Propriétés algébriques et analytiques de certaines suites indexées par les nombres premiers

Lucile Devin

NNT : 2017SACLS139

THÈSE DE DOCTORAT

de

L'UNIVERSITÉ PARIS-SACLAY

École doctorale de mathématiques Hadamard (EDMH, ED 574)

Établissement d'inscription : Université Paris-Sud

Laboratoire d'accueil : Laboratoire de mathématiques d'Orsay, UMR 8628 CNRS

Spécialité de doctorat : Mathématiques fondamentales

Lucile DEVIN

Propriétés algébriques et analytiques de certaines suites indexées par les nombres premiers

Date de soutenance : 26 Juin 2017

Après avis des rapporteurs : PHILIPPE MICHEL (Ecole Polytechnique Fédérale de Lausanne)
ZEÉV RUDNICK (Tel-Aviv University)

Jury de soutenance :

FARRELL BRUMLEY	(Université Paris 13) Examinateur
GAËTAN CHENEVIER	(Université Paris-Sud) Examinateur
ETIENNE FOUVRY	(Université Paris-Sud) Président du jury
FLORENT JOUVE	(Université de Bordeaux) Directeur de thèse
PHILIPPE MICHEL	(EPFL) Rapporteur
ZEÉV RUDNICK	(Tel-Aviv University) Rapporteur

Thèse préparée au
Département de Mathématiques d'Orsay
Laboratoire de Mathématiques (UMR 8628), Bât. 425
Université Paris-Sud 11
91405 Orsay CEDEX

Propriétés algébriques et analytiques de certaines suites indexées par les nombres premiers

Lucile Devin

Remerciements

Je remercie tout d'abord mon directeur de thèse Florent Jouve pour m'avoir proposé ces sujets de recherche passionnants, pour avoir encouragé mes recherches, m'avoir mise en contact avec de nombreux mathématiciens pour répondre à mes interrogations diverses et m'avoir ainsi convaincue qu'une part importante de la recherche consiste à se tenir au courant de ce que font les autres afin de savoir qui contacter quand on se pose des questions à la limite de son domaine d'expertise (!). Merci pour les nombreuses relectures et corrections (et corrections de corrections) de mes diverses versions d'articles et de manuscrit. Enfin, même s'il a fallu débattre sur l'utilité du café pour faire des mathématiques [1], merci pour la confiance et le soutien apportés durant ces trois années.

Je suis reconnaissante envers Philippe Michel pour avoir accepté de rédiger un rapport sur ma thèse ainsi que de participer à mon jury. J'ai aussi pu bénéficier d'une conversation sur les fonctions L au moment où je commençais mes recherches sur ce qui est devenu mon chapitre 3, qui m'a permis de partir dans une direction fructueuse.

I thank Zeév Rudnick for his report on my thesis and for his participation in my jury. The discussion we had in Luminy after he read my thesis was illuminating and should lead to interesting new applications of my results.

Je remercie le professeur Etienne Fouvry pour sa présence et son intérêt constant pour mes recherches, ainsi que pour m'avoir donné le goût de la théorie analytique des nombres. Sa participation à mon jury de thèse compte beaucoup pour moi.

Enfin, Je remercie Farrell Brumley et Gaëtan Chenevier pour avoir accepté de faire partie de mon jury de thèse. Je les remercie de s'être intéressé à mes recherches, ainsi que d'avoir accepté de partager leurs connaissances avec moi (cf. (!)).

Pour revenir à (!), de nombreux mathématiciens se sont montrés disponibles et la plupart des résultats obtenus dans cette thèse ont été imaginés ou améliorés grâce à eux. En plus des membres de mon jury déjà cités, je voudrais remercier pour cela Emmanuel Kowalski, Gérard Laumon, Antoine Chambert-Loir, Daniel Fiorilli, François Charles, Olivier Benoist, Alena Pirutka, Anne de Roton, Davide Lombardo, Yang Cao, Tiago Jardim da Fonseca... ainsi que beaucoup de professeurs de l'équipe AGA d'Orsay et d'ailleurs.

