Proposition 6.3.11 *Soit $p \equiv 3 \bmod 4$ un nombre premier, et soit C l'ensemble des carrés non nuls modulo p. On a alors*

$$\sum_c \frac{1}{|1-\zeta^c|^2} = \frac{p^2-1}{24}. \tag{6.33}$$

Preuve En effet, on a

$$\sum_{c\in C} \frac{1}{|1-\zeta^c|^2} = \sum_{c\in C} \frac{-\zeta}{(1-\zeta)^2}$$

Pour calculer cette dernière somme, on va plutôt calculer

$$\begin{aligned}\sum_{x=1}^{p-1} \left(\frac{x}{p}\right) \frac{-\zeta^x}{(1-\zeta^x)^2} &= \sum_{x=1}^{p-1} \frac{\left(\frac{x}{p}\right)}{1-\zeta^x} - \sum_{x=1}^{p-1} \frac{\left(\frac{x}{p}\right)}{(1-\zeta^x)^2} \\ &= \sqrt{-p}h(-p) - \sum_{x=1}^{p-1} \frac{\left(\frac{x}{p}\right)}{(1-\zeta^x)^2}.\end{aligned}$$

Pour calculer $\sum_{x=1}^{p-1} \frac{\left(\frac{x}{p}\right)}{(1-\zeta^x)^2}$, on va faire son produit avec la somme de Gauss classique $\sum_{x=1}^{p-1} \left(\frac{x}{p}\right) \zeta^x = \sqrt{-p}$ $(p \equiv 3 \bmod 4)$:

$$\begin{aligned}\sum_{x=1}^{p-1} \frac{\left(\frac{x}{p}\right)}{(1-\zeta^x)^2} \left(\sum_{y=1}^{p-1} \left(\frac{y}{p}\right) \zeta^y\right) &= \sum_{x=1}^{p-1}\sum_{y=1}^{p-1} \frac{\left(\frac{xy}{p}\right) \zeta^y}{(1-\zeta^x)^2} \\ &= \sum_{x=1}^{p-1}\sum_{z=1}^{p-1} \frac{\left(\frac{z}{p}\right) \zeta^{zx}}{(1-\zeta^x)^2} \\ &= \sum_{z=1}^{p-1} \left(\frac{z}{p}\right) \sum_{z=1}^{p-1} \frac{\zeta^{zx}}{(1-\zeta^x)^2} \\ &= \sum_{z=1}^{p-1} \left(\frac{z}{p}\right) \mathbf{Tr}\left(\frac{\zeta^z}{(1-\zeta)^2}\right),\end{aligned}$$

où **Tr** est la trace relative à l'extension $\mathbb{Q}(\zeta)/\mathbb{Q}$. Fixons donc un entier z, $1 \leq z < p$, et calculons $\mathbf{Tr}\left(\frac{\zeta^z}{(1-\zeta)^2}\right)$. On a

$$\begin{aligned}\mathbf{Tr}\left(\frac{-\zeta^z}{(1-\zeta)^2}\right) &= \mathbf{Tr}\left(\frac{1-\zeta^z-1}{(1-\zeta)^2}\right)\\ &= \mathbf{Tr}\left(\frac{1}{1-\zeta}\frac{1-\zeta^z}{1-\zeta}\right) - \mathbf{Tr}\left(\frac{1}{(1-\zeta)^2}\right)\\ &= \mathbf{Tr}\left(\frac{1+\zeta+\ldots+\zeta^{z-1}}{1-\zeta}\right) - \mathbf{Tr}\left(\frac{1}{(1-\zeta)^2}\right)\\ &= \sum_{l=0}^{z-1}\mathbf{Tr}\left(\frac{\zeta^l}{1-\zeta}\right) - \mathbf{Tr}\left(\frac{1}{(1-\zeta)^2}\right).\end{aligned}$$

Lemme 6.3.12 *Soit ζ une racine primitive p-ième de l'unité et soit $1 \leq n < p$ un entier. Soit $\boldsymbol{Tr} = \boldsymbol{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}$ la trace relative à l'extension $\mathbb{Q}(\zeta)/\mathbb{Q}$. On a*

$$\boldsymbol{Tr}\left(\frac{\zeta^n}{1-\zeta}\right) = n - 1 - \frac{p-1}{2}. \tag{6.34}$$

Preuve Raisonnons par récurrence sur n. Rappelons d'abord que $\mathbf{Tr}\left(\frac{1}{1-\zeta}\right) = \frac{p-1}{2}$. En effet, le polynôme minimal $Q(X)$ de $\frac{1}{1-\zeta}$ sur $\mathbb{Q}$ vérifie $Q(X) = \frac{1}{p}X^{p-1}\Phi_p(\frac{X-1}{X})$, où Φ_p est le p-ième polynôme cyclotomique. On vérifie alors que la trace de $\frac{1}{1-\zeta}$ est donné par :

$$\mathbf{Tr}\left(\frac{1}{1-\zeta}\right) = \frac{-1}{p}\sum_{i=1}^{p-1} -i = \frac{p-1}{2}.$$

Passons à la preuve de (6.34). Supposons d'abord que $n = 1$. On a

$$\frac{\zeta}{1-\zeta} = -1 + \frac{1}{1-\zeta},$$

d'où en prenant la trace

$$\mathbf{Tr}\left(\frac{\zeta}{1-\zeta}\right) = -(p-1) + \frac{p-1}{2} = -\frac{p-1}{2}.$$

Le résultat étant supposé vrai en $n < p-1$, on a (rappelons que $\mathbf{Tr}(\zeta) = -1$) :

$$\begin{aligned}\mathbf{Tr}\left(\frac{\zeta^{n+1}}{1-\zeta}\right) = \mathbf{Tr}\left(\frac{(\zeta^{n+1}-1)+1}{1-\zeta}\right) &= \mathbf{Tr}\left(-\left(1+\zeta+\cdots+\zeta^n\right) + \frac{1}{1-\zeta}\right)\\ &= -(p-1) + n + \frac{p-1}{2} = n - \frac{p-1}{2},\end{aligned}$$

l'avant dernière égalité étant due au fait que $n < p$.$\square$

On a donc via le lemme (6.34) :

$$\begin{aligned}\mathbf{Tr}\left(\frac{-\zeta^z}{(1-\zeta)^2}\right) &= \sum_{l=0}^{z-1}\mathbf{Tr}\left(\frac{\zeta^l}{1-\zeta}\right) - \mathbf{Tr}\left(\frac{1}{(1-\zeta)^2}\right)\\ &= \begin{cases} \frac{p^2-1}{12} & \text{si } z=1,\\ \frac{(z-2)(z-1)}{2} - \frac{p-1}{2}(z-1) + \frac{p^2-1}{12} & \text{si } z>1.\end{cases}\end{aligned}$$

On a donc

$$\begin{aligned}\sum_{z=1}^{p-1}\left(\frac{z}{p}\right)\mathbf{Tr}\left(\frac{-\zeta^z}{(1-\zeta)^2}\right) &= \mathbf{Tr}\left(\frac{-\zeta}{(1-\zeta)^2}\right) + \sum_{z=2}^{p-1}\left(\frac{z}{p}\right)\left(\frac{z^2}{2} - \frac{3}{2}z + 1 - \frac{p-1}{2}z + \frac{p^2-1}{12}\right)\\ &= \frac{p^2-1}{12} - \frac{p^2-1}{12} + \sum_{z=1}^{p-1}\left(\frac{z}{p}\right)\left(\frac{z^2}{2} - \frac{3}{2}z + 1 - \frac{p-1}{2}z + \frac{p^2-1}{12}\right)\\ &= \sum_{z=1}^{p-1}\left(\frac{z}{p}\right)\left(\frac{z^2}{2} - \frac{p+2}{2}z\right),\end{aligned}$$

cette dernière égalité étant due au fait que $\sum_{x=1}^{p-1}\left(\frac{x}{p}\right) = 0$. Comme le seul caractère du corps $\mathbb{Q}(\sqrt{-p})$ est le symbole de Legendre, et qu'un tel corps ne contient que ± 1 comme racines de l'unité si $p > 3$, il vient donc pour $p > 3$

$$\sum_{x=1}^{p-1} x\left(\frac{x}{p}\right) = -ph(-p).$$

Or, si χ est un caractère de Dirichlet, posons $\delta_\chi = 0$ si χ est pair et $\delta_\chi = 1$ sinon. On a alors

$$\mathcal{B}_{n,\chi} = 0, \text{si } n \neq \delta_\chi \bmod 2.$$

De plus, si F est un multiple du conducteur f de χ, on a la relation suivante :

$$\mathcal{B}_{n,\chi} = F^{n-1}\sum_{a=1}^{F-1}\chi(a)B_n\left(\frac{a}{F}\right),$$

où B_n est le n-ième polynôme de Bernoulli. En particulier, pour le symbole de Legendre, comme $\delta_{\left(\frac{-}{p}\right)} = 0$, car $p \equiv 3 mod 4$, on a

$$0 = \sum_{a=1}^{p-1}\left(\frac{a}{p}\right)B_2\left(\frac{a}{p}\right).$$

Comme $B_2(X) = X^2 - X + \frac{1}{6}$, on obtient

$$\sum_{a=1}^{p-1} a^2 \left(\frac{a}{p}\right) = -p^2 h(-p).$$

On a donc

$$\sum_{z=1}^{p-1} \left(\frac{z}{p}\right) \mathbf{Tr}\left(\frac{-\zeta^z}{(1-\zeta)^2}\right) = -\frac{1}{2}p^2 h(-p) + \left(\frac{p}{2}+1\right) p h(-p) = p h(-p).$$

On a donc

$$\sum_{z=1}^{p-1} \left(\frac{z}{p}\right) \frac{1}{(1-\zeta^z)^2} = \sqrt{-p} h(-p).$$

Comme $\mathbf{Tr}\left(\frac{1}{(1-\zeta^z)^2}\right) = \frac{1-p^2}{12} + \frac{p-1}{2}$, on a donc

$$\sum_{c \in C} \frac{1}{(1-\zeta^c)^2} = \frac{p-1}{4} + \frac{1-p^2}{24} + \frac{\sqrt{-p} h(-p)}{2}.$$

Comme on a aussi $\sum_{c \in C} \frac{1}{1-\zeta^c} = \frac{p-1}{4} + \frac{\sqrt{-p} h(-p)}{2}$, on a donc

$$\begin{aligned}
\sum_{c \in C} \frac{1}{|1-\zeta^c|^2} &= \sum_{c \in C} \frac{1}{1-\zeta^c} - \sum_{c \in C} \frac{1}{(1-\zeta^c)^2} \\
&= \left(\frac{p-1}{4} + \frac{\sqrt{-p} h(-p)}{2}\right) - \left(\frac{p-1}{4} + \frac{1-p^2}{24} + \frac{\sqrt{-p} h(-p)}{2}\right) \\
&= \frac{p^2-1}{24}
\end{aligned}$$

□ En appliquant l'inégalité de Hadamard à la matrice $\mathcal{M}(p,1)$, on obtient donc, via le calcul explicite de $\mathcal{C}(p,1)$:

$$p^{\frac{p-7}{4}} \left| \frac{p-1}{4h(-p)} + \frac{\sqrt{-p}}{2} \right| h_p^- \leq \left(\frac{p^2-1}{24}\right)^{\frac{p-1}{4}},$$

d'où

$$\begin{aligned} h_p^- &\leq 4h(-p)\frac{\left(\frac{p^2-1}{24}\right)^{\frac{p-1}{4}}}{p^{\frac{p-7}{4}}p\left|\frac{\frac{p-1}{4h(-p)}+\frac{\sqrt{-p}}{2}}{\frac{p}{4h(-p)}}\right|} \\ &\leq 4h(-p)\frac{\left(\frac{p^2-1}{p^2}\right)^{\frac{p-1}{4}}\left(\frac{p^2}{24}\right)^{\frac{p-1}{4}}}{p^{\frac{p-7}{4}}p\left|\frac{\frac{p-1}{4h(-p}+\frac{\sqrt{-p}}{2}}{\frac{p}{4h(-p)}}\right|} \\ &\leq 6h(-p)\frac{p^{\frac{p-1}{2}-\frac{p}{4}+\frac{7}{4}-1}}{24^{\frac{p-1}{4}}} \\ &\leq 6h(-p)\sqrt{-p}\left(\frac{p-1}{24}\right)^{\frac{p-1}{4}}, \end{aligned}$$

qui est l'inégalité voulue.

6.3.8 Une expression générale pour $\mathcal{E}(p,a,b)$.

Nous justifions ici la remarque une formule générale pour l'entier $E(p,a,b)$ qui généralise celle donnant la valeur de $E(p,a,\pm 1)$.

Lemme 6.3.13 *Soient b,n deux entiers tels que $0 \leq n < p$ et $b > 1$. Posons*

$$\tau(n,b) = \boldsymbol{Tr}\left(\frac{\zeta^n}{b-\zeta}\right).$$

On a

$$\tau(n,b) = \begin{cases} \frac{1+b^{p-1}(bp-b-p)}{\varphi_p(b)(1-b)^2} & \text{si } n = 0\,; \\ -b^{n-1}\left(p-1-\frac{n-1}{b}\right) + b^n\frac{1+b^{p-1}(bp-b-p)}{\varphi_p(b)(1-b)^2} & \text{sinon.} \end{cases}$$

Preuve On va commencer par calculer $\mathbf{Tr}\left(\frac{1}{b-\zeta}\right)$. Il s'agit donc de calculer la somme des racines du polynôme $P(X)$ défini par

$$P(X) = \prod_{k=1}^{p-1}\left(X - \frac{1}{b-\zeta^k}\right).$$

Ce polynôme s'écrit aussi

$$P(X) = \frac{1}{\varphi_p(b)}X^{p-1}\prod_{k=1}^{p-1}\left(\frac{bX-1}{X} - \zeta^k\right) = \frac{1}{\varphi_p(b)}X^{p-1}\varphi_p\left(\frac{bX-1}{X}\right).$$

On en déduit ($a > 1$) :

$$\begin{aligned}\mathbf{Tr}\left(\frac{1}{b-\zeta}\right) &= \frac{1}{\varphi_p(b)}\sum_{i=1}^{p-1} ib^{i-1} \\ &= \frac{1+b^{p-1}\left(bp-b-p\right)}{\varphi_p(b)(1-b)^2}.\end{aligned}$$

Calculons maintenant $\mathbf{Tr}\left(\frac{\zeta^n}{b-\zeta}\right)$, n entier, $n > 0$. On a

$$\begin{aligned}\mathbf{Tr}\left(\frac{\zeta^n}{b-\zeta}\right) &= b^{n-1}\mathbf{Tr}\left(\frac{\left(\frac{\zeta}{b}\right)^n}{1-\frac{\zeta}{b}}\right) \\ &= b^{n-1}\mathbf{Tr}\left(\frac{\left(\frac{\zeta}{b}\right)^n-1}{1-\frac{\zeta}{b}}\right) + b^n\mathbf{Tr}\left(\frac{1}{b-\zeta}\right) \\ &= -b^{n-1}\mathbf{Tr}\left(1+\frac{\zeta}{b}+\ldots+\left(\frac{\zeta}{b}\right)^{n-1}\right) + b^n\mathbf{Tr}\left(\frac{1}{b-\zeta}\right) \\ &= -b^{n-1}\left(p-1-\frac{n-1}{b}\right) + b^n\frac{1+b^{p-1}\left(bp-b-p\right)}{\varphi_p(b)(1-b)^2}.\end{aligned}$$

□ On peut maintenant démontrer le lemme suivant :

Lemme 6.3.14 *Soit p un nombre premier et χ un caractère de $\mathbb{F}_p^\times$. Soit $b \neq 1$ un entier. Posons*

$$\mathcal{S}(\chi, b) = \sum_{x=1}^{p-1}\frac{\chi(x)}{b-\zeta^x}.$$

On a alors avec les notations usuelles

$$\tau(\overline{\chi})\mathcal{S}(\chi, b) = \sum_{z=1}^{p-1}\overline{\chi}(z)\left(-b^{z-1}\left(p-1-\frac{z-1}{b}\right)+b^z\tau(0,b)\right).$$

Preuve En effet,

$$\begin{aligned}\tau(\overline{\chi})\mathcal{S}(\chi, b) &= \sum_{x,y}\frac{\chi\left(\frac{x}{y}\right)\zeta^y}{b-\zeta^x} \\ &= \sum_{z,y}\frac{\chi(z)\zeta^y}{b-\zeta^{yz}} = \sum_{z=1}^{p-1}\chi(z)\tau(z^{-1},b),\end{aligned}$$

où z^{-1} est l'unique représentant de l'inverse de z mod p, tel que $0 < z^{-1} < p$. On a donc

$$\tau(\overline{\chi})\mathcal{S}(\chi, b) = \sum_{z=1}^{p-1} \overline{\chi}(z)\tau(z, b),$$

d'où, via le lemme (6.3.13) :

$$\tau(\overline{\chi})\mathcal{S}(\chi, b) = \sum_{z=1}^{p-1} \overline{\chi}(z) \left(-b^{z-1} \left(p - 1 - \frac{z-1}{b} \right) + b^z \tau(0, b) \right).$$

□ On procède, à partir du lemme précédent, comme pour le calcul de $\mathcal{E}(p, a, \pm 1)$, et on obtient si $b > 0$ est un nombre rationnel :

$$E(p, a, b) = -\frac{1}{p^{\frac{p+1}{4}}} \prod_{\chi \in \hat{G}^-} \sum_{z=1}^{p-1} \overline{\chi}(z) \left(-b^{z-1} \left(p - 1 - \frac{z-1}{b} \right) + b^z \tau(0, b) \right).$$

6.3.9 Sous-convenabilité d'un couple (p, q).

Dans ce paragraphe, on démontre les assertions enoncées dans la proposition (6.1.10). Il suffit de montrer celles lorsque b est un entier fixé. Nous utiliserons dans la suite, les notations de la preuve de la proposition (6.1.3).

Commençons par démontrer la deuxième assertion. Fixons nous un couple de premiers impairs distincts (p, q), $q \neq 1$ mod p, qui soit b-sous-convenable, c'est à dire tel que l'entier Q_b soit premier à q. Raisonnons par l'absurde, et supposons que le couple (p, q) ne soit pas b-convenable. Par définition, le nombre rationnel $E(p, 1, b)$ vérifie $\nu_q\left(E(p, 1, b)\right) > 0$ ou $E(p, 1, b) = 0$. Supposons d'abord que l'on soit dans le premier cas : $E(p, 1, b) \neq 0$, et $\nu_q\left(E(p, 1, b)\right) > 0$. Lors de la preuve de la proposition (6.1.3), on a montré

$$E(p, 1, b)\sqrt{-p} = P_{1,b}(1)P_{1,b}(\xi)\dots P_{1,b}(\xi^{\frac{p-3}{2}}), \tag{6.35}$$

où ξ est une racine primitive $\frac{p-1}{2}$-ième de l'unité. Soit $\mathfrak{q}$ un facteur premier quelconque de $\mathbb{Q}(\zeta)$ au-dessus de q. Le premier $\mathfrak{q}$ étant totalement ramifié dans l'extension $\mathbb{Q}(\zeta, \xi)/\mathbb{Q}(\zeta)$ (voir au besoin le lemme 3.3.30 de [28]), désignons par $\mathfrak{q}'$ l'unique premier de $\mathbb{Q}(\zeta, \xi)$ au-dessus de $\mathfrak{q}$. Comme q divise le numérateur de $E(p, 1, b)$, la relation (6.35) montre qu'il existe un entier $k \in \{0, \dots, \frac{p-3}{2}\}$, tel que

$$P_{1,b}(\xi^k) = \mathcal{O}(\mathfrak{q}'),$$

c'est à dire, en revenant à la définition du polynôme $P_{1,b}(X)$:

$$\frac{1}{b - \zeta_0} - \frac{1}{b - \zeta_0^{-1}} + \sum_{k=1}^{\frac{p-3}{2}} \frac{\xi^k}{b - \zeta_0^{g^{2k}}} - \frac{\xi^k}{b - \zeta_0^{-g^{2k}}} = \mathcal{O}(\mathfrak{q}'). \tag{6.36}$$

Soit **Tr** la trace relative à l'extension $\mathbb{Q}(\zeta,\xi)/\mathbb{Q}(\zeta)$. Le premier $\mathfrak{q}$ étant totalement ramifié dans $\mathbb{Q}(\zeta,\xi)/\mathbb{Q}(\zeta)$, en prenant la trace de (6.36), on obtient (rappelons que $\mathbf{Tr}(\xi)=-1$) :

$$(q-1)\left(\frac{1}{b-\zeta_0}-\frac{1}{b-\zeta_0^{-1}}\right)-\sum_{k=1}^{\frac{p-3}{2}}\frac{1}{b-\zeta_0^{g^{2k}}}-\frac{1}{b-\zeta_0^{-g^{2k}}}=\mathcal{O}(\mathfrak{q}).$$

On en déduit donc que

$$\sum_{k=0}^{\frac{p-3}{2}}\frac{1}{b-\zeta_0^{g^{2k}}}-\frac{1}{b-\zeta_0^{-g^{2k}}}=\mathcal{O}(\mathfrak{q}),$$

c'est à dire

$$\sum_{x=1}^{p-1}\frac{\left(\frac{x}{p}\right)}{b-\zeta_0^x}=\mathcal{O}(\mathfrak{q}).$$

Comme $b>1$, un développement en série entière de chacun des quotients $\frac{1}{b-\zeta_0^{\pm g^{2k}}}$, montre que l'on a

$$\sum_{x=1}^{p-1}\frac{\left(\frac{x}{p}\right)}{b-\zeta_0}=\left(\sum_{c\in C}\frac{1}{b^c}-\sum_{n\in N}\frac{1}{b^n}\right)\frac{b^{p-1}}{b^p-1}\sqrt{-p},$$

d'où $((b,q)=1)$:

$$\sum_{c\in C}\frac{1}{b^c}-\sum_{n\in N}\frac{1}{b^n}\equiv 0 \bmod q,$$

d'où

$$Q_b\equiv 0 \bmod q,$$

en contradiction avec le fait que (p,q) est b-convenable. Si $p=1+2q$, la b-sous-convenabilité du couple (p,q) entraîne bien sa b-convenabilité.

Pour finir de prouver la proposition (6.1.10), il reste à montrer que si (p,q) est b-convenable et $q\neq 1 \bmod p$, alors (p,q) est b-sous-convenable. Soit donc (p,q) un tel couple. S'il n'était pas b-sous-convenable, alors il existerait par définition un premier $\mathfrak{q}'$ de $\mathbb{Q}(\zeta,\xi)$ au-dessus de q, tel que $P_{1,1}(1)=\mathcal{O}(\mathfrak{q}')$. Comme $\mathcal{N}(b-\zeta_0)=\frac{b^p-1}{b-1}$, dont les facteurs premiers (autres que p) valent tous 1 mod p (lemme (5.3.13)), on a donc $\nu_{\mathfrak{q}'}\left(P_{1,b}(\xi^k)\right)\geq 0$, d'où

$$P_{1,b}(1)P_{1,b}(\xi)\dots P_{1,b}(\xi^{\frac{p-3}{2}})=\mathcal{O}(\mathfrak{q}'),$$

d'où $q|E(p,1,b)$, ce qui contredit le fait que (p,q) est b-convenable.

La proposition (6.1.10) est prouvée.

6.4 Quelques éléments sur les corps de type CM.

6.4.1 Rappels succints.

Soit K un corps de type CM, I_K son groupe des idéaux fractionnaires, $\iota : K^* \to I_K$ l'application canonique, j la conjugaison complexe de K (voir [77]), K^+ son sous-corps réel maximal et $\mathcal{O}_K$ l'anneau des entiers de K. On désigne par h_K^- le nombre de classes relatives de K. On rappelle maintenant des résultats qui seront appliquées lors de la preuve de la proposition (6.4.4) due à Schwarz (voir [70]).

Théorème 6.4.1 *Soit C^+ (respectivement C) le groupe des classes de K^+ (respectivement de K). Soit $\varphi : C^+ \to C$ l'application canonique. Son noyau est d'ordre au plus deux.*

Preuve Soit $I \in Ker\,(\varphi)$. Il existe $\alpha \in K$ tel que dans K, on a $I = (\alpha)$. I étant réel, $\frac{\alpha^j}{\alpha}$ est une unité de K, donc une racine de l'unité. Soient W le groupe des racines de l'unité de K, U_K son groupe des unités et soit $W_0 = \left\{ \frac{u^j}{u} : \quad u \in U_K \right\}$. Un autre choix de α pour I, laisse invariant le quotient $\frac{u^j}{u}$ modulo W_0. On a donc

$$\phi : Ker\,(\varphi) \to \frac{W}{W_0}.$$

Une telle application est injective. En effet, supposons que $\phi(I) = 1$. Il existe alors une unité u telle que $\frac{u^j}{u} = \frac{\alpha^j}{\alpha}$. Le nombre algébrique $\frac{\alpha}{u}$ est donc réel. Comme il engendre I dans K, $I = \left(\frac{\alpha}{u}\right)$ dans K^+, c'est à dire est trivial dans C^+. Comme $W^2 \subset W_0$, le quotient est d'ordre au plus deux. ■

Remarque 6.4.2 *Il se peut que son noyau soit d'ordre 2 (voir [77]) ou d'ordre 1 (cas du p-ième corps cyclotomique).*

On rapelle le lemme suivant, nécessaire à la preuve de la proposition (6.4.4). On trouvera des preuves différentes dans [40] ou [70] :

Lemme 6.4.3 *Soit K un corps de nombres, et $\mathcal{Q}$ un ensemble fini d'idéaux de K. Toute classe d'idéaux de K contient un idéal premier à $\mathcal{Q}$.*

Preuve En effet, soit C une classe de K, et soit $\mathfrak{a}$ un élément de C. Soient L le corps de classes de Hilbert de K et G le groupe de Galois de l'extension L/K. Soit S les idéaux premiers de K divisant les éléments de $\mathcal{Q}$. Soit I_K^S les idéaux fractionnaires de K premiers à S. Comme L/K est abélienne non ramifiée, par le théorème de densité de Frobenius, le symbole d'Artin réalise une surjection de I_K^S vers G. Par la théorie du corps de classes, le

symbole d'Artin induit un isomorphisme entre G et C_K, le groupe des classes de K. Soit $g \in G$ associé à C par cet isomorphisme. Soit aussi $\mathfrak{a}' \in I_K^S$, un antécédent de g. Par la théorie du corps de classes, on a $\mathfrak{a}$ et $\mathfrak{a}'$ sont dans la même classe de C_K et $\mathfrak{a}'$ est premier à $\mathcal{Q}$ par définition. ■

6.4.2 Proposition de Schwarz.

Rappelons et démontrons maintenant la proposition due à Schwarz :

Proposition 6.4.4 *Soit $\mathcal{Q}$ un ensemble fini d'idéaux de K. Il existe un sous-groupe I_0 de I_K vérifiant les propriétés suivantes :*

1. *Les idéaux de $\mathcal{Q}$ n'apparaissent pas dans la factorisation des idéaux de I_0.*
2. *Le groupe $I_K/(i(K^*)I_0)$ a pour cardinal h_K^- ou $2h_K^-$.*
3. *Si ϵ est un élément de $\in K^*$, et si $(\epsilon) \in I_0$, alors ϵ^{1-j} est une racine de l'unité.*

Preuve Soit I_K^+ le groupe des idéaux fractionnaires de K^+. Soit I_0 les idéaux de I_K, qui sont une image par l'application canonique $I_K^+ \to I_K$, et qui sont premiers à $\mathcal{Q}$. Soit alors $(\epsilon) \in I_0$. Par définition de I_0, $(\epsilon^j) = (\epsilon)$. Il existe alors une unité u de K telle que $\epsilon = u\epsilon^j$. L'unité u est alors de module 1. Par le théorème de Kronecker, u est une racine de l'unité. Les assertions (1) et (3) sont démontrées. Montrons l'assertion (2). Considérons le groupe $I_K/(i(K^*)I_0)$. Comme toute classe d'idéaux contient un idéal premier à $\mathcal{Q}$ (lemme 6.4.3), ce groupe est le quotient de C_K par $\varphi(C_K^+)$. Par le théorème (6.4.1), ce groupe est d'ordre h_K^- ou $2h_K^-$. ■

6.5 Démonstration du théorème (6.1.1).

Si q ne divise pas h_p^- et si $q < Sup\left(p, \frac{p(p-20)}{16}\right)$, alors la deuxième assertion du théorème (6.1.1) est simplement l'énoncé du théorème 2 de [52]. Démontrons les trois autres assertions. On pose pour la suite $\zeta = \zeta_0 = e^{\frac{2i\pi}{p}}$.

6.5.1 Cas où $q|x+y$.

Soit donc fixée une solution de (6.1) avec $q|x+y$, où $\zeta = \zeta_0 = e^{\frac{2i\pi}{p}}$. Soient $a \neq b$ deux entiers non nuls modulo p. Comme $(x, y, z) = 1$, on a $\left(x + \zeta^a y, x + \zeta^b y\right) | \mathfrak{p}$, l'unique premier de l'anneau $\mathbb{Z}[\zeta]$ au-dessus de p. Il existe donc un idéal $\mathfrak{a}$ de l'anneau $\mathbb{Z}[\zeta]$ tel que

$$\left(\frac{x+\zeta y}{(1-\zeta)^e}\right) = \mathfrak{a}^q. \tag{6.37}$$

Soit θ un élément de $\mathcal{I}_{st}(K)$, $\theta \geq 0$. Soit g une racine primitive modulo p, et soit $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ défini par $\zeta^\sigma = \zeta^{g^2}$. Posons $c_k = g^{2k}, k = 0, \ldots, \frac{p-3}{2}$. Comme $p \equiv 3 \bmod 4$, -1 n'est pas un résidu quadratique modulo p, et on peut donc définir des entiers $a_k, b_k, k = 0, \ldots, \frac{p-3}{2}$ de sorte que

$$\theta = \sum_{k=0}^{\frac{p-3}{2}} a_k \sigma_{c_k} + b_k \sigma_{-c_k}.$$

On suppose que θ est choisi de sorte que pour au moins un entier k, la différence $a_k - b_k$ est première à q (un tel choix et sa validité seront justifiés plus loin dans la preuve). Par la proposition (4.5.11), et la proposition (4.4.13), comme $(q, 2p) = 1$, il existe un entier algébrique γ tel que

$$\left(\frac{x + \zeta y}{(1-\zeta)^e}\right)^\theta = \gamma^q. \tag{6.38}$$

Plus précisément, les propositions (4.5.11) et (4.4.13) montrent qu'il existe $\epsilon = \pm 1$ et ζ^l une racine p-ième de l'unité, tels que

$$\left(\frac{x + \zeta y}{(1-\zeta)^e}\right)^\theta = \epsilon \zeta^l \gamma^q.$$

Comme $(q, 2p) = 1$, $\epsilon\zeta^l$ est une puissance q-ième dans $\mathbb{Z}[\zeta]$, et quitte à modifier γ on peut donc bien supposer que $\epsilon\zeta^l = 1$. L'équation (6.38) s'écrit aussi

$$\left(1 + \frac{x+y}{y(\zeta - 1)}\right)^\theta = \frac{(1-\zeta)^{(e-1)\theta}\gamma^q}{y^{W(\theta)}}.$$

Par hypothèse, q divise $x + y$. Soit $\mathfrak{q}$ un idéal premier de q dans K. Si a, b sont deux entiers distincts modulo p, $\mathfrak{p}$ est engendré par $\zeta^a - \zeta^b$. Comme $q \neq p$ et y est premier à q (car $(x, y) = 1$), on obtient donc :

$$1 - \frac{x+y}{y} \sum_{k=0}^{\frac{p-3}{2}} \frac{a_k}{1 - \zeta^{\sigma^k}} + \frac{b_k}{1 - \zeta^{-\sigma^k}} = \frac{(1-\zeta)^{\theta(e-1)}\gamma^q}{y^{W(\theta)}} + \mathcal{O}(\mathfrak{q}^2). \tag{6.39}$$

De même, on a en prenant $\mathfrak{q}^j$ au lieu de $\mathfrak{q}$, j étant la conjugaison complexe :

$$1 - \frac{x+y}{y} \sum_{k=0}^{\frac{p-3}{2}} \frac{a_k}{1 - \zeta^{\sigma^k}} + \frac{b_k}{1 - \zeta^{-\sigma^k}} = \frac{(1-\zeta)^{\theta(e-1)}\gamma^q}{y^{W(\theta)}} + \mathcal{O}(\mathfrak{q}^{2j}). \tag{6.40}$$

On en déduit, en faisant la différence de (6.39) par la conjugaison complexe de (6.40) :

$$\frac{x+y}{y} \sum_{k=0}^{\frac{p-3}{2}} (b_k - a_k)\left(\frac{1}{1 - \zeta^{\sigma^k}} - \frac{1}{1 - \zeta^{-\sigma^k}}\right) = \frac{(1-\zeta)^{\theta(e-1)}\gamma^q}{y^{W(\theta)}} - \frac{(1-\overline{\zeta})^{\theta(e-1)}\overline{\gamma}^q}{y^{W(\theta)}} + \mathcal{O}(\mathfrak{q}^2) \tag{6.41}$$

Il existe une racine p-ième de l'unité r telle que $\frac{\left(1-\overline{\zeta}\right)^{(e-1)\theta}}{(1-\zeta)^{(e-1)\theta}} = \left(-\overline{\zeta}\right)^{(e-1)\theta} = r^q$. Il vient donc

$$\begin{aligned}\frac{(1-\zeta)^{\theta(e-1)}\gamma^q}{y^{W(\theta)}} - \frac{(1-\overline{\zeta})^{\theta(e-1)}\overline{\gamma}^q}{y^{W(\theta)}} &= \frac{(1-\zeta)^{\theta(e-1)}\gamma^q}{y^{W(\theta)}} - \overline{\zeta}^{(e-1)\theta}\frac{(1-\zeta)^{\theta(e-1)}\overline{\gamma}^q}{y^{W(\theta)}} \\ &= \frac{(1-\zeta)^{\theta(e-1)}\gamma^q}{y^{W(\theta)}} - r^q\frac{(1-\zeta)^{\theta(e-1)}\overline{\gamma}^q}{y^{W(\theta)}}.\end{aligned}$$

D'après (6.41), il existe donc $\gamma_1 \in K$ tel que

$$\frac{x+y}{y}\sum_{k=0}^{\frac{p-3}{2}}(b_k-a_k)\left(\frac{1}{1-\zeta^{\sigma^k}} - \frac{1}{1-\zeta^{-\sigma^k}}\right) = \frac{(1-\zeta)^{\theta(e-1)}}{y^{W(\theta)}}(\gamma^q - \gamma_1^q) + \mathcal{O}(\mathfrak{q}^2). \qquad (6.42)$$

Le terme de gauche de (6.42) est un $\mathcal{O}(\mathfrak{q})$ vu que $q|x+y$ et $q \neq p$. On en déduit que $\gamma^q - \gamma_1^q = \mathcal{O}(\mathfrak{q})$.

Lemme 6.5.1 *Soient L un corps de nombre, $\mathcal{Q}$ un idéal premier de L divisant le nombre premier q. Soient $\alpha, \beta \in L$. Supposons que $\alpha^q - \beta^q = \mathcal{O}(\mathcal{Q})$. On a alors $\alpha^q - \beta^q = \mathcal{O}(\mathcal{Q}^2)$.*

Preuve En effet, par la formule du binôme, on a

$$\alpha^q - \beta^q = \sum_{k=1}^{q}\binom{q}{k}(\alpha-\beta)^k\beta^{q-k}.$$

Comme $\alpha^q - \beta^q = \mathcal{O}(\mathcal{Q})$ et $q|\binom{q}{k}$ si $1 \leq k < q$, on déduit que $(\alpha-\beta)^q = \mathcal{O}(\mathcal{Q})$. Comme $\mathcal{Q}$ est premier, $\alpha - \beta = \mathcal{O}(\mathcal{Q})$. On a donc

$$\alpha^q - \beta^q = \sum_{k=1}^{q}\binom{q}{k}(\alpha-\beta)^k\beta^{q-k} = \mathcal{O}(\mathcal{Q}^2).\square$$

De ce lemme, on déduit que $\gamma^q - \gamma_1^q = \mathcal{O}(\mathfrak{q}^2)$, d'où

$$\frac{x+y}{y}\sum_{k=0}^{\frac{p-3}{2}}(b_k-a_k)\left(\frac{1}{1-\zeta^{\sigma^k}} - \frac{1}{1-\zeta^{-\sigma^k}}\right) = \mathcal{O}(\mathfrak{q}^2).$$

S'il existe un idéal premier $\mathfrak{q}$ de K au-dessus de q, tel que $\mathfrak{q}^2|x+y$, alors, par transitivité de l'action de G sur les facteurs premiers de q dans K (voir par exemple [69], chapitre 6), on a $q^2|x+y$. Supposons maintenant que tout facteur premier $\mathfrak{q}$ de q dans K soit un facteur

premier simple de $x+y$, c'est à dire $\mathfrak{q}||x+y$ dans K, et montrons que $q|h_p^-$. La relation (6.42), montre que l'on a alors pour tout facteur premier $\mathfrak{q}$ de q dans K :

$$\sum_{k=0}^{\frac{p-3}{2}}(a_k-b_k)\left(\frac{1}{1-\zeta^{\sigma^k}}-\frac{1}{1-\zeta^{-\sigma^k}}\right)=\mathcal{O}(\mathfrak{q}). \tag{6.43}$$

Soient $\delta_l=a_l-b_l$ et posons

$$X=\left(\delta_0\cdots\delta_{\frac{p-3}{2}}\right)^t,\quad Z=\frac{1}{1-\zeta}-\frac{1}{1-\zeta^{-1}}.$$

Soit $\mathfrak{q}$ un facteur premier fixé de q dans K. On pose $\mathcal{M}=\mathcal{M}(p,1)$, la matrice carrée de taille $\left(\frac{p-1}{2}\right)^2$ dont les lignes sont celles de $\mathcal{E}(p,1,1)$. D'après (6.43), le vecteur $\mathcal{M}X$ est tel que sa i-ième coordonnée notée $(\mathcal{M}X)_i$, vérifie $(\mathcal{M}X)_i=\mathcal{O}(\mathfrak{q})$, pour tout i, $1\leq i\leq\frac{p-1}{2}$. En effet, pour tout facteur $\mathfrak{q}'$ de q dans K, on a

$$\sum_{k=0}^{\frac{p-3}{2}}\delta_k Z^{\sigma^k}=\mathcal{O}(\mathfrak{q}').$$

Prenons $\mathfrak{q}'=\mathfrak{q}^{\sigma^{-(i-1)}}$ où i est un entier, $1\leq i\leq\frac{p-1}{2}$. On a alors

$$\sum_{k=0}^{\frac{p-3}{2}}\delta_k Z^{\sigma^{k+i-1}}=\mathcal{O}(\mathfrak{q}),$$

c'est à dire $(\mathcal{M}X)_i=\mathcal{O}(\mathfrak{q})$, $1\leq i\leq\frac{p-1}{2}$. Soit $\mathcal{M}'$ la transposée de la comatrice de $\mathcal{M}$. On a $\mathcal{M},\mathcal{M}'\in\mathcal{M}_{r+1}\left(\mathbb{Z}\left[\zeta,\frac{1}{1-\zeta}\right]\right)$. De plus, $q\neq p$, et p est totalement ramifié dans $K/\mathbb{Q}$, dont le seul diviseur premier $\mathfrak{p}$ dans K est engendré par $1-\zeta$. On a donc

$$(\mathcal{M}'\mathcal{M}X)_i=\mathcal{O}(\mathfrak{q}),$$

c'est à dire

$$(\mathcal{E}(p,1,1)X)_i=\mathcal{O}(\mathfrak{q}),$$

Si $(E(p,1,1),q)=1$, on a donc pour tout i, $X_i=\mathcal{O}(\mathfrak{q})$, c'est à dire $a_i-b_i=\delta_i=\mathcal{O}(\mathfrak{q})$, en contradiction avec le choix de θ. On doit donc avoir $q|E(p,1,1)$. Comme q est premier impair et distinct de p, on a donc par la proposition (6.1.3) $q|h_p^-$. Il reste à montrer que l'on peut choisir $\theta\in\mathcal{I}_{st}(K)$ positif, tel que $a_k\neq b_k \bmod q$, pour au moins un entier k, où on rappelle que

$$\theta=\sum_{k=0}^{\frac{p-3}{2}}a_k\sigma^k+b_kj\sigma^k.$$

Prenons par exemple $\theta = \psi_2.\ \theta$. Si pour tout k, $a_k \equiv b_k \bmod q$, on a

$$\theta \equiv \sum_{k=0}^{\frac{p-3}{2}} a_k \sigma^k + a_k j \sigma^k \bmod q\mathbb{Z}[G],$$

d'où

$$(1-j)\theta \equiv 0 \bmod q\mathbb{Z}[G],$$

c'est à dire $\theta - (2\mathcal{N} - \theta) = 2\theta - 2\mathcal{N} \equiv 0 \bmod q\mathbb{Z}[G]$. On en déduit que pour tout k, $a_k, b_k \equiv 1 \bmod q$. Comme il existe $\frac{p-1}{2}$ entiers k tel que $a_k = 0$ ou $b_k = 0$, on obtient une contradiction. ■

6.5.2 Cas où $q|x-y$.

La démonstration est identique à celle du cas $f = 1$. En effet, on a dans ce cas

$$\left(\frac{x+\zeta y}{(1-\zeta)^e}\right)^\theta = y^{W(\theta)} (\zeta+1)^\theta \left(1 + \frac{x-y}{y(1+\zeta)}\right)^\theta.$$

L'entier algébrique $1+\zeta$ est une unité de l'anneau $\mathbb{Z}[\zeta]$, donc est premier à q. De plus, $\frac{1+\overline{\zeta}}{1+\zeta} = \overline{\zeta}$, donc est une puissance q-ième de $\mathbb{Z}[\zeta]$. Néanmoins, le determinant intervenant est $\mathcal{E}(p, 1, -1)$, d'où le théorème dans le cas où $q|x-y$. ■

6.5.3 Cas où $q|x$.

A partir de l'identité $\left(\frac{x+\zeta y}{(1-\zeta)^e}\right)^\theta = \gamma^q$, comme $q|x$, il existe deux nombres algébriques γ, γ_1 de $\mathbb{Q}(\zeta)$, tels que pour tout diviseur premier $\mathfrak{q}$ de q dans ce corps

$$\frac{x}{y} \sum_{k=1}^{p-1} (a_k - a_{p-k})\, \zeta^{k^{-1}} = \frac{(1-\zeta)^e}{\zeta^\theta y^{W(\theta)}} (\gamma^q - \gamma_1^q) + \mathcal{O}(\mathfrak{q}^2),$$

où on a posé $\theta = \sum_{k=1}^{p-1} a_k \sigma_k^{-1}$, et k^{-1} l'inverse de k moduo p. S'il existe un premier $\mathfrak{q}$ tel que $\mathfrak{q}^2|x$, alors $q^2|x$ par transitivité de l'action de $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ sur les facteurs premiers de q dans $\mathbb{Z}[\zeta]$ (voir par exemple [69], chapitre 6). Si pour tout facteur premier $\mathfrak{q}$ de q dans $\mathbb{Z}[\zeta]$, $\mathfrak{q}||x$, alors, par le lemme (6.5.1)

$$\sum_{k=1}^{p-1} (a_k - a_{p-k})\, \zeta^{k^{-1}} = \mathcal{O}(\mathfrak{q}),$$

d'où dans $\mathbb{Z}[\zeta]$, on a

$$q|\sum_{k=1}^{p-1}(a_k - a_{p-k})\,\zeta^{k^{-1}}.$$

Le lemme 1.9 de [77], montre donc

$$\forall k \in \{1,\ldots,p-1\}, q|a_k - a_{p-k}.$$

Prenons $\theta = \psi_2$. On a alors $a_{\frac{p-1}{2}} = 1$ et $a_{\frac{p+1}{2}} = 0$. Par conséquent, l'entier $a_{\frac{p-1}{2}} - a_{\frac{p+1}{2}}$ est premier à q. On a donc bien $q^2|x$. ■

6.5.4 Autre preuve dans le cas $r_q < \frac{p-1}{2}$.

Dans ce paragraphe, on donne une deuxième démontration des trois dernières assertion du théorème, basée, non pas sur l'utilisation du théorème de Stickelberger, mais sur celle de la proposition de Schwarz, et qui s'inspire de [70] (voir aussi [63]), article dans lequel Schwarz l'applique à l'équation de Catalan. Néanmoins, cette seconde preuve ne couvre que le cas $r_q < \frac{p-1}{2}$, r_q étant le q-rang du groupe des classes relatif du p-ième corps cyclotomique. Elle est donc en particulier valable si $q > p$. En effet, on a le lemme connu suivant :

Lemme 6.5.2 *Soit p un nombre premier. On a $h_p^- < p^{\frac{p-1}{2}}$.*

Preuve Pour le prouver, on peut appliquer les majorations de [33]. Dans le cas $p \equiv 3 \bmod 4$, c'est aussi une conséquence de l'inégalité (6.3), et de la majoration $h(-p) \leq \frac{2}{\pi}\sqrt{p}log(4p)$ (voir [32]).□

Les preuves étant similaires dans les trois cas, on ne détaillera que le cas $q|x+y$.

Posons $\zeta = e^{\frac{2i\pi}{p}}$. Il existe un idéal $\mathfrak{a}$ de l'anneau $\mathbb{Z}[\zeta]$ tel que

$$\left(\frac{x+y\zeta}{(1-\zeta)^e}\right) = \mathfrak{a}^q.$$

Soit g une racine primitive modulo p, et soit $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ défini par $\zeta^\sigma = \zeta^{g^2}$. Appliquons le lemme (6.4.4) au corps $K = \mathbb{Q}(\zeta)$ qui est de type CM, et à $\mathcal{Q}$ l'ensemble des idéaux premiers de K qui divisent q. Comme $q > 2$, le groupe $I_K/(i(K^*)I_0)$ a pour q-rang celui du groupe des classes relatives, c'est à dire r_q. Les éléments d'ordre divisant q de I_K engendrent donc un $\mathbb{F}_q$-espace vectoriel de dimension r_q dans $I_K/(i(K^*)I_0)$. Il existe donc des entiers non tous nuls modulo q, $a_0,\ldots,a_{r_q}$ tels que

$$\mathfrak{a}^{a_0+a_1\sigma+\cdots+a_{r_q}\sigma^{r_q}} \in i(K^*)I_0. \tag{6.44}$$

Par hypothèse, $r_q < \frac{p-1}{2}$. Donc, quitte à poser $a_{r_q+1} = \ldots = a_{\frac{p-3}{2}} = 0$, on peut supposer que l'indexation des a_i va jusqu'à la valeur $r = \frac{p-3}{2}$. Prenons la puissance q-ième de l'idéal donné par (6.44). Posons $\theta = a_0 + a_1\sigma + \cdots + a_r\sigma^r$. Il existe deux nombres algébriques ϵ et α tels que $(\epsilon) \in I_0$, α est premier à tout facteur premier dans K de q, et

$$(x + y\zeta)^{a_0+a_1\sigma+\cdots+a_r\sigma^r} = \epsilon u_e \, (1-\zeta)^{eA} \, \alpha^q,$$

où on a posé $A = W(\theta)$, avec u_e unité de K. Il existe alors une unité u telle que

$$\left(1 - \frac{x+y}{y(1-\zeta)}\right)^{\theta} = \frac{\epsilon u (1-\zeta)^{A(e-1)} \alpha^q}{y^A}.$$

Par hypothèse, q divise $x + y$. Soit $\mathfrak{q}$ un idéal premier de q dans K. Comme $q \neq p$, on obtient :

$$1 - (x+y)\sum_{k=0}^{r} \frac{a_k}{1-\zeta^{\sigma^k}} = \left(1 + \frac{x+y}{y(\zeta-1)}\right)^{\theta} = \frac{\epsilon u (1-\zeta)^{A(e-1)} \alpha^q}{y^A} + \mathcal{O}(\mathfrak{q}^2). \tag{6.45}$$

De même, en prenant $\mathfrak{q}^j$ au lieu de $\mathfrak{q}$, j étant la conjugaison complexe, on a :

$$1 - (x+y)\sum_{k=0}^{r} \frac{a_k}{1-\zeta^{\sigma^k}} = \left(1 + \frac{x+y}{y(\zeta-1)}\right)^{\theta} = \frac{\epsilon u (1-\zeta)^{A(e-1)} \alpha^q}{y^A} + \mathcal{O}(\mathfrak{q}^{2j}). \tag{6.46}$$

En faisant la différence de (6.45) par la conjugaison complexe de (6.46), on obtient :

$$-(x+y)\sum_{k=0}^{r} \frac{a_k}{1-\zeta^{\sigma^k}} - \frac{a_k}{1-\zeta^{-\sigma^k}} = \frac{\epsilon u (1-\zeta)^{A(e-1)} \alpha^q}{y^A} - \frac{\epsilon^j u^j (1-\zeta^{-1})^{A(e-1)} \alpha^{qj}}{y^A} + \mathcal{O}(\mathfrak{q}^2).$$

Par le lemme (6.4.4), le quotient $\frac{\epsilon}{\epsilon^j}$ est une racine de l'unité de K. Comme les racines de l'unité de ce corps sont les racines $2p$-ième de l'unité et que $(q, 2p) = 1$, il existe une racine de l'unité r_1 telle que $\epsilon^j = \epsilon r_1^q$. Si u est une unité de K, alors $\frac{u}{u^j}$ est une racine $2p$-ième de l'unité. Donc, il existe une racine de l'unité r_2 telle que $u^j = u r_2^q$. Comme $\frac{1-\zeta}{1-\zeta^{-1}} = -\zeta$, on conclut de même. Finalement, il existe $\beta \in K$, tel que

$$-(x+y)\sum_{k=0}^{r} \frac{a_k}{1-\zeta^{\sigma^k}} - \frac{a_k}{1-\zeta^{-\sigma^k}} = \frac{\epsilon u (1-\zeta)^{A(e-1)}}{y^A} (\alpha^q - \beta^q) + \mathcal{O}(\mathfrak{q}^2).$$

La preuve se conclut alors comme les précédentes (par définition, au moins un des a_i est premier à q).

6.6 Démonstration du corollaire (6.1.11).

Si $p \equiv 3 \bmod 4$, c'est une conséquence du théorème (6.1.1) appliqué avec $y = -1$. Si $p \equiv 1 \bmod 4$, c'est une conséquence du théorème 1 de [54].

6.7 Démonstration du corollaire (6.1.14).

Supposons qu'il existe une solution en nombres entiers X, Z fixée de l'équation (6.5). On va montrer pour chacun des cas, qu'elle ne peut exister si le critère de divibilité qui porte sur $h(-B^*Y_0^r)$ ou h_p^- n'a pas lieu, d'où le corollaire. Pour la démonstration, on utilisera, outre le théorème (6.1.1), le théorème (3.1.1), ainsi que son corollaire (3.1.9).

Pour simplifier, dans la suite, **le théorème (3.1.1) sera nommé théorème** A**. Le corollaire (3.1.9) sera nommé corollaire** B.

6.7.1 Cas $q = 2, p \geq 7$.

Supposons que $(h(-B^*Y_0^r), p) = 1$ et montrons alors que la solution X, Z ne peut exister. Si l est pair, on peut apliquer le théorème (3.1.1), qui montre que (6.5) n'a aucune solution entière. Supposons l impair. 0n peut mettre (6.5) sous la forme

$$B^*Z^2 + Y_0^{l-1}Y_0 = X^p, \quad (X, Z, Y_0) = 1.$$

Y_0 est un premier autre que 3. Le théorème A montre encore que (6.5) n'a aucune solution entière. Donc l'existence de la solution (X, Z) montre bien dans ce cas que $p|h(-B^*Y_0^r)$.

6.7.2 Cas $q = 2, p = 3, B^* = 1$.

Si $Y_0 = 1$, le théorème de Lebesgue montre que l'équation (6.5) est sans solution entière. On suppose dans la suite $Y_0 > 1$.

Supposons d'abord que l soit pair. Supposons que $Y_0 = 2$. L'équation (6.5) s'écrit

$$Z^2 + 2^l = X^3, \quad (Z, X) = 1.$$

L'étude du paragraphe (3.4.5) montre que cette équation est sans solution entière sauf si $l = 1$ ou $l = 2$, valeurs pour lesquelles on a les solutions respectives

$$11^2 + 2^2 = 5^3, \quad 5^2 + 2 = 3^3.$$

Comme on a supposé $Y_0^l \neq 2, 4$, l'équation (6.5) est sans solution entière.

Supposons $Y_0 > 2$. Vu les hypothèses faites dans ce cas, le théorème (3.1.1) montre qu'il existe un entier naturel A_0 et $\epsilon_0 = \pm 1$ tels que

$$Y_0^l = 3A_0^2 + \epsilon_0. \tag{6.47}$$

Comme l est pair, $Y_0^l \equiv 1 \bmod 3$, d'où $\epsilon_0 = 1$.

Proposition 6.7.1 *Soit $n > 2$ un entier. L'équation diophantienne*

$$3X^2 + 1 = Y^n \tag{6.48}$$

admet pour seule solution en nombres entiers $X = 0, Y = 1$.

Preuve Si n possède un facteur premier impair p, quitte à poser $Z = Y^{\frac{n}{p}}$ et se ramener à l'équation $3X^2 + 1 = Z^p$, on peut supposer n premier impair. De même, si n est une puissance de deux, on peut supposer que $n = 4$.

L'anneau $\mathbb{Z}[\sqrt{-3}]$ étant principal, si n est premier impair, la proposition est une conséquence du théorème A. C'est aussi un cas particulier du théorème 3 de [14]. Etudions en détails le cas $n = 4$. Comme $n > 2$, remarquons que Y est impair. En effet, si Y est pair, alors $n > 2$ donne $8|Y$. D'autre part, $2|Y$ implique X impair, donc $3X^2 + 1 \equiv 4 \bmod 8$, ce qui contredit $3X^2 + 1 = Y^4$. L'entier Y est donc bien impair. Les entiers algébriques $1 + X\sqrt{-3}$ et $1 - X\sqrt{-3}$ sont donc premiers entre eux. Comme

$$\left(1 + X\sqrt{-3}\right)\left(1 - X\sqrt{-3}\right) = Y^4,$$

il existe une racine 3-ième de l'unité U, $\epsilon = \pm 1$, et deux entiers A, B de même parité tels que

$$1 + X\sqrt{-3} = \epsilon U \left(\frac{A + B\sqrt{-3}}{2}\right)^4.$$

Comme U est d'ordre impair, quitte à modifier A et B, on peut supposer que $U = 1$. Supposons A et B impairs. En identifiant les parties réelles, il vient

$$2^4 = \epsilon\left(A^4 - 18A^2B^2 + 9B^4\right) = \pm\left(\left(A^2 - 9B^2\right)^2 - 72B^4\right).$$

Comme on a supposé A et B impairs, on a $A^2 \equiv B^2 \equiv 1 \bmod 8$, d'où

$$A^2 - 9B^2 \equiv 0 \bmod 8,$$

d'où $2^6 | \left(A^2 - 9B^2\right)^2$. On doit donc avoir $2^4 | 72B^4$, ce qui montre que B est pair : contradiction. Les entiers A et B sont donc pairs, et quitte à poser $A' = \frac{A}{2}$, $B' = \frac{B}{2}$, on a

$$1 + X\sqrt{-3} = \pm\left(A + B\sqrt{-3}\right)^4.$$

L'identification des parties réelles donne

$$1 = \epsilon\left(A^4 - 18A^2B^2 + 9B^4\right) = \pm\left(\left(A^2 - 9B^2\right)^2 - 72B^4\right).$$

En se plaçant modulo 3, on voit que seul le signe + convient. On est donc ramené à résoudre l'équation

$$C^2 - 72D^4 = 1.$$

Soit donc (C, D) une solution entière positive de cette équation, autre que $C = 1, D = 0$. On a

$$\frac{C+1}{2}\frac{C-1}{2} = 18D^4.$$

Il existe donc des entiers S, T tels que $D = ST$, et

1. soit $\frac{C+1}{2} = 2S^4, \quad \frac{C-1}{2} = 9T^4$,
2. soit $\frac{C-1}{2} = 2S^4, \quad \frac{C+1}{2} = 9T^4$,
3. soit $\frac{C+1}{2} = 18S^4, \quad \frac{C-1}{2} = T^4$,
4. soit $\frac{C-1}{2} = 18S^4, \quad \frac{C+1}{2} = T^4$.

Dans les deux premiers cas, on a $2S^4 - 9T^4 = \pm 1$, et dans les deux derniers, on a $18S^4 - T^4 = \pm 1$. En se plaçant modulo 3, on obtient que les équations $2S^4 - 9T^4 = 1$ et $18S^4 - T^4 = 1$ n'ont aucune solution entière.

Lemme 6.7.2 *L'équation* $18S^4 - T^4 = -1$ *a pour seule solution entière* $S = 0, T = \pm 1$.

Preuve En effet, on peut aussi écrire cette équation sous la forme

$$(T^2 + 1)(T^2 - 1) = 18S^4,$$

d'où $2|T^2 \pm 1$. De plus, $2||T^2 + 1$ car sinon on aurait $T^2 \equiv 3 \bmod 4$, ce qui est impossible. Supposons $T \neq \pm 1$. Comme $\left(\frac{T^2+1}{2}, T^2 - 1\right) = 1$ et $\left(\frac{T^2+1}{2}\right)(T^2 - 1) = (3S^2)^2$, il existe donc un entier Z tel que $T^2 - 1 = Z^2$, d'où $T = \pm 1$: contradiction. On en déduit donc que $T = \pm 1$.□ Il nous reste à prouver le lemme suivant :

Lemme 6.7.3 *L'équation* $2S^4 - 9T^4 = -1$ *n'a aucune solution entière* S, T.

Preuve On peut écrire cette équation sous la forme

$$\frac{3T^2+1}{2}\frac{3T^2-1}{2} = 8\left(\frac{S}{2}\right)^4.$$

Comme précédemment, il existe des entiers U, V tels que

$$U^4 - 8V^4 = \pm 1, \quad UV = \frac{S}{2}.$$

En se plaçant modulo 8, on obtient que seul le signe + est possible. On est donc amener à résoudre $U^4 - 8V^4 = 1$:

Lemme 6.7.4 *([58], page 208) L'équation $U^4 - 8V^4 = 1$ a pour seule solution en nombres entiers $U = 1, V = 0$.*

Preuve Soit donc U, V une solution entière. Soit $\theta = 2^{\frac{1}{4}}$, et $K = \mathbb{Q}(\theta)$. Comme $U^4 - 8V^4 = 1$, l'entier algébrique $U + V\theta^3$ est une unité de K. Le groupe des unités de ce corps est de rang 2 sur $\mathbb{Z}$, et admet comme système d'unités fondamentales

$$1 + \theta, \quad 1 + \theta^2.$$

Il existe donc deux entiers x, y tels que

$$(1 + \theta)^x \left(1 + \theta^2\right)^y = U + V\theta^3.$$

Comme $\theta^4 = 2$, en appliquant la formule du binôme à cette identité, on obtient :

$$\sum_{i=0}^{3} \sum_{l+2k \equiv i \bmod 4} 2^{\frac{l+2k-i}{4}} \binom{x}{l} \binom{y}{2k} \theta^i = U + V\theta^3.$$

Le coefficient de θ dans l'expression de gauche est donc nul. On obtient donc

$$x + 2\left(\binom{x}{5} + \binom{x}{3} y + x\binom{y}{2}\right) + 2^2\left(\binom{x}{9} + ...\right) + ... = 0. \tag{6.49}$$

En particulier, l'entier x est pair. Supposons $x \neq 0$. Soit alors ν l'entier défini par $2^\nu || x$. Si $n \geq 1$ entier, on a

$$\binom{x}{2n+1} = \frac{x}{2n+1}\binom{x-1}{2n}. \tag{6.50}$$

L'entier, que l'on notera x', auquel on ajoute x dans l'expression de gauche de (6.49), est donc divisible par au moins $2^{\nu+1}$. Comme $x + x' = 0$ par (6.49), on a donc $2^{\nu+1} | x$, en contradiction avec la définition de ν. On a donc $x = 0$, d'où

$$\left(1 + \theta^2\right)^y = U + V\theta^3.$$

Le coefficient de θ^2 dans l'expression précédente s'annule. On obtient l'équation

$$y + 2\binom{y}{3} + 2^2\binom{y}{5} + \ldots = 0.$$

De la même façon que précédemment, en utilisant (6.50) avec y au lieu de x, on obtient encore $y = 0$. L'entier algébrique $U + V\theta$ vaut donc 1, c'est à dire $U = 1, V = 0$.□ Comme $S = 2UV$, le lemme précédent montre donc que $S = 0$, puis $9T^4 = 1$, ce qui est impossible.□ La proposition est prouvée. ■

Comme l est pair, la proposition précédente montre donc que $l = 0$ ou $l = 2$. Si $l = 0$, les entiers X, Z constituent une solution non triviale de

$$Z^2 + 1 = X^3, \quad Z \neq 0. \tag{6.51}$$

Or, le théorème de Lebesgue montre que cette équation n'a aucune solution entière. On doit donc avoir $l = 2$. Or on suppose $l \neq 2$ si $Y_0 > 2$. Ainsi, dans le cas où l est pair, l'équation (6.5) n'admet aucune solution entière X, Z. Comme dans le cas où l'on s'est placé $h(-B^*) = h(-1) = 1$, le corollaire est vérifié.

Supposons maintenant l impair et $3 \nmid h(-Y_0)$. Si l est premier à 3, alors l'équation (6.47) est sans solution par hypothèse.

Supposons maintenant que $3|l$. Si $\epsilon_0 = 1$, on conclut comme précédemment. Si $\epsilon_0 = -1$, l'équation (6.47) s'écrit

$$Y_0^{3l'} + 1 = 3A^2, \tag{6.52}$$

où on a posé $l' = \frac{l}{3} \in \mathbb{N}^*$. On peut aussi écrire (6.52) sous la forme

$$\left(Y_0^{l'} + 1\right) \frac{Y_0^{3l'} + 1}{Y_0^{l'} + 1} = 3A^2.$$

Il existe donc $B|A$ tel que

$$\frac{Y_0^{3l'} + 1}{Y_0^{l'} + 1} = 3B^2. \tag{6.53}$$

Montrons le lemme général suivant :

Lemme 6.7.5 *Soit $p \geq 2$ un nombre premier. L'équation*

$$1 + T + T^2 = 3B^p$$

a pour seules solutions entières $T = B = 1$, et $T = -2, B = 1$.

Preuve Le cas où $p > 2$ est du à Nagell et est traité au chapitre 1. Etudions le cas $q = 2$. On va se ramener à la résolution d'une équation de type Pell-Fermat. L'équation se met en effet sous la forme

$$(2T + 1)^2 + 3 = 12B^2.$$

En particulier, l'entier $2x + 1$ est divisible par 3. Soit $Z = \left|\frac{2T+1}{3}\right| \in \mathbb{N}$. On a

$$3Z^2 + 1 = 4B^2.$$

L'unité fondamentale de $\mathbb{Q}(\sqrt{3})$ étant $\eta = 2+\sqrt{3}$, il existe donc un entier $n \geq 1$ tel que

$$2B + Z\sqrt{3} = \eta^n.$$

Posons $\eta^n = a_n + b_n\sqrt{3}$, $a_n, b_n \in \mathbb{Z}$. Par récurrence sur n, on vérife que a_n est impair si $n > 1$. On a donc $n = 1$, $Z = 1$, d'où $2T + 1 = \pm 3$. On obtient donc $T = -2$ ou $T = 1$, qui sont bien solutions.□ Comme $Y_0 > 0$, le lemme précédent appliqué avec $p = 2$ et $T = -Y_0^{l'}$, montre donc que $Y_0^{l'} = 2$, incompatible avec (6.52). L'équation (6.5) n'a donc aucune solution dans ce cas si $3 \nmid h(-Y_0)$. L'existence d'une solution de (6.5) montre donc bien encore dans ce cas que $3|h(-Y_0)$.

6.7.3 Cas $q = 2, p = 3, B^* > 1$.

Si $Y_0 \neq 2$ on peut appliquer directement le theoréme (3.1.1) qui montre qu'il n'y a pas de solution entière si $h(-B^*Y_0^r)$ est premier à 3.

Si $Y_0 = 2$ et $l > 0$ pair (respectivement l impair) on applique le corollaire (3.1.9) (respectivement le théorème (3.1.14)).

6.7.4 Cas $q = 2, p = 5, B^* > 1$

Si $Y_0 = 2$, si $2|l$ (respectivement $2 \nmid l$) on applique le corollaire (3.1.9) (respectivement le théorème (3.1.14)).

Si $Y_0 > 2$, si $2|l$ (respectivement $2 \nmid l$) on applique le corollaire (3.1.17) (respectivement le corollaire (3.1.19)).

6.7.5 Cas $q > 2$, $q \neq p$, $p|B$, $Y_0 = 1$.

Supposons que l'on ait une solution X, Z de l'équation (6.5). Comme $X \neq 1$, on peut mettre celle-ci sous la forme

$$\frac{X^p - 1}{X - 1}(X - 1) = p^{v+qw}B'Z'^q,$$

où $B = p^vB'$ $(v > 0)$, $Z = p^wZ'$, avec $(B'Z', p) = 1$. Rappelons (lemme (6.3.7)) que si a, b sont des entiers premiers entre eux, alors

$$\left(\frac{a^p - b^p}{a - b}, a - b\right) = (a - b, p)\,.$$

Autrement dit, p divisera $\frac{a^p-b^p}{a-b}$ si et seulement si p divise $a - b$, et alors $p||\frac{a^p-b^p}{a-b}$. Dans notre cas, on a donc $p^{v+qw-1}|X - 1$, $p||\frac{X^p-1}{X-1}$, et

$$\left(\frac{X^p - 1}{p(X - 1)}, \frac{X - 1}{p^{v+qw-1}}\right) = 1.$$

Comme $(\Psi(B), p) = 1$, en particulier, $(\Psi(B'), p) = 1$. Cette dernière condition est équivalente au fait qu'aucun des facteurs premiers l de B' (si $|B'| > 1$) vérifie $l \equiv 1 \bmod p$. Or, par le lemme (5.3.13), si l est un facteur premier de $\frac{X^p-1}{X-1}$, on a $l \equiv 1 \bmod p$. L'entier B' est donc un diviseur de $X-1$, et on a donc dans $\mathbb{Z}$:

$$\frac{X-1}{p^{v+qw-1}B'}\frac{X^p-1}{p(X-1)} = Z^q, \quad \left(\frac{X^p-1}{p(X-1)}, X-1\right) = 1.$$

Il existe donc des entiers Z_1, Z_2 tels que

$$\frac{X^p-1}{X-1} = pZ_1^q, \quad X-1 = p^{v+qw-1}B'Z_2^q.$$

En particulier, par le théorème principal de [30], q divise h_p^-.

6.7.6 Etude des cas (5c) et (5d).

Comme précédemment, il existe des entiers relatifs Z_1, Z_2 et un entier $e \in \{0; 1\}$ (suivant que p divise $X - Y_0$ ou non) tels que

$$\frac{X^p - Y_0^p}{X - Y_0} = p^e Z_1^q, \quad X - Y_0 = p^{v+qw-e}B'Z_2^q. \tag{6.54}$$

En particulier, $q|X - Y_0$, puisque $q|B'$. Raisonnons par l'absurde et supposons que $q \nmid h_p^-$. On peut alors en déduire dans différents cas qu'en fait $q^2|X - Y_0$.

En effet, sous les hypothèses de la situation (5c) (donc $Y_0 = 1$), le corollaire (6.1.11) montre que $q^2|X - 1$.

Dans la situation (5d), les assertions (2) et (3) du théorème (6.1.1) montrent que l'on a encore $q^2|X - Y_0$.

Plaçons nous dans l'une des deux situations précédentes, qui montrent que $q^2|X - Y_0$. D'après (6.54),

$$q^2|p^{v+qw-e}B'Z_2^q.$$

Par hypothèse, q est un facteur simple de B. On doit donc avoir $q|Z_2$, c'est à dire

$$X \equiv Y_0 \bmod q^{q+1}.$$

Posons $\alpha = \frac{X-Y_0\zeta}{(1-\zeta)^e}$. La factorisation de la première équation de (6.54) dans $\mathbb{Q}(\zeta)$ et le fait que $(X, Y_0, Z) = 1$ montrent qu'il existe un idéal entier $\mathfrak{a}$ de $\mathbb{Z}[\zeta]$, tel que

$$(\alpha) = \mathfrak{a}^q.$$

Comme $q \nmid h_p^-$, il existe un idéal réel $\mathfrak{b}$ de K et $\gamma \in K^\times$, tels que $\mathfrak{a} = (\gamma)\mathfrak{b}$. L'idéal $\mathfrak{b}^q$ est en particulier principal : il existe $\beta \in K^+$ tel que $\mathfrak{b}^q = (\beta)$. On a donc $(\alpha) = (\gamma^q\beta)$. Il existe donc une unité u de K telle que $\alpha = u\beta\gamma^q$. Le quotient $\frac{u}{u^j}$ est une racine $2p$-ième de l'unité. Il existe donc un entier l et $\epsilon = \pm 1$ tels que $\frac{u}{u^j} = \left(\epsilon\zeta^l\right)^q$. On a donc en notant $1/2$ l'inverse de 2 modulo p :

$$\frac{\alpha}{\alpha^j} = \left(\epsilon\frac{\zeta^{l/2}\gamma}{\zeta^{-l/2}\overline{\gamma}}\right)^q = \left(\epsilon\frac{\omega}{\omega^j}\right)^q = \mu^q.$$

Dans la suite, si $\eta \in K$, on notera η^j plutôt $\overline{\eta}$. La suite de la démonstration consiste construire une unité ϕ de $\mathbb{Z}[\zeta]$, à partir de μ et α, qui sera telle que sa norme (sur $\mathbb{Q}$) ne pourra être ± 1, ce qui est impossible. On en déduira donc que $q|h_p^-$. Comme la forme de cette unité dépend de la valeur de $e \in \{0;1\}$, **on commence par supposer que** $e = 0$. On montre d'abord le lemme suivant :

Lemme 6.7.6 *On a $\mu = 1 + \mathcal{O}(\mathfrak{p})$, c'est à dire $\omega \equiv \epsilon\overline{\omega} \bmod \mathfrak{p}$.*

Preuve Supposons d'abord que $Y_0 = 1$. On a $\frac{\alpha}{\overline{\alpha}} = \epsilon\frac{\omega^q}{\overline{\omega}^q}$, c'est à dire $\epsilon\alpha\overline{\omega}^q = \overline{\alpha}\omega^q$. Le nombre premier p étant totalement ramifié dans l'extension $K/\mathbb{Q}$, $\alpha \equiv \overline{\alpha} \bmod \mathfrak{p}$. Comme $(\alpha, \mathfrak{p}) = 1$, on obtient

$$\omega^q \equiv \epsilon\overline{\omega}^q \bmod \mathfrak{p}.$$

Si $\omega \neq \epsilon\overline{\omega} \bmod \mathfrak{p}$, $\left(\frac{\mathbb{Z}[\zeta]}{\mathfrak{p}}\right)^* \simeq \mathbb{F}_p^*$ aurait un élément d'ordre q, d'où $q|p-1$. Donc, par (6.54), il existerait des entiers X, Z_1 et deux nombres premiers impairs distincts p, q tels que

$$\frac{X^p - 1}{X - 1} = Z_1^q, \quad p \equiv 1 \bmod q. \tag{6.55}$$

L'équation (6.55) est sans solution entière. En effet, posons $p = 1 + qk$. Les entiers X^k, Z_1 sont alors aussi solutions de

$$XE^q - (X-1)F^q = 1. \tag{6.56}$$

D'après [4], cette equation admet au plus une solution entière non triviale. Comme $E = F = 1$ convient, on obtient $X^k = 1$, donc $X = -1$ (car $X \neq 1$). Comme $X - 1 = p^{v+qw-e}B'Z_2^q$, on a en particulier $-2 = p^{v+qw-e}B'Z_2^q$. C'est impossible, car $q|B'$ et $q > 2$. Si $Y_0 = -1$, on se ramène à $Y_0 = 1$, en posant $X' = -X$, $Z' = -Z$, et on réitère le raisonnement précédant.

On a donc bien $\omega \equiv \epsilon\overline{\omega} \bmod \mathfrak{p}$. Sous les hypothèses de (5d), si $Y_0 \neq \pm 1$, alors $p \neq 1 \bmod q$. Le groupe $\mathbb{F}_p^\times$ n'a donc aucun élément d'ordre q, et $\mu = 1 + \mathcal{O}(\mathfrak{p})$.□

Considérons le nombre algébrique suivant :

$$\phi = \frac{X - Y_0\overline{\zeta}}{(1-\overline{\zeta})^q Y_0^q}\,(\mu - 1)^q\,. \tag{6.57}$$

On a lemme suivant :

Lemme 6.7.7 *Le nombre algébrique ϕ est une unité de l'anneau $\mathbb{Z}[\zeta]$.*

Preuve Pour montrer le lemme, il suffit de montrer que ϕ est un entier algérique, et qu'il existe un autre entier algébrique ϕ' tel que $\phi\phi' \in \mathbb{Z}[\zeta]^\times$.