Je souhaite remercier particulièrement Jean-Pierre Serre pour s'être intéressé spontanément à mon travail et avoir offert quelques critiques constructives sur mon manuscrit.

L'atmosphère de théorie analytique des nombres parisienne dans laquelle j'ai évolué pendant ces trois années a été très agréable, notamment grâce aux rencontres de théorie analytique et élémentaire des nombres de Régis de la Bretèche où j'ai eu l'occasion de rencontrer de nombreux chercheurs, ainsi que de présenter l'avancée de mes recherches à deux occasions. Plus généralement j'ai pu participer pendant ces années à plusieurs conférences très intéressantes, dont je voudrais remercier les organisateurs ainsi que Hédi Daboussi qui était souvent là.

Je remercie aussi les doctorants et anciens doctorants de théorie analytique des nombres de région parisienne et d'ailleurs avec qui on a pu organiser des groupes de travail et d'autres distractions : Ramon, Djordjo, Kevin qui a ouvert la voie, Didier, Elie, Corentin, Alisa, David, Marine, Charlotte, Coline, Giacomo...

1. Malgré la pression, je n'ai pas cédé à l'attrait du café pour rédiger cette thèse.

Cette thèse a été préparée à l'université Paris-Sud, je remercie mesdames Blandin-Lavigne et Rey pour leur aide dans les démarches administratives.

Je remercie mes collègues doctorants de l'université d'Orsay, mais surtout ceux du bureau 014 : Cong, Lison, Mikolaj, Tiago, Yang et Alfonso qui était presque là, pour ces trois années studieuses et pleines d'aventures.

Enfin pour la bonne humeur et les aventures, ma famille et mes amis ont comptés pour beaucoup, pour les moments de détente, les vacances et les week-ends à la campagne, merci à tous de m'avoir offert votre temps, votre amour et votre soutien même quand je n'y étais pas très réceptive. Enfin pour tout et le reste, je remercie Valentin.

Table des matières

Introduction

La théorie des nombres modernes utilise une grande diversité d'outils de l'analyse mais aussi de la géométrie algébrique notamment dans l'étude des nombres premiers. Le travail présenté ici est une illustration de l'interaction possible de ces méthodes. Nous étudions deux types de suites indexées sur les nombres premiers en utilisant des méthodes aussi variées que celles de la géométrie algébrique, du grand crible, ou de l'analyse complexe.

Cette thèse est composée de deux parties indépendantes qui traitent chacune d'un type de suites indexées sur les nombres premiers. Pour chacune de ces suites, on s'intéresse à l'ensemble des indices pour lesquels le terme de la suite vérifie une certaine propriété algébrique (dans la première partie) ou plus analytique (dans la seconde). Une première information qui nous intéresse sur ces ensembles est leur taille : sont-ils finis ou infinis ? et s'ils sont infinis sont-ils de taille comparable à l'ensemble des nombres premiers tout entier ?

Pour estimer la taille d'un ensemble, on peut utiliser deux notions de densité. La première est la densité naturelle :

Définition 1. Soit A un sous-ensemble d'un ensemble $\mathcal{P}$, on définit la densité naturelle de A dans $\mathcal{P}$ par

$$\mathrm{dens}_{\sup}(A) = \limsup_{X\to\infty} \frac{|\{p \in A : p \leq X\}|}{|\{p \in \mathcal{P} : p \leq X\}|}$$

et

$$\mathrm{dens}_{\inf}(A) = \liminf_{X\to\infty} \frac{|\{p \in A : p \leq X\}|}{|\{p \in \mathcal{P} : p \leq X\}|}.$$

Si ces deux quantités sont égales, on dit que l'ensemble A admet une densité naturelle. Leur valeur commune est appelée *densité naturelle* de A.