Montrons d'abord que $\phi \in \mathbb{Z}[\zeta]$. Mettons l'idéal principal (μ) sous la forme $(\mu) = \mathfrak{a}\mathfrak{b}^{-1}$, où $\mathfrak{a}$ et $\mathfrak{b}$ sont des idéaux entiers de $\mathbb{Z}[\zeta]$. Par définition de μ, on a $\left(\frac{X-Y_0\zeta}{X-Y_0\overline{\zeta}}\right) = \mathfrak{a}^q\mathfrak{b}^{-q}$. Les idéaux $(X-Y_0\zeta)$ et $(X-Y_0\overline{\zeta})$ étant premiers entre eux, on a $(X-Y_0\zeta) = \mathfrak{a}^q$, $(X-Y_0\overline{\zeta}) = \mathfrak{b}^q$. D'autre part, il existe un idéal entier $\mathfrak{c}$ de $\mathbb{Z}[\zeta]$, tel que $(\mu-1) = \mathfrak{c}\mathfrak{b}^{-1}$. On obtient

$$(\phi) = \mathfrak{b}^q\mathfrak{p}^{-q}\mathfrak{c}^q\mathfrak{b}^{-q}(Y_0)^{-q} = \mathfrak{p}^{-q}\mathfrak{c}^q(Y_0)^{-q}.$$

Le lemme (6.7.6) montre que $\nu_\mathfrak{p}(\mathfrak{c}) \geq 1$. Si $Y_0 = 1$, l'idéal (ϕ) est donc bien entier, c'est à dire $\phi \in \mathbb{Z}[\zeta]$. Etudions le cas $Y_0 \neq 1$: nous allons montrer que sous les hypothèses faites dans (5d), l'idéal (ϕ) est encore entier. Dans ce cas, il suffit de montrer que $\nu_\mathcal{L}(\mathfrak{c}) \geq \nu_\mathcal{L}(Y_0)$, pour tout facteur premier $\mathcal{L}$ de Y_0 dans K. Fixons nous un idéal premier $\mathcal{L}$ de K, tel que $\nu_\mathcal{L}(Y_0) = e > 0$, et montrons que $\nu_\mathcal{L}(\mathfrak{c}) \geq e$. En effet, par définition de μ, on a

$$\mu^q = \frac{X - Y_0\zeta}{X - Y_0\overline{\zeta}} \equiv 1 \bmod \mathcal{L}^e.$$

Le groupe $\left(\frac{\mathbb{Z}[\zeta]}{\mathcal{L}^e}\right)^\times$ a pour ordre (voir [13], exercice 4, page 256) $\mathcal{N}(\mathcal{L})^{e-1}(\mathcal{N}(\mathcal{L})-1) = l^{(e-1)f}(l^f-1)$, où f est l'inertie de l dans $\mathbb{Q}(\zeta)/\mathbb{Q}$, inertie qui est aussi l'ordre de l modulo p (voir [77]). Comme $(X, Y_0, Z) = 1$, Y_0 est premier à q : sinon, comme $X = Y_0 + BZ^q$, on aurait $q|X$, puis $q|(X, Y_0, Z)$. Comme $Y_0 \in \mathcal{F}_{p,q}$, $l^f - 1$ est premier à q. Le groupe $\left(\frac{\mathbb{Z}[\zeta]}{\mathcal{L}^e}\right)^\times$ est donc d'ordre premier q. Par conséquent, $\mu \equiv 1 \bmod \mathcal{L}^e$. On a donc bien $\nu_\mathcal{L}(\mathfrak{c}) \geq e$. L'idéal (ϕ) est donc bien entier.

Considérons également

$$\phi' = (X - Y_0\overline{\zeta})^{q-1}\left(\frac{\mu^q - 1}{\mu - 1}\right)^q.$$

En utilisant le fait que $\frac{\mu^q-1}{\mu-1} = 1 + \mu + \ldots + \mu^{q-1}$, on montre comme pour ϕ, que $\phi' \in \mathbb{Z}[\zeta]$. On a

$$\phi\phi' = \frac{(X - Y_0\overline{\zeta})^q}{(1-\overline{\zeta})^q Y_0^q}(\mu^q - 1)^q = -(\zeta+1)^q,$$

qui est une unité de $\mathbb{Z}[\zeta]$. Donc ϕ définit bien une unité de $\mathbb{Z}[\zeta]$.□ L'égalité $\mu^q = \frac{\alpha}{\overline{\alpha}} = \frac{X-Y_0\zeta}{X-Y_0\overline{\zeta}}$ s'écrit aussi

$$\mu^q = -\zeta \left(1 + \frac{X - Y_0}{Y_0(1-\zeta)}\right)\left(1 + \frac{X - Y_0}{Y_0(1-\overline{\zeta})}\right)^{-1}. \tag{6.58}$$

On a montré que $q^{q+1}|X - Y_0$. En particulier, les séries $\left(1 + \frac{X-Y_0}{Y_0(1-\zeta)}\right)^{\frac{1}{q}}$ et $\left(1 + \frac{X-Y_0}{Y_0(1-\overline{\zeta})}\right)^{-\frac{1}{q}}$ sont convergentes dans le corps $\mathbb{Q}_q(\zeta)$. Soit r l'inverse de q modulo p ($q \neq p$). Dans $\mathbb{Q}_q(\zeta)$, l'égalité (6.58) s'écrit aussi

$$\mu = \xi(-\zeta^r)\left(1 + \frac{X - Y_0}{Y_0(1-\zeta)}\right)^{\frac{1}{q}}\left(1 + \frac{X - Y_0}{Y_0(1-\overline{\zeta})}\right)^{-\frac{1}{q}}, \tag{6.59}$$

où $\xi \in \mathbb{Q}_q(\zeta)$ est une racine q-ième de l'unité. On va montrer que $\xi = 1$. On la tour d'extensions suivantes :

$$\mathbb{Q}_q \hookrightarrow \mathbb{Q}_q(\xi) \hookrightarrow \mathbb{Q}_q(\zeta).$$

L'extension $\mathbb{Q}_q(\xi)/\mathbb{Q}_q$ est totalement ramifiée et $\mathbb{Q}_q(\zeta)/\mathbb{Q}_q$ ne l'est pas. L'extension $\mathbb{Q}_q(\xi)$ est donc triviale, c'est à dire $\xi \in \mathbb{Q}_q$. ξ est donc une racine q-ième de l'unité de $\mathbb{Q}_q$. Comme q est impair, rappelons que le groupe des racines de l'unité de $\mathbb{Q}_q$ est exactement celui des racines $(q-1)$-ième de l'unité. En effet :

Lemme 6.7.8 *Soit $q > 2$ un nombre premier. Le groupe des racines de l'unité de $\mathbb{Q}_q$ est celui des racines $q-1$-ième de l'unité.*

Preuve Soit μ le groupe des racines de l'unité de $\mathbb{Q}_q$. Soit ϵ l'homomorphisme de réduction modulo q des éléments de μ :

$$\epsilon : \mu \to \mathbb{F}_q^{\times}.$$

Cette application est surjective par le lemme de Hensel. Montrons son injectivité. Soit donc $\zeta = 1 + qt \in Ker(\epsilon) \quad (t \in \mathbb{Z}_q)$. Soit n l'ordre de ζ. On peut supposer que $n|q$, quitte à élever ζ à une puissance convenable. Par définition de n :

$$(1 + qt)^n = 1,$$

d'où

$$t\left(q + \binom{q}{2}qt + \ldots + q^{n-1}t^{n-1}\right) = 0.$$

Cela montre que $t = 0$ ou $q|n$. Si $t \neq 0$, on a donc $n = q$, et l'équation précédente s'écrit $(q > 2)$:

$$0 = q + \binom{q}{2} qt + \ldots + q^{n-1}t^{n-1} \equiv q \bmod q^2,$$

ce qui est absurde. On a donc $t = 0$ et μ est le groupe des racines $q-1$-ième de l'unité.□
La racine q-ième de l'unité $\xi = 1$ est donc également une racine $(q-1)$-ième de l'unité. On a donc bien $\xi = 1$. Comme $q^{q+1}|X - 1$, il vient

$$\mu = -\zeta^r + \mathcal{O}(q^q). \tag{6.60}$$

En effet, comme $q^{q+1}|X - Y_0$, on a

$$\frac{X - Y_0}{qY_0(1-\zeta)} = \mathcal{O}(q^q), \quad \frac{X - Y_0}{qY_0(1-\overline{\zeta})} = \mathcal{O}(q^q). \tag{6.61}$$

Si $k \geq 2$ est un entier, on a

$$\nu_q\left(\binom{\frac{1}{q}}{k}\left(\frac{X - Y_0}{Y_0(1-\zeta)}\right)^k\right) > k(q+1) - k - \frac{1}{2}k = k(q - \frac{1}{2}) > q. \tag{6.62}$$

(6.61) et (6.62) donnent bien (6.60). Comme $X \equiv Y_0 \bmod q^{q+1}$, (6.60) donne

$$\begin{aligned}
\phi &= \frac{X - Y_0\overline{\zeta}}{Y_0^q(1-\overline{\zeta})^q}\left(-\zeta^r - 1 + \mathcal{O}(q^q)\right)^q \\
&= \frac{Y_0(1-\overline{\zeta})}{Y_0^q(1-\overline{\zeta})^q}\left(-\zeta^r - 1\right)^q + \mathcal{O}(q^{q+1}) \\
&= \frac{1}{Y_0^{q-1}(1-\overline{\zeta})^{q-1}}\left(-\zeta^r - 1\right)^q + \mathcal{O}(q^{q+1}).
\end{aligned}$$

$1 + \zeta^r$ et ϕ étant des unités de K, et la norme de $1 - \zeta$ valant p, on obtient en prenant la norme de la dernière égalité :

$$Y_0^{(q-1)(p-1)}p^{q-1} \equiv \pm 1 \bmod q^{q+1}.$$

En se plaçant modulo q, on voit que seul le signe + est possible :

$$Y_0^{(q-1)(p-1)}p^{q-1} \equiv 1 \bmod q^{q+1}.$$

Cela contredit une des hypothèses de (5d). On a donc bien montré que $q|h_p^-$ si $e = 0$. Il nous reste à étudier le cas $e = 1$. Dans ce cas, on reprend l'unité que l'on avait introduit dans [30], mais adaptée au cas $|Y_0| \geq 1$. On pose (r inverse de $q \bmod p$) :

$$\phi = \frac{\overline{\alpha}}{Y_0^q}\left(\mu + \zeta^{-r}\right)^q, \quad \phi' = \overline{\alpha}^{q-1}\left(\sum_{k=0}^{q-1}\mu^k(-\zeta^{-r})^{q-1-k}\right)^q.$$

L'étude de ce cas est similaire au cas $e = 0$, et on obtient

$$Y_0^{(q-1)(p-1)} \equiv 1 \bmod q^{q+1},$$

qui n'a pas lieu par hypothèse. Le corollaire est donc démontré pour les situations (5c) et (5d).

6.7.7 Etude du cas (5b).

Elle est identique à la précédente, cas $e = 1$, puisque $p|B$.

6.8 Démonstration du corollaire (6.1.16).

Supposons qu'il existe des entiers x, y_0, z premiers entre eux dans leur ensemble tels que

$$\frac{x^p + y_0^p}{x + y_0} = p^e z^q.$$

Sous les hypothèses de la première assertion, on a alors $q|h_p^-$ par le théorème 4 de [54].

Plaçons nous sous les hypothèses de la seconde assertion, c'est à dire $y_0 \neq \pm 1$, et $e = 0$. Raisonnons par l'absurde et supposons que $q \nmid h_p^-$. Comme $q < Sup\left(p, \frac{p(p-20)}{16}\right)$, la seconde assertion du théorème (6.1.1), montre qu'il existe $f \in \{-1, 0, 1\}$ tel que $q^2|x + fy_0$. Supposons dans un premier temps, que $f = 1$. Comme lors de la preuve du corollaire (6.1.11), il existe $\mu \in \mathbb{Q}(\zeta)^\times$, tel que

$$\frac{\alpha^j}{\alpha} = \mu^q,$$

où $\alpha = x + y_0\zeta$. On introduit alors l'unité $\phi = \frac{x+y_0\zeta}{(1-\zeta)^q y_0^q}(\mu - 1)^q$. Comme $q^2|x + y_0$, en particulier

$$\mu^q = -\overline{\zeta} + \mathcal{O}(q),$$

d'où

$$\mu = -\overline{\zeta}^r + \mathcal{O}(q),$$

r étant l'inverse de q mod p. On a alors

$$\begin{aligned}\phi &= \frac{x + y_0\zeta}{(1-\zeta)^q y_0^q}(\mu - 1)^q = \frac{y_0(\zeta - 1)}{y_0^q(1-\zeta)^q}(-\zeta^r - 1 + \mathcal{O}(q))^q + \mathcal{O}(q^2) \\ &= \frac{1}{(1-\zeta)^{q-1} y_0^{q-1}}(\zeta^r + 1)^q + \mathcal{O}(q^2).\end{aligned}$$

En prenant la norme, on obtient :

$$\left(py_0^{(p-1)}\right)^{q-1} \equiv \pm 1 \bmod q^2.$$

En se plaçant modulo q, on obtient que seul le signe + est possible, soit

$$\left(py_0^{(p-1)}\right)^{q-1} \equiv 1 \bmod q^2,$$

en contradiction avec les hypothèses. On a donc bien $q|h_p^-$. Les autres cas se traitent de façon analogue. ■

6.9 démonstration de la proposition (6.1.17).

Par le théorème 1 de [37], on a

$$\frac{q^n-1}{q-1} = p^a.$$

Lemme 6.9.1 *(lemme 1 de [31]).*

1. *S'il existe un entier $x > 1$ tel que $\frac{x^n-1}{x-1} = p^a$, alors n est premier, $n \neq p$ et $p \neq 2$.*
2. *Si $x = r^m$ puisance entière d'un nombre premier et $\frac{x^n-1}{x-1} = p^a$, alors $m = n^e$ et $p \equiv 1 \bmod n^{e+1}$.*

Preuve

– preuve de la première assertion :
Supposons n non premier. Il existe donc des entiers $\alpha > 1$ et $\beta > 1$ tels que $n = \alpha\beta$. Alors

$$p^a = \frac{x^n-1}{x^\alpha-1}\frac{x^\alpha-1}{x-1},$$

d'où $x^\alpha - 1 \equiv 0 \bmod p$, d'où $\frac{x^n-1}{x^\alpha-1} \equiv \beta \bmod p$. On en déduit que p divise β. Comme ceci est vrai pour tout diviseur $\beta > 1$ de n, l'entier n est donc une puissance de p. Supposons d'abord que $p = 2$. Si n est une puissance de 2, comme $n > 2$, il existe un entier b tel que

$$(x+1)(x^2+1) = \frac{x^4-1}{x-1} = 2^b.$$

Comme $x^2 + 1 \neq 0 \bmod 4$, alors $x^2 + 1 = 2$ et $x + 1 = 2^{b-1}$ donc $x = 1$, ce qui n'est pas. Supposons $p > 2$. Si n est une puissance de p, il existe un entier b tel que

$$\frac{x^p-1}{x-1} = p^b.$$

Nécessairement $b = 1$ (donc $p \equiv 1 \bmod x$) et $p|x-1$, d'où $x = -(p-1) < 0$, ce qui n'est pas.

L'entier n est donc premier, $n \neq p$.

– preuve de la seconde assertion :

Il suffit de montrer que si m est premier, alors $m = n$. Supposons le contraire. Alors

$$p^a = \frac{r^{mn}-1}{r^m-1} = \Phi_{mn}(r)\Phi_n(r). \tag{6.63}$$

Si $m \neq p$, comme $n \neq p$ par la première assertion, on en déduit que le polynôme $X^{mn}-1$ n'a que des racines simples modulo p. Or, de (6.63), comme $\Phi_n(r) > 1$, on déduit que $p|\Phi_n(r)$, donc $r^n \equiv 1 \bmod p$ et le polynôme $X^{mn}-1$ aurait des racines multiples modulo p. Ainsi, on a $m = p$. Si $r \equiv 1 \bmod p$, en particulier $x \equiv 1 \bmod p$ et alors $\frac{x^n-1}{x-1} \equiv n \bmod p$. Comme $\frac{x^n-1}{x-1}$ est une puissance de p, alors $n = p$, en contradiction avec la première assertion du lemme. On doit donc avoir $r \neq 1 \bmod p$, soit $r^p - 1 \neq 0 \bmod p$. Par (6.63), on a donc

$$r^{np} \equiv 1 \bmod p^a \Rightarrow r^n \equiv 1 \bmod p^{a-1}.$$

On a alors $(m = p)$:

$$p^a = \frac{r^{mn}-1}{r^m-1} = \sum_{k=1}^{p} \binom{p}{k} (r^p-1)^{k-1} \equiv p \bmod p^{a-1},$$

ie $p^{a-1}|p^a - p$, ie $a \leq 2$. Par (6.63), comme $m = p$, on doit avoir $\Phi_{np}(r) = p^i$, $i = 0, 1$ ou 2. Comme $\Phi_n(r) > 1$, en fait $i = 0$ ou $i = 1$. Supposons d'abord que $i = 0$. Alors par (6.63)

$$(r^{np}-1)(r-1) = (r^p-1)(r^n-1).$$

Modulo r^2, cela donne $r \equiv 0 \bmod r^2$: absurde. Si $i = 1$, alors $\Phi_{np}(r) = p = \Phi_n(r)$, ce qui donne

$$\Phi_n(r)^2\Phi_p(r) = \frac{r^{np}-1}{r-1},$$

ie

$$(r^{np}-1)(r-1)^2 = (r^p-1)(r^n-1)^2.$$

En développant le terme de gauche, on voit que si on lui soustrait 1, le terme obtenu est de valuation r-adique au moins 2, tandis celui de droite auquel on soustrait 1 est

de valuation r-adique 1 : absurde ; l'entier m, s'il est premier, est donc égal à n. Dans le cas général, c'est donc une puissance entière de n : $m = n^e$.
Montrons que $p \equiv 1 \bmod n^{e+1}$. Comme $q = r^{n^e}$, alors

$$r^{n^{e+1}} - 1 = q^n - 1 \equiv 0 \bmod p.$$

Si $q \equiv 1 \bmod p$, alors $p^a = \frac{q^n-1}{q-1} \equiv n \bmod p$, donc $n = p$, ce qui n'est pas, par la première assertion du lemme. Le premier r est donc d'ordre n^{e+1} modulo p, soit $p \equiv 1 \bmod n^{e+1}$ par le théorème de Lagrange.

□

En particulier, le lemme montre que n est premier. Si l'entier a est premier à n, alors la proposition (6.1.17) découle du corollaire (6.1.16). Il nous reste à montrer que $(a, n) = 1$. Supposons que cela ne soit pas le cas. Comme n est premier, il existe un entier $m > 1$ tel que $a = nm$. Soit $f = p^m$. Alors

$$f^n = \frac{q^n - 1}{q - 1} \equiv 1 \bmod q.$$

On a $f \neq 1 \bmod q$, car sinon $f^n > q^n > \frac{q^n-1}{q-1}$. Comme n est premier, f est donc d'ordre n modulo q. L'entier q est par hypothèse, une puissance d'un nombre premier : $q = r^b$. Par le théorème de Lagrange, $n | r^{b-1}(r-1)$. Si $r \equiv 1 \bmod n$, alors

$$\frac{q^n - 1}{q - 1} \equiv 0 \bmod n.$$

C'est impossible, car alors n divise une puissance d'un nombre premier et donc $n^2 | \frac{q^n-1}{q-1}$ ce qui est impossible.

On a donc $r = n$. Ainsi, $f^n \equiv 1 \bmod n^b$, donc $f \equiv 1 \bmod n^{b-1}$. Il existe donc un entier t tel que $f - 1 = q\frac{t}{n}$. Alors

$$\left(q\frac{t}{n} + 1\right)^n = \frac{q^n - 1}{q - 1} \Rightarrow (q-1)\left(q\frac{t}{n}\right)^n < q^n \Rightarrow q - 1 < \left(\frac{n}{t}\right)^n.$$

Par le lemme précédent, l'entier m est une puissance de n : $m = n^\lambda$. Si $\lambda = 0$, alors $q = n$ et $f \equiv f^n \equiv 1 \bmod n$, donc $f > n = q$, et on conclut comme précédemment. On a donc $\lambda \geq 1$ et $q \geq n^n$. Alors

$$n^n \leq q < 1 + \left(\frac{n}{t}\right)^n.$$

On a donc $t = \lambda = 1$ et $f - 1 = n^{n-1}$. Comme n est impair, f est pair, donc $p = 2$, en contradiction avec le lemme.

6.10 Sur le système (6.6).

6.10.1 Démonstration du théorème (6.1.18).

Fixons nous une solution en entiers X, A, Z de (6.6), telle que $Z > 0$, $Z \in \mathcal{S}$. Par la première équation du système (6.6), on a

$$(X - Y_0)\frac{X^p - Y_0^p}{X - Y_0} = B_1 Z^q = p^{qw} B_1 Z'^q,$$

où w est la valuation p-adique de Z. Par le lemme (6.3.7), il existe donc $e \in \{0; 1\}$ et des entiers Z'_1, Z'_2, divisant Z' tels que

$$\begin{cases} \frac{X^p - Y_0^p}{X - Y_0} = p^e Z'^q_1, \\ X - Y_0 = p^{qw-e} B_1 Z'^q_2, \\ Z' = Z'_1 Z'_2. \end{cases} \tag{6.64}$$

Si $Y_0 = \pm 1$ et $p \equiv 1 \bmod 4$, par hypothèse $q < Sup\left(p, \frac{p(p-20)}{16}\right)$. Par (6.64), l'équation $\frac{X^p - Y_0^p}{X - Y_0} = p^e Z'^q_1$ admettant une solution non triviale (car $X \neq \pm 1$), le théorème 4 de [54] montre alors que le nombre premier q divise au moins l'un des trois entiers suivants :

$$h_p^-, \quad \frac{p^{q-1} - 1}{q}, \quad \mathbf{Tr}\left(\frac{1 - \zeta^{1-q}}{(1 + \zeta^{-q})(1 - \zeta)}\right).$$

Si $Y_0 \neq \pm 1$ et $p \equiv 1 \bmod 4$, l'équation $\frac{X^p - Y_0^p}{X - Y_0} = p^e Z'^q_1$ admettant une solution le corollaire (6.1.16) montre que le nombre premier q divise au moins l'un des quatres entiers suivants :

$$h_p^-, \quad \frac{Y_0^{(q-1)(p-1)} - 1}{q}, \quad \frac{\left(pY_0^{p-1}\right)^{q-1} - 1}{q}, \quad \frac{Y_0^{(q-1)(p-1)} - p^{q-1}}{q}.$$

Supposons dorénavant que $p \equiv 3 \bmod 4$.

Comme $Z \neq 0$, et $Z \in \mathcal{S}$, le lemme (5.3.13), montre que Z'_1 vaut ± 1 ou est une puissance d'un nombre premier. Les entiers X et Y_0 sont premiers entre eux. En effet, sinon il existe un nombre premier l tel que $l|(X, Y_0)$. Le nombre premier l divise donc $\frac{X^p - Y_0^p}{X - Y_0} = p^e Z'^q_1$, donc $l|Z'_1$. Comme Z'_1 est un diviseur de Z, on a alors $l|Z$, en contradiction avec $(X, Y_0, Z) = 1$. On a donc bien $(X, Y_0) = 1$.

Comme $Z \in \mathcal{S}$, $Z = 0$ ou possède au plus un facteur premier valant $1 \bmod p$; or on a supposé $Z \neq 0$, et si Z n'a aucun facteur premier valant $1 \bmod p$, le lemme (5.3.13) montre que $Z'_1 = \pm 1$ vu que $Z'_1|Z$. Comme $Z > 0$, $X^p > Y_0^p$, d'où $Z'_1 > 0$, soit $Z'_1 = 1$. En particulier $\frac{X^p - Y_0^p}{X - Y_0} \in \{1, p\}$. Comme $X \neq \pm 1$ et $(X, Y_0) = 1$, on a $X > Y_0 > 0$, ou bien $X > -Y_0 > 0$ ou bien $-Y_0 > X > 0$.

Si $X > Y_0 > 0$ le lemme (6.2.8) montre que l'on ne peut avoir $\frac{X^p - Y_0^p}{X - Y_0} \in \{1, p\}$.

Si $X > -Y_0 > 0$, comme $\frac{(-Y_0)^p + X^p}{-Y_0 + X} \in \{1, p\}$, le lemme (6.2.8) montre que $p = 3$, $X = 2$, $Y_0 = -1$, donc qu'il existe $\epsilon = \pm 1$ tel que $Z = \epsilon$, $B_1 = 9\epsilon$, en contradiction avec le fait que $(B_1, p) = 1$.

Si $-Y_0 > X > 0$, comme $\frac{X^p + (-Y_0)^p}{X + (-Y_0)} \in \{1, p\}$, le lemme (6.2.8) montre que $X = 1$, en contradiction avec l'hypothèse $X \neq \pm 1$.

On vient donc de montrer que $Z_1' \neq 1$. Comme $Z \in \mathcal{S}$, Z_1' est une puissance entière de l, l'unique facteur premier de Z valant 1 mod p : $Z_1' = l^v$. Par définition de Z_2', on a alors $Z_2' = \frac{Z'}{l^v}$, où $v = \nu_l(Z)$.

Ceci est également valable pour la deuxième équation du système. L'entier l etant unique, les facteurs premiers de $\frac{A^p+1}{A+1}$ valant 1 mod p ($A \neq -1$ car $Z \neq 0$), on a $\frac{A^p+1}{A+1} = \pm p^e l^v$. Comme $\frac{A^p+1}{A+1} > 0$, on a en fait $\frac{A^p+1}{A+1} = p^e l^v$. On doit donc avoir $A + 1 = p^{qw-e} B_2 Z_2'^q$.

On a donc montré qu'il existe un entier Z_2' divisant Z tel que

$$\begin{cases} X = Y_0 + p^{v_1 + qw - e} B_1' Z_2'^q, \\ A = -1 + p^{v_2 + qw - e} B_2' Z_2'^q. \end{cases}$$

On obtient

$$\begin{aligned} X + AY_0 &= Y_0 + p^{qw-e} B_1 Z_2'^q - Y_0 + Y_0 p^{qw-e} B_2 Z_2'^q \\ &= p^{qw-e} Z_2'^q \, (B_1 + Y_0 B_2) \equiv 0 \bmod q, \end{aligned}$$

car $q | B_1 + Y_0 B_2$ par hypothèse.

Il existe un idéal $\mathfrak{a}$ de l'anneau $\mathbb{Z}[\zeta]$ tel que

$$\left(\frac{X - Y_0 \zeta}{(1 - \zeta)^e} \right) = \mathfrak{a}^q.$$

Comme pour le début de la preuve du théorème (6.1.1), on obtient :

$$\left(\frac{X - Y_0 \zeta}{(1 - \zeta)^e} \right)^\theta = \gamma^q,$$

c'est à dire

$$(X + AY_0 + Y_0(-A - \zeta))^\theta = (1 - \zeta)^{e\theta} \gamma^q,$$

c'est à dire

$$\left(1 + \frac{X + AY_0}{Y_0(-A - \zeta)} \right)^\theta = \frac{(1 - \zeta)^{e\theta} \gamma^q}{Y_0^{W(\theta)} (-A - \zeta)^\theta}.$$

Désignant par $\mathfrak{q}$ un facteur premier quelconque de $\mathbb{Z}[\zeta]$ au-dessus de q, on obtient :

$$\frac{X+AY_0}{Y_0}\sum_{k=0}^{\frac{p-3}{2}}(b_k-a_k)\left(\frac{1}{-A-\zeta^{\sigma^k}}-\frac{1}{-A-\zeta^{-\sigma^k}}\right)=$$
$$\frac{(1-\zeta)^{e\theta}}{Y_0^{W(\theta)}(-A-\zeta)^{\theta}}\left(\gamma^q-\frac{(1-\overline{\zeta})^{e\theta}}{(1-\zeta)^{e\theta}}\frac{(-A-\zeta)^{\theta}}{(-A-\overline{\zeta})^{\theta}}\overline{\gamma}^q\right)+\mathcal{O}(\mathfrak{q}^2).$$

Comme $\frac{A^p+1}{A+1}=p^eZ_1'^q$, l'idéal de $\mathbb{Z}[\zeta]$ $(-A-\zeta)(1-\zeta)^{-e}$ est une puissance q-ième. Le nombre algébrique $\left(\frac{-A-\zeta}{-A-\overline{\zeta}}\right)^{\theta}$ est donc une puissance q-ième dans $\mathbb{Q}(\zeta)^{\times}$, ainsi que le quotient $\frac{(1-\overline{\zeta})^{e\theta}}{(1-\zeta)^{e\theta}}=(-\overline{\zeta})^{e\theta}$ et il existe donc $\gamma_1\in\mathbb{Q}(\zeta)$ tel que

$$\frac{(1-\overline{\zeta})^{e\theta}}{(1-\zeta)^{e\theta}}\left(\frac{-A-\zeta}{-A-\overline{\zeta}}\right)^{\theta}\overline{\gamma}^q=\gamma_1^q.$$

Le développement précédent s'écrit donc

$$\frac{X+AY_0}{Y_0}\sum_{k=0}^{\frac{p-3}{2}}(b_k-a_k)\left(\frac{1}{-A-\zeta^{\sigma^k}}-\frac{1}{-A-\zeta^{-\sigma^k}}\right)=\frac{(1-\zeta)^{e\theta}}{Y_0^{W(\theta)}(-A-\zeta)^{\theta}}(\gamma^q-\gamma_1^q)+\mathcal{O}(\mathfrak{q}^2).$$

Comme $q\neq 1 \bmod p$, l'entier algébrique $-A-\zeta$ est premier à q. On peut alors reprendre la démonstration du théorème (6.1.1), le determinant circulant apparaissant étant alors $\mathcal{E}(p,1,-A)$. En particulier, soit q divise le numérateur de $E(p,1,-A)$, soit $X+AY_0$ est divisible par q^2. Dans le premier cas, il existe un entier $c\in\{1,\ldots,q-1\}$, tel que q divise le numérateur de $E(p,1,c)$. En effet, on a le lemme suivant :

Lemme 6.10.1 *Soit p un nombre premier, x_1,x_2 deux entiers, et soit q un nombre premier tel que $q\neq 1 \bmod p$. Si $x_1\equiv x_2 \bmod q$, alors $E(p,1,x_1)\equiv E(p,1,x_2)$.*

Preuve Comme $x_1\equiv x_2 \bmod q$, dans $\mathbb{Z}[\zeta]$, on a $x_1+\zeta\equiv x_2+\zeta \bmod q$. Comme $q\neq 1 \bmod p$, les entiers algébriques sont premiers à q, d'où $\frac{1}{x_1+\zeta}\equiv\frac{1}{x_2+\zeta} \bmod q$, et ce pour toute racine primitive p-ième de l'unité. On a donc $\mathcal{E}(p,1,x_1)\equiv\mathcal{E}(p,1,x_2)$.□ Le lemme précédent montre donc que $q|E(p,1,c)$ avec $c\equiv -A \bmod q$, $c\in\{0,\ldots,q-1\}$. Si la valeur $c=0$ était possible, l'entier $E(p,1,0)$ serait divisible par q. Or par la proposition (6.1.3), $E(p,1,0)=p^{\frac{p-3}{4}}\sqrt{-p}$, donc premier à q. On doit donc avoir $1\leq c\leq q-1$. Si $c=1$, la proposition (6.1.3) montre que $q|h_p^-$. Si $c=q-1$ le lemme précédent montre que $E(p,1,-1)\equiv 0 \bmod q$. La proposition (6.1.3) montre alors que $q|h_p^-\left(2^{\frac{m}{2^{\frac{1-\epsilon}{2}}}}-\epsilon\right)$. Le nombre premier q divise donc h_p^-, ou bien $2^{\frac{m}{2^{\frac{1-\epsilon}{2}}}}-\epsilon$, ou bien le numérateur de l'un des $E(p,1,c)$, $2\leq c\leq q-2$.

Si aucun des numérateurs des rationnels $E(p,1,c)$, $c \in \{1,\ldots,q-1\}$ n'est divisible par q, on a $q^2|X+AY_0 = p^{qw-e}Z_2'^q\,(B_1+Y_0B_2)$. Par hypothèse, $q||B_1+Y_0B_2$. L'entier Z_2' est donc divisible par q, d'où $X-Y_0 \equiv 0 \bmod q^q$ (en effet, on a vu que $X-Y_0 = p^{qw-e}B_1Z_2'^q$).

Si $Y_0 = \pm 1$, comme $X \neq 1$, la démonstration du théorème 4 de [54] montre qu'alors $q^q|p^{q-1}-1$. Si $Y_0 \neq \pm 1$, comme pour la démonstration du corollaire (6.1.11), en introduisant l'unité $\phi = \frac{X-Y_0\zeta}{(1-\zeta)^qY_0^q}\,(\mu-1)^q$ si $e=0$, et $\phi = \frac{X-Y_0\zeta}{(1-\zeta)Y_0^q}\,(\mu+\zeta^u)^q$ (avec $uq \equiv 1 \bmod p$), si $e=1$, on obtient que q^q divise au moins l'un des trois entiers suivants :

$$y^{(q-1)(p-1)}-1, \quad (py^{p-1})^{q-1}-1, \quad y^{q-1}-p^{q-1}.$$

Le théorème (6.1.18) est prouvé. ■

6.10.2 Démonstration du corollaire (6.1.20).

Supposons que le système (6.7) ait une solution entière X, Z, A, $Z \neq 0$. Le théorème (6.1.18) montre alors que l'on a cinq cas possibles : cas (1)à (5). Comme $p = 1+2q$, la proposition (2.2.6) montre que le nombre de classes relatif h_p^- est premier à h_p^-. Donc les conditions (1) et (2) se simplifient en les conditions (1) et (2) du corollaire.

De plus, comme $p = 1+2q$, la proposition (6.1.10) montre que si le numérateur de l'un des rationnels $E(p,1,c)$, $1 < c < p-1$ est divisible par q, alors l'un au moins des entiers Q_c (définis en (6.1.8)) est divisible par q. Donc la condition (3) se simplifie en les conditions (3) et (4) du corollaire. Les deux dernières conditions du corollaire et du théorème sont les mêmes.

6.11 Sur l'équation $x^p + y^p = z^q$

On se fixe deux nombres premiers impairs distincts p, q, ainsi que ζ (respectivement ξ) une racine primitive p-ième (respectivement q-ième de l'unité). On utilise la notation suivante : si x, y sont des éléments du corps $\mathbb{Q}(\zeta,\xi)$ où ξ est une racine primitive q-ième de l'unité, alors on pose $x =_q y$ s'il existe γ, un nombre q-primaire de $\mathbb{Q}(\zeta,\xi)$, tel que $x = \gamma y$.

6.11.1 Quelques lemmes.

Lemme 6.11.1 *Soit ϵ une unité de $\mathbb{Z}[\zeta,\xi]$ telle que $\epsilon =_q 1$. Si $q \nmid h_{pq}^-$, alors cette unité est une puissance q-ième dans $\mathbb{Z}[\zeta,\xi]$.*

Preuve En effet, sinon, l'extension $\mathbb{Q}(\zeta,\xi,\epsilon^{1/q})/\mathbb{Q}(\zeta,\xi)$ serait de degrés q. Comme ϵ est une unité et $\epsilon =_q 1$, ϵ est un nombre q-primaire singulier. L'extension $\mathbb{Q}(\zeta,\xi,\epsilon^{1/q})/\mathbb{Q}(\zeta,\xi)$

est donc abélienne non ramifiée. Etant de degrés q, la théorie du corps de classe montre que $q|h_{pq}$ et donc h_{pq}^- : contradiction.$\square$

Lemme 6.11.2 *Supposons $q \nmid h_{pq}^-$ et $p \neq 1 \bmod q$. Soit ϵ une unité de $\mathbb{Z}[\zeta, \xi]$ telle que $\epsilon =_q a$ où $a \in \mathbb{Z}$. Alors ϵ est une puissance q-ième dans $\mathbb{Z}[\zeta, \xi]$.*

Preuve Soit $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta, \xi)/\mathbb{Q})$ et $\delta_\sigma = \epsilon^{1-\sigma}$. Comme $\epsilon =_q a$, a entier, on a $\delta_\sigma =_q 1$. Par le lemme (6.11.1), δ_σ est donc une puissance q-ième dans $\mathbb{Z}[\zeta, \xi]$. En particulier c'est vrai pour $\prod_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta,\xi)/\mathbb{Q})} \delta_\sigma$. Or ce produit est égal à $\pm\epsilon^{(p-1)(q-1)}$. Comme $(p-1)(q-1)$ est premier à q, ϵ est donc une puissance q-ième dans $\mathbb{Z}[\zeta, \xi]$.$\square$

Enfin, on montre le

Lemme 6.11.3 *Soit ϵ une unité de l'anneau $\mathbb{Z}[\zeta]$ telle que $\epsilon =_q c(1-\zeta)$, $c \in \mathbb{Q}$. Si $p \neq 1 \bmod q$ et m est l'inverse de $p-1$ modulo q, alors*

$$\epsilon =_q \frac{1-\zeta}{p^m} =_q \left(\frac{(1-\zeta)^{p-1}}{p}\right)^m = \gamma \in \mathbb{Z}[\zeta]^\times.$$

Preuve Soit $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ un générateur. On pose également

$$\Omega = \sum_{i=0}^{p-3} (p-2-i)\sigma^i \in \mathbb{Z}[G],$$

de sorte que $(\sigma - 1)\Omega + p - 1 = \mathcal{N}$. Par hypothèse

$$\epsilon^{\sigma-1} =_q (1-\zeta)^{\sigma-1}.$$

Soit $\eta = (1-\zeta)^{\sigma-1}$. ϵ étant une unité

$$\pm 1 = \mathcal{N}(\epsilon) = \epsilon^{p-1+\Omega(\sigma-1)} =_q \epsilon^{p-1}\eta^\Omega,$$

ie

$$\epsilon^{p-1} =_q \eta^{-\Omega},$$

autrement dit

$$\epsilon =_q \eta^{-m\Omega}.$$

Mais

$$\eta^\Omega = (1-\zeta)^{(\sigma-1)\Omega} = (1-\zeta)^{\mathcal{N}-p+1} = \frac{p}{(1-\zeta)^{p-1}}.$$

$\square$

6.11.2 Factorisation d'un nombre algébrique.

Dans ce paragraphe, on se fixe trois nombres entiers x, y, z tels que

$$x^p + y^p = z^q, \quad (x, y, z) = (y, q) = 1. \tag{6.65}$$

On suppose également que h_{pq}^- est premier à q (donc h_{pq} est premier à q), que $q \neq 1 \bmod p$ et que $q < Sup\left(p, \frac{p(p-20)}{16}\right)$. En particulier, $q^2 | x + fy$, $f \in \{-1, 0, 1\}$. On note comme d'habitude par $e \in \{0; 1\}$ l'entier qui vaut 1 ssi $p | x + y$. De l'équation (6.65), comme $q \nmid h_{pq}$, il existe une unité ϵ de l'anneau $\mathbb{Z}[\zeta]$ et ρ, nombre algébrique de ce même anneau, tel que

$$\frac{x + \zeta y}{(1-\zeta)^e} = \epsilon \rho^q.$$

Dans la suite, on pose $\alpha = \frac{x+\zeta y}{(1-\zeta)^e}$.