On définit aussi la densité logarithmique :

Définition 2. Soit A un sous-ensemble d'un ensemble $\mathcal{P}$, on définit la densité logarithmique de A dans $\mathcal{P}$ par

$$\delta_{\sup}(A) = \limsup_{X\to\infty} \frac{\sum_{\substack{p\in A\\ p\leq X}} \frac{1}{p}}{\sum_{\substack{p\in \mathcal{P}\\ p\leq X}} \frac{1}{p}}$$

et

$$\delta_{\inf}(A) = \liminf_{X\to\infty} \frac{\sum_{\substack{p\in A\\ p\leq X}} \frac{1}{p}}{\sum_{\substack{p\in \mathcal{P}\\ p\leq X}} \frac{1}{p}}.$$

Si ces deux quantités sont égales, on dit que l'ensemble A admet une densité logarithmique. Leur valeur commune est appelée *densité logarithmique* de A.

Les deux notions de densité coïncident si elles existent, mais il existe des ensembles qui ont une densité logarithmique sans avoir de densité naturelle. C'est le cas par exemple pour l'ensemble des nombres premiers dont le premier chiffre est 1 (voir [FL96]).

Il est clair qu'un ensemble qui admet une densité (inférieure) naturelle (ou logarithmique) non-nulle par rapport à un ensemble infini est lui-même infini.

Pour des questions de concision, écrira parfois « densité » à la place de « densité naturelle » ou « densité logarithmique » si le contexte est clair. Notamment dans le chapitre 1 la densité dont on parle est toujours la densité naturelle, tandis que dans le chapitre 3 on est contraint d'utiliser la densité logarithmique.

Les chapitres 1 et 2 qui suivent constituent la première partie de cette thèse. C'est une version légèrement améliorée et plus approfondie de l'article [Dev17]. On s'intéresse à une suite indexée par les nombres premiers dont la provenance est géométrique. Étant donné un schéma affine X de type fini sur $\mathbf{Z}$, on considère pour tout p premier la quantité $N_X(p)$: le nombre de $\mathbf{F}_p$-points de la réduction modulo p de X. L'objet d'étude de notre première partie est la suite $N_X(p) \pmod p$. En particulier on s'intéresse à l'ensemble $\{p \text{ premier } : p \nmid N_X(p)\}$, c'est-à-dire l'ensemble des p tel que la coordonnée d'indice p de la suite est non-nulle.

La motivation pour cette étude vient des travaux de Fouvry et Katz : dans [FK01] les auteurs montrent que si l'ensemble $\{p \text{ premier } : p \nmid N_X(p)\}$ est infini, alors via un processus de stratification de X, on affine les estimations de Weil de certaines sommes exponentielles indexées sur les $\mathbf{F}_p$-points de X.

On montre dans le chapitre 1 que sous certaines conditions sur la géométrie du schéma X, l'ensemble $\{p \text{ premier } : p \nmid N_X(p)\}$ est soit infini soit inclus dans un ensemble fini de « premiers de mauvaise réduction ». De plus si cet ensemble est infini, on montre qu'il est « assez gros » : il a une densité naturelle inférieure strictement positive (selon la définition 1). Le résultat principal de ce chapitre est le suivant.

Théorème 1. *Soit X un schéma de type fini sur $\mathbf{Z}$. On suppose que $X \times_{\mathbf{Z}} \mathbf{Q}$ est birationnelle à une variété projective lisse $Y_0/\mathbf{Q}$ satisfaisant :*

1. $\dim(Y_0) \leq 3$ *et*
2. *le nombre de Hodge $h^{0,3}(Y_0)$ est nul.*

Alors il existe un ensemble fini $\Sigma'_{X,Y}$ de mauvais premiers, ne dépendant que de X, de Y un modèle de Y_0 sur $\mathbf{Z}$ et de l'application birationnelle entre X_0 et Y_0, tel que pour tout $a_1, \dots, a_n \in \mathbf{Z}$, soit l'ensemble $\{p \notin \Sigma'_{X,Y} : p \nmid \prod_{i=1}^n (N_X(p) - a_i)\}$ est vide, soit il admet une densité naturelle inférieure strictement positive.

On donne plus de précisions sur l'ensemble de mauvais premiers dans la définition 1.36. On redonne la définition des nombres de Hodge dans la sous-section 1.1.3. Ce théorème est une version améliorée de [Dev17, Th. 1.1] où l'hypothèse 2 est plus forte : on suppose que dans le cas où $\dim(Y_0) = 3$, le troisième nombre de Betti $b_3(Y_0)$ est nul. Les méthodes utilisées dans ce chapitre sont principalement issues de la géométrie algébrique. La preuve du théorème 1 se base notamment sur la notion de fonction frobenienne utilisée systématiquement par Serre dans [Ser12]. Cela nous permet de trouver d'autres exemples d'applications des résultats de Fourvy et Katz.