- Supposons d'abord que $e = 0$ et $f = -1$. Comme $f = -1$, $x \equiv y \bmod q^2$, ie

  $$\epsilon \rho^q \equiv x(1 + \zeta) \bmod q^2.$$

  Soit l'unité $\delta = \frac{\epsilon}{1+\zeta}$. Par qui précède

  $$\delta =_q x.$$

  Le lemme (6.11.2) montre que δ est une puissance q-ième dans $\mathbb{Z}[\zeta, \xi]$. Il existe donc $\rho_1 \in \mathbb{Z}[\zeta, \xi]$ tel que $\delta = \rho_1^q$. Soit $\mathcal{N}_q$ la norme relative à l'extension $\mathbb{Q}(\zeta, \xi)/\mathbb{Q}(\zeta)$. Alors

  $$\left(\frac{\epsilon}{1+\zeta}\right)^{q-1} = \left(\frac{\epsilon}{1+\zeta}\right)^{\mathcal{N}_q} = \left(\rho_1^{\mathcal{N}_q}\right)^q \in \mathbb{Z}[\zeta]^q.$$

  L'unité $\frac{\epsilon}{1+\zeta}$ est donc une puissance q-ième dans $\mathbb{Z}[\zeta]$ (dans la suite, on omettra ce type de détails et on se contentera de dire que c'est une puissance q-ième dans $\mathbb{Z}[\zeta]$). Quitte à modifier ρ, on a donc $\alpha = (1 + \zeta)\rho^q$.
- Supposons que $e = 0$ et $f = 0$. Dans ce cas, $\epsilon =_q y$. Le lemme (6.11.2) montre que ϵ est une puissance q-ième dans $\mathbb{Z}[\zeta]$. Quitte à modifier ρ, on a $\alpha = \rho^q$.
- Supposons que $e = 0$ et $f = 1$. Dans ce cas, $\alpha =_q y(\zeta - 1)$. Le lemme (6.11.3) montre que $\epsilon =_q \gamma$. Comme $q \nmid h_{pq}^-$, le lemme (6.11.1) montre que l'unité $\frac{\epsilon}{\gamma}$ est une puissance q-ième dans $\mathbb{Z}[\zeta]$. Quitte à modifier ρ, on a $\alpha = \gamma \rho^q$.
- Supposons que $e = 1$ et $f = -1$. Alors

  $$\alpha = \frac{x + \zeta y}{1 - \zeta} \equiv \frac{x(1 + \zeta)}{1 - \zeta} \bmod q^2,$$

ie $\epsilon =_q \frac{x(1+\zeta)}{1-\zeta}$. L'unité $\frac{1+\zeta}{\epsilon}$ vérifie donc

$$\frac{1+\zeta}{\epsilon} =_q \frac{1}{x}(1-\zeta).$$

Le lemme (6.11.3) montre que $\frac{1+\zeta}{\epsilon} =_q \gamma$. Le lemme (6.11.2) montre alors que l'unité $\frac{1+\zeta}{\epsilon\gamma}$ est une puissance q-ième de $\mathbb{Z}[\zeta]$. Quitte à modifier ρ, on a donc

$$\alpha = \frac{1+\zeta}{\gamma}\rho^q.$$

– Supposons que $e = 1$ et $f = 0$. Alors

$$\alpha = \frac{x+\zeta y}{1-\zeta} \equiv \frac{\zeta y}{1-\zeta} \bmod q^2.$$

On a donc $\epsilon =_q \alpha =_q \frac{\zeta y}{1-\zeta} =_q \frac{y}{1-\zeta}$. Le lemme (6.11.3) montre que $\epsilon\gamma$ est une puissance q-ième dans $\mathbb{Z}[\zeta]$. Quitte à modifier ρ, on a donc

$$\alpha = \frac{1}{\gamma}\rho^q.$$

– Supposons que $e = 1$ et $f = 1$. Alors

$$\alpha = \frac{x+\zeta y}{1-\zeta} \equiv x \bmod q^2,$$

ie $\epsilon =_q x$. Le lemme (6.11.2) montre que ϵ est une puissance q-ième dans $\mathbb{Z}[\zeta]$. Quitte à modifier ρ, on a donc

$$\alpha = \rho^q.$$

On a donc la proposition suivante :

Proposition 6.11.4 *Supposons que* $p \neq 1 \bmod q$, $q \nmid h_{pq}^-$, *et* $q < Sup\left(p, \frac{p(p-20)}{16}\right)$. *Soit* (x, y, z) *une solution de (6.65). Soient* $0 < m < q$ *l'inverse de* $p - 1 \bmod q$ *et* $\gamma = \left(\frac{(1-\zeta)^{p-1}}{p}\right)^m \in \mathbb{Z}[\zeta]^\times$. *On a alors*

$$\alpha = \frac{x+\zeta y}{(1-\zeta)^e} = (1+\zeta)^{\delta_{f,-1}} \cdot \gamma^{\delta_{f,1}-e} \cdot \rho^q, \quad \rho \in \mathbb{Z}[\zeta].$$

6.11.3 Une minoration.

Lemme 6.11.5 *Soit $\rho \in \mathbb{Z}[\zeta]$ tel que dans $\mathbb{Z}_q[\zeta]$ on ait*

$$\rho = a \cdot \sum_{m=0}^{\infty} \binom{1/q}{m} (\mu b)^m, \quad \mu \in \left\{\zeta, \frac{1}{1 \pm \zeta}\right\}, \quad a \in \mathbb{Z}_q - \{0\}, \quad b \in \mathbb{Q}^\times,$$

le rationnel b vérifiant $\nu_q(b) = k \geq 2$. Supposons qu'il existe un réel M tel que $|\sigma(\rho)| \leq M$ pour tout $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, et que

$$\forall \sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}), \quad \rho^\sigma = a \cdot \sum_{m=0}^{\infty} \binom{1/q}{m} (\mu^\sigma b)^m, \quad \mu \in \left\{\zeta, \frac{1}{1 \pm \zeta}\right\}$$

On a alors

$$M \geq \frac{1}{p-1} \cdot \frac{q^{1+(p-2)\left(k - \frac{q}{q-1}\right)}}{2^{p-2}}.$$

Preuve On pose

$$\nu = (\zeta^2 - \zeta) \cdot \begin{cases} 1 & \text{si } \mu = \zeta, \\ \mu^{-(p-3)} & \text{sinon.} \end{cases}$$

Soit $\mathbf{Tr}$ la trace relative à $\mathbb{Q}(\zeta)/\mathbb{Q}$. Soit $i \in \{0, 1, \ldots, p-3\}$. Si $\mu = \zeta$, comme $0 < i+1 < i+2 < p$, on a

$$\mathbf{Tr}\left(\nu \cdot \mu^i\right) = \mathbf{Tr}\left(\zeta^{i+2} - \zeta^{i+1}\right) = (-1) - (-1) = 0.$$

Si $\mu = \frac{1}{1 \pm \zeta}$, alors

$$\begin{aligned} \mathbf{Tr}\left(\nu \cdot \mu^i\right) &= \mathbf{Tr}\left(\left(\zeta^2 - \zeta\right) \cdot (1 \pm \zeta)^{p-3-i}\right) \\ &= \sum_{j=0}^{p-3-i} (\pm 1)^j \binom{p-3-i}{j} \mathbf{Tr}\left(\left(\zeta^2 - \zeta\right)\zeta^j\right) = 0. \end{aligned}$$

Ainsi, dans tous les cas,

$$\mathbf{Tr}\left(\nu \cdot \mu^i\right) = 0, \quad i \in \{0, 1, \ldots, p-3\}. \tag{6.66}$$

Posons $\delta = \nu \cdot \rho \in \mathbb{Z}[\zeta]$ et $\Delta = \mathbf{Tr}(\delta) \in \mathbb{Z}$. Par (6.66) et le fait que le développement de ρ^σ s'obtient par hypothèse en conjugant μ par σ, on a

$$\Delta = a\binom{1/q}{p-2} b^{p-2} \cdot \left(\mathbf{Tr}\left(\mu^{p-2}\nu\right) + \mathcal{O}(q)\right). \tag{6.67}$$

De plus, comme $\nu_q\left(\binom{1/q}{p-2}\right) = -(p-2) - \nu_q((p-2)!)$, on a

$$\begin{aligned}\nu_q\left(\binom{1/q}{p-2}b^{p-2}\right) &= k(p-2) - (p-2) - \nu_q((p-2)!) \\ &> (p-2)\left(k - 1 - \frac{1}{q-1}\right) = (p-2)\left(k - \frac{q}{q-1}\right).\end{aligned}$$

On a donc $(p-2)\left(k-\frac{q}{q-1}\right)+1 \leq \nu_q(\Delta)$. Admettons momentanément que $\Delta \neq 0$. On a alors

$$q^{(p-2)\left(k-\frac{q}{q-1}\right)+1} \leq |\Delta| \leq \sum_{\sigma} |\sigma(\nu \cdot \rho)| \leq 2^{p-2} \cdot (p-1) \cdot M,$$

d'où le lemme. Pour terminer la démonstration, il nous reste à montrer que $\Delta \neq 0$. Supposons d'abord que $\mu = \zeta$. Par (6.67)

$$\Delta = a\binom{1/q}{p-2}b^{p-2} \cdot \left(\mathbf{Tr}((\zeta^2-\zeta)\zeta^{p-2}) + \mathcal{O}(q)\right) = a\binom{1/q}{p-2}b^{p-2} \cdot (p + \mathcal{O}(q)).$$

Comme $p \neq q$ et $a\binom{1/q}{p-2}b^{p-2} \neq 0$, $\Delta \neq 0$ dans ce cas. Si $\mu = \frac{1}{1-\zeta}$, alors

$$\Delta = a\binom{1/q}{p-2}b^{p-2} \cdot \left(\mathbf{Tr}((\zeta^2-\zeta)\frac{1}{1-\zeta}) + \mathcal{O}(q)\right) = a\binom{1/q}{p-2}b^{p-2} \cdot (1 + \mathcal{O}(q)) \neq 0.$$

Enfin, si $\mu = \frac{1}{1+\zeta}$, alors (rappelons que $\mathbf{Tr}\left(\frac{1}{1+\zeta}\right) = \frac{p-1}{2}$)

$$\begin{aligned}\Delta &= a\binom{1/q}{p-2}b^{p-2} \cdot \left(\mathbf{Tr}((\zeta^2-\zeta)\frac{1}{1+\zeta}) + \mathcal{O}(q)\right) \\ &= a\binom{1/q}{p-2}b^{p-2} \cdot \left(\mathbf{Tr}\left(\zeta - 2 + \frac{2}{\zeta+1}\right) + \mathcal{O}(q)\right) \\ &= a\binom{1/q}{p-2}b^{p-2} \cdot (-p + \mathcal{O}(q)) \neq 0.\end{aligned}$$

Le lemme est prouvé.□

6.11.4 Un résultat de Mihăilescu.

Dans [52], Mihăilescu démontre le théorème suivant, qui nous sera utile lors de la démonstration du théorème (6.1.22) :

Théorème 6.11.6 *Soient p, q deux nombres premiers impairs distincts tels que $q \nmid h^-_{pq}$, $p \neq 1 \bmod q$, et $Sup\left(p, \frac{p(p-20)}{16}\right) > q$. Supposons qu'il existe des entiers x, y, z tels que*

$$x^p + y^p = z^q, \quad (x, y, z) = 1.$$

On a alors $Sup\,(|x|,|y|) \geq Inf\left(\frac{2}{p^{m+1}}, \frac{1}{2p^{q-m}}\right) \cdot \left(\frac{q^{1+(p-2)\left(\frac{q-2}{q-1}\right)}}{2^{p-2}\cdot(p-1)}\right)^q$, *où* $1 \leq m \leq q-1$, m *inverse de* $p-1$ *modulo* q.

Preuve

– Supposons que $f = -1$. Par la proposition (6.11.4)

$$\frac{x+\zeta y}{(1-\zeta)^e} = \frac{1+\zeta}{\gamma^e}\rho^q = (1+\zeta)\left(\frac{p}{(1-\zeta)^{p-1}}\right)^{em}\rho^q,$$

ie

$$\frac{y}{(1-\zeta)^e}\left(1+\frac{x-y}{y(1+\zeta)}\right) = \frac{p^{em}}{(1-\zeta)^{(p-1)em}}\rho^q,$$

autrement dit

$$y\left(1+\frac{x-y}{y(1+\zeta)}\right) = p^{em}(1-\zeta)^{(1-(p-1)m)e}\rho^q.$$

Comme m est l'inverse de $p-1$ modulo q, l'entier $(1-(p-1)m)e$ est divisible par q. Il existe donc $\rho_1 \in \mathbb{Z}[\zeta]$ tel que

$$yp^{e(q-m)}\left(1+\frac{x-y}{y(1+\zeta)}\right) = \rho_1^q.$$

Lemme 6.11.7 *L'entier* $yp^{e(q-m)}$ *est une puissance* q*-ième dans* $\mathbb{Z}_q$.

Preuve Supposons d'abord que $e = 0$. Par définition, il existe un entier z tel que (x, y, z) soit une solution de (6.65). Comme $e = 0$, il existe en particulier un entier a tel que $x + y = a^q$. Mais f valant -1, on a aussi $q^2|y - x$, d'où

$$2y \equiv a^q \bmod q^2.$$

Comme $x^p + y^p = z^q$, on a aussi $2y^p \equiv z^q \bmod q^2$. On a donc en divisant les deux dernières relations obtenues

$$y^{p-1} \equiv z^q a^{-q} \bmod q^2.$$

L'entier y^{p-1} est donc une puissance q-ième dans $\mathbb{Z}_q$. Comme $q \nmid p-1$, il en est de même pour y.

Supposons que $e = 1$. Il existe un entier z_1 tel que

$$\frac{x^p+y^p}{x+y} = pz_1^q.$$

Comme $q^2|y-x$, on tire $y^{p-1} \equiv pz_1^q \bmod q^2$, ie en élevant à la puissance m

$$yp^{q-m} \equiv y^{1-(p-1)m} p^{-q} z_1^{qm} \bmod q^2,$$

ce qu'on voulait ($q|1-(p-1)m$, par définition de m).□ L'entier $yp^{e(q-m)}$ étant une puissance q-ième dans $\mathbb{Z}_q$, il existe $w \in \mathbb{Z}_q$ tel que $w^q = yp^{q-m}$. Le nombre q-adique w est unique, le groupe des racines de l'unité de $\mathbb{Z}_q$ étant celui des racines $(q-1)$-ième de l'unité. De l'égalité

$$yp^{e(q-m)} \left(1 + \frac{x-y}{y(1+\zeta)}\right) = \rho_1^q,$$

on déduit qu'il existe une racine q-ième de l'unité disons $\xi_0 \in \mathbb{Z}_q[\zeta]$ telle que

$$\rho_1 = \xi_0 w \sum_{k=0}^{\infty} \binom{1/q}{k} \left(\frac{x-y}{y(1+\zeta)}\right)^k,$$

cette dernière série convergeant dans $\mathbb{Z}_q[\zeta]$ car $q^2|x-y$. En fait $\xi_0 = 1$. En effet, on a la tour d'extensions suivante

$$\mathbb{Q}_q \hookrightarrow \mathbb{Q}_q(\xi_0) \hookrightarrow \mathbb{Q}_q(\zeta).$$

Comme $\mathbb{Q}_q(\zeta)/\mathbb{Q}_q$ est non ramifiée et $\mathbb{Q}_q(\xi_0)/\mathbb{Q}_q$ l'est totalement, on a $\mathbb{Q}_q(\xi_0) = \mathbb{Q}_q$, ie $\xi_0 \in \mathbb{Z}_q$. Le groupe des racines de l'unité de $\mathbb{Z}_q$ étant celui des racines $(q-1)$-ième de l'unité, on doit avoir $\xi_0 = 1$:

$$\rho_1 = w \sum_{k=0}^{\infty} \binom{1/q}{k} \left(\frac{x-y}{y(1+\zeta)}\right)^k.$$

Soit $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. On a

$$\rho_1^\sigma = w \sum_{k=0}^{\infty} \binom{1/q}{k} \left(\frac{x-y}{y(1+\zeta^\sigma)}\right)^k.$$

En effet, comme $\rho_1^q = yp^{e(q-m)} \left(1 + \frac{x-y}{y(1+\zeta)}\right)$, on a

$$\rho_1^\sigma = \xi_0 w \sum_{k=0}^{\infty} \binom{1/q}{k} \left(\frac{x-y}{y(1+\zeta^\sigma)}\right)^k,$$

ξ_0 racine q-ième de l'unité de $\mathbb{Z}_q[\zeta]$. Comme avant, $\xi_0 = 1$, d'où le développement de ρ_1^σ. (Pour les autres cas, on omettra cette étape, les détails étant les mêmes).

Par ailleurs,

$$|\rho| = \left| p^{(q-m)e} \cdot \frac{x+\zeta y}{1+\zeta} \right|^{1/q} \leq p^{(1-m/q)e} \cdot \left(\frac{|x|+|y|}{|1+\zeta|} \right)^{1/q} \leq \left(2p^{(q-m)e} \cdot Sup(|x|,|y|) \right)^{1/q},$$

car on peut choisir ζ de sorte que $|1+\zeta| \geq 1$. Cette dernière inégalité est valable pour tous les conjugués de $\rho \in \mathbb{Z}[\zeta]$. On est donc en mesure d'appliquer le lemme (6.11.5) avec $M = \left(2p^{(q-m)e} \cdot Sup(|x|,|y|) \right)^{1/q}$ et $k = 2$, ce qui donne

$$\frac{1}{p-1} \cdot \frac{q^{1+(p-2)\left(2-\frac{q}{q-1}\right)}}{2^{p-2}} \leq \left(2p^{(q-m)e} \cdot Sup(|x|,|y|) \right)^{1/q},$$

ie

$$Sup\left(|x|,|y|\right) \geq \frac{1}{2} \left(\frac{q^{1+(p-2)\frac{q-2}{q-1}}}{2^{p-2} \cdot (p-1) \cdot p^{1-\frac{m}{q}}} \right)^q.$$

– Supposons $f = 0$ ie $q^2|x$. Par la proposition (6.11.4)

$$\frac{x+\zeta y}{(1-\zeta)^e} = \frac{1}{\gamma^e} \rho^q,$$

ie

$$x + \zeta y = (1-\zeta)^{e(1-(p-1)m)} p^{me} \rho^q,$$

autrement dit, vu que $q|e(1-(p-1)m)$

$$\left(1 + \frac{x}{y}\overline{\zeta} \right) \zeta y = p^{me} \rho_1^q.$$

Comme ζ est une puissance q-ième, on obtient

$$\left(1 + \frac{x}{y}\overline{\zeta} \right) y p^{e(q-m)} = \rho_2^q, \quad \rho_2 \in \mathbb{Z}[\zeta]. \tag{6.68}$$

Par définition de x et y, il existe un entier z tel que (6.65) ait lieu. Si $e = 0$, il existe donc un entier a tel que $x + y = a^q$. Comme $q^2|x$, $y \equiv a^q \bmod q^2$ et est donc une puissance q-ième dans $\mathbb{Z}_q$. Si $e = 1$, par (6.65), il existe un entier z_1 tel que $\frac{x^p+y^p}{x+y} = pz_1^q$. Comme $q^2|x$, on a donc $y^{p-1} \equiv pz_1^q \bmod q^2$. En l'élevant à la puissance m, inverse de $p-1 \bmod q$, on en déduit l'existence d'un entier z_2 tel que :

$$y p^{q-m} \equiv z_2^q \bmod q^2.$$

L'entier est donc une puissance q-ième dans $\mathbb{Z}_q$. Comme dans le cas $f = 0$, on va appliquer alors le lemme (6.11.5) avec M majorant de ρ_2. Par (6.68), on a

$$|\rho_2|^q \leq 2p^{e(q-m)} Sup\,(|x|, |y|).$$

On peut donc appliquer (6.11.5) avec $M = \left(2p^{e(q-m)} Sup\,(|x|, |y|)\right)^{1/q}$ et $k = 2$. On obtient

$$\frac{1}{p-1} \cdot \frac{q^{1+(p-2)\left(2-\frac{q}{q-1}\right)}}{2^{p-2}} \leq M = \left(2p^{e(q-m)} Sup\,(|x|, |y|)\right)^{1/q},$$

donc la même minoration que précédemment.

– Supposons $f = 1$, ie $q^2 | x + y$. Par la proposition (6.11.4)

$$\frac{x + \zeta y}{(1-\zeta)^e} = \gamma^{1-e}\rho^q = \frac{(1-\zeta)^{(p-1)(1-e)m}}{p^{(1-e)m}}\rho^q,$$

ie

$$\frac{x + \zeta y}{1-\zeta} = \frac{(1-\zeta)^{(1-e)((p-1)m-1)}}{p^{(1-e)m}}\rho^q.$$

Comme $q|(p-1)m - 1$, il existe $\rho_1 \in \mathbb{Z}[\zeta]$ tel que

$$p^{(1-e)m}\frac{x + \zeta y}{1-\zeta} = \rho_1^q,$$

ie

$$p^{(1-e)m} y \left(1 - \frac{x+y}{1-\zeta}\right) = (-\rho_1)^q.$$

Comme dans les cas précédents, avant d'appliquer le lemme (6.11.5) à un majorant M de $|\rho_1|$, on va vérifier que $p^{(1-e)m} y \equiv w^q \bmod q^2$ pour un certain entier w. Or par définition de x et y, il existe un entier z_1 tel que

$$\frac{x^p + y^p}{x+y} = p^e z_1^q,$$

ie $\sum_{k=0}^{p-1} (-y)^k x^{p-1-k} = p^e z_1^q$. Comme $q^2 | x + y$, il vient

$$y p^{(1-e)m} \equiv z_1^q \bmod q^2.$$

Le nombre algébrique ρ_1 étant majorer en valeur absolue par $M = \left(\frac{p^{1+(1-e)m}}{2} Sup\,(|x|, |y|)\right)^{1/q}$ (en prenant $\zeta = e^{\frac{2i\pi}{p}}$, $|1-\zeta| \geq \frac{4}{p}$), le lemme (6.11.5) montre

$$\frac{1}{p-1} \cdot \frac{q^{1+(p-2)\left(2-\frac{q}{q-1}\right)}}{2^{p-2}} \leq \left(\frac{p^{1+(1-e)m}}{2} Sup\,(|x|, |y|)\right)^{1/q}$$

ie

$$\frac{2}{p^{m+1}}\left(\frac{1}{p-1}\cdot\frac{q^{1+(p-2)\left(2-\frac{q}{q-1}\right)}}{2^{p-2}}\right)^q \leq Sup\,(|x|,|y|).$$

Le théorème est prouvé. ■

Remarque 6.11.8 *En fait, Mihăilescu énonce le résultat précédent avec la condition* $q \nmid h(p,q)$ *où* $h(p,q)$ *est un diviseur de* h_{pq}^-*, mais la condition précédente nous suffit.*

6.11.5 Démonstration du théorème (6.1.22).

Soient X, Z deux entiers fixés tels que

$$X^p = Y_0^p + BZ^q, \quad (X, Y_0, Z) = 1, \tag{6.69}$$

p, q premiers impairs distincts tels que $3 < p < q$ et $q \nmid h_{pq}^+$. Soit w la valuation p-adique de Z, et t celle de B ($wv = 0$ car $(Y_0, Z) = 1$). On définit l'entier B' par $B = p^t B'$. Il existe des entiers Z_1, Z_2 divisant Z et $e \in \{0; 1\}$ tels que

$$\begin{cases} \frac{X^p+Y_0^p}{X+Y_0} = p^e Z_1^q, \\ X = Y_0 + p^{qw+t-e} B' Z_2^q. \end{cases} \tag{6.70}$$

Soit $\alpha = \frac{X+Y_0\zeta}{(1-\zeta)^e}$. L'équation (6.70) montre qu'il existe un idéal entier $\mathfrak{a}$ de l'anneau $\mathbb{Z}[\zeta]$ tel que

$$\left(\frac{X+Y_0\zeta}{(1-\zeta)^e}\right) = \mathfrak{a}^q.$$

Soient ξ une racine primitive q-ième de 'unité et $g = (-1)^e(\zeta)^{e-1}\frac{\alpha}{\alpha^j}$. On a

$$g \equiv 1 \bmod q(1-\xi). \tag{6.71}$$

En effet, $q^2|B$, d'où par (6.70), $X \equiv Y_0 \bmod q^2$. On a alors

$$\frac{\alpha}{\alpha^j} = \frac{X+Y_0\zeta}{X+Y_0\overline{\zeta}}\left(\frac{1-\overline{\zeta}}{1-\zeta}\right)^e \equiv \frac{1+\zeta}{1+\overline{\zeta}}\left(\frac{1-\overline{\zeta}}{1-\zeta}\right)^e \equiv (-1)^e\zeta^{1-e} \bmod q^2,$$

d'où (6.71). En particulier, g est un nombre q-primaire de $\mathbb{Q}(\zeta, \xi)$. Soit $\mathbb{L} = \mathbb{Q}(\zeta, \xi, g^{1/q}) = \mathbb{Q}(\zeta, \xi, \left(\frac{\alpha}{\alpha^j}\right)^{1/q})$. Raisonnons par l'absurde et supposons que

$$|X| \geq 8\,|Y_0|\left(\frac{2}{5}\,|Y_0|\,qp^{\frac{1}{p-1}+v}\right)^q.$$

Proposition 6.11.9 *Soient x, y des entiers tels qu'il existe un idéal entier $\mathfrak{a}_0$ de l'anneau $\mathbb{Z}[\zeta]$, tel que*

$$\left(\frac{x+y\zeta}{(1-\zeta)^e}\right) = \mathfrak{a}_0^q, \quad |x| \geq 8|y| \left(\frac{2}{5}|y|qp^{\frac{1-e}{p-1}+v}\right)^q,$$

où v est la valuation p-adique de y. Soient $\alpha_0 = \frac{x+y\zeta}{(1-\zeta)^e}$, u_0 une unité de $\mathbb{Q}(\zeta)$, et $g_0 = u_0\frac{\alpha_0}{\alpha_0^j}$. Le nombre algébrique g_0 n'est pas une puissance q-ième dans $\mathbb{Q}(\zeta, \xi)$.

Preuve Supposons démontré le fait que ce n'est pas une puissance q-ième dans $\mathbb{Q}(\zeta)$. Supposons qu'il existe $Z \in \mathbb{Q}(\zeta, \xi)$ tel que $Z^q = g_0$. Soit $\mathcal{N}$ la norme relative à l'extension $\mathbb{Q}(\zeta, \xi)/\mathbb{Q}(\zeta)$. Comme $g_0 \in \mathbb{Q}(\zeta)$, on a

$$\mathcal{N}(Z)^q = g_0^{q-1}, \tag{6.72}$$

d'où $g_0 = \left(\frac{g_0}{\mathcal{N}(Z)}\right)^q$, en contradiction avec le fait que g_0 n'est pas une puissance q-ième dans $\mathbb{Q}(\zeta)$.

Il reste à montrer que ce n'est pas une puissance q-ième dans $\mathbb{Q}(\zeta)$. Raisonnons par l'absurde et supposons qu'il existe un nombre algébrique $z \in \mathbb{Q}(\zeta)$ tel que $z^q = g_0$. Par définition de $\mathfrak{a}_0$, on a donc

$$\mathfrak{a}_0^{q(1-j)} = (z)^q,$$

ce qui montre que $\mathfrak{a}_0^{1-j} = (z)$. L'égalité $\mathfrak{a}_0^{1-j} = (z)$ montre qu'il existe une unité u de $\mathbb{Q}(\zeta)$ telle que

$$z^j = u\frac{1}{z}.$$

Comme $\mathfrak{a}^q = (\alpha)$, il existe une unité u telle que

$$z^j = u\frac{1}{z},$$

d'où

$$z^{jq} = u^q\frac{1}{z^q} = u^q\frac{\alpha^j}{u_0\alpha}. \tag{6.73}$$

Par définition de z, $z^q = u_0\frac{\alpha}{\alpha^j}$. De (6.73), on obtient $u_0u_0^j = u^q$. Comme u_0 est une unité de $\mathbb{Q}(\zeta)$, il existe une racine p-ième de l'unité $\zeta^l, \epsilon = \pm 1$ et une unité réelle u_r tels que $u_0 = \epsilon\zeta^l u_r$. On a donc $u_r^2 = u^q$. Comme $(q, 2p)$, u_r, donc u_0, est une puissance q-ième dans $\mathbb{Q}(\zeta)$. Comme $z^q = u_0\frac{\alpha}{\alpha^j}$, $(x+y\zeta)^{1-j} \in \mathbb{Q}(\zeta)^{*q}$. Autrement dit, $1-j$ est un élément de taille 2 de l'idéal d'augmentation de Mihăilescu de $\mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})]$. Comme $|x| \geq 8|y|\left(\frac{2}{5}|y|qp^{\frac{1-e}{p-1}}\right)^q$, cela contredit le corollaire (6.2.4).□

La proposition précédente montre en particulier que le nombre algébrique g n'est pas une puissance q-ième dans $\mathbb{Q}(\zeta,\xi)$. L'extension $\mathbb{L}/\mathbb{Q}(\zeta,\xi)$ est donc une extension cyclique de degrés q. Elle est également non ramifiée. En effet, elle n'est pas ramifiée au-dessus de q, car g est un nombre q-primaire de $\mathbb{Q}(\zeta,\xi)$ (on peut aussi montrer qu'un tel choix de u_f implique que la différente de cette extension est première à q). Il reste à montrer qu'elle ne ramifie pas ailleurs. On rappelle la proposition suivante (voir le chapitre 5) :

Proposition 6.11.10 *Si K est un corps de nombres et $a \in K$ tel que $(a) = I^n$, pour un idéal de K, alors l'extension $K(a^{1/n})/K$ est au plus ramifiée en les diviseurs premiers de n.*

En particulier, l'extension $L/\mathbb{Q}(\zeta)$ est au plus ramifiée en q. Elle est donc non ramifiée.

Soit $z = \left(\frac{\alpha}{\alpha^j}\right)^{1/q}$. On a $L = \mathbb{Q}(\zeta,\xi,z)$. Soit τ un générateur de $\mathrm{Gal}(L/\mathbb{Q}(\zeta,\xi))$, donné par $\tau(z) = \xi z$. Il existe $J \in \mathrm{Gal}(L/\mathbb{Q}(\zeta,\xi)^+)$ tel que $J(z) = \frac{1}{z}$, $J(\xi) = \xi^{-1}$, $\quad J(\zeta) = \zeta^{-1}$. En effet, soit j la conjugaison complexe de $\mathbb{Q}(\zeta,\xi)$. Par la théorie de Galois, il existe $J \in \mathrm{Gal}(L/\mathbb{Q}(\zeta,\xi)^+)$, qui prolonge j. On a

$$J(z)^q = J(z^q) = \left(\frac{\alpha}{\alpha^j}\right)^J = \left(\frac{\alpha}{\alpha^j}\right)^j = \frac{1}{z^q}.$$

Il existe donc un entier a tel que $z^J = \frac{1}{\xi^a z}$. Si $a = 0$, il n'y a plus rien à faire. Sinon, soit $\sigma_a \in \mathrm{Gal}(L/\mathbb{Q}(\zeta,\xi))$ tel que $\sigma_a(z) = \xi^a z$. On a

$$\begin{cases} \sigma_a^{-1} J(z) = \frac{1}{z}, \\ \sigma_a^{-1} J_{|\mathbb{Q}(\zeta,\xi)} = j. \end{cases}$$

Quitte à prendre $\sigma_a^{-1}J$, on peut donc supposer que J convient.

On a $\tau J = J\tau$. En effet $\tau J(z) = \tau(z)^{-1} = \xi^{-1}z^{-1} = J(\xi)J(z) = J(\xi z) = J\tau(g)$. Le groupe $\mathrm{Gal}(L/\mathbb{Q}(\zeta,\xi)^+)$ est donc engendré par J et τ. On a le diagramme suivant :

$$\begin{array}{ccc} \mathbb{Q}(\zeta,\xi) & \to & L \\ \uparrow & & \uparrow \\ \mathbb{Q}(\zeta,\xi)^+ & \to & L^{<J>} \end{array}$$

L'extension $L^{<J>}/\mathbb{Q}(\zeta,\xi)^+$ est abélienne de degrés q. De plus, elle est non ramifiée. Les places à l'infini y sont non ramifiées. De plus, si un premier fini $\mathfrak{c}$ s'y ramifie, comme q est premier, $\mathfrak{c}$ y est totalement ramifié, d'indice de ramification q. Comme $q > 2$, l'extension $L/\mathbb{Q}(\zeta,\xi)$ se ramifie au-dessus de $\mathfrak{c}$, en contradiction avec le fait qu'elle est non ramifiée. L'extension $L^{<J>}/\mathbb{Q}(\zeta,\xi)^+$ est donc abélienne de degrés q et non ramifiée. La théorie du corps de classe montre que q divise h^+_{pq}, le nombre de classes de $\mathbb{Q}(\zeta,\xi)^+$, en contradiction avec les hypothèses. On a donc bien $|X| \leq 8\,|Y| \left(\frac{2}{5}\,|Y|\, qp^{\frac{1}{p-1}+v}\right)^q$.■

6.12 Démonstration du corollaire (6.1.23).

Si $q \nmid h_{pq}^{+}$, par le théorème (6.1.22), on doit avoir

$$|X| \leq 8\,|Y|\left(\frac{2}{5}\,|Y|\,qp^{\frac{1}{p-1}}\right)^{q}.$$

Par (6.70), comme $p \nmid BC$, on a $X = Y_0 + p^{qw-e}BC^qZ_2^q$, d'où $(Y_0, Z_2 \geq 0)$:

$$BC^q < 8\,|Y|\left(\frac{2}{5}\,|Y|\,qp^{\frac{1}{p-1}}\right)^{q},$$

en contradiction avec les hypothèses. Le nombre premier q divise donc bien h_{pq}^{+}. En particulier, par la proposition (6.16.2) q divise h_{pq}^{-}. ■

6.13 preuve du corollaire (6.1.24).

Supposons qu'il existe des entiers x, y non nuls tels que $x^p - y^q = 1$. On peut montrer (voir [28] et [38]) que l'on a

$$\begin{array}{l} q^2|x, \quad p^2|y, \\ |x| \geq Sup\,(p^{q-1}(q-1)^q + 1, q(2p+1)(2q^{p-1}+1)), \\ |y| \geq Sup\,(q^{p-1}(p+1)^p - 1, p(q-1)(p^{q-1}(q-1)^q + 1)). \end{array}$$

Comme $q^2|x$, la preuve du théorème (6.1.22) peut facilement être adaptée au cas de l'équation de Catalan. En particulier, si $q \nmid h_{pq}^{+}$, on obtient

$$p^{q-1}(q-1)^q < |x| < 8 \cdot q^q \cdot p^{\frac{q}{p-1}},$$

d'où

$$2^{3+q} > p^{q-1-\frac{q}{p-1}} \geq p^{\frac{q}{2}-1}.$$

Pour les solutions de l'équation de Catalan, $p, q \geq 43$ (voir [28]). On a donc

$$2^{3+q} > 43^{\frac{q}{2}-1},$$

montrant que $q < 5$, ce qui n'est pas. On a donc bien $q|h_{pq}^{+}$. ■

6.14 Démonstration du théorème (6.1.25).

Soient donc y_0 un entier fixé et p, q deux nombres premiers impairs distincts, comme dans l'énoncé. On suppose que ces entiers sont choisis de sorte que

$$|y_0| < \left(\frac{5^q q^{q\left(\frac{pq-2p-3q+5}{q-1}\right)}}{4^{q+2}(p-1)p^{\frac{q}{p-1}+1}} \right)^{\frac{1}{2q+1}}, \quad 3 < p < q < \frac{p(p-20)}{16}.$$

Supposons qu'il existe des entiers (x, z) tels que

$$x^p + y_0^p = z^q, \quad (x, y_0, z) = 1, \quad |x| \geq |y_0|.$$

On souhaite montrer que q divise h_{pq}^-. Raisonnons par l'absurde et supposons que ce ne soit pas le cas. Etant alors dans son champs d'application, le théorème (6.11.6) montre (puisque $|x| \geq |y_0|$) :

$$Inf\left(\frac{2}{p^{m+1}}, \frac{1}{2p^{q-m}}\right) \cdot \left(\frac{q^{1+(p-2)\left(\frac{q-2}{q-1}\right)}}{2^{p-2} \cdot (p-1)} \right)^q \leq |x|. \tag{6.74}$$

Par le critère de Masley-Montgomery (proposition (6.16.3)), h_p^- est premier à q. Comme $q \nmid h_p^-$, il existe $\gamma \in \mathbb{Q}(\zeta)^*$, tel que $\frac{x+\zeta y_0}{x+\overline{\zeta} y_0} = \gamma^q$. L'idéal $\mathcal{I}_M^{aug}(x, y, p, q)(2)$ contient $1 - j$, et est donc non trivial. Comme $3 < p < q$, le corollaire (6.2.4) montre que x et y_0 vérifient :

$$|x| < 8|y_0| \left(\frac{2}{5} q p^{\frac{1-e}{p-1}+v} |y_0| \right)^q,$$

où v et la valuation p-adique de y_0. L'inégalité précédente et l'inégalité (6.74) donnent les inégalités suivantes :

$$Inf\left(\frac{2}{p^{m+1}}, \frac{1}{2p^{q-m}}\right) \cdot \left(\frac{q^{1+(p-2)\left(\frac{q-2}{q-1}\right)}}{2^{p-2} \cdot (p-1)} \right)^q \leq |x| < 8|y_0| \left(\frac{2}{5} q p^{\frac{1-e}{p-1}+v} |y_0| \right)^q,$$

d'où

$$|y_0| > \left(Inf\left(\frac{2}{p^{m+1}}, \frac{1}{2p^{q-m}}\right) \cdot \frac{5^q}{2^{q(p-1)+3}(p-1)^q p^{\frac{q}{p-1}}} q^{\frac{q(q-2)(p-2)}{p-1}} \right)^{\frac{1}{2q+1}},$$

en contradiction avec les hypothèses, ce qui démontre le corollaire. ■

6.15 Démonstration du corollaire (6.1.26).

La démonstration de l'inégalité est une simple réecriture de la démonstration du théorème 5 de [19] adaptée au cas $|y| \geq 1$. En effet, sans perdre de généralité, on peut supposer par exemple que $|x| \geq |y|$. Avec les notations de [19], au lieu de travailler avec le quotient $\frac{A(x)^\rho}{A(x)}$, on travaille alors avec $\frac{A(x/y)^\rho}{A(x/y)}$. Dans le cas où $p \neq 1 \bmod 8$, la forme linéaire Λ considérée dans [19], se majore de la façon suivante :

$$|\Lambda| \leq \frac{2p}{|x/y|}. \tag{6.75}$$

De plus, on a

$$log\,|\Lambda| \geq -c_0 a H(q)^2, \tag{6.76}$$

où on a

$$c_0 = 8.87, \quad a = 11\pi + \frac{1}{2}log|y|, \quad H(q) = Sup\left(17, 2log\left(\left(\frac{1}{22\pi} + \frac{1}{68.9}\right)q\right) + 9.73\right).$$

Des inégalités (6.75) et (6.76), on obtient

$$\left(\frac{q}{p-1} - \frac{c_0 H(q)^2}{2}\right) log|z| \leq log(2p) + log|y| + \frac{log(p)}{p-1} + 11\pi c_0 H(q)^2. \tag{6.77}$$

Si $\frac{q}{p-1} - \frac{c_0 H(q)^2}{2} < 0$, on obtient

$$\sqrt{q} \leq 17 c_0 \frac{p-1}{2},$$

d'où

$$q \leq c_0 \frac{p-1}{2} H^2, \quad H = \sup\left(17, 2log\left(\left(\frac{1}{22\pi} + \frac{1}{68.9}\right)\left(17 c_0 \frac{p-1}{2}\right)^2\right) + 9.73\right).$$

On vérifie alors que $q < \frac{p(p-20)}{16}$ si $p \geq 358747$.

Dans l'autre cas, c'est à dire $\frac{q}{p-1} - \frac{c_0 H(q)^2}{2} \geq 0$, comme $|z| \geq 2p+1$ (par le lemme (5.3.13)), on obtient

$$\sqrt{q} \leq (p-1)\left(17 c_0\left(\frac{1}{2} + \frac{11\pi}{log(2p+1)}\right) + \frac{1}{\sqrt{5} log(2p+1)}\left(log(2p) + log|y| + \frac{log(p)}{p-1}\right)\right), \tag{6.78}$$

car $M = Sup_{q \geq 3}\left(\frac{H^2}{\sqrt{q}}\right) \leq 167$. Pour avoir $q < \frac{p(p-20)}{16}$, il suffit donc d'avoir $p \geq 23$ et

$$|y| \leq \frac{1}{2p^{\frac{p}{p-1}}} e^{\sqrt{5} log(2p+1)\left(\frac{p^2 (p-20)^2}{256(p-1)} - 17 c_0\left(\frac{1}{2} + \frac{11\pi}{log(2p+1)}\right)\right)}. \tag{6.79}$$

On a donc bien montré que si $p \geq 358747$, alors $q < \frac{p(p-20)}{16}$.

6.16 Réflection cyclotomique et application.

Avec des notations usuelles, on a

Théorème 6.16.1 *(voir [77], théorème* 10.11*) Soit p un nombre premier impair. Soit L un corps de type CM, tel que $\zeta_p \in L$, t soit A le p-sous-groupe de Sylow du groupe des classes de L. Alors, on a*

$$r_p\left(A^+\right) \leq 1 + r_p\left(A^-\right).$$

Soit W le groupe des racines de l'unité de L. Si l'extension $L\left(W^{1/p}\right)/L$ est ramifiée, alors

$$r_p\left(A^+\right) \leq r_p\left(A^-\right).$$

On en déduit :

Proposition 6.16.2 *Si le nombre premier q divise h_{pq}^+, alors il divise également $q|h_{pq}^-$.*

Preuve En effet, l'extension $\mathbb{Q}(\zeta_{pq^2})/\mathbb{Q}(\zeta_{pq})$ est ramifiée en q. Par le théorème précédent, le p-rang du groupe des classes relatif de $\mathbb{Q}(\zeta_{pq})$ vaut au moins 1, donc $q|h_{pq}^-$.□

6.16.1 Critère de Masley et Montgomery.

Proposition 6.16.3 *(voir [49]) Soient m, n deux entiers tels que $m|n$. Alors l'entier h_m^- divise h_n^-.*

Remarque 6.16.4 *On peut aussi montrer que si $m|n$, alors $h_m^+|h_n^+$ (voir par exemple [3]).*

6.17 Exemple (6.1.30) détaillé.

Supposons d'abord que $p' = 2$, et que m soit tel que l'équation (6.10) admette une solution en entiers positifs x, n, $n > 1$. Si $2|n$, alors nécessairement $n = m = 2$ et $x = p-1$. En effet, posons $n = 2k$. L'équation $x^2 + q^m = p^n$ s'écrit

$$q^m = \left(p^k + x\right)\left(p^k - x\right).$$

Comme q est premier et $\left(p^k + x, p^k - x\right) = 1$, on a

$$q^m = p^k + x, \quad 1 = p^k - x,$$

donc

$$q^m + 1 = 2p^k. \tag{6.80}$$

L'entier m est pair. En effet, la relation $q^2+1=2p$ montre que q est d'ordre 4 modulo p. De la relation (6.80) précédente, on déduit que $q^{2m} \equiv 1 \bmod p$, donc que $2|m$.

L'équation (6.80) a pour seule solution $m=2$, $k=1$ si $k<3$, car $q^2+1=2p$. Si $k \geq 3$, elle n'en a aucune par [46] et [74]. Le résultat est donc prouvé pour n pair.

Supposons n impair. Si $q \equiv 3 \bmod 4$, c'est une conséquence de [76]. Supposons $q \equiv 1 \bmod 4$. On peut alors appliquer le théorème (3.1.1). En effet, si m est impair, on peut poser $m=2k+1$, et l'équation s'écrit

$$x^2 + q^{2k} \cdot q = y^n.$$

On peut appliquer le théorème (3.1.1), la condition "$b|D$" étant vérifiée. De même, si m est pair, la condition $Rad(n) \nmid q-1$ nous assure de l'existence d'un premier $l|n$ tel que $q \neq \left(\frac{-1}{q}\right) \bmod l$.

Le théorème (3.1.1) montre que $3|n$ et qu'il existe un entier A tel que

$$3A^2 = \epsilon + q^m, \epsilon = \pm 1.$$

En se plaçant modulo 4, on voit que $\epsilon = -1$, et donc les entiers A et m sont solutions de

$$3A^2 + 1 = q^m.$$

L'équation diophantienne $3X^2+1=Y^n$ est sans solution entière X, Y si $n>1$. On en déduit dans notre cas que $m=1$, c'est à dire $q=3A^2+1$. Le théorème (3.1.1) montre aussi que les entiers $p^{n/3}$ et A sont liés par la relation

$$p^{n/3} = 4A^2 + 1 = (2A)^2 + 1.$$

Le théorème de Lebesgue montre donc que $n=3$. On a ainsi montré qu'il existe un entier A tel que

$$\begin{cases} 4A^2+1 = p, \\ 3A^2+1 = q. \end{cases}$$

Comme $q^2+1=2p$, l'entier A est donc solution de

$$\left(3A^2+1\right)^2 + 1 = 2\left(4A^2+1\right),$$

c'est à dire $9A^4 = 2A^2$, d'où $A=0$, ce qui est impossible.

6.18 Démonstration du théorème (6.1.31).

Supposons que l'équation (6.11) admette une solution entière non triviale. Il existe un idéal entier $\mathfrak{a}$ tel que

$$\left(\frac{x+y_0\zeta}{(1-\zeta)^e}\right) = \mathfrak{a}^q. \tag{6.81}$$

Soit θ un élément de l'idéal de Stickelberger de $\mathbb{Q}(\zeta)$. Par (6.81), il existe $\eta \in \mathbb{Z}[\zeta]^\times$ et $\nu(\theta) \in \mathbb{Z}[\zeta]$ tel que

$$(x+y_0\zeta)^\theta = \eta(1-\zeta)^{e\theta}\nu(\theta)^q.$$

En notant j la conjugaison complexe, on en déduit qu'il existe une racine $2p$-ième de l'unité $\epsilon(\theta)$ telle que

$$(x+y_0\zeta)^{\theta(1-j)} = \left(\epsilon(\theta)\frac{\nu(\theta)}{\nu(\theta)^j}\right)^q.$$

Soit $f[\theta, x]$ la série de Mihăilescu associée à θ et à l'exposant premier q (voir le chapitre 5). Ce qui précède montre qu'il existe $\kappa(\theta) \in \mathbb{Z}/q\mathbb{Z}$ tel que

$$\beta(\theta) := \epsilon(\theta)\frac{\nu(\theta)}{\nu(\theta)^j} = \xi^{\kappa(\theta)} f\left[(1-j)\theta, \frac{y_0}{x}\right].$$

L'application $\kappa : \mathbb{Z}[G] \to \mathbb{Z}/q\mathbb{Z}$ ainsi définie vérifie le lemme suivant :

Lemme 6.18.1 *L'application κ est additive ie*

$$\kappa(\theta_1+\theta_2) = \kappa(\theta_1) + \kappa(\theta_2)$$

et vérifie $\kappa(j\theta) = -\kappa(\theta)$.

Preuve Soient donc θ_1, θ_2 deux éléments de l'idéal de Stickelberger. Les seules racines de l'unité contenues dans le corps $\mathbb{Q}(\zeta)$ sont les racines $2p$-ième de l'unité. Comme

$$\begin{aligned}\beta(\theta_1+\theta_2)^q &= (x+y_0\zeta)^{(\theta_1+\theta_2)(1-j)} \\ &= (x+y_0\zeta)^{\theta_1(1-j)}\,(x+y_0\zeta)^{\theta_2(1-j)} \\ &= \beta(\theta_1)^q\beta(\theta_2)^q,\end{aligned}$$

on en déduit que

$$\beta(\theta_1+\theta_2) = \beta(\theta_1)\beta(\theta_2).$$

Il vient alors

$$\begin{aligned}\xi^{\kappa(\theta_1+\theta_2)} &= \frac{\beta(\theta_1+\theta_2)}{f\left[(1-j)(\theta_1+\theta_2), \frac{y_0}{x}\right]} \\ &= \frac{\beta(\theta_1+\theta_2)}{f\left[(1-j)\theta_1, \frac{y_0}{x}\right] f\left[(1-j)\theta_2, \frac{y_0}{x}\right]} \\ &= \frac{\beta(\theta_1)}{f\left[(1-j)\theta_1, \frac{y_0}{x}\right]} \frac{\beta(\theta_2)}{f\left[(1-j)\theta_2, \frac{y_0}{x}\right]} \\ &= \xi^{\kappa(\theta_1)}\xi^{\kappa(\theta_2)},\end{aligned}$$

d'où l'additivité de κ. La seconde assertion se montre de même.□

Rappelons que si $a \in \left\{1, \ldots, \frac{p-1}{2}\right\}$, on note $\phi_a \in \mathcal{I}_{st}$ le a-ième élément de Fueter (voir le chapitre 2). Posons

$$I = \left\{ \phi_a + \phi_b + \phi_c \,|\quad a, b, c \in \left\{1, \ldots, \frac{p-1}{2}\right\}\right\}.$$

Comme la famille des éléments de Fueter est $\mathbb{Z}$-libre, en particulier

$$M := |I| = \frac{p-1}{2}\frac{p-3}{2}\frac{p-5}{2} + \frac{p-1}{2}\frac{p-3}{2} + \frac{p-1}{2} = \frac{(p-1)(p^2-6p+13)}{8}.$$

Comme $|x| \geq 2|y_0|$, on peut reprendre la démonstration du théorème 5 de [19] En particulier, il existe une constante effective C telle que si $p \geq C$, alors $q < M$. L'application κ restreinte à I ne peut donc être injective : il existe deux éléments de I, disons θ_1 et θ_2 tels que

$$\kappa(\theta_1) = \kappa(\theta_2).$$

Soit $\theta = \theta_1 + j\theta_2$ et considérons

$$\phi = \epsilon(\theta)\nu(\theta) - \overline{\nu(\theta)} \in \mathbb{Z}[\zeta].$$

Par le lemme (6.18.1)

$$\kappa(\theta) = \kappa(\theta_1) + \kappa(j\theta_2) = \kappa(\theta_1) - \kappa(\theta_2) = 0.$$

On peut donc mettre l'entier algébrique sous la forme

$$\phi = \overline{\nu(\theta)}\left(\epsilon(\theta)\frac{\nu(\theta)}{\overline{\nu(\theta)}} - 1\right) = \overline{\nu(\theta)}\left(f\left[\theta(1-j), \frac{y_0}{x}\right] - 1\right).$$

Par l'inégalité (5.15) du chapitre 5, appliquée avec $m = 0$ donne[3] :

$$\left| f\left[\theta(1-j), \frac{y_0}{x}\right] - 1 \right| \leq \frac{3(p-1)}{q} \cdot \frac{\left|\frac{y_0}{x}\right|}{\left(1 - \left|\frac{y_0}{x}\right|\right)^{1+\frac{3(p-1)}{q}}}. \tag{6.82}$$

Comme $\kappa(j\theta) = -\kappa(\theta) = 0$, de même

$$\left| f\left[j\theta(1-j), \frac{y_0}{x}\right] - 1 \right| \leq \frac{3(p-1)}{q} \cdot \frac{\left|\frac{y_0}{x}\right|}{\left(1 - \left|\frac{y_0}{x}\right|\right)^{1+\frac{3(p-1)}{q}}}. \tag{6.83}$$

Il existe $\eta \in \mathbb{Z}[\zeta]^\times$ telle que

$$(x + y_0\zeta)^\theta = \eta(1-\zeta)^{e\theta}\nu(\theta)^q.$$

En prenant la norme, on en déduit

$$|\mathcal{N}(\nu(\theta))| \leq |z|^{3(p-1)}. \tag{6.84}$$

Enfin, si $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, $\sigma \neq 1, j$

$$\left| \left(\epsilon(\theta) \frac{\nu(\theta)}{\overline{\nu(\theta)}} \right)^\sigma - 1 \right| \leq 2. \tag{6.85}$$

Des inégalités (6.82) à (6.85), il vient

$$|\mathcal{N}(\phi)| \leq |z|^{3(p-1)} \cdot \left(\frac{3(p-1)}{q} \cdot \frac{\left|\frac{x}{y_0}\right|^{\frac{3(p-1)}{q}}}{\left(\left|\frac{x}{y_0}\right| - 1\right)^{1+\frac{3(p-1)}{q}}} \right)^2 \cdot 2^{p-3}. \tag{6.86}$$

On a $1 \leq |\mathcal{N}(\phi)|$ sauf si $\phi = 0$. Si cela était possible, on aurait $\epsilon(\theta)\frac{\nu(\theta)}{\overline{\nu(\theta)}} = 1$, ie en élevant cette égalité à la puissance q-ième

$$(x + y_0\zeta)^{\theta(1-j)} = 1,$$

ie $\theta = j\theta$. Comme $\theta \in \mathcal{I}_{st}$, l'élément θ est donc un multiple entier de la norme :

$$\exists a \in \mathbb{Z}, \quad \theta = a\mathcal{N}. \tag{6.87}$$

Rappelons que si ψ est un élément de Fueter (donc de poids $\frac{p-1}{2}$), $(1+j)\psi = \mathcal{N}$. En particulier

$$j\theta_2 = 3\mathcal{N} - \theta_2.$$

[3] rappelons que les éléments de Fueter sont de poids $\frac{p-1}{2}$, donc $|\theta| = W(\theta) = 3(p-1)$.

Par (6.87), il existe donc un entier b tel que

$$\theta_1 - \theta_2 = b\mathcal{N}.$$

Comme la famille des éléments de Fueter, avec l'élément norme $\mathcal{N}$ réalise une $\mathbb{Z}$-base de $\mathcal{I}_{st}$ (voir le chapitre 4), cette dernière égalité n'est possible que si $b = 0$, ce qui implique que $\theta_1 = \theta_2$, ce qui n'est pas. On a donc bien $\phi \neq 0$, et donc $1 \leq \mathcal{N}(\phi)$, ie

$$1 \leq |z|^{3(p-1)} \cdot \left(\frac{3(p-1)}{q} \cdot \left(\frac{\left|\frac{x}{y_0}\right|^{1+\frac{3(p-1)}{q}}}{\left(\left|\frac{x}{y_0}\right| - 1\right)^{1+\frac{3(p-1)}{q}}} \right) \cdot \frac{1}{\left|\frac{x}{y_0}\right|} \right)^2 \cdot 2^{p-3}$$

On peut supposer $q \geq 3(p-1)$ (sinon il n'y a rien à démontrer), ce qui donne :

$$\left|\frac{x}{y_0}\right| \leq 2^{\frac{p+1}{2}} |z|^{\frac{3(p-1)}{2}}. \tag{6.88}$$

De l'équation (6.11), on déduit que $|z|^q < |x|^p$, ce qui donne

$$|z|^{\frac{q}{p} - \frac{3(p-1)}{2}} \leq 2^{\frac{p+1}{2}} |y_0|.$$

Par le lemme (5.3.13), pour tout facteur premier l de z, on a $l \equiv 1 \bmod p$. On en déduit donc

$$(2p+1)^{\frac{q}{p} - \frac{3(p-1)}{2}} \leq 2^{\frac{p+1}{2}} |y_0|.$$

Si $q > 2p(p-1)$, on aurait

$$(2p+1)^{\frac{p-1}{2}} \leq 2^{\frac{p+1}{2}} |y_0|,$$

en contradiction avec les hypothèses. ■

6.19 Démonstration du théorème (6.1.32).

Considérons l'ensemble J suivant :

$$J = \left\{ \sum_{c=1}^{\frac{p-1}{2}} n_c \sigma_c | \quad n_c \in \{-1, 0, 1\} \right\}.$$

Dans la preuve précédente, on a introduit la fonction κ définie sur $\mathcal{I}_{st}$. Comme dans l'énoncé du théorème (6.1.32) on suppose que $q \nmid h_p^-$, en particulier, pour $\theta \in \mathbb{Z}[G]$, le nombre

algébrique $(x+y_0\zeta)^{(1-j)\theta}$ est une puissance q-ième dans $\mathbb{Q}(\zeta)$. On peut donc définir la fonction κ sur $\mathbb{Z}[G]$, donc sur J. Soit $k \in \mathbb{Z}/q\mathbb{Z}$. On pose

$$J'_k = \{\theta \in J; \quad \kappa(\theta) = k\}.$$

Comme $\sum_{k=0}^{q-1} |J'_k| = |J|$, il existe un entier k tel que $|J'_k| \geq \frac{|J|}{q}$. On pose alors

$$J_1 = J'_k.$$

Notons que $|J_1| \geq \frac{|J|}{q} > 1$ par le théorème (6.1.31). Soit $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Posons

$$J_{1,\sigma,l} = \{\theta \in J_1; \quad \kappa(\sigma\theta) = l\}.$$

Comme $\bigsqcup_l \bigsqcup_{\sigma \neq 1,j} J_{1,\sigma,l} = J_1$, il existe donc au moins un entier $l_2 \in \{0,\ldots,q-1\}$ et $\sigma_2 \neq 1, j$ tel que $|J_{1,\sigma_2,l_2}| \geq \frac{|J|}{q^2(p-3)} > 1$. On pose alors $J_2 = J_{1,\sigma_2,l_2}$. Soit $H = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) - \{1, j, \sigma_2, j\sigma_2\}$. De la même façon, il existe un entier l_3 et $\sigma_3 \in H$ tels que $|J_{2,\sigma_3,l_3}| \geq \frac{|J|}{q^3(p-3)(p-5)} > 1$.

On construit ainsi de proche en proche une suite $(\sigma_i)_i$ de $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ et une suite d'ensembles J_i tels que

$$J_i \subset J_{i-1} \ldots \subset J_1, \quad |J_i| \geq \frac{|J|}{q^i(p-3)\cdots(p-2i+1)}.$$

On répète le processus tant que $i \leq \frac{p-1}{2}$ et $\frac{|J|}{q^i(p-3)\cdots(p-2i+1)} > 1$. On peut supposer que $p < q$ car sinon le théorème à prouver est en particulier vrai. On a alors

$$|J_i| \geq \frac{|J|}{q^i(p-3)\cdots(p-2i+1)} \geq \frac{|J|}{q^{2i-1}}.$$

On peut donc au moins construire les $J_1,\ldots,J_n$ où l'entier n est défini par

$$\frac{|J|}{q^{2n-1}} > 1 \geq \frac{|J|}{q^{2n+1}} \Rightarrow n \geq \frac{(p-1)log(3)}{4log(q)} - \frac{1}{2}. \tag{6.89}$$

Soient alors $\theta_1 \neq \theta_2$ deux éléments de J_n. Par construction,

$$\forall i \in \{1,\ldots,n\}, \quad \kappa(\sigma_i\theta_1) = \kappa(\sigma_i\theta_2), \quad \kappa(j\sigma_i\theta_1) = \kappa(j\sigma_i\theta_2).$$

Par construction, les σ_i et $j\sigma_l$ sont deux à deux distincts. On dispose ainsi d'une famille $\aleph$ de $2n$ éléments σ de $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ tels que

$$\kappa(\sigma\theta_1) = \kappa(\sigma\theta_2).$$

Avec les notations de la preuve précédente, on considère

$$\phi = z\left(\beta(\theta_1) - \beta(\theta_2)\right).$$

Comme les coefficients de θ_1 et θ_2 sont -1, 0 ou 1, $z\beta(\theta_i) \in \mathbb{Z}[\zeta]$ car les facteurs premiers l de z se décomposent totalement dans $\mathbb{Z}[\zeta]$. Notons également que $\phi \neq 0$. En effet, dans le cas contraire

$$\beta(\theta_1) = \beta(\theta_2) \Rightarrow \theta_1(1-j) = \theta_2(1-j) \Rightarrow \theta_1 - \theta_2 = j\left(\theta_1 - \theta_2\right).$$

On en déduit que

$$2\left(\theta_1 - \theta_2\right) = \theta_1 - \theta_2 + j\left(\theta_1 - \theta_2\right) = (1+j)\left(\theta_1 - \theta_2\right) \in (1+j)\mathbb{Z}[G].$$

Un élément $\theta = \sum_{c=1}^{p-1} n_c\sigma_c \in (1+j)\mathbb{Z}[G]$ ssi $n_c = n_{p-c}$, $1 \leq c \leq \frac{p-1}{2}$. Or, les coefficients de θ_1 et θ_2 d'indice strictement plus grand que $\frac{p-1}{2}$ valent zéro. Par conséquent

$$2\left(\theta_1 - \theta_2\right) \in (1+j)\mathbb{Z}[G] \Rightarrow \theta_1 = \theta_2,$$

ce qui n'est pas. On a donc bien $\phi \neq 0$, d'où $\mathcal{N}\left(\phi\right) = \pm 1$.

Majorons $|\mathcal{N}\left(\phi\right)|$. L'entier algébrique ϕ s'écrit aussi

$$\phi = z\beta(\theta_2)\left(\frac{\beta(\theta_1)}{\beta(\theta_2)} - 1\right).$$

On a

$$\beta(\theta_1) = \xi^{\kappa((1-j)\theta_1)} f\left[(1-j)\theta_1, \frac{y_0}{x}\right].$$

Le lemme (6.18.1) montre que $\kappa((1-j)\theta_1) = \kappa(\theta_1) - \kappa(-\theta_1) = 2\kappa(\theta_1) = 2k$. Par définition des θ_i, $\kappa((1-j)\theta_2) = 2k$. On a donc

$$\beta(\theta_1) = \xi^{2k} f\left[(1-j)\theta_1, \frac{y_0}{x}\right], \quad \beta(\theta_2) = \xi^{2k} f\left[(1-j)\theta_2, \frac{y_0}{x}\right],$$

d'où

$$\frac{\beta(\theta_1)}{\beta(\theta_2)} = f\left[(1-j)(\theta_1 - \theta_2), \frac{y_0}{x}\right] - 1.$$

Plus généralement, comme $\kappa(\sigma\theta_1) = \kappa(\sigma\theta_2)$, pour tout élément σ de $\aleph$, on a

$$\forall \sigma \in \aleph, \quad \left(\frac{\beta(\theta_1)}{\beta(\theta_2)}\right)^{\sigma} = \frac{\beta(\sigma\theta_1)}{\beta(\sigma\theta_2)} = f\left[\sigma(1-j)(\theta_1 - \theta_2), \frac{y_0}{x}\right] - 1.$$

Pour chaque $\sigma \in \aleph$, on peut majorer ϕ^σ comme dans la preuve précédente :

$$\begin{aligned}
|\phi^\sigma| = \left|z\beta(\sigma\theta_2)\left(\frac{\beta(\sigma\theta_1)}{\beta(\sigma\theta_2)} - 1\right)\right| &= \left|z\left(f\left[\sigma(\theta_1-\theta_2)(1-j), \frac{y_0}{x}\right] - 1\right)\right| \\
&\leq |z|\frac{2(p-1)}{q}\frac{\left|\frac{y_0}{x}\right|}{\left(1-\left|\frac{y_0}{x}\right|\right)^{1+\frac{2(p-1)}{q}}} \\
&\leq |z|\frac{2(p-1)}{q}\frac{\left|\frac{x}{y_0}\right|^{1+\frac{2(p-1)}{q}}}{\left|\frac{x}{y_0}\right|\left(\left|\frac{x}{y_0}\right|-1\right)^{1+\frac{2(p-1)}{q}}} \\
&\leq 16|z|\frac{1}{\left|\frac{x}{y_0}\right|}.
\end{aligned}$$

Si σ n'est pas un élément de $\aleph$, on majore $|\phi^\sigma|$ par $2|z|$. On a donc

$$\begin{aligned}
1 \leq |\mathcal{N}(\phi)| &\leq |z|^{p-1-2n}2^{p-1-2n}\left(16|z|\frac{1}{\left|\frac{x}{y_0}\right|}\right)^{2n} \\
&\leq |z|^{p-1}2^{p-1+6n}\frac{1}{\left|\frac{x}{y_0}\right|^{2n}}.
\end{aligned}$$

Comme $|x|^p > |z|^q$ et $|z| \geq 2p+1$, il vient

$$(2p+1)^{2n\frac{q}{p}-(p-1)} \leq |y_0|^{2n}2^{p-1+6n},$$

ie

$$q \leq \frac{\log|y_0|}{\log(2p+1)}p + \frac{(p-1+6n)\log(2)}{2n\log(2p+1)}p + \frac{(p-1)p}{2n}.$$

Mais

$$\frac{1}{2n} \leq \frac{1}{\frac{(p-1)\log(3)}{2\log(q)} - 1} < \frac{1}{\frac{(p-1)\log(3)}{6\log(p)}}$$

en utilisant $q \leq 2p(p-1) < p^3$, inégalité justifiée par le théorème (6.1.31). On en déduit

$$q < \left(\frac{\log|y_0| + 3\log(2)}{\log(2p+1)} + 6 + \frac{6\log(p)}{\log(3)}\right)p.$$

■

Chapitre 7

Sur l'équation $X^p - 1 = BZ^q$.

7.1 Introduction

On se fixe p et q deux nombres premiers impairs. Soit $B \in \mathbb{N}^*$ tel que $(\varphi(Rad(B)), p) = 1$. On s'intéresse aux solutions entières X, Z d'équation de la forme

$$X^p - 1 = BZ^q, X \neq 1.$$

Si une telle solution existe, alors $X - 1$ est de la forme $\frac{BC^q}{p^e}$ avec $e = 0$ si $(p, X - 1) = 1$, et $e = 1$ sinon. Toute solution (X, Z) pour laquelle en fait $X - 1 = \pm\frac{B}{p^e}$ sera dite *solution particulière éventuelle*. On se propose de montrer les résultats suivant :

Théorème 7.1.1 *Supposons $q \neq p$ et $p \neq 1 \bmod 8$. On se fixe un entier v tel que $v = 1$ ou $v \neq 1$ et $\frac{q-1}{2}|v$. Si $v = 1$ on suppose que $B^2 \equiv 1 \bmod q$. Si $v \neq 1$, on suppose $q \nmid B$. Il existe une constante absolue effective C_0, telle que si l'équation*

$$X^p - 1 = B^v Z^q, X \neq 1. \tag{7.1}$$

admet une autre solution que la solution particulière éventuelle avec $p > C_0$, alors de deux choses l'une, soit $q|h_p^-$, soit il existe au moins un diviseur premier r de $X - 1$ tel que $r^2 \neq 1[q]$.

Corollaire 7.1.2 *On garde les hypothèses précédentes. Soient de plus des nombres premiers $l_1, \ldots, l_t$, distincts deux à deux, premiers à p et tels que $l_i^2 \equiv 1[q]$. Supposons qu'il existe des entiers $X, a_1, \ldots, a_t \in \mathbb{N}$ tels que*

$$X^p - 1 = B(l_1^{a_1} \ldots l_t^{a_t})^q. \tag{7.2}$$

On suppose $X \neq 1 \pm B^v$[1]. q est alors un diviseur premier de h_p^-.

[1]On peut remplacer cette hypothèse par "il existe i,tel que $l_i \neq 1[p]$."

Corollaire 7.1.3 *Soit $p \neq 3$, $p > 2$ un nombre premier, $p \neq 1[8]$. Soient de plus des nombres premiers $l_1, \ldots, l_t$, distincts deux à deux, et premiers à p, tels que $(l_i, 3) = 1$. Soit B un entier premier à 3. Supposons qu'il existe des entiers $X, a_1, \ldots, a_t \in \mathbb{N}$ tels que*

$$X^p - 1 = B(l_1^{a_1} \ldots l_t^{a_t})^3. \tag{7.3}$$

Alors de deux choses l'une, soit $29 \leq p < C_0$, soit $p \geq C_0$, et 3 est alors un diviseur premier de h_p^-. De plus $p \equiv 5[6]$.

Par exemple, si on prend $B = 2^5.5^2$ et si on prend p nombre premier tel que $p \neq 3$, $p \neq 1[8]$, $p = 2$ y compris, alors, l'équation diophantienne

$$X^p - 1 = 2^5.5^2(l_1^{a_1} \ldots l_t^{a_t})^6, \tag{7.4}$$

n'admet aucune solution entière $(X, a_1, \ldots, a_t)$ si $p < 23$, et $3|h_p^-$ si $p \geq C_0$. Le cas $p = 2$ résulte d'un résultat de Ribenboim (voir [65]).

Corollaire 7.1.4 *Soit $B \in \mathbb{N}^*$ tel que $q|\,(B^2 - 2)$ et $(p, B^2 - 1) = 1$. Soient de plus des nombres premiers $l_1, \ldots, l_t$, distincts deux à deux, premiers à p et tels que $l_i^2 \equiv 1[q]$. Supposons qu'il existe des entiers $X, a_1, \ldots, a_t \in \mathbb{N}$ tels que*

$$X^p - 1 = (B^2 - 1)(l_1^{a_1} \ldots l_t^{a_t})^q. \tag{7.5}$$

Alors, $q|h_p^-$.

Corollaire 7.1.5 *Soit $t \in \mathbb{N}^*$, soit $z \in [2, 20] - \{11\}$ un entier, soit l un nombre premier tel que $(l, q - 1) = 1$. On pose $B = z^t - 1$ ou $B = l^t - 1$. On suppose que $q|B^2 - 1$, et $(B, p) = 1$.*

Soient de plus des nombres premiers $l_1, \ldots, l_t$, distincts deux à deux, premiers à p et tels que $l_i^2 \equiv 1[q]$. Supposons qu'il existe des entiers $X, a_1, \ldots, a_t \in \mathbb{N}$ tels que

$$X^p - 1 = B(l_1^{a_1} \ldots l_t^{a_t})^q. \tag{7.6}$$

Alors, $q|h_p^-$.

Théorème 7.1.6 *Soient p, q deux nombres premiers impairs distincts tels que $q \geq 8(p-1)$, $p \equiv 3 \bmod 4$, et $q||B$. Soient $r \neq p$, $r \leq 10 \cdot q^{\frac{8q}{q-2}}$ un nombre premier d'ordre pair modulo p et $v > 0$ un entier. On suppose qu'il existe un entier $i \in \left\{1, \ldots, \frac{p-1}{2}\right\}$ tel que $p^2|(i+1)^p - 1 - i^p$. Soit $j \in \left\{1, \ldots, \frac{p-1}{2}\right\}$. On pose*

$$\epsilon_j = \left[\frac{(i+1)j}{p}\right] - \left[\frac{ij}{p}\right].$$

Supposons que $\mathcal{I}m\left(\sum_{j=1}^{\frac{p-1}{2}} \frac{\epsilon_j}{1-\zeta^{jp-2}}\right) \neq 0$.

S'il existe des entiers X, Z *tels que*

$$X^p - 1 = B\,(r^v Z)^q\,, \quad X \neq 1,$$

alors $q|h_{pq}^-$.

Exemple 7.1.7 *Pour* $p = 7$, *l'entier* $(i+1)^p - 1 - i^p$ *est divisible par* 7^2 *si* $i = 3$. *De plus* $\epsilon_j = 0$ *pour* $j = 1$ *et* 3, *et vaut* 1 *sinon. Soit* B *un entier dont aucun des facteurs premier ne vaut* 1 mod 7. *Soit* $q > 2$ *un premier,* $q \neq 7$, $q \nmid h_{7q}^-$, $q||B$. *Alors l'équation*

$$X^7 - 1 = BZ^q$$

admet pour seule solution entière $X = 1$, $Z = 0$.

Théorème 7.1.8 *Il existe un ensemble effectif* $\mathcal{C}$ *de couples de nombres premiers impairs distincts* (p, q), *tels que si l'équation*

$$X^p - 1 = B\,(r^v Z)^q\,, \quad X \neq 1,$$

admet une solution entière (X, Z), *l'entier* r *vérifiant*

$$\log(r^v) \geq \frac{16\log(16)}{17(\sqrt{17}-1)} + 64\log(q)\frac{1}{\left[\sqrt{\frac{q}{5}}\right]} + \frac{4\log(3)}{17},$$

alors $q|h_{pq}^-$.

7.2 preuve du théorème (7.1.1).

Il existe deux entiers C et Y premiers entre eux tels que

$$\frac{X^p - 1}{X - 1} = p^e Y^q, \quad X - 1 = \frac{BC^q}{p^e}, \quad C \neq 1.$$

Si $e = 1$, le théorème (1.1.1) montre que $q|h_p^-$. On peut donc supposer que $e = 0$. Supposons que $q \nmid h_p^-$. Raisonnons par l'absurde et supposons que pour tout diviseur premier r de C, on ait $r^2 \equiv 1[q]$. Alors $(X-1)^2 \equiv 1[q]$, car $B^{2v} \equiv 1 \bmod q$ vu que $(q, B) = 1$ et $q-1|2v$ (ou $v = 1$ et $B^2 \equiv 1 \bmod q$). q étant un nombre premier, on en déduit que $q|X$ ou $q|X-2$. Soit $\alpha = X - \zeta$. Comme il existe un entier Y tel que $\frac{X^p-1}{X-1} = Y^q$, et que les entiers algébriques $X - \zeta^c, c = 1, \ldots, p-1$ sont premiers entre eux deux à deux, il existe un idéal entier $\mathcal{I}$ de $\mathbb{Q}(\zeta)$ tel que $(\alpha) = \mathcal{I}^q$. Comme $(q, h_p^-) = (p, q) = 1$, il existe $\gamma \in \mathbb{Q}(\zeta)^*$ premier à $1 - \zeta$, tel que $\frac{\alpha}{\overline{\alpha}} = \left(\frac{\gamma}{\overline{\gamma}}\right)^q = \mu^q$. On pose $(\mu) = \mathfrak{a}\mathfrak{b}^{-1}$, où $\mathfrak{a}$ et $\mathfrak{b}$ sont des idéaux entiers premiers entre eux de $\mathbb{Q}(\zeta)$. Comme α et $\overline{\alpha}$ sont premiers entre eux, $(\alpha) = \mathfrak{a}^q$ et $(\overline{\alpha}) = \mathfrak{b}^q$.

Proposition 7.2.1 *([51], page 309) Soient p, q des nombres premiers impairs distincts. S'il existe X, Y des entiers, vérifiant $\frac{X^p-1}{X-1} = Y_1^q$, tels que $(X, Y_1, p, q) \neq ((3, 11, 5, 2))$, alors $(q, p-1) = 1$.*

En particulier, cette proposition montre que $\nu_{\mathfrak{p}}(\mu - 1) \geq 1$, $\mathfrak{p} = (1 - \zeta)$. Soit

$$\phi = \frac{X - \overline{\zeta}}{(1 - \overline{\zeta})^q} (\mu - 1)^q . \tag{7.7}$$

On a $\phi \in \mathbb{Z}[\zeta]$. En effet, il existe un idéal entier $\mathfrak{c}$ divisible par $\mathfrak{p}$, tel que $(\phi) = (\mathfrak{c}\mathfrak{p}^{-1})^q$. Soit également $\phi' = (X - \overline{\zeta})^{q-1} \left(\frac{\mu^q - 1}{\mu - 1}\right)^q$. On vérifie comme avant que $\phi' \in \mathbb{Z}[\zeta]$. On a $\phi\phi' = \frac{(X-\overline{\zeta})^q}{(1-\overline{\zeta})^q}(\mu^q - 1)^q = \left(\frac{\overline{\zeta}-\zeta}{1-\zeta}\right)^q$, qui est une unité de $\mathbb{Z}[\zeta]$. Donc ϕ définit une unité de $\mathbb{Z}[\zeta]$.

On a vu précédemment que $q|X$ ou $q|X - 2$. Supposons d'abord que $q|X$. D'après le théorème (6.1.1), $q^2|X$. Il existe donc une racine q-ième de l'unité ξ telle que dans $\mathbb{Z}_q[\zeta]$ on ait

$$\mu = \xi\zeta^{2r_0} \left(\frac{1 - x\zeta}{1 - x\zeta^{-1}}\right)^{1/q} . \tag{7.8}$$

où r_0 vérifie $r_0 q \equiv 1[p]$ (Rappelons que $q \neq p$). En effet, soit r_0 un tel entier. On a

$$\begin{aligned} \mu^q &= \frac{\alpha}{\overline{\alpha}} \\ &= \frac{X - \zeta}{X - \overline{\zeta}} \\ &= \zeta^2 \left(\frac{1 - \overline{\zeta}X}{1 - \zeta X}\right) \end{aligned} \tag{7.9}$$

Il existe donc une racine q-ième de $\mathbb{Q}_q(\zeta)$, disons ξ, telle que $\mu = \xi\zeta^{2r_0} \left(\frac{1-\overline{\zeta}X}{1-\zeta X}\right)^{1/q}$.

Comme $\mathbb{Q}_q(\xi)$ est totalement ramifiée et se plonge dans $\mathbb{Q}_q(\zeta)$ non ramifiée car $q \neq p$, on en déduit que $\xi \in \mathbb{Q}_q$. Comme $q \neq 2$, on en déduit que $\xi = 1$. On a donc

$$\mu = \zeta^{2r_0} \left(\frac{1 - X\overline{\zeta}}{1 - X\zeta}\right)^{1/q} . \tag{7.10}$$

On obtient

$$\mu = \zeta^{2r_0} \left(1 + (\zeta - \zeta^{-1})\frac{x}{q} + \mathcal{O}((x/q)^2)\right) . \tag{7.11}$$

En substituant ce développement dans (7.7), on trouve, qu'il existe une unité ϕ' de $\mathbb{Z}[\zeta]$ telle que

$$\phi' = 1 - \left(\frac{\zeta^{2r_0-1} - \zeta}{\zeta^{2r_0} - 1}\right) x + \mathcal{O}(qx). \tag{7.12}$$

On pose $\chi_{r_0} = \frac{\zeta - \zeta^{2r_0-1}}{\zeta^{2r_0}-1}$. Soit $\mathcal{N}$ l'élément norme de $\mathbb{Z}[\zeta]$. On a $\mathcal{N}(\phi') = \pm 1$. Comme $q \neq 2$ et que $q|X$, on a en fait que $\mathcal{N}(\phi') = 1$, donc $q|\mathbf{Tr}(\sigma_q(\chi_{r_0}))$. Supposons d'abord que $r_0 \neq 1[q]$. Soit $n \in \{1, \ldots, p-1\}$ un représentant de $q-2$ modulo p. On a

$$\mathbf{Tr}(\sigma_q(\chi_{r_0})) = a_n - (n+1), \tag{7.13}$$

où $a_n = 0$ si n est impair et $a_n = p$ sinon. Supposons d'abord $q > p$. Alors $n = q - 2 - mp$ avec $m \geq 0$. Si n est impair, alors par (7.13), $\mathbf{Tr}(\sigma_q(\chi_{r_0})) = mp - (q-1) \equiv mp + 1[q]$ et $0 < mp + 1 < q$ car $n > 0$. Si $2|n$, alors $\mathbf{Tr}(\sigma_q(\chi_{r_0})) = p - (n+1) = (m+1)p + 1 - q$ avec $mp + 1 + p < 2q$. Donc si $q|\mathbf{Tr}(\sigma_q(\chi_{r_0}))$, on en déduit que $mp + 1 + p = q$ et donc $q \equiv 1[p]$. Alors $r_0 = 1$ et

$$\phi' = 1 - \binom{1/q}{2} x^2 + \mathcal{O}\left(\frac{x^3}{q^3}\right). \tag{7.14}$$

En prenant la norme, on trouve $(p-1)\binom{1/q}{2} x^2 = \mathcal{O}\left(\frac{x^3}{q^3}\right)$ ce qui est impossible q-adiquement vu que $q^2|X$ et $p \neq 1[q]$. Supposons $q < p$. Alors $n = q - 2$. n est alors impair, et on a $\mathbf{Tr}(\sigma_q(\chi_{r_0})) = 1 - q$ pemier à q. Il reste le cas où $q|X - 2$. On a le lemme suivant :

Lemme 7.2.2 *Soient p, q deux nombres premiers impairs distincts tels que $p \neq 1[8]$ et $(q, h_p^-) = 1$. Il existe une constante absolue c_0, telle que si $p > c_0$, et si (X, Y, p, q) est une solution de $\frac{X^p-1}{X-1} = Y^q$, alors $X \equiv f[q^2]$, où $f \in \{-1, 0, 1\}$.*

Preuve (du lemme) Comme $p \neq 1[8]$, par [19], on a $q \ll plog(p)^2$. Donc, il existe une constante absolue c_0, telle que pour $p > c_0$, on ait $q < Sup\left(p, \frac{p(p-20)}{16}\right)$. Comme $(q, h_p^-) = 1$, on peut donc appliquer le théorème (6.1.1), qui donne le résultat.□

Donc en fait $(q, X(X-2)) = 1$. On en déduit qu'il existe un diviseur premier r de C tel que $r^2 \equiv 1[q]$. ■

7.2.1 preuve du corollaire (7.1.3).

Supposons $p \geq C_0$. Alors, si h_p^- est premier à 3, on déduit que $X = 1$ ou $X = 3$. Le cas $X = 1$ est impossible et donc $X = 3$. On est donc ramené à une équation de la forme $3^p - 1 = 2Z^3, Z \neq 0$, qui est sans solution par [50]. Donc $3|h_p^-$. De plus, par un théorème de Nagell-Ljunggren, on a aussi $p \equiv 5[6]$. En effet, ils ont montré que si x, y, n sont solutions de $\frac{x^n-1}{x-1} = y^3$, il n'y a pas d'autres solution que $x = 18, n = 3$, si $n \neq 5[6]$. Comme ici, $p \neq 3$ et que l'on est dans le cas où $\frac{X^p-1}{X-1} = Y^3$ admet une solution non triviale autre que celle précédemment citée, on doit donc avoir $p \equiv 5[6]$, ainsi que $p \geq 29$ dans le cas général. En effet, il a été montré (voir [24]) que si $\frac{x^n-1}{x-1} = y^q$ admet une autre solution que celles déjà connues, alors n admet au moins un facteur premier supèrieur ou égal à 29. Comme ici $n = p$ avec p premier et $p > 3$, on a $p \geq 29$.□

7.2.2 preuve du corollaire (7.1.4).

La démonstration est la même que précédemment. En effet, comme $X \in \mathbb{N}$, si q ne divise pas h_p^-, on a $X = B^2$. En effet, comme $(p, B) = 1$, on a $e = 0$. Donc l'équation de Nagell-Ljunggren $\frac{X^p-1}{X-1} = Y^q$ admet une solution telle que X est un carré d'entier, en contradiction avec [23]

7.2.3 preuve du corollaire (7.1.5).

Idem que précédemment sauf qu'on utilise le théorème 1 de [22].

7.3 Sur l'équation $X^p - 1 = B(r^v E)^q$.

Fixons deux nombres premiers impairs distincts p et q, $q > 8(p-1)$. Supposons que l'on puisse trouver deux entiers X, Z tels que

$$X^p - 1 = BZ^q,$$

l'entier B étant supposé avoir tous ses facteurs premiers ne valant pas 1 mod p, si $B \neq \pm 1$. Il existe deux entiers C et D premiers entre eux et un entier $e \in \{0, 1\}$, tels que

$$\frac{X^p - 1}{X - 1} = p^e D^q, \quad X - 1 = \frac{B}{p^e} C^q.$$

On pose $u_c = \frac{p}{\pi_1^{\sigma_c}}$. $\mathcal{I}$ désigne l'idéal de Stickelberger de $\mathbb{K}$. Soit $\theta \in \mathcal{I}$. Rappelons que l'on définit le quotient de Fermat $\phi(\theta) \in \mathbb{F}_p$ via $\zeta^\theta = \zeta^{\phi(\theta)}$. Le module de Fermat I_f est défini comme les éléments positifs de $\mathcal{I}$, qui annulent le quotient de Fermat. Rappelons quelques définitions.

Definition 7.3.1 *Si $\Theta = \sum_i a_i \sigma_i$ est un élément de l'idéal de Stickelberger de $\mathbb{Q}(\zeta)$, on appelle poids relatif de Θ l'entier relatif noté $\varsigma(\Theta)$ et défini par*

$$(1 + j)\Theta = \varsigma(\Theta)\mathcal{N}, \tag{7.15}$$

où $\mathcal{N} = \sum_{\sigma \in G} \sigma$. Le poids de Θ est l'entier relatif noté $W(\Theta)$ et défini par $W(\Theta) = \sum_i a_i$. La norme de θ, notée $||\theta||$ est définie par $||\theta|| = \sum_i |a_i|$.

En particulier, on a $2W(\Theta) = \varsigma(\Theta)(p-1)$.

Definition 7.3.2 *Soit $f(T) = \sum_k a_k T^k$ une série à coefficients complexes, et soit $g(T) = \sum_k A_k T^k$ une série à coefficients positifs. On dit que f est dominée par g et on note $f \ll q$ si et seulement si $\forall k \geq 0, |a_k| \leq A_k$.*

Soit $\Theta \in \mathbb{Z}[G]$. On pose

1. $f[\Theta, T] = \left(1 + \frac{1}{1-\zeta}T\right)^{\Theta/q} = \sum_{k=0}^{\infty} a_k[\theta]T^k$,
2. $b_k[\theta] = p^k k! q^k a_k[\theta]$,
3. $\rho[\sum_c \eta_c \sigma_c] = \sum_c \eta_c u_c \in \mathbb{Z}[\zeta]$.
4. $||\sum_c \eta_c \sigma_c|| = \sum_c |\eta_c|$.

On a

Proposition 7.3.3 *Soit $\theta \in \mathbb{Z}[G]$. On a les assertions suivantes :*

1. $|a_k[\theta]| \leq p^k(-1)^k\binom{-||\theta||/q}{k}$,
2. $b_k[\theta] \in \mathbb{Z}[\zeta]$.
3. $b_k[\theta] \equiv \rho[\theta]^k mod[q]$.

Preuve Montrons d'abord l'assertion (1). Si $\theta = \eta\sigma_c$, alors $a_k[\theta] = \frac{1}{\pi_1^{k\sigma_c}}\binom{\eta/q}{k}$, d'où le résultat dans ce cas. On a alors $f[\theta, T] \ll (1-T)^{-\eta/q}$. Une telle relation est stable au produit des séries entières. Le cas général s'en déduit.

Montrons l'assertion (2). Supposons d'abord que $\theta = \eta\sigma_c$. Alors

$$b_k[\theta] = q^k k! p^k a_k[\theta] = \frac{p^k}{\pi_1^{k\sigma_c}} q^k \prod_{l=0}^{k-1} \frac{\eta}{q} - l \in \mathbb{Z}[\zeta]$$

car $\frac{p^k}{\pi_1^{k\sigma_c}} \in \mathbb{Z}[\zeta]^\times$. Raisonnons par récurrence sur le poids de θ. Posons $\theta = \theta_1 + \theta_2$ et supposons le résultat vrai pour $b_k[\theta_i], i = 1, 2$. On a la relation suivante :

$$a_k[\theta] = \sum_{l=0}^{k} a_l[\theta_1] a_{k-l}[\theta_2]. \tag{7.16}$$

On a alors

$$\begin{aligned} b_k[\theta] &= q^k k! p^k \sum_{l=0}^{k} a_l[\theta_1] a_{k-l}[\theta_2] \\ &= \sum_{l=0}^{k} \binom{k}{l} q^l l! p^l a_l[\theta_1] q^{k-l}(k-l)! p^{k-l} a_{k-l}[\theta_2] \in \mathbb{Z}[\zeta]. \end{aligned} \tag{7.17}$$

par hypothèse de récurrence.

Montrons l'assertion (3). Supposons d'abord que $\theta = \eta\sigma_c$. Alors

$$b_k[\theta] = \left(\frac{p}{\pi^{\sigma_c}}\right)^k \eta(\eta - q)\dots(\eta - q(k-1)) \equiv (u_c\eta)^k\,[q].$$

Dans le cas général, on raisonne par récurrence sur le poids de θ. On pose $\theta = \theta_1 + \theta_2$. On a alors

$$\begin{aligned} b_k[\theta] &= q^k k! p^k \sum_{l=0}^{k} a_l[\theta_1] a_{k-l}[\theta_2] \\ &= \sum_{l=0}^{k} \binom{k}{l} q^l l! p^l a_l[\theta_1] q^{k-l}(k-l)! p^{k-l} a_{k-l}[\theta_2] \\ &\equiv \sum_{l=0}^{k} \binom{k}{l} \rho[\theta_1]^k \rho[\theta_2]^{k-l}[q] \\ &\equiv (\rho[\theta_1] + \rho[\theta_2])^k \equiv \rho[\theta]^k. \end{aligned} \tag{7.18}$$

□

Soit $\alpha = \frac{X-\zeta}{(1-\zeta)^e}$. Si p est premier à $X-1$, ie si $e=0$, on pose $c_X \equiv \frac{1}{X-1}[p]$ et si $p|X-1$, ie si $e=1$, on pose $c_X = 0$. D'après (1), il existe un idéal entier J de $\mathbb{Z}[\zeta]$ tel que $(\zeta^{(1-e)c_x}\alpha) = (\alpha) = J^q$. Soit alors $\theta \in \mathcal{I}^+$ (éléments de $\mathcal{I}$ à coefficients positifs)tel que $2|\varsigma(\theta)$ (voir la définition (7.3.1)). Il existe $\beta[\theta] \in \mathbf{J}$ tel que $((\zeta^{(1-e)c_x}\alpha)^\theta) = (\beta[\theta]^q)$. Par la proposition (4.4.13), il existe un entier v et $\epsilon = \pm 1$, tels que

$$(\zeta^{(1-e)c_x}\alpha)^\theta = \epsilon\zeta^v\beta[\theta]^q \tag{7.19}$$

On a le lemme suivant :

Lemme 7.3.4 *On a $\epsilon\zeta^v = 1$.*

Preuve Supposons d'abord que $e=0$. Il existe $\epsilon = \pm 1$ et $v \in \mathbb{Z}$ tels que

$$(\zeta^{c_x}\alpha)^\theta = \epsilon\zeta^v\beta[\theta]^q.$$

On a

$$\zeta^{c_X} = (1 + \zeta - 1)^{c_X} = (1 + c_X(\zeta - 1) + \mathcal{O}(\pi_1^2)).$$

On a alors

$$\begin{aligned} \zeta^{c_X}\alpha &= (1 + c_X(\zeta-1))(X - 1 + 1 - \zeta) + \mathcal{O}(\pi_1^2) \\ &= X - 1 + 1 - \zeta + c_X(\zeta-1)(X-1) + \mathcal{O}(\pi_1^2) \\ &= X - 1 + \mathcal{O}(\pi_1^2) \end{aligned} \tag{7.20}$$

car $c_X(X-1) \equiv 1[p]$ et en particulier $1-\zeta+c_X(X-1)(\zeta-1) = \mathcal{O}(\pi_1^2)$. On a donc $(\zeta^{c_X}\alpha)^\theta = (X-1)^{W(\theta)} + \mathcal{O}(\pi_1^2) = 1 + \mathcal{O}(\pi_1^2)$, car $p-1|W(\theta)$ vu que $2|\varsigma(\theta)$ par hypothèse. D'après la relation d'Iwasawa, on a aussi $\beta[\theta] \equiv 1[\pi_1^2]$. Par conséquent, l'unité $\epsilon\zeta^v$ vérifie $\epsilon\zeta^v \equiv 1[\pi_1^2]$. Donc $\epsilon = 1$ et $p|v$, ie $\epsilon\zeta^v = 1$. Supposons maintenant que $e = 1$. On a alors $\alpha^\theta = \epsilon\zeta^v\beta[\theta]^q$. Comme $\alpha \equiv 1[\pi_1^2]$ et $\beta[\theta] \equiv 1[\pi_1^2]$ par la relation d'Iwasawa, on en déduit $\epsilon\zeta^v \equiv 1[\pi_1^2]$, ie $p|v$ et $\epsilon = 1$.□

Donc, si $\theta \in \mathcal{I}$ de poids relatif pair, alors

$$(\zeta^{(1-e)c_x}\alpha)^\theta = \beta[\theta]^q. \tag{7.21}$$

Montrons maintenant le lemme suivant :

Lemme 7.3.5 *Soit $\theta \in \mathcal{I}$. On a*

$$(1-\zeta)^{4\theta} = \zeta^{2\phi(\theta)}p^{2\varsigma(\theta)}. \tag{7.22}$$

Preuve Il suffit de prouver (3.25) pour $\theta = \psi$, avec ψ un élément de Fueter. Pour ψ, on a de manière générale que $\varsigma(\psi) = 1$ ie $(1+j)\psi = \mathcal{N}$. On a d'une part

$$(1-\zeta)^{2j\psi} = (1-\zeta)^{2\mathcal{N}-2\psi} = p^2(1-\zeta)^{-2\psi}.$$

D'autre part

$$(1-\zeta)^{2j\psi} = (1-\zeta^{-1})^{2\psi} = \zeta^{-\phi(2\psi)}(-1)^{2W(\psi)}(1-\zeta)^{2\psi}.$$

Donc

$$(1-\zeta)^{4\psi} = p^2\zeta^{\phi(2\psi)} = p^{2\varsigma(\psi)}\zeta^{2\phi(\psi)}.$$

□

Lemme 7.3.6 *Le module de Fermat I_f du p-ième corps cyclotomique contient un élément positif de poids $p-1$.*

Preuve Si I_f contient un élément de Fueter ψ, alors 2ψ convient. Supposons que les éléments de Fueter ne soit pas dans le module de Fermat. Soient ψ_1, ψ_2 deux éléments de Fueter quelconques. Posons $\phi_i = \phi(\psi_i)$ et

$$\theta = \sigma_{\phi_2}\psi_1 + \sigma_{-\phi_1}\psi_2.$$

C'est un élément de I_f de poids $p-1$.□

On se fixe pour la suite $\theta = 8\theta_0$, où θ_0 est un élément du module de Fermat de poids $p-1$ donné par le lemme précéent. On a

$$\beta[\theta_0]\overline{\beta[\theta_0]} = y^2. \tag{7.23}$$

En effet, on a

$$\beta[\theta_0]^q\overline{\beta[\theta_0]^q} = \alpha^{\theta_0(1+j)} = \alpha^{\varsigma(\theta_0)\mathcal{N}} = y^{2q}.$$

Lemme 7.3.7 *Soit $\theta \in \mathcal{I}^+$, et soit $\theta' \in \mathbb{N}[G]$. Alors*

$$\beta[\theta'\theta] = \beta[\theta]^{\theta'}. \tag{7.24}$$

Preuve On a

$$\begin{aligned}\beta[\theta\theta']^q &= \left(\zeta^{(1-e)c_X}\alpha\right)^{\theta\theta'} \\ &= \beta[\theta]^{q\theta'}.\end{aligned} \tag{7.25}$$

Comme $(q, 2p) = 1$, on a le résultat.□

Remarque 7.3.8 *Le résultat précédent reste vrai si $p = q$ via la relation d'Iwasawa.*

En particulier, avec $\theta' = 2$, et en utilisant (3.27) et le fait que $\theta_0 \in I_f$, on obtient

$$\begin{aligned}\beta[8\theta_0]^q &= \beta[4\theta_0]^{2q} \\ &= \beta[4\theta_0]^q\frac{y^{8q}}{\overline{\beta[4\theta_0]}^q} \\ &= y^{8q}\frac{(\zeta^{(1-e)c_x}\alpha)^{4\theta_0}}{(\zeta^{(1-e)c_x}\alpha)^{j4\theta_0}} = y^{8q}\frac{\left(1+\frac{X-1}{1-\zeta}\right)^{4\theta_0}}{\left(1+\frac{X-1}{1-\zeta}\right)^{4j\theta_0}}\end{aligned} \tag{7.26}$$

la dernière égalité étant due au fait que $(1-\zeta)^{4\theta_0} = p^4$ et donc $\frac{(1-\zeta)^{4\theta_0}}{(1-\zeta)^{4j\theta_0}} = 1$. On a donc

$$\beta[8\theta_0]^q = y^{8q}\left(1+\frac{X-1}{1-\zeta}\right)^{4(1-j)\theta_0}. \tag{7.27}$$

Supposons que C soit divisible par un nombre premier $r \neq p$. Soit $\mathcal{K} = \mathbb{Q}_r(\zeta)$. C'est une extension galoisienne de $\mathbb{Q}_r$ non ramifiée, de groupe de Galois noté $D(r)$, d'ordre l'ordre de r modulo p. On se place dans $\mathcal{K}$. D'après (7.27), il existe une racine q-ième de l'unité ξ telle que

$$\beta[8\theta_0] = \xi y^8\left(1+\frac{X-1}{1-\zeta}\right)^{4(1-j)\theta_0/q}. \tag{7.28}$$

La série précédente est convergente dans $\mathcal{K}$ car $r^q|X-1$. Soit $\mathcal{L} = \mathbb{Q}_r(\xi)$. On désigne par $\mathcal{S}$ un système de représentants du groupe quotient $G/D(r)$. On désigne par $\mathcal{N}_r$ la norme de

l'extension $\mathcal{K}/\mathbb{Q}_r$. Soit $S = \mathrm{Gal}(\mathbb{Q}_r(\zeta)/\mathbb{Q}_r(\xi))$. Soit $N(r,q)$ l'ordre de ce groupe. r et q étant fixés, on notera N cet ordre. On pose $S = \{\sigma_{a_1}, \ldots, \sigma_{a_N}\}$. Soient $\theta_i = 8\sigma_{a_i}(1-j)\theta_0, i \in \{1,\ldots,N\}$ et $\theta_i' = 4(1-j)\sigma_{a_i}\theta_0, i \in \{1,\ldots,N\}$. On définit pour la suite, la matrice $\mathcal{A}$ suivante :

$$\mathcal{A}(\theta_0) = (b_{k-1}[\theta_i])_{1\leq k,i\leq N}\,.$$

Posons $\theta = 4(1-j)\theta_0$. On a avec les notations de la proposition (7.3.3)

$$\beta[8\theta_0] = \xi y^8 \sum_{k=0}^{+\infty} a_k[\theta](X-1)^k. \tag{7.29}$$

Par la proposition (7.3.3), $b_k[\theta] \in \mathbb{Z}[\zeta]$. Mais $b_k[\theta] = (pq)^k k! a_k[\theta]$. Donc

$$v_r(k!) + k\delta_{k,q} + v_r(a_k[\theta]) \geq 0, \tag{7.30}$$

ie, en appliquant le théorème de Legendre

$$v_r(a_k[\theta]) \geq -2k. \tag{7.31}$$

Comme $C^q | X-1$ et $r^v | C$, on en déduit les minorations suivantes

$$v_r(a_k[\theta](X-1)^k) \geq k(qv-2), \tag{7.32}$$

Soit $L \in \mathbb{N}^*$. On a donc

$$\frac{\beta[8\theta_0]}{\xi y^8} = \sum_{k=0}^{L-1} a_k[\theta](X-1)^k + \mathcal{O}(r^{L(qv-2)}). \tag{7.33}$$

Soit $R(p,q)$ un entier tel que, $\mathcal{A}'$, la sous-matrice de $\mathcal{A}$ formée des R-premières lignes et colonnes de $\mathcal{A}$, soit inversible. p et q étant fixés, on pose $R = R(p,q)$. Donnons un exemple où il est possible de choisir $R > 1$:

Lemme 7.3.9 *On suppose qu'il existe un entier $i \in \left\{1,\ldots,\frac{p-1}{2}\right\}$ tel que*

$$p^2 | (i+1)^p - 1 - i^p.$$

Soit $j \in \left\{1,\ldots,\frac{p-1}{2}\right\}$. On pose

$$\epsilon_j = \left[\frac{(i+1)j}{p}\right] - \left[\frac{ij}{p}\right].$$

Supposons que $\mathcal{I}m\left(\sum_{j=1}^{\frac{p-1}{2}} \frac{\epsilon_j}{1-\zeta^{jp-2}}\right) \neq 0$ et que r soit d'ordre pair modulo p. Alors on peut prendre $R > 1$.

Preuve Comme $(i+1)^p - 1 - i^p \equiv 0 \bmod p^2$, la proposition (4.5.15) montre que l'élément de Fueter ψ_i est un élément de I_f. On peut donc prendre $\theta_0 = 2\psi_i$. Si on ne pouvait prendre $R = 2$ quelque soit le choix des a_i, alors, vu que la première ligne de la matrice $\mathcal{A}$ est constituée de 1, on aurait $a_1[4(1-j)\theta_0] = a_1[4(1-j)\sigma_{a_t}\theta_0]$ pour tout t. En particulier, comme r est d'ordre pair modulo p, en prenant $a_t = -1$, il viendrait

$$a_1[4(1-j)\theta_0]^j = a_1[4(1-j)\theta_0].$$

Or, de façon générale $a_1[4(1-j)\theta_0]^j = -a_1[4(1-j)\theta_0]$. On aurait donc $a_1[4(1-j)\theta_0] = 0$, c'est à dire $\mathcal{I}m\left(\sum_{j=1}^{\frac{p-1}{2}} \frac{\epsilon_j}{1-\zeta^{jp-2}}\right) = 0$.□

Soit $C(p,q) = det(\mathcal{A}')$. p et q étant fixés, on pose $C = C(p,q)$. Considérons le système linéaire suivant

$$\forall k \in \{0, \ldots, R-1\}, \sum_{i=1}^{R} \lambda_i b_k[\theta_i] = \delta_{R-1,k}, \tag{7.34}$$

où $\delta_{i,j}$ est le symbole de Kronecker en (i,j), ie $\delta_{i,j} = 1$ si $i = j$ et $\delta_{i,j} = 0$ sinon. Soit $\mathcal{A}_i$ la matrice de taille R^2 dont les colonnes sont celles de $\mathcal{A}'$ sauf celle d'indice i, qui est égale au vecteur colonne correspondant au second membre de (7.34). Par les formules de Cramer, $\lambda_i = \frac{det(\mathcal{A}_i)}{D}$. On pose

$$\Lambda_i = det(\mathcal{A}_i) \in \mathbb{Z}[\zeta]. \tag{7.35}$$

et

$$\Delta(\theta_0) = \sum_{i=1}^{R} \Lambda_i \beta[8\sigma_{a_i}\theta_0]. \tag{7.36}$$

Comme $\sigma_{a_i} \in \mathrm{Gal}(\mathbb{Q}_r(\zeta)/\mathbb{Q}_r(\xi))$, de la relation (7.29) on a

$$\frac{\beta[8\sigma_{a_i}\theta_0]}{\xi y^8} = \sum_{k=0}^{R-1} a_k[\theta_i'](X-1)^k + \mathcal{O}(r^{R(qv-2)}). \tag{7.37}$$

Dans la suite, le terme $\mathcal{O}_{r,R}$ désigne un $\mathcal{O}(r^{R(qv-2)})$. On pose aussi $D = det(\mathcal{A}')$.

$$\begin{aligned}
\frac{1}{\xi y^8}\Delta(\theta_0) = \sum_{i=1}^{R} \frac{1}{\xi y^8}\beta[8\sigma_{a_i}\theta_0]\Lambda_i &= \sum_{i=1}^{R} \Lambda_i \sum_{k=0}^{R-1} a_k[\theta_i'](X-1)^k + \mathcal{O}_{r,R} \\
&= \sum_{k=0}^{R-1} \frac{det(\mathcal{A})(X-1)^k}{(pq)^k k!} \sum_{i=1}^{R} \lambda_i b_k[\theta_i'] + \mathcal{O}_{r,R} \\
&= \sum_{k=0}^{R-1} \frac{det(\mathcal{A})(X-1)^k}{(pq)^k k!}\delta_{R-1,k} + \mathcal{O}_{r,R} \\
&= \frac{det(\mathcal{A})(X-1)^{R-1}}{(pq)^{R-1}(R-1)!} + \mathcal{O}_{r,R}.
\end{aligned} \tag{7.38}$$

Lemme 7.3.10 *On a $\Delta(\theta_0) \neq 0$ dans les deux cas suivant*

1. *$R = 2$, $p \equiv 3 mod 4$, $q \nmid h_p^-$, $q||B$;*
2. *$R > 1$, B a un facteur premier r' premier à $det(\mathcal{A})$ tel que*

$$\nu_{r'}(B) > 2R - \nu_{r'}((R-1)!);$$

Preuve Etudions maintenant le premier cas. Supposons que l'on puisse avoir $\Delta(\theta_0) = 0$. Comme $q|X-1$ (car $q|B$), $p \equiv 3 \bmod 4$ et $q \nmid h_p^-$ le théorème (6.1.1) montre que $q^2|X-1$. Comme $q||B$, c'est donc que $q|C$ et $\nu_q(X-1) \geq q+1$. Le système linéaire (7.34) est formel, ie que la combinaison linéaire des séries formelles $\sum_i \Lambda_i \left(1 + \frac{T}{1-\zeta}\right)^{\theta/q}$, a pour premier coefficient non nul, celui d'indice $R-1$. Les calculs précédents appliqués à $r' = q$ donnent $(R = 2)$

$$\frac{det(\mathcal{A})(X-1)}{pq} = \mathcal{O}\left(q^{2(\nu_q(X-1)-2)}\right),$$

ie

$$\nu_q(D) + 3 \geq \nu_q(X-1) \geq q+1. \tag{7.39}$$

L'inégalité de Hadamard montre que $|D| \leq p^4 q^2$. Cette majoration est valable pour les conjugués de D sous le groupe $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. On a donc

$$|\mathcal{N}(D)| \leq \left(p^4 q^2\right)^{p-1}.$$

En particulier, il vient $(p < q)$: $\nu_q(D) \leq 6(p-1)$. L'inégalité (7.39) donne $q+1 \leq 6p-3$ en contradiction avec $q \geq 8(p-1)$.

Pour le second cas, $\Delta(\theta_0) = 0$ donne dans $\mathbb{Q}_{r'}(\zeta)$

$$\nu_r(X-1) \leq 2R - \nu_r((R-1)!).$$

d'où

$$\nu_r(B) \leq \nu_r(X-1) \leq 2R - \nu_r((R-1)!).$$

□

Soit s un élément fixé de $\mathcal{S}_r$, système de représentants du groupe quotient $G/D(r)$.

Faisons agir s sur $\Delta(\theta_0)$. Comme $b_k[\theta]^s = b_k[s\theta]$ et $\beta[\theta]^s = \beta[s\theta]$, on a

$$\begin{aligned}\Delta(\theta_0)^s &= \sum_{i=1}^{R} \Lambda_i^s \beta[s\theta_i'] \\ &= \sum_{k=0}^{R-1} \frac{det(\mathcal{A})^s (X-1)^k}{(pq)^k k!} \sum_{i=1}^{R} \lambda_i^s b_k[s\theta_i'] + \mathcal{O}_{r,R} \\ &= \sum_{k=0}^{R-1} \frac{det(\mathcal{A})^s (X-1)^k}{(pq)^k k!} \sum_{i=1}^{R} \lambda_i^s b_k[\theta_i']^s + \mathcal{O}_{r,R} \\ &= \frac{det(\mathcal{A})^s (X-1)^{R-1}}{(pq)^{R-1}(R-1)!} + \mathcal{O}_{r,R}.\end{aligned} \tag{7.40}$$

On a donc en notant f_r l'inertie de r dans l'extension $\mathbb{Q}(\zeta)/\mathbb{Q}$:

$$\begin{aligned}\mathcal{N}(\Delta(\theta_0)) &= \prod_{s \in \mathcal{S}_r} \Delta(\theta_0^{s\mathcal{N}_r}) \\ &= \mathcal{O}(r^{(qv-2)(N-1)f_r|\mathcal{S}_r|}) \\ &= \mathcal{O}(r^{(qv-2)(N-1)(p-1)}).\end{aligned} \tag{7.41}$$

Si $\Delta(\theta_0) \neq 0$, on en déduit

$$\mathcal{N}(\Delta(\theta_0)) \geq r^{(qv-2)(R-1)(p-1)}. \tag{7.42}$$

Il nous reste à majorer $\Delta(\theta_0)$. Majorons d'abord les $b_k[\theta_i']$. On a via la proposition (7.3.3) si $q \geq 8(p-1)$:

$$|b_k[\theta_i']| \leq p^{2k} q^k k!. \tag{7.43}$$

Proposition 7.3.11 (Inégalité de Hadamard.) *Soit $A \in \mathcal{M}_n(\mathbb{C})$. Soit X_i la colonne d'indice i de A. Soit $|X_i| = \sqrt{X_i X_i^*}$ la norme euclidienne standard. Alors*

$$|det(\mathcal{A})| \leq \prod_{i=1}^{n} |X_i|. \tag{7.44}$$

Par (7.43), on en déduit

$$|\Lambda_i| = |det(\mathcal{A}_i)| \leq (p^2 q)^{R\frac{(R-1)}{2}} (R-1)^{\frac{1}{2}(R-2)(R-1)}. \tag{7.45}$$

En appliquant (7.45), il vient

$$|\Delta(\theta_0)| \leq R|y|^8 (p^2 q)^{R\frac{(R-1)}{2}} (R-1)^{\frac{1}{2}(R-2)(R-1)}. \tag{7.46}$$

En combinant (7.46) et (7.42), puis en prenant le log, on trouve

$$(q-2)log(r)(R-1) \leq 8log(|D|) + \left(1 + \frac{1}{2}(R-2)(R-1)\right) log(R) + R(R-1)log(p(p-1)). \tag{7.47}$$

7.3.1 démonstration du théorème (7.1.6).

Supposons que $q \nmid h_{pq}^-$. En particulier $q \nmid h_p^-$, donc $p \nmid X-1$ par le théorème (1.1.1). Comme r est d'ordre pair modulo p, en particulier $r \neq 1 \bmod p$. Le lemme (5.3.13) montre donc que $r^v | X-1$. Il existe donc deux entiers C et D premiers entre eux tels que

$$X - 1 = B\,(r^v C)^q\,, \quad \frac{X^p - 1}{X - 1} = D^q.$$

Les hypothèses du théorème permettent de reprendre les calculs du paragraphe précédent : l'inégalité (7.47) a lieu avec $R = 2$ et avec ces entiers r et D.

Comme $q \nmid h_{pq}^-$, le théorème (6.1.22) appliqué avec $Y_0 = -1$ montre que

$$|X| \leq 8 \left(\frac{2}{5} q p^{\frac{1}{p-1}}\right)^q.$$

Comme $\frac{X^p-1}{X-1} = D^q$ et $p < q$, on a $|D| \leq 2|X| \leq 16 \left(\frac{2}{5} q p^{\frac{1}{p-1}}\right)^q$. En appliquant (7.47), on en déduit

$$r < 10 \cdot q^{\frac{8q}{q-2}}.$$

en contradiction avec les hypothèses.

7.3.2 démonstration du théorème (7.1.8).

Soit (p, q) un couple de deux nombres premiers impairs distincts tel que l'on puisse choisir $R \geq \sqrt{\frac{q}{5}} + 1$ (rappelons que $q < (p-1)^2$; voir [54]). Notons $\mathcal{C}$ l'ensemble des ces couples.

Supposons que $q \nmid h_{pq}^-$. Soient X, Z des entiers tels que

$$X^p - 1 = B\,(r^v Z)^q\,.$$

Il existe deux entiers C et D premiers entre eux tels que

$$X-1 = B\left(r^v C\right)^q, \quad \frac{X^p-1}{X-1} = D^q,$$

avec $|D| \leq 16\left(\frac{2}{5}qp^{\frac{1}{p-1}}\right)^q$. L'inégalité (7.47) montre alors

$$(qv-2)\log(r)(R-1) \leq 8log(|D|) + \left(1+\frac{1}{2}(R-2)(R-1)\right)log(R) + R(R-1)log(p(p-1)),$$

ie

$$q\log(r^v)(R-1) \leq 16log(|D|) + (2+(R-2)(R-1))\,log(R) + 2R(R-1)log(p(p-1)).$$

On en déduit

$$\log(r^v) \leq \frac{16\log(16)}{17(\sqrt{17}-1)} + 32\log(q)\left(\frac{1}{R-1} + 5\frac{R-1}{q}\right) + \frac{4\log(3)}{17},$$

ie

$$\log(r^v) \leq \frac{16\log(16)}{17(\sqrt{17}-1)} + 64\log(q)\frac{1}{\left[\sqrt{\frac{q}{5}}\right]} + \frac{4\log(3)}{17},$$

d'où le théorème.

Remarque 7.3.12 *Le choix de la valeur $R \geq \sqrt{\frac{q}{5}}+1$ minimise la quantité $\frac{1}{R-1} + 5\frac{R-1}{q}$ en $R = \left[\sqrt{\frac{q}{5}}\right]+1$.*

Chapitre 8

Deux nouvelles démonstrations de la valeur de la signature du Frobenius d'un corps fini ; application.

8.1 Introduction et notations.

Si I est un ensemble fini d'ordre n et σ une permutation de I, la signature de σ est alors défini comme la signature de la permutation $f^{-1} \circ f \circ \sigma$, où f est une bijection de $\{1, \ldots, n\}$ vers I. On vérifie rapidement que la valeur est indépendante du choix de f. Dans ce chapitre, indépendant des précédents, on se propose de donner deux nouvelles preuves de la valeur de la signature de l'automorphisme de Frobenius de $\mathbb{F}_q$, $q = p^n$, p premier.

Théorème 8.1.1 *On pose $n = 2^s m$ où m est un entier impair.*

1. *Si $p = 2$, alors la signature de $\mathcal{F}$ vaut 1 sauf si $q = 4$.*
2. *Si $p > 2$, alors*
   - *si $s = 0$, $\epsilon(\mathcal{F}) = 1$;*
   - *si $s > 0$, et $p \equiv 1 \bmod 4$, alors $\epsilon(\mathcal{F}) = 1$;*
   - *si $s > 0$, et $p \equiv 3 \bmod 4$, alors $\epsilon(\mathcal{F}) = -1$.*

Notre première nouvelle preuve est beaucoup plus simple que celles déjà données, en ce sens qu'elle est directe, et ne fait pas appel par exemple au symbole de Zolotarev. Afin de pouvoir comparer les différents démonstrations, on commencera par en rappeller deux classiques. La première se base sur le symbole de Zolotarev. Elle aura pour but initial de calculer la signature de la multiplication par n dans $\mathbb{Z}/m\mathbb{Z}$, m et n étant premiers entre eux. Ce sera ce que l'on fait dans la deuxième nouvelle preuve, mais on utilisera des arguments locaux. On rappelera également celle utilisant le théorème de Frobenius-Zolotarev. Cette dernière ne se plaçera que dans le cas $p > 2$.

Enfin, dans un dernier paragraphe, en guise d'application du théorème (8.1.1), on se propose d'obtenir comme nouveau résultat la parité du nombre $N(q, D)$ de polynômes irréductibles unitaires de degrés divisant $D \geq 1$, et à coefficients dans $\mathbb{F}_q = \mathbb{F}_{p^n}$. Le résultat obtenu est le suivant :

Proposition 8.1.2 *On a les assertions suivantes :*

1. *Si* $2|n$, *alors* $N(q, D)$ *et* p *ont même parité ;*
2. *Si* $2 \nmid n$, *alors*
   (a) *Si* $p = 2$, *alors* $N(q, D)$ *est pair sauf si* $D = 2$;
   (b) *Si* $p > 2$, *alors*
   - $N(q, D)$ *est impair si* $2 \nmid D$,
   - $N(q, D)$ *est impair si* $2|D$ *et* $p \equiv 1 \bmod 4$,
   - $N(q, D)$ *est pair si* $2|D$ *et* $p \equiv 3 \bmod 4$.

Par exemple, si $q = p = 3$ et $D = 4$, $N(q, D)$ est pair. On peut vérifier qu'il y a 18 polynômes irréductibles de degrés 4 sur $\mathbb{F}_3$, et 3 de degrés 2 donc $N(3, 4) = 3+3+18 = 24$.

8.2 Démonstration via le symbole de Zolotarev.

Comme $\mathbb{F}_q^*$ est cyclique, calculer la signature de $\mathcal{F}$ revient à calculer la signature de la permutation de $\mathbb{Z}/(q-1)\mathbb{Z}$, qui multiplie ses éléments par p. S. Graillat se propose donc plus généralement de calculer la signature de $\pi_{n,m}$ qui multiplie les éléments de $\mathbb{Z}/m\mathbb{Z}$ par n, où m, n sont deux entiers premiers entre eux.

Definition 8.2.1 *On appelle symbole de Zolotarev, que l'on note* $(n|m)$ *la signature de* $\pi_{n,m}$.

On va montrer le théorème suivant :

Théorème 8.2.2 *([36])*

1. *Pour tous entiers* m *impairs et* n *quelconques, on a* $(n|m) = \left(\frac{n}{m}\right)$.
2. *Soit* m *un entier pair et* n *un entier premier avec* m. *Alors le symbole de Zolotarev vérifie* $(n|m) = (-1)^{\left(\frac{m}{2}+1\right)\frac{n-1}{2}}$.

Remarque 8.2.3 *Le symbole de Zolotarev permet de donner une autre preuve de la loi de réciprocité quadratique de Gauss.*

8.2.1 Trois lemmes auxiliaires.

Lemme 8.2.4 *La signature de la permutation de $\mathbb{Z}/m\mathbb{Z}$ qui à x associe $x+r$ a pour signature $(-1)^{r(m-1)}$.*

Preuve En effet, cette permutation est la puissance m-ième de celle qui à x associe $x+1$. Or cette dernière est un cycle de longueur m, donc de signature $(-1)^{m-1}$. La signature cherchée est donc $(-1)^{r(m-1)}$.□

Soit I un ensemble fini d'ordre n et σ une permutation de I. Soit f une bijection fixée de $\{1,\ldots,n\}$ vers I. Soient $a=f(i)$ et $b=f(j)$ deux éléments distincts de I. On définit sur I une relation d'ordre, en posant $a<b$ si et seulement si $i<j$. La permutation σ présente une inversion en (a,b) si et seulement si $f^{-1}\circ\sigma\circ f$ présente une inversion en (i,j). En effet, si σ présente une inversion en (a,b), alors par définition

$$i<j,\quad f^{-1}(\sigma(a))>f^{-1}(\sigma(b)),$$

ie

$$i<j,\quad f^{-1}(\sigma(f(i)))>f^{-1}(\sigma(f(j))),$$

ie $f^{-1}\circ\sigma\circ f$ présente une inversion en (i,j). La réciproque se traite de même. Ainsi, la signature de σ est également $(-1)^{Inv(\sigma)}$, $Inv(\sigma)$ étant son nombre d'inversions. Dans le cas où on travaille avec un ensemble produit $I\times J$, I, J finis, on peut prendre comme ordre, l'ordre lexicographique droit ie

$$(i,j)<(i',j')\Leftrightarrow i<i'\quad\text{ou}\quad i=i',j<j'.$$

En effet, soit n (respectivement m) l'ordre de I (respectivement l'ordre de J). Soit $E_{nm}=\{1,\ldots,nm\}$. Soit $x\in E_{nm}$. Soit $q_m(x-1)$ (respectivement $r_m(x-1)$) le quotient (respectivement le reste) de la division Euclidienne de $x-1$ par m. On définit alors la bijection f de E_{nm} vers $I\times J$ par

$$f(x)=\left(f_I(q_m(x-1)+1),g_J(r_m(x-1)+1)\right).$$

où f_I (respectivement g_J) est une bijection de $\{1,\ldots,n\}$ vers I (respectivement est une bijection de $\{1,\ldots,m\}$ vers J). Comme avant, si $x=f_I(a)$, $y=f_I(b)$, on pose que $x<y$ si $a<b$. Idem pour les éléments de J (avec g_J au lieu de f_I). Alors, si x,y sont deux entiers de E_{nm}, on a $x<y$ si et seulement si $f(x)<f(y)$ au sens lexicographique droit. En effet, effectuons les divisions euclidiennes de $x-1$ et $y-1$ par m suivantes :

$$x-1=qm+r,\quad y-1=q'm+r'.$$

Supposons $x < y$. Alors $q < q'$ ou $q = q'$ et $r < r'$ (on ne peut avoir $q > q'$, car alors $q \geq q' + 1$, donc $qm > q'm + r$, d'où $x > y$). Dans le premier cas, $f_I(q+1) < f_I(q'+1)$. Dans le second, on a $f_I(q+1) = f_I(q'+1)$, et $g_J(r+1) < g_J(r'+1)$. Dans tous les cas $f(x) = (f_I(q+1), g_J(r)) < f(y) = (f_I(q'+1), g_J(r'))$ au sens lexicographique droit. La réciproque se traite de même.

La signature d'une permutation de $I \times J$ va donc pouvoir se calculer en comptant son nombre d'inversions pour l'ordre lexicographique droit. En particulier, on va montrer le

Lemme 8.2.5 *Soient I, J deux ensembles finis d'ordres respectifs $|I|$ et $|J|$. Soit σ (respectivement τ) une permutation de I (respectivement de J). Soit $\sigma \times \tau$ la permutation de $I \times J$ définie par*

$$\sigma \times \tau(i,j) = (\sigma(i), \tau(j)).$$

Alors

$$\epsilon(\sigma \times \tau) = \epsilon(\sigma)^{|J|}\epsilon(\tau)^{|I|}.$$

Preuve La permutation $\sigma \times \tau$ présente une inversion en $(i,j),(i',j')$ si et seulement si (i,i') est une inversion pour σ, j, j' quelconques, ou bien $i = i'$ et (j,j') est une inversion pour τ. Le nombre d'inversions pour $\sigma \times \tau$ est donc

$$Inv(\sigma \times \tau) = Inv(\sigma)|J|^2 + Inv(\tau)|I|.$$

Il vient alors

$$\epsilon(\sigma \times \tau) = (-1)^{Inv(\sigma\times\tau)} = \epsilon(\sigma)^{|J|^2}\epsilon(\tau)^{|I|} = \epsilon(\sigma)^{|J|}\epsilon(\tau)^{|I|}.$$

□

Soient maintenant m, n deux entiers. On définit l'application $\lambda : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/mn\mathbb{Z}$ par $\lambda(\overline{x}) = \overline{nj+i}$, où i (respectivement j) est le quotient (respectivement le reste) de la division euclidienne de $x \in \{0, \ldots, mn-1\}$ par m.

Lemme 8.2.6 *La signature de λ est $(-1)^{\frac{n(n-1)m(m-1)}{4}}$.*

Preuve Calculons le nombre d'inversions de λ. Soient $x, y \in \{0, \ldots, mn-1\}$ tels que $x < y$. Effectuons leur division euclidienne par m

$$x = mi_x + j_x, \quad y = mi_y + j_y.$$

Supposons que λ présente une inversion en $(\overline{x}, \overline{y})$. Si $i_x = i_y$, alors $j_x < j_y$. Comme λ présente une inversion en $(\overline{x}, \overline{y})$, on a aussi $nj_y + i_y < nj_x + i_x = nj_x + i_y$, ie $j_y < j_x$. On a donc $i_x < i_y$ et λ présentant une inversion en $(\overline{x}, \overline{y})$, $j_y < j_x$. Inversement, si x, y sont tels que $i_x < i_y$ et $j_y < j_x$, λ présente une inversion en $(\overline{x}, \overline{y})$. On a donc

$$Inv(\lambda) = \frac{n(n-1)}{2}\frac{m(m-1)}{2},$$

d'où le résultat.□

8.2.2 Preuve du théorème (8.2.2), cas m impair.

Dans le cas où m est impair, on va montrer que le symbole de Zolotarev $(n|m)$ coïncide avec le symbole de Jacobi $\left(\frac{n}{m}\right)$.

Proposition 8.2.7 *Le symbole de Zolotarev vérifie les propriétés suivantes*

1. $(nn'|m) = (n|m)(n'|m)$;
2. $(2|m) = (-1)^{\frac{m^2-1}{8}}$;
3. $(n|m) \equiv n^{\frac{m-1}{2}} \bmod m$ *si* m *est premier* ;

Preuve

1. On a $\pi_{nn',m} = \pi_{n,m} \circ \pi_{n',m}$. La signature étant un morphisme on obtient

$$(nn'|m) = \epsilon(\pi_{nn',m}) = \epsilon(\pi_{n,m} \circ \pi_{n',m}) = \epsilon(\pi_{n,m})\epsilon(\pi_{n',m}) = (n|m)(n'|m).$$

2. Comme m est impair : $m = 2q+1$, $q \in \mathbb{Z}$. La multiplication par 2 dans $\mathbb{Z}/m\mathbb{Z}$ est

$$\begin{pmatrix} 0 & 1 & 2\cdots q & q+1 & q+2\cdots 2q \\ 0 & 2 & 4\cdots 2q & 1 & 3 \quad \cdots 2q-1 \end{pmatrix}.$$

   Le nombre d'inversions de cette permutation est donc $1 + 2 + \cdots q = \frac{q(q+1)}{2} = \frac{m^2-1}{8}$.

3. Comme

$$\epsilon(\pi_{n,m}) = \prod_{1 \le i < j \le m} \frac{\pi_{n,m}(i) - \pi_{n,m}(j)}{i-j},$$

   modulo m, on a donc

$$\epsilon(\pi_{n,m}) = \prod_{1 \le i < j \le m} \frac{ni - nj}{i-j} = \prod_{1 \le i < j \le m} n = n^{\frac{m(m-1)}{2}}.$$

   Comme $n^m \equiv n \bmod m$ on a le résultat.

□

Théorème 8.2.8 *Si n et m sont impairs et premiers entre eux, alors le symbole de Zolotarev vérifie la loi de réciprocité quadratique*

$$(n|m)(m|n) = (-1)^{\frac{(n-1)(m-1)}{4}}.$$

Preuve On définit les deux permutations σ et τ de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ par

$$\sigma(i,j) = (mi + j, j), \quad \tau(i,j) = (i, nj + i).$$

Soit σ_j la permutation de $\mathbb{Z}/n\mathbb{Z}$ définie par

$$\sigma_j(i) = mi + j.$$

Par le lemme (8.2.4), n étant impair, la signature des translations est 1. Donc

$$\epsilon(\sigma_j) = \epsilon(\pi_{m,n}) = (m|n).$$

Or $\sigma = \sigma_j \times Id$. Par le lemme (8.2.5), on a donc

$$\epsilon(\sigma) = (m|n)^m = (m|n),$$

m étant impair. De la même façon on trouve

$$\epsilon(\tau) = (n|m).$$

Soit $\theta : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ l'homomorphisme d'anneaux du théorème chinois :

$$\theta(mi + j) = (mi + j, j), \quad \theta(nj + i) = (i, nj + i).$$

Soit λ la permutation du lemme (8.2.6). On a

$$\lambda \circ \theta^{-1} \circ \sigma = \theta^{-1} \circ \tau.$$

Mais par le lemme (8.2.6) on a $\epsilon(\lambda) = (-1)^{\frac{m(m-1)}{2}\frac{n(n-1)}{2}} = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$, m et n étant impairs, d'où en passant aux signatures

$$(-1)^{\frac{m-1}{2}\frac{n-1}{2}}(m|n) = (n|m),$$

ce qu'on voulait.□

Lemme 8.2.9 *Pour tous entiers m et m' impairs et n premier à mm' on a*

$$(n|m)(n|m') = (n|mm').$$

Preuve

1. Cas où n est impair : par le théorème (8.2.8), on a

$$(n|m) = (m|n)(-1)^{\frac{n-1}{2}\frac{m-1}{2}}, \quad (n|m') = (m'|n)(-1)^{\frac{n-1}{2}\frac{m'-1}{2}}.$$

Par conséquent,

$$\begin{aligned}(n|m)(n|m') &= (m|n)(m'|n)(-1)^{\frac{n-1}{2}\frac{m-1}{2}}(-1)^{\frac{n-1}{2}\frac{m'-1}{2}} \\ &= (mm'|n)(-1)^{\frac{n-1}{2}\left(\frac{m-1}{2}+\frac{m'-1}{2}\right)}.\end{aligned}$$

En appliquant le théorème (8.2.8) à $(mm'|n)$, il vient

$$(n|m)(n|m') = (n|mm')(-1)^{\frac{n-1}{2}\left(\frac{m-1}{2}+\frac{m'-1}{2}+\frac{mm'-1}{2}\right)}.$$

Comme m et m' sont impairs, on a $m = 2k+1$, $m' = 2k'+1$, et

$$\frac{m-1}{2} + \frac{m'-1}{2} + \frac{mm'-1}{2} = 2k + 2k' + 2kk',$$

d'où

$$(n|m)(n|m') = (n|mm').$$

2. Cas où n est pair : n étant pair posons $n = 2^i r$, $i \geq 1$, r impair. Alors

$$\begin{aligned}(n|m)(n|m') &= (2^i|m)(2^i|m')(r|m)(r|m') \\ &= \left((2|m)(2|m')\right)^i (r|mm'),\end{aligned}$$

car r est impair (cas étudié précédemment). Par la proposition (8.2.7)

$$(2|m)(2|m') = (-1)^{\frac{m^2+m'^2-2}{8}}.$$

Comme $\frac{m^2+m'^2-2}{8}$ et $\frac{(mm')^2-1}{8}$ ont même parité

$$(2|m)(2|m') = (-1)^{\frac{(mm')^2-1}{8}} = (2|mm').$$

Au final, on a

$$(n|m)(n|m') = (2|mm')^i (r|mm') = (n|mm'),$$

ce qui était à démontrer.

□ On peut maintenant montrer que le symbole de Zolotarev et Jacobi coïncident :

Théorème 8.2.10 *Soient m et n deux entiers premiers entre eux, m impair. Alors*

$$(n|m) = \left(\frac{n}{m}\right).$$

Preuve Soit $m = \prod_{i=1}^{r} p_i^{\alpha_i}$ la décomposition de m en produit de facteurs premiers. Par ce qui précède, on a

$$(n|m) = (n|\prod_{i=1}^{r} p_i^{\alpha_i}) = \prod_{i=1}^{r} (n|p_i)^{\alpha_i}.$$

Mais par la proposition (8.2.7), $(n|p_i) = \left(\frac{n}{p_i}\right)$, d'où

$$(n|m) = \prod_{i=1}^{r} \left(\frac{n}{p_i}\right)^{\alpha_i} = \left(\frac{n}{m}\right).$$

□ Le théorème (8.2.2), cas m impair est donc prouvé.

8.2.3 Preuve du théorème (8.2.2), cas m pair.

Lemme 8.2.11 *Soit $k \geq 2$ un entier et n un entier impair. Alors la signature de $\pi_{n,2^k}$ est $(-1)^{\frac{n-1}{2}}$.*

Preuve Dans le cas $k = 2$, la permutation $\pi_{n,2^k}$ est la transposition $(\overline{1},\overline{3})$ si $n \equiv 3 \bmod 4$ et est l'identité sinon, d'où le lemme dans ce cas. Supposons $k \geq 3$. Comme $\epsilon(\pi_{nn',2^k}) = \epsilon(\pi_{n,2^k})\epsilon(\pi_{n',2^k})$ et $(-1)^{\frac{nn'-1}{2}} = (-1)^{\frac{n-1}{2}}(-1)^{\frac{n'-1}{2}}$ il suffit de montrer le lemme pour -1 et 5 qui engendrent $\left(\mathbb{Z}/2^k\mathbb{Z}\right)^{\times}$.

1. Cas $n = -1$; La permutation $\pi_{-1,2^k}$ est le produit des transpositions $(a, 2^k - a)$, $1 \leq a \leq 2^{k-1} - 1$, d'où

   $$\epsilon(\pi_{-1,2^k}) = (-1)^{2^{k-1}-1} = -1.$$

2. Cas $n = 5$; Soit $c \in \mathbb{Z}/2^k\mathbb{Z}$, $c \neq 0$. Deux représentants de c ont la même valuation 2-adique et on peut donc poser $\nu_2(c) = \nu_2(x)$, où x est un représentant de c. Soit r un entier, $1 \leq r \leq 2^{k-2}$. Posons

   $$V_r = \left\{c \in \mathbb{Z}/2^k\mathbb{Z} : \nu_2(c) = r\right\}.$$

   Comme 5 est d'ordre 2^{k-2} modulo 2^k, il est d'ordre 2^{k-r-2} modulo 2^r, donc

   $$V_r = \left\{\pm 2^r 5, \ldots \pm 2^r 5^{2^{k-r-2}}\right\}.$$

   De plus, $V_{k-1} = \{2^{k-1}\}$. Les ensembles V_r sont stables par $\pi_{5,2^k}$. Si $r < k-2$, alors $\pi_{5,2^k}$ restreinte à V_r se décompose en produit de deux cycles de longueur 2^{k-r-2} :

   $$\left(2^r, \ldots 2^r 5^{2^{k-r-3}}\right)\left(-2^r, \ldots -2^r 5^{2^{k-r-3}}\right).$$

   Enfin, restreinte à $\{0\}$, $V_{k-2} = \{2^{k-2}\}$, ou $V_{k-1} = \{2^{k-1}\}$, $\pi_{5,2^k}$ est l'identité. On en déduit que $\epsilon(\pi_{5,2^k}) = 1$.

□ L'entier m étant pair, posons $m = 2^k r$, r impair, $k \geq 1$. Comme $\mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/2^k\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$, le lemme (8.2.5) et le lemme précédent montrent

$$(n|m) = (-1)^{\frac{n-1}{2}r}(n|r)^{2^k} = (-1)^{\frac{n-1}{2}r}.$$

Si $k = 1$, la signature est $1 \cdot (n|r)^{2^k} = 1$. On a donc dans tous les cas

$$(n|m) = (-1)^{\frac{n-1}{2}\left(\frac{m}{2}+1\right)}$$

8.2.4 Signature du Frobenius.

Calculons maintenant $\epsilon(\mathcal{F})$. Il s'agit de calculer $(p|q-1)$. Rappelons que l'on a déjà posé $q = p^n$, avec $n = 2^s m$, m impair. Supposons d'abord $p > 2$. Alors $q - 1$ est pair et le théorème précédent montre que

$$\epsilon(\mathcal{F}) = (-1)^{\left(\frac{q-1}{2}+1\right)\frac{p-1}{2}}.$$

Si $p \equiv 1 \bmod 4$, on trouve $\epsilon(\mathcal{F}) = 1$.

Supposons que $p \equiv 3 \bmod 4$. Si $s = 0$, alors $q = p^n \equiv -1 \bmod 4$, donc $2|\frac{q-1}{2} + 1$ et $\epsilon(\mathcal{F}) = 1$. Si $s > 0$, alors $q = p^n \equiv 1 \bmod 4$, $(\frac{q-1}{2} + 1)\frac{p-1}{2}$ est impair et $\epsilon(\mathcal{F}) = -1$.

Dans le cas où $p = 2$, on a par le théorème (8.2.2)

$$\epsilon(\mathcal{F}) = (2|2^n - 1) = (-1)^{\frac{(q-1)^2-1}{8}}.$$

On a

$$(q-1)^2 - 1 = 2^{n+1}(2^{n-1} - 1).$$

Si $n \geq 3$ ou si $n = 1$, $\epsilon(\mathcal{F}) = 1$. Si $n = 2$, $\epsilon(\mathcal{F}) = -1$.

Remarque 8.2.12 *On donne dans le cas $p = 2$, un énoncé plus simple que celui de [36].*

8.3 Démonstration via le théorème de Zolotarev dans le cas $p > 2$.

8.3.1 Théorème de Frobenius-Zolotarev.

Rappelons le théorème de Frobenius-Zolotarev :

Théorème 8.3.1 *Soient p un nombre premier impair et V un $\mathbb{F}_p$-espace vectoriel de dimension finie. Soit $u \in GL(V)$. Sa signature en tant que permutation de V est donnée par*

$$\epsilon(u) = \left(\frac{det(u)}{p}\right).$$

Pour le montrer, on peut par exemple appliquer la relation de Cartier (voir [26]).

8.3.2 Démonstration du théorème (8.1.1).

Considérons $\mathbb{F}_q$ muni de sa structure de $\mathbb{F}_p$-espace vectoriel. L'automorphisme de Frobenius est un endomorphisme cyclique de cet espace vectoriel. Il existe donc un élément x de $\mathbb{F}_q$, tel que $\{x, \ldots, \mathcal{F}^{n-1}(x)\}$ réalise une $\mathbb{F}_p$-base de $\mathbb{F}_q$. En se plaçant dans une telle base, on a $det\,(\mathcal{F}) = (-1)^{n+1}$. Par le théorème de Frobenius-Zolotarev, il vient

$$\epsilon(\mathcal{F}) = \left(\frac{det(\mathcal{F})}{p}\right) = (-1)^{\frac{(p-1)(n-1)}{2}}.$$

Remarque 8.3.2 *En fait, dans [79], les auteurs justifient l'existence d'une telle base, en utilisant le théorème de la base normale.*

8.4 Démonstration combinatoire.

Nous proposons ici la première des deux nouvelles démonstrations. Elle est plus simple que les précédentes, car on s'intéresse directement à $\mathcal{F}$, que l'on va décomposer en produits de cycles à supports disjoints. La méthode nous oblige à séparer les cas p pair et impair. Les calculs étant similaires, on détaillera seulement le cas $p > 2$.

8.4.1 Cas où p est impair.

On pose $n = 2^s m$ où m est impair, et $s \geq 0$. Supposons d'abord $s > 0$. Comme m est impair, $\mathcal{F}$ et $\mathcal{F}^m$ ont la même signature. Le corps invariant par $G = \mathcal{F}^m$ est $\mathbb{F}_{p^m}$. Pour simplifier, on pose $q = p^m$. Soit t un entier tel que $t \in [1, \ldots, s]$. Soit $x \in \mathbb{F}_{q^{2^t}} - \mathbb{F}_{q^{2^{t-1}}}$. La G-orbite de x sous G est donc de longueur 2^t. Comme $\mathbb{F}_{q^{2^t}} - \mathbb{F}_{q^{2^{t-1}}}$ est de cardinal $q^{2^t} - q^{2^{t-1}}$, la permutation G se décompose donc en $\frac{q^{2^t}-q^{2^{t-1}}}{2^t}$ cycles de longueur 2^t. De plus, G vaut l'identité sur $\mathbb{F}_q$. Comme la signature d'un cycle de longueur l est $(-1)^{l-1}$, on en déduit que la signature de G est :

$$\epsilon\,(G) = (-1)^{\sum_{t=1}^{s} \frac{q^{2^t}-q^{2^{t-1}}}{2^t}(2^t-1)}.$$

Il nous reste donc à étudier la parité de $\sum_{t=1}^{s} \frac{q^{2^t}-q^{2^{t-1}}}{2^t}(2^t - 1)$. La parité du quotient $\frac{q^{2^t}-q^{2^{t-1}}}{2^t}$ est celui de $\frac{q^{2^{t-1}}-1}{2^t}$. On a le lemme suivant :

Lemme 8.4.1 *Si $a \geq 1$ est un entier, alors on a $q^{2^a} \equiv 1 \bmod 2^{a+2}$.*

Preuve La preuve de ce lemme se fait par récurrence sur a. Si $a = 1$, il n'y a rien à faire. Supposons l'assertion vérifiée pour $a > 1$. On a alors :

$$q^{2^{a+1}} = \left(q^{2^a}\right)^2 = \left(1 + \lambda 2^{a+2}\right)^2 = 1 + 2^{a+3}\lambda + 2^{2a+4}\lambda^2 \equiv 1 \bmod 2^{a+3}.$$

□ La parité de la somme précédente, est donc la même que celle du quotient $\frac{q-1}{2} = \frac{p^m-1}{2}$, ie celle de $\frac{p-1}{2}$, car m est impair. Donc, si $s > 0$:

- on a $\epsilon(\mathcal{F}) = 1$ si $p \equiv 1 \bmod 4$,
- on a $\epsilon(\mathcal{F}) = -1$ si $p \equiv 3 \bmod 4$.

Si $s = 0$, alors $\epsilon(\mathcal{F}) = \epsilon(G) = 1$.

8.4.2 Cas où $p = 2$.

On suppose maintenant que $p = 2$, et on pose $n = 2^s m$ ou m est un entier impair. Soit aussi $q = 2^m$. Comme avant, si $s = 0$, $\epsilon(\mathcal{F}) = 1$. Supposons donc $s > 0$. On a

$$\epsilon(\mathcal{F}) = (-1)^{\sum_{t=1}^{s} \frac{q^{2^t} - q^{2^{t-1}}}{2^t}(2^t-1)}.$$

Si $s = 1$, on a en particulier

$$\epsilon(\mathcal{F}) = (-1)^{\frac{q(q-1)}{2}} = (-1)^{2^{m-1}}.$$

Si $s = 1$, on a donc $\epsilon(\mathcal{F}) = -1$ si $m = 1$ (c'est à dire $q = 4$) et $\epsilon(\mathcal{F})$ vaut 1 sinon. (Remarquons que si $q = 4$, $\mathcal{F}$ est simplement la transposition (jj^2) où $j^2 + j + 1 = 0$).

Si $s \geq 2$, on vérifie que $\sum_{t=1}^{s} \frac{q^{2^t} - q^{2^{t-1}}}{2^t}(2^t - 1)$ est paire, c'est à dire $\mathcal{F} = 1$.

8.5 Démonstration via des considérations locales.

8.5.1 Notations et quelques rappels.

On propose dans ce paragraphe, de donner une deuxième démonstration, cette fois formelle qui s'inspire des travaux de Zahidi sur les symboles quadratiques.(voir [81] et [80]). On commence par rappeler quelques notations et résulats classiques.

8.5.2 Le symbole de Hilbert.

Soient k un corps de nombres, $\mathfrak{p}$ un idéal premier de k et $n > 1$ un entier premier à la caractérisique du corps résiduel de $k_{\mathfrak{p}}$, le complété de k en $\mathfrak{p}$. On suppose dans la suite que $k_{\mathfrak{p}}$ contient le groupe des racines n-ièmes de l'unité μ_n. Soit $a \in k_{\mathfrak{p}}^*$. Supposons que

l'extension $k_{\mathfrak{p}}(a^{1/n})/k_{\mathfrak{p}}$ ne soit pas ramifiée, donc cyclique. Soit σ_0 son automorphisme de Frobenius. On définit $\left(\frac{a}{\mathfrak{p}}\right)_n$ comme suit :

$$\left(\frac{a}{\mathfrak{p}}\right)_n = \sqrt[n]{a}^{\sigma_0 - 1} \in \mu_n.$$

On a le lemme suivant :

Lemme 8.5.1

$$\left(\frac{a}{\mathfrak{p}}\right)_n \equiv u^{\frac{\mathcal{N}(\mathfrak{p})-1}{n}} \bmod \mathfrak{p},$$

où on a posé $a = u\pi^w$, avec π paramètre local de $k_{\mathfrak{p}}$ et u unité.

Preuve Comme $k_{\mathfrak{p}}(a^{1/n})/k_{\mathfrak{p}}$ est non ramifiée, on peut écrire a sous la forme $a = u\pi^w$ où w est un entier divisible par n, u une unité de $k_{\mathfrak{p}}$ et π un paramètre local de $k_{\mathfrak{p}}$. Soit ω le caractère de Teichmüller de $k_{\mathfrak{p}}$. $\omega(u)$ est une racine $(\mathcal{N}(\mathfrak{p})-1)$-ième de l'unité et $\frac{u}{\omega(u)}$ est une unité locale. En utilisant le lemme de Hensel, on montre en particulier que $\frac{u}{\omega(u)}$ est une puissance n-ième dans $k_{\mathfrak{p}}$. On a donc

$$\left(\frac{a}{\mathfrak{p}}\right)_n = \sqrt[n]{\omega(u)}^{\sigma_0 - 1} \in \mu_n.$$

Par définition de σ_0, il vient

$$\left(\frac{a}{\mathfrak{p}}\right)_n = \omega(u)^{\frac{\mathcal{N}(\mathfrak{p})-1}{n}} \equiv u^{\frac{\mathcal{N}(\mathfrak{p})-1}{n}} \bmod \mathfrak{p},$$

par propriété de $\omega(u)$.□

Definition 8.5.2 *Soient $a, b \in k_{\mathfrak{p}}^*$. Posons $a = a_0\pi^{\nu_{\mathfrak{p}}(a)}$ et $b = b_0\pi^{\nu_{\mathfrak{p}}(b)}$. Le symbole de Hilbert de a et b pris dans cet ordre noté $\left(\frac{a,b}{\mathfrak{p}}\right)$ est défini par*

$$\left(\frac{a,b}{\mathfrak{p}}\right) = \left(\frac{-1}{\mathfrak{p}}\right)_n^{\nu_{\mathfrak{p}}(a)\nu_{\mathfrak{p}}(b)} \left(\frac{a_0}{\mathfrak{p}}\right)_n^{-\nu_{\mathfrak{p}}(b)} \left(\frac{b_0}{\mathfrak{p}}\right)_n^{\nu_{\mathfrak{p}}(a)}$$

On a la propostion suivante :

Proposition 8.5.3 *Soit $K_\beta/k_{\mathfrak{p}}$ une extension finie. Soit $a = \mathcal{N}_{K_\beta/k_{\mathfrak{p}}}(A)$. On a alors*

$$\left(\frac{A,b}{\beta}\right) = \left(\frac{a,b}{\mathfrak{p}}\right).$$

Preuve Il suffit de démontrer la proposition quand $K_\beta/k_\mathfrak{p}$ est non ramifiée et totalement ramifiée. En effet, supposons la démontrée dans ces deux cas. Soit $\mathcal{R}$ la composante non ramifiée de l'extension. On peut écrire a sous la forme

$$a = \mathcal{N}_{\mathcal{R}/k_\mathfrak{p}}\left(\mathcal{N}_{K_\beta/\mathcal{R}}(A)\right).$$

Comme $\mathcal{R}/k_\mathfrak{p}$ est non ramifiée et $K_\beta/\mathcal{R}$ totalement ramifiée, on a alors

$$\begin{aligned}\left(\frac{a,b}{\mathfrak{p}}\right) &= \left(\frac{\mathcal{N}_{\mathcal{R}/k_\mathfrak{p}}\left(\mathcal{N}_{K_\beta/\mathcal{R}}\left(A\right)\right),b}{\mathfrak{p}}\right)\\ &= \left(\frac{\mathcal{N}_{K_\beta/\mathcal{R}}\left(A\right),b}{\beta\cap\mathcal{R}}\right) = \left(\frac{A,b}{\beta}\right).\end{aligned}$$

Il ne reste plus qu'à montrer que $\left(\frac{A,b}{\beta}\right) = \left(\frac{a,b}{\mathfrak{p}}\right)$ lorsque $K_\beta/k_\mathfrak{p}$ est non ramifiée, puis totalement ramifiée. Supposons donc d'abord que $K_\beta/k_\mathfrak{p}$ soit non ramifiée. Posons $[K_\beta : k_\mathfrak{p}] = m$. Le paramètre local π de $k_\mathfrak{p}$ est donc également un paramètre local de K_β. Posons $A = A_0\pi^{\nu_\mathfrak{p}(A)}$. Posons $a = a_0\pi^{\nu_\mathfrak{p}(a)}$. On a $\mathcal{N}_{K_\beta/k_\mathfrak{p}}(A_0) = a_0$ et $\nu_\mathfrak{p}(a) = m\nu_\mathfrak{p}(A) = m\nu_\beta(A)$. D'après le lemme (8.5.1), on a modulo β :

$$\begin{aligned}\left(\frac{A_0}{\beta}\right)_n &\equiv A_0^{\frac{\mathcal{N}(\beta)-1}{n}} \equiv A_0^{\frac{\mathcal{N}(\mathfrak{p})^m-1}{n}}\\ &\equiv \left(A_0^{1+\mathcal{N}(\mathfrak{p})+\cdots+\mathcal{N}(\mathfrak{p})^{m-1}}\right)^{\frac{\mathcal{N}(\mathfrak{p})-1}{n}}\\ &\equiv \left(\mathcal{N}_{K_\beta/k_\mathfrak{p}}(A_0)\right)^{\frac{\mathcal{N}(\mathfrak{p})-1}{n}} \equiv \left(\frac{\mathcal{N}_{K_\beta/k_\mathfrak{p}}(A_0)}{\mathfrak{p}}\right).\end{aligned}$$

Comme $\left(\frac{A_0}{\beta}\right)_n$ et $\left(\frac{\mathcal{N}_{K_\beta/k_\mathfrak{p}}(A_0)}{\mathfrak{p}}\right)$ sont des racines n-ième de l'unité donc d'ordre premier à β. Ils sont donc en fait égaux :

$$\left(\frac{A_0}{\beta}\right) = \left(\frac{\mathcal{N}_{K_\beta/k_\mathfrak{p}}(A_0)}{\mathfrak{p}}\right) = \left(\frac{a_0}{\mathfrak{p}}\right). \tag{8.1}$$

En particulier, pour b_0, comme $\mathcal{N}_{K_\beta/k_\mathfrak{p}}(b_0) = b_0^m$, il vient

$$\left(\frac{b_0}{\beta}\right) = \left(\frac{b_0^m}{\mathfrak{p}}\right) = \omega(b_0^m)^{\frac{\mathcal{N}(\mathfrak{p})-1}{n}} = \left(\frac{b_0}{\beta}\right)^m. \tag{8.2}$$

En revenant à la définition du symbole de Hilbert, et en utilisant (8.1) et (8.2), on obtient la relation souhaitée.

Supposons maintenant que l'extension $K_\beta/k_\mathfrak{p}$ soit totalement ramifiée. Soit Π un paramètre local de K_β. On peut prendre $\pi = \mathcal{N}_{K_\beta/k_\mathfrak{p}}(\Pi)$. Posons $A = A_0\Pi^{\nu_\beta(A)}$. On a $a_0 = \mathcal{N}_{K_\beta/k_\mathfrak{p}}(A_0)$ et $\nu_\mathfrak{p}(a) = \nu_\beta(A)$. On a modulo β :

$$\left(\frac{A_0}{\beta}\right)^m \equiv A_0^{m\frac{(\mathcal{N}(\beta)-1)}{n}} \equiv A_0^{m\frac{(\mathcal{N}(\mathfrak{p})-1)}{n}}.$$

Comme $K_\beta/k_\mathfrak{p}$ est totalement ramifiée, il existe une unité x de $k_\mathfrak{p}$ tel que $A_0 \equiv x \bmod \beta$. Soit A_1 un conjugué de A_0. $A_1 - x$ et $A_0 - x$ sont conjugués sur $k_\mathfrak{p}$. En particulier, on a $A_1 - x \equiv A_0 - x \bmod \beta$, c'est à dire $A_1 \equiv A_0 \bmod \beta$. Il vient donc :

$$\left(\frac{A_0}{\beta}\right)^m \equiv \mathcal{N}_{K_\beta/k_\mathfrak{p}}(A_0)^{\frac{(\mathcal{N}(\beta)-1)}{n}} \equiv \left(\frac{\mathcal{N}_{K_\beta/k_\mathfrak{p}}(A_0)}{\mathfrak{p}}\right) = \left(\frac{a_0}{\mathfrak{p}}\right).$$

On a donc :

$$\left(\frac{A_0}{\beta}\right)^m = \left(\frac{\mathcal{N}_{K_\beta/k_\mathfrak{p}}(A_0)}{\mathfrak{p}}\right) = \left(\frac{a_0}{\mathfrak{p}}\right). \tag{8.3}$$

De la même façon, il vient :

$$\left(\frac{b_0}{\beta}\right) = \left(\frac{b_0}{\mathfrak{p}}\right). \tag{8.4}$$

Soit c_0 l'unité de $k_\mathfrak{p}$ définie par $\pi = c_0\Pi^m$. L'unité c_0 vérifie $c_0 \equiv (-1)^{m-1} \bmod \beta$. En effet, soit $P(X)$ le polynôme minimal de Π défini par

$$P(X) = X^m + a_1X^{m-1} + \cdots + a_m, \quad a_m = (-1)^m\mathcal{N}_{K_\beta/k_\mathfrak{p}}(\Pi).$$

(Le degrés de P est m, car $K_\beta/k_\mathfrak{p}$ étant totalement ramifié, si d est le degrés de $k_\mathfrak{p}(\Pi)$ sur $k_\mathfrak{p}$, on a $\nu_\beta\left(\mathcal{N}_{K_\beta/k_\mathfrak{p}}(\Pi)\right) = d\nu_\beta(\Pi) = d = m\nu_\mathfrak{p}\left(\mathcal{N}_{K_\beta/k_\mathfrak{p}}(\Pi)\right)$; donc $d = m$). Comme $a_i \equiv 0 \bmod \mathfrak{p}$ et

$$1 + \frac{a_1}{\Pi} + \cdots + \frac{a_m}{\Pi^m} = 0,$$

il vient :

$$\frac{a_m}{\Pi^m} \equiv -1 \bmod \beta,$$

d'où

$$c_0 = \frac{\pi}{\Pi^m} = \frac{(-1)^m a_m}{\Pi^m} \equiv (-1)^{m-1} \bmod \beta.$$

Comme $b = b_0\pi^{\nu_\mathfrak{p}(b)} = b_0c_0^{\nu_\mathfrak{p}(b)}\Pi^{\nu_\beta(b)}$, on obtient la relation souhaitée en utilisant aussi (8.3) et (8.4).□

Remarque 8.5.4 *En fait, on appliquera la proposition lors du calcul de la signature du Frobenius seulement dans le cas d'une extension non ramifiée.*

Corollaire 8.5.5 *Soit F/E une extension de corps locaux, d'indice de ramification e. Soit u une unité de F. On a alors*

$$\left(\frac{\mathcal{N}_{F/E}(u)}{\mathfrak{p}_E}\right)_2 = \left(\frac{u}{\mathfrak{p}_F}\right)_2^e$$

Preuve Soit π (respectivement Π) un paramètre local de E (respectivement de F). D'après la définition du symbole de Hilbert et la proposition (8.5.3), on a

$$\left(\frac{\mathcal{N}_{F/E}(u)}{\mathfrak{p}_E}\right)_2 = \left(\frac{\mathcal{N}_{F/E}(u), \pi}{\mathfrak{p}_E}\right) = \left(\frac{u, \pi}{\mathfrak{p}_F}\right)_2.$$

Il existe une unité u' telle que $\pi = u'\Pi^e$. On a alors

$$\left(\frac{u, \pi}{\mathfrak{p}_F}\right) = \left(\frac{u, u'\Pi^e}{\mathfrak{p}_F}\right) = \left(\frac{u, \Pi}{\mathfrak{p}_F}\right)^e = \left(\frac{u}{\mathfrak{p}_F}\right)_2^e.$$

□

8.5.3 Le lemme d'abhyankar.

On rappelle et démontre le lemme suivant dit lemme d'Abhyankar :

Lemme 8.5.6 *Soit K un corps local, et soient L, L' deux extensions finies de K. Soit $e = e(L|K)$ (respectivement $e' = e(L'|K)$) l'indice de ramification de L/K (respectivement de L'/K). Supposons que e divise e' et que L/K soit modérée. L'extension LL'/L' est alors un extension non ramifiée.*

Preuve Soit E (respectivement E') la composante non ramifiée de L/K (respectivement de L'/K). En particulier :

$$\begin{cases} L/K & \text{est totalement ramifiée}; \\ EE'/E & \text{est non ramifiée}; \end{cases}$$

On a donc

$$\begin{aligned} [LE'/E] &= [L : E] \cdot [EE' : E] \\ &= e(L|E) \cdot [EE' : E], \end{aligned}$$

soit $[LE' : EE'] = e(L|E)$. Comme

$$e(LE'|EE') = e(LE'|K) = e(LE'|L)e(L|E),$$

il vient

$$\begin{aligned} e(L|E) = [LE' : EE'] &= e(LE'|EE')f(LE'|EE') \\ &= e(L|E)e(LE'|L)f(LE'|EE'), \end{aligned}$$

et on obtient

$$\begin{cases} LE'/L & \text{est non ramifiée}\,; \\ LE'/EE' & \text{est totalement ramifiée}\,; \end{cases}$$

Cette dernière est même modérément ramifiée car $e(LE'|EE') = e(L|E) = e$. Remarquons que par symétrie on a

$$\begin{cases} L'E/L' & \text{est non ramifiée}\,; \\ L'E/EE' & \text{est totalement ramifiée}\,; \end{cases}$$

et cette dernière extension est de degrés e'.Comme LE/EE' est modérée de degrés e, il existe une uniformisante π de EE' telle que $LE' = EE'(\pi^{1/e})$. Soit ω une uniformisante de $L'E$. Comme $L'E/EE'$ est totalement ramifiée, il existe une unité u de $L'E$ telle que $\pi = \omega^{e'}u$. Comme e divise e', on a

$$LL' = L'(LE') = L'E(u^{1/e}).$$

L'extension L/K étant modérée, $L'L/L'E$ est non ramifiée. Admettons brièvement ce fait. Comme on a montré avant que $L'E/L'$ est non ramifiée, il vient alors que $L'L/L'$ est non ramifiée.

Montrons que $L'L/L'E$ est non ramifiée. Soit en effet $P(X)$ le polynôme de $L'E[X]$ défini par $P(X) = X^e - u$ et soit $\overline{P}(X) = X^e - \overline{u} \in F_{LE'}$, où $F_{LE'}$ est le corps résiduel de LE'. Soit D le corps de décomposition de $\overline{P}$ sur $F_{LE'}$. Soit $\mathcal{D}$ l'unique extension (à isomorphisme près) non ramifiée de LE' dont le corps résiduel est D. Comme la caractéristique de $F_{LE'}$ ne divise pas e, le lemme de Hensel montre que P est totalement décomposé dans $\mathcal{D}$. En particulier, il contient $LE'(u^{1/e})$ qui est donc bien non ramifiée sur LE'.□

8.5.4 Une relation quadratique.

Dans la suite on se fixe un entier $e > 0$ pair. Soit F/E une extension totalement et modérément ramifiée de degrés e. Soit q le cardinal du corps résiduel de E. Soit s la

signature de la permutation de $\mathbb{Z}/e\mathbb{Z}$ définit par la multiplication par q. On note $\mathfrak{p}_E$ l'idéal maximal de l'anneau de valuation de E. On rappelle que si x est un élément non nul de E, on désigne par $\left(\frac{x}{\mathfrak{p}_E}\right)$ l'entier défini par

$$\left(\frac{x}{\mathfrak{p}_E}\right) = \begin{cases} 1 & \text{si } x \in E^2 \\ -1 & \text{si } E(\sqrt{x})/E \text{ est quadratique non ramifiée} \\ 0 & \text{si } E(\sqrt{x})/E \text{ est ramifiée} \end{cases}$$

Il vérifie la relation suivante :

Lemme 8.5.7 *Si* $\left(\frac{x}{\mathfrak{p}_E}\right)$ *et* $\left(\frac{y}{\mathfrak{p}_E}\right)$ *sont non nuls, alors*

$$\left(\frac{x}{\mathfrak{p}_E}\right) = \left(\frac{x}{\mathfrak{p}_E}\right)\left(\frac{y}{\mathfrak{p}_E}\right).$$

Preuve Comme les symboles sont non nuls, en particulier l'extension $E(\sqrt{x}, \sqrt{y})/E$ est non ramifiée, et donc il en va de même pour $E(\sqrt{xy})/E$. Si en fait cette extension est triviale, xy est un carré dans E, et les extensions $E(\sqrt{x}), E(\sqrt{y})$ coïncident. On a donc

$$1 = \left(\frac{xy}{\mathfrak{p}_E}\right) = \left(\frac{x}{\mathfrak{p}_E}\right) \cdot \left(\frac{y}{\mathfrak{p}_E}\right).$$

Si $E(\sqrt{xy})/E$ est quadratique, comme elle est non ramifiée et par unicité d'une telle extension, elle coincide par exemple avec $E(\sqrt{x})$ tandis que $E(\sqrt{y})$ est triviale. On a alors

$$-1 = \left(\frac{xy}{\mathfrak{p}_E}\right) = \left(\frac{x}{\mathfrak{p}_E}\right) \cdot \left(\frac{y}{\mathfrak{p}_E}\right).$$

□

On montre maintenant le lemme suivant qui lie s au symbole précédent :

Lemme 8.5.8 *Soit* π *une uniformisante de* E*. Il existe une unité* u_π *de* E *telle que*

$$\left(\frac{u_\pi}{\mathfrak{p}_E}\right) = \left(\frac{\pi}{\mathfrak{p}_F}\right) s.$$

Preuve Comme l'extension F/E est totalement et modérément ramifiée de degrés e, il existe une uniformisante ω de E, telle que $F = E(\omega^{1/e})$. Soit N la clôture normale de F, obtenue en adjoignant à F une racine primitive e-ième de l'unité ζ. L'extension N/F est non ramifiée car $(e, p) = 1$, ainsi que $F(\sqrt{\pi})/F$. En effet, sinon, π serait un carré dans le corps résiduel de F, qui est celui de E. Le polynôme $X^2 - \pi$ serait donc totalement décomposé dans le corps résiduel de E. Comme ce corps est de caractéristique différente de 2, le

polynôme le serait aussi dans F, en contradiction avec $[F(\sqrt{\pi}) : F] = 2$. La composée de N et $F(\sqrt{\pi})$ est donc cyclique sur F. Soit τ le Frobenius de l'extension N/F. En particulier, on a $\tau(\zeta) = \zeta^{q_E}$. Soit τ' un générateur de $\mathrm{Gal}(N(\sqrt{\pi})/F)$ dont la restriction à N est τ. Soit δ la classe de $\left(\prod_{i<j} \omega^{1/e} (\zeta^i - \zeta^j)\right)^2$ modulo E^2. Ce représentant d est le discriminant du polynôme $X^e - \omega$. Un tel discriminant est aussi donné par $d = e^e(-\omega)^{e-1}(-1)^{\frac{e(e-1)}{2}}$. Comme e est pair, il existe une unité u_π de E telle que $d \equiv u_\pi \pi \bmod E^2$.

Comme avant, on voit que les extensions $E(\sqrt{u_\pi})/E$ et $E(\sqrt{\omega\pi^{-1}})/E$ sont non ramifiées. Donc, par définition, $\left(\frac{u_{pi}}{\mathfrak{p}_E}\right) \quad \left(\frac{\omega\pi^{-1}}{\mathfrak{p}_E}\right) \neq 0$. On a

$$\left(\frac{u_\pi}{\mathfrak{p}_E}\right) = 1 \Leftrightarrow \frac{d}{\pi} \in E^2.$$

Néanmoins, les deux extensions F/E et $E(\zeta_e)/E$ étant linéairement disjointes, il vient :

$$\left(\frac{u_\pi}{\mathfrak{p}_E}\right) = 1 \Leftrightarrow \frac{d}{\pi} \in E(\zeta_e)^2, \quad \frac{d}{\pi} \in F^2.$$

On peut écrire d sous la forme $d = \omega^{e-1} \prod_{i<j} (\zeta^i - \zeta^j)^2$. Comme e est pair, il vient

$$\frac{d}{\pi} \in E(\zeta_e)^2 \Leftrightarrow \frac{\omega}{\pi} \in E(\zeta_e)^2.$$

On a donc

$$\left(\frac{d\pi^{-1}}{\mathfrak{p}_{E(\zeta)}}\right) = \left(\frac{\omega\pi^{-1}}{\mathfrak{p}_{E(\zeta)}}\right).$$

Comme $\omega\pi^{-1}$ est un élément de E, d'après le corollaire (8.5.5), on a

$$\left(\frac{\omega\pi^{-1}}{\mathfrak{p}_{E(\zeta)}}\right) = \left(\frac{\omega\pi^{-1}}{\mathfrak{p}_E}\right)^f.$$

Le fait que $\frac{X^2}{\pi}$ soit un carré de F, est équivalent à $\tilde{\tau}\left(\frac{X}{\sqrt{\pi}}\right) = \frac{X}{\sqrt{\pi}}$. Comme $X \in F$, c'est équivalent à $\frac{\tau(X)}{X} = \frac{\tilde{\tau}(\sqrt{\pi})}{\pi} = \left(\frac{\pi}{\mathfrak{p}_F}\right)$. L'élément τ, considéré comme la permutation de $\mathbb{Z}/e\mathbb{Z}$ qui multiplie ses éléments par q_E a pour signature $s = \frac{\tau(X)}{X}$. On a donc

$$\left(\frac{u_\pi}{\mathfrak{p}}\right) = 1 \Leftrightarrow \left(\frac{\omega\pi^{-1}}{\mathfrak{p}_E}\right)^f = 1, \quad s = \left(\frac{\pi}{\mathfrak{p}_F}\right).$$

Comme F/E est totalement ramifiée, et $E(\sqrt{\omega\pi^{-1}})/E$ est non ramifiée, ces extensions sont linéairement disjointes. En particulier, $\left(\frac{\omega\pi^{-1}}{\mathfrak{p}_E}\right) = \left(\frac{\omega\pi^{-1}}{\mathfrak{p}_F}\right)$. En effet, d'abord, ces deux

symboles sont non nuls. De plus, si $\omega\pi^{-1}$ est un carré de E, en particulier, c'est un carré de F. Inversement, s'il existe $y \in F$ tel que $\omega\pi^{-1} = y^2$, alors $E(\sqrt{\omega\pi^{-1}})/E$ est une sous-extension non ramifiée de F/E totalement ramifiée. Donc $E(\sqrt{\omega\pi^{-1}})/E$ est triviale et $y \in E$, c'est à dire $\omega\pi^{-1}$ est un carré de E. On a donc bien $\left(\frac{\omega\pi^{-1}}{\mathfrak{p}_E}\right) = \left(\frac{\omega\pi^{-1}}{\mathfrak{p}_F}\right)$. Comme ω est un carré de F car e est pair, on a

$$\left(\frac{\omega\pi^{-1}}{\mathfrak{p}_E}\right) = \left(\frac{\omega\pi^{-1}}{\mathfrak{p}_F}\right) = \left(\frac{\pi}{\mathfrak{p}_F}\right).$$

Donc

$$\left(\frac{u_\pi}{\mathfrak{p}}\right) = 1 \Leftrightarrow \left(\frac{\pi}{\mathfrak{p}_F}\right)^f = 1 \quad s = \left(\frac{\pi}{\mathfrak{p}_F}\right).$$

Supposons donc que $\left(\frac{u_\pi}{\mathfrak{p}}\right) = 1$. Comme $s = \left(\frac{\pi}{\mathfrak{p}_F}\right)$, on a $s\left(\frac{\pi}{\mathfrak{p}_F}\right) = 1$. Supposons que $\left(\frac{u_\pi}{\mathfrak{p}}\right) = -1$. Si f est pair, alors on doit avoir $s \neq \left(\frac{\pi}{\mathfrak{p}_F}\right)$, et comme ces symboles sont non nuls, il vient $s\left(\frac{\pi}{\mathfrak{p}_F}\right) = -1$. Si f est impair, et si $\left(\frac{\pi}{\mathfrak{p}_F}\right) = 1$, alors on doit avoir $s\left(\frac{\pi}{\mathfrak{p}_F}\right) = -1$. Supposons que f soit impair, et que $\left(\frac{\pi}{\mathfrak{p}_F}\right) = -1$. L'élément τ est d'ordre f. En particulier, $s^f = 1$, donc $s = 1$. On a alors $s\left(\frac{\pi}{\mathfrak{p}_F}\right) = -1$. On a donc bien dans tous les cas

$$\left(\frac{u_\pi}{\mathfrak{p}_E}\right) = \left(\frac{\pi}{\mathfrak{p}_F}\right) s.$$

□ D'un autre côté, on a le lemme suivant :

Lemme 8.5.9 *Soit π une uniformisante de E. On a alors :*

$$\left(\frac{u_\pi}{\mathfrak{p}_E}\right) = \left(\frac{\pi}{\mathfrak{p}_F}\right)\left(\frac{-1}{\mathfrak{p}_E}\right)^{\frac{e}{2}+1}.$$

Preuve Soit π' un paramètre local de E tel que $F = E(\pi'^{1/e})$. e étant pair, π' est un carré de F. Soit $P(X) = X^e - \pi'$. Son discriminant d est donné par $d = (-1)^{\frac{e}{2}+1} e^e \pi'^{e-1}$. Soit δ la classe de d modulo les carrés non nuls de E. Comme e est pair

$$\delta \equiv (-1)^{\frac{e}{2}+1}\pi' \bmod E^2.$$

Rappelons que l'on a posé dans la preuve du lemme précédent $\delta \equiv u_\pi \pi \bmod E^2$. On a donc

$$\left(\frac{u_\pi}{\mathfrak{p}_E}\right) = \left(\frac{\delta\pi^{-1}}{\mathfrak{p}_E}\right) = \left(\frac{(-1)^{\frac{e}{2}+1}\pi'\pi^{-1}}{\mathfrak{p}_E}\right) = \left(\frac{(-1)^{\frac{e}{2}+1}}{\mathfrak{p}_E}\right)\left(\frac{\pi'\pi^{-1}}{\mathfrak{p}_E}\right).$$

Comme F/E est totalement ramifiée, les extensions $E(\sqrt{\pi'\pi^{-1}})/E$ et $F(\sqrt{\pi'\pi^{-1}})/F$ sont de même degrés, et on a

$$\left(\frac{\pi'\pi^{-1}}{\mathfrak{p}_E}\right) = \left(\frac{\pi'\pi^{-1}}{\mathfrak{p}_F}\right).$$

Comme π' est un carré de F :

$$\left(\frac{\pi'\pi^{-1}}{\mathfrak{p}_E}\right) = \left(\frac{\pi^{-1}}{\mathfrak{p}_F}\right) = \left(\frac{\pi}{\mathfrak{p}_F}\right).$$

□

Les deux lemmes précédents montrent

$$s = \left(\frac{-1}{\mathfrak{p}_E}\right)^{\frac{e}{2}+1}.$$

Dans le cas qui nous intéresse, on a $e = q-1$ et $q_E = p$. On peut prendre $E = \mathbb{Q}_p$ et $F = E(p^{1/(q-1)})$. Comme $p > 2$, l'entier $\left(\frac{-1}{\mathfrak{p}_E}\right)$ est non nul et vaut 1 ssi -1 est un carré modulo p. Donc

$$s = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}+1\right)},$$

et on retrouve la relation de Graillat.

Remarque 8.5.10 *Pour le calcul de $\left(\frac{x}{\mathfrak{p}_E}\right)$, on dispose de la relation suivante de Cartier (voir [26]) : soit F un corps fini et soit V un espace vectoriel de dimension fini sur F. Soit u un automorphisme de V. On a alors :*

$$\binom{u}{V} = \binom{det(u)}{F}.$$

Elle permet de montrer le théorème de Frobenius Zolotarev. En effet, dans ce cas $F = \mathbb{F}_p$. De plus, si E est un corps local dont l'idéal maximal de l'anneau de valuation est $\mathfrak{p}_E$, et si x est une unité de E, alors on a

$$\left(\frac{x}{\mathfrak{p}_E}\right) = \binom{x}{\mathfrak{p}_E}.$$

Si on prend $E = \mathbb{Q}_p$, on a

$$\binom{det(u)}{F} = \left(\frac{det(u)}{\mathfrak{p}_E}\right) = \left(\frac{det(u)}{p}\right).$$

8.6 Application.

Notons par $\mathcal{I}_d(q)$ l'ensemble des polynômes irréductibles unitaires de degrés $d > 0$ à coefficient dans $\mathbb{F}_q$. Soit $i_q(d) = |\mathcal{I}_d(q)|$. Soit $\mathcal{F}$ l'automorphisme de Frobenius de $\mathbb{F}_{q^D}$. Commençons par calculer $\epsilon(\mathcal{F}^n)$. Si x et y sont deux éléments de $\mathbb{F}_{q^D}$, ils ont même polynôme minimal sur $\mathbb{F}_q$ si et seulement si y est dans l'orbite de x sous l'action de $\mathcal{F}^n$. Donc, si P est le polynôme minimal de x, $\mathcal{F}^n$ restreint aux racines de P, devient un cycle de longueur le degrés de P. On a donc :

$$\epsilon(\mathcal{F}^n) = (-1)^{\sum_{d|D}(d+1)i_q(d)}.$$

Mais il est connu que $\sum_{d|D} d \cdot i_q(d) = q^D$. Il vient :

$$\epsilon(\mathcal{F})^n = (-1)^{q^D + \sum_{d|D} i_q(d)} = (-1)^{q^D + N(q,D)}.$$

Si $2|n$, alors $N(q, D)$ a la même parité que p. Supposons n impair. Alors $(-1)^{q^D+N(q,D)}$ est la signature de $\mathcal{F}$, automorphisme de Frobenius de $\mathbb{F}_{p^{nD}}$. On va appliquer le théorème (8.1.1).

1. Cas $p = 2$; la signature de $\mathcal{F}$ est 1 sauf si $nD = 2$, ie $N(p^n, D)$ est pair sauf si $D = 2$.
2. Cas $p > 2$; alors $\epsilon(\mathcal{F}) = (-1)^{N(p^n,D)-1}$;
   (a) Cas $2 \nmid D$; alors $\epsilon(\mathcal{F}) = 1$, ie $N(p^n, D)$ est impair.
   (b) Cas $2|D$ et $p \equiv 1 \bmod 4$, alors $\epsilon(\mathcal{F}) = 1$, ie $N(p^n, D)$ est impair.
   (c) Cas $2|D$ et $p \equiv 3 \bmod 4$, alors $\epsilon(\mathcal{F}) = -1$, ie $N(p^n, D)$ est pair.

La proposition (8.1.2) est prouvée.

Bibliographie

[1] Abouzaid, Mourad. Les nombres de Lucas et de Lehmer sans diviseur primitif. j. Théor. Nombres Bordeaux **18** (2006), no.2, 299 − 313.

[2] Aigner A. Die diophantische Gleichung $x^2 + 4D = y^p$ im Zusammenhang mit Klassenzahlen (German). Monatsh.Math. **72** (1968), 1 − 5.

[3] Ankeny, N. Chowla, S. On the class number of the cyclotomic field. Canad. Journ. of ath. **3**, 1951, 486 − 494.

[4] Bennett, M. Rational approximation to algebraic numbers of small height. J. reine angew. Math. **535**, 2001, 1 − 49.

[5] Bennett, M. Györy, K. Mignotte, M. Pinter, A. Binomial Thue equations and polynomial powers. Compositio Math. **142**, (2006), 1103 − 1121.

[6] Beukers F. The multiplicity of binary recurrences. Compositio Mathematica **40** (1980), no.2, 251 − 267.

[7] Yu. Bilu, Catalan's conjecture (after Mihăilescu), Séminaire Bourbaki, Exposé 909, 55ème année (2002-2003).

[8] Bilu, Y. Catalan without logarithmic forms. Journal de théorie des nombres de Bordeaux. **17**, (2005), 69 − 85.

[9] Bilu, Y. On Le's and Bugeaud's Papers about the equation $ax^2+b^{2m-1} = 4c^p$, Monatsh. Math. **137** (2002), 1 − 3.

[10] Bilu, Bugeaud, Mignotte. The problem of Catalan. Springer, à paraître.

[11] Bilu, Y. Hanrot, G. Solving superelliptic Diophantine equations by Baker's method. Compositio. Math. **112**, 1998, no.3, 273 − 312.

[12] Bilu, Y. Hanrot, G. Voutier, P.M. Existence of primitive divisors of Lucas and Lehmers numbers, J. Reine angew. Math. **539** (2001), 75 − 122.

[13] Borevitch Z., Chafarevitch, I. Théorie des nombres. Editions Jacques Gabay.

[14] Brown, E. Diophantine equations of the form $ax^2 + Db^2 = y^p$, J. Reine Angew. Math. **291** (1977), 118 − 127.

[15] Y. Bugeaud, M. Mignotte, L'équation de Nagell-Ljunggren $\frac{x^n-1}{x-1} = y^q$, Enseign. Math. (2) **48** (2002), 147-168.

[16] Bugeaud, Yann. On some exponential Diophantine equations, Monatsh. Math. **132** (2001), $93-97$.

[17] Bugeaud, Yann. On the Diophantine equation $x^2 - 2^m = \pm y^n$. Proc. Amer. Math. Soc. **125** (1997), no.11, $3203-3208$.

[18] Bugeaud Yann. On the diophantine equation $x^2 - p^m = \pm y^n$. Acta Arith. **80** (1997), no.3, $213-223$.

[19] Bugeaud Y, Hanrot G, Mignotte M. Sur l'équation diophantienne $\frac{x^n-1}{x-1} = y^q \quad III$. Proc London Math Soc. **84**, 2002, $59-78$.

[20] Bugeaud Y, Hanrot G. Un nouveau critère pour l'équation de Catalan. Mathematika. **47**, (2000), $63-73$.

[21] Bugeaud, Yann ; Luca Florian ; Mignotte, Maurice ; Siksek, Samir. Perfect powers from products of terms in Lucas sequences. J. Reine Angew. Math. **611** (2007), $109-129$.

[22] Bugeaud, Y. Mignotte, M. On integers with identical digits. Mathematika, **46** 1999, $411-417$.

[23] Bugeaud, Y. Mignotte, M. Roy, Y. Shorey, T. The diophantine equation $\frac{x^n-1}{x-1} = y^q$ has no solution with x square, Math. Proc. Cambridge Phil. Soc. **127**, 1999, $353-372$.

[24] Bugeaud, Y. Mihăilescu, P. On the Nagell-Ljunggren equation $\frac{x^n-1}{x-1} = y^q$. Math. Scand. **101** (2007), $177-183$.

[25] Bugeaud, Yann ; Shorey, T.N. On the number of solutions of the generalized Ramanujan-Nagell equation. J.Reine Angew. Math. **539** (2001), $55-74$.

[26] Cartier P. Sur une généralisation des symboles de Legendre-Jacobi. L'enseignement matématiques. IIiéme série, **16**, tome 1, 1970, $31-48$.

[27] J. W. S. Cassels, On the equation $a^x - b^y = 1$ II, Proc. Camb. Philos. Soc. **56** (1960), 97-103 ; Corrigendum : Ibid. **57** (1961), 187.

[28] Cohen H. Number theory, Graduate texts in Mathematics **239**, Springer Verlag, New York.

[29] Cohn J.H.E. On square Fibonacci numbers, j. London Math. Soc.**39** 1964, $537-540$.

[30] Dupuy, Benjamin. A class number criterion for the equation $\frac{x^p-1}{x-1} = py^q$. Acta Arith. **127**, no.4, 2007, $391-401$.

[31] Estes, D. Guralnick, R. Schacher, M. Strauss, E. Equations in prime powers. Pacific journal of Mathematics, **118**, (1985), $359-367$.

[32] Faisant, Alain. L'équation diophantienne du second degrés. Hermann, Paris. 1991.

[33] Feng, Ke Qin. On the first factor of the class number of a cyclotomic field, Proc. Amer. Math. Soc., **84**, 1982, no.4, $479-482$.

[34] Gannoukh Said. Factorisation de certains nombres de classes relatifs, Thèse de l'IRMA, 2003.

[35] Granville, A.; Soundararajan K. Large character sums : pretentious characters and the Polya-Vinogradov theorem, j.Amer.Math.Soc. **20** (2007), no.2, $357-384$.

[36] Graillat, S. Sur la signature de l'automorphisme de Frobenius. http ://gala.univ-perp.fr/ graillat/papers/SignFrob.pdf

[37] Guralnick, R. Subgroups of prime power index in a simple group. Journal of Algebra, **81**, (1983), $304-311$.

[38] Hyyrö, S. Über das Catalan'sche Problem. Ann. Univ. Turku Ser. **79**, 1964, $3-10$.

[39] Iwasawa, K. A note on Jacobi's sums. Symp. Math. **15**, 1975, $447-459$.

[40] Janusz, G. Algebraic number fields. Pure and Applied Mathematics, Academic press, **55**, 1973.

[41] Jha Vijay, The Stickelberger ideal in the spirit of Kummer with application to the first case of the last Fermat's theorem, Queen's papers in pure and applied mathematics, **93**.

[42] Lehmer D. Prime factor of cyclotomic class numbers, Math. comp. **31**, 1977, $599-607$.

[43] Le Maohua. A note on the Diophantine Equation $x^2+4D=y^p$, Monatsh. Math. **116** (1993), no. $3-4$, $283-285$.

[44] Le Maohua. The applications of the method of Gelfond's-Baker to diophantine equations, Science Press, Beijing, 1998.

[45] Ljunggren, W. Über die gleichungen $1+Dx^2=2y^n$ und $1+Dx^2=4y^n$, Kong. Norsk. Vid. Selsk. Forth. Trond. **15**, (1943), $115-118$.

[46] Ljunggren, W. Zur Theorie der Gleichung $x^2+1=Dy^4$, Avh. Norske Vid. Akad. Oslo. **5**, (1942), $1-27$.

[47] Long, R. Algebraic number theory, Monographs and textbooks in pure and applied mathematics, **41**, 1977.

[48] Louboutin, S. Majorations explicites de $|L(1,\chi)|$ (suite). C. R. Acad. Sci. Paris **323**, 1996, $443-446$.

[49] Masley,J. Montgomery, L. Cyclotomic fields with unique factorisation. J. Number Theory. **10**, 1978, *no.*3, $273-290$.

[50] Mignotte, Laurent ; Nesterenko Yuri. Formes linéaires en deux logarithmes et determination d'interpolation. Journal of number theory **55** (1995), 285 − 321.

[51] Mignotte, M. On the diophantine equation $\frac{x^n-1}{x-1} = y^q$. Algebraic Number Theory and Diophantine Analysis, Halter-Koch Franz, F. Tichy Robert, p. 305 − 310.

[52] Mihăilescu, P. A cyclotomic inverstigation of the Catalan-Fermat conjecture, preprint.

[53] Mihăilescu, Preda. Class number conditions for the diagonal case of the equation of Nagell-Ljunggren. Diophantine Approximation, 245 − 273, Springer Verlag, Development in Mathematics, **16**, 2008.

[54] Mihăilescu, Preda. New bounds and conditions for the equation of Nagell-Ljunggren. J. Number Theory, **124**, 2007, *no.*2, 380 − 395.

[55] P. Mihăilescu, On the class groups of cyclotomic extensions in presence of a solution to Catalan's equation, J. Number Theory **118** (2006), 123–144.

[56] P. Mihăilescu, Primary cyclotomic units and a proof of Catalan's conjecture, J. reine angew. Math. **572** (2004), 167–195.

[57] Leu, Ming-Guang ; Li, Guan-Wei. The diophantine equation $2x^2+1 = 3^n$, Proc. Amer. Math. Soc. **131** (2003), no.12, 3643 − 3645.

[58] Mordell L.J. Diophantine equations, Academic Press, New York, (1969).

[59] Muriefah, F. On the diophantine equation $Ax^2 + 2^{2m} = y^n$, Int.j. Math.Sci. **25** (2001), no. 6, 373 − 381.

[60] Muriefah, F. On the diophantine equation $px^2 + q^{2m} = y^p$, journal of number theory. **128** (2008), 1670 − 1675.

[61] Nagell, T. Contributions to the theory of a category of diopantine equations of the second degree with two unknown. Nova Acta Soc. Sci. Upsal. **16**, (1955), 1 − 38.

[62] T. Nagell, Des équations indéterminées $x^2 + x + 1 = y^n$ et $x^2 + x + 1 = 3y^n$, Norsk Matem. Forenings Skrifter I, 2 (1921), 14 pp. (See also : Collected papers of Trygve Nagell, ed. P. Ribenboim, Queens Papers in Pure and Applied Mathematics 121, Kingston, 2002 ; Vol.1, pp. 79–94.)

[63] Puchta, J. On a criterion for Catalan's conjecture. Ramanujan J. **5**, 2001, 405 − 407.

[64] Ribenboim P. Catalan's conjecture. Academic press, boston, 1994

[65] Ribenboim P. The terms Cx^h in Lucas sequences : an algorithm and aplications to diophantine equations. Acta Arith. **106** (2003), no. 2, 105 − 114.

[66] Ribenboim P. ; Mc Daniel, Wayne L.The square terms in Lucas sequences. J. Number Theory 58 (1996), no.1, 104 − 123.

[67] Robbins Neville. Lucas numbers of the form px^2, where p is prime. Internat. J. Math. Math. Sci. **14** (1991), no.4, $697-703$.

[68] Robbins Neville. On Fibonacci numbers of the form px^2, where p is prime. Fibonacci Quart. **21** (1983), no.4, $266-271$.

[69] Samuel, P. Théorie algébrique des nombres. Hermann.

[70] Schwarz, W. Acta Arith., **72**, 1995, no.3, $277-279$.

[71] Serre, J.P. Cours d'Arithmétique, Puf éditions, 4-ième édition, 1995.

[72] Skolem, T. The use of a p-adic method in the theory of diophantine equations, Bull. Soc. Math. Belg., **7** (1955), 83-95.

[73] Steiner, R. Class number bound and Catalan equation. Math. comp. **67**, (1998), $1317-$ 1322.

[74] Störmer, C. L'équation $mArctan\left(\frac{1}{x}\right)+nArctan\left(\frac{1}{y}\right)=k\frac{\pi}{4}$. Bull. Soc. Math. France. **27**, (1899), $160-170$.

[75] Tao Liqun. A note on the diophantine equation $X^2+3^m=Y^n$, à paraître dans le journal Integers.

[76] Terai, N. The diophantine equation $x^2+q^m=p^n$. Acta Arithmetica, **63**, 1993, $351-$ 358.

[77] Washington, L. Introduction to Cyclotomic Fields, Springer, Berlin, seconde édition, 1997.

[78] Weil, A. Jacobi's sums as "grossencharaktere". Trans. Amer. Math. Soc. **73**, (1952), $457-495$.

[79] www.h-k.fr/publications/objectif-agregation.

[80] Zahidi M. Symboles des restes quadratiques des discriminants dans les extensions modérément ramifiées. Acta. Arith. **92**, (2000), $239-250$.

[81] Zahidi M. Symboles et restes quadratiques, Thèse de l'université de Limoges, 1999.

Résumé

Dans cette thèse, on étudie deux types d'équations diophantiennes. Une première partie de notre étude porte sur la résolution des équations dites de Ramanujan-Nagell $Cx^2 + b^{2m}D = y^n$. Une deuxième partie porte sur les équations dites de Ngell-Ljunggren $\frac{x^p+y^p}{x+y} = p^e z^q$ incluant le cas diagonal $p = q$. Les nouveaux résultats obtenus seront appliqués aux équations de la forme $x^p + y^p = Bz^q$. L'équation de Catalan-Fermat (cas $B = 1$) fera l'objet d'un traitement à part.

Mots clés : Nagell-Ljunggren, Ramanujan-Nagell, formes linéaires en deux logarithmes, nombres de Lucas, nombres de Lehmer, diviseurs primitifs, théorie du corps de classe, idéaux de Mihăilescu généralisés, nombres de classes, idéal de Stickelberger, entiers de Jacobi.

Abstract

In this thesis, we study two types of diophantine equations. A first part of our study is about the resolution of the Ramanujan-Nagell equations $Cx^2 + b^{2m}D = y^n$. A second part of our study is about the Nagell-Ljungren equations $\frac{x^p+y^p}{x+y} = p^e z^q$ including the diagonal case $p = q$. Our new results will be applied to the diophantine equations of the form $x^p + y^p = Bz^q$. The Fermat-Catalan equation (case $B = 1$) will be the subject of a special study.

Key words : Nagell-Ljunggren, Ramanujan-Nagell, linear forms in two logarithms, Lucas numbers, Lehmers numbers, primitive divisors, class field theory, generalized Mihăilescu ideals, class number, Stickelberger ideal, Jacobi integers.