Dans un deuxième temps dans le chapitre 2, on s'intéresse au plus petit premier p pour lequel le terme $N_X(p) \pmod p$ évite un ensemble de valeurs fixées. Par exemple dans le cas initial : on cherche le plus petit premier p qui vérifie $p \nmid N_X(p)$.

Le théorème 1 garantit en effet qu'il suffit de trouver un élément de bonne réduction dans l'ensemble $\{p : p \nmid \prod_{i=1}^n (N_X(p) - a_i)\}$ pour assurer qu'il est assez gros. Il est donc naturel de chercher si cet élément va être assez facilement accessible. On se restreint au cas où X est une courbe hyperelliptique et on utilise le fait qu'alors les ensembles $\{p : p \nmid \prod_{i=1}^n (N_X(p) - a_i)\}$ ont de bonnes propriétés algébriques. Des méthodes de grand crible telles que celles présentées dans [Kow08a] permettent alors de donner des bornes sur ce plus petit élément pour certaines familles de courbes hyperelliptiques. On déduit notamment par application du crible le résultat suivant.

Théorème 2. *Soit $f \in \mathbf{Z}[X]$ un polynôme séparable de degré $2g$. On s'intéresse à la famille de courbes*

$$C_u : y^2 = f(t)(t-u)$$

où u décrit $\mathbf{Z} - \{x, f(x) = 0\}$. Alors

$$\frac{1}{T}|\{u \in \mathbf{Z} : |u| \leq T, p \mid \prod_{i=1}^{n}(N_{C_u}(p) - a_i), \forall p < Q_{g,1}(T) \text{ de bonne réduction }\}| \ll \frac{Q_{g,1}(T)}{T \log T}$$

avec $Q_{g,1}(T) = (2K_g\gamma \log T)^{\gamma/2} (\log(2K_g\gamma \log T))^{\frac{\gamma}{2}(1-\frac{2}{\gamma+2n-2})}$ pour une constante K_g ne dépendant que de g et $\gamma = 4g^2 + 2g + 4$.

On a donc à genre fixé, une borne logarithmique en la taille des coefficients pour la taille du plus petit premier de l'ensemble $\{p : p \nmid \prod_{i=1}^{n}(N_{C_u}(p) - a_i)\}$ pour la plupart des paramètres $u \in \mathbf{Z}$. Ce théorème est l'objet de [Dev17, Sect. 5], on obtient aussi dans le chapitre 2 des bornes pour le plus petit premier dans l'ensemble $\{p : p \nmid \prod_{i=1}^{n}(N_X(p) - a_i)\}$ dans le cadre de familles plus générales à plusieurs paramètres. On prouve les résultats de ce type en utilisant deux techniques de crible imbriquées selon une technique inspirée de l'article [EEHK09].

Le chapitre 2 est aussi l'occasion de revoir quelques méthodes de grand crible. On s'intéresse notamment à une nouvelle variante du grand crible introduite par Bellaïche dans [Bel16]. L'idée est de ne plus seulement prendre en compte la taille des ensembles criblants mais aussi leur structure dans le cas où le crible se fait sur un groupe. Dans le cas où la table des caractères du groupe en question est connue, cela peut donner de meilleures bornes que le grand crible développé par Kowalski dans [Kow08a].

Enfin le chapitre 3 est dédié à la généralisation des courses de nombres premiers de Chebyshev. On s'intéresse à une suite du type $\lambda_f(p)$ de coefficients de fonctions L assez générales. Sous des conjectures classiques, si la fonction L est auto-duale, la suite associée s'équirépartit dans un intervalle de $\mathbf{R}$ de façon symétrique par rapport à 0. Les questions de biais de Chebyshev généralisées à ces suites sont : que peut-on dire du signe de la fonction $\sum_{p \leq x} \lambda_f(p)$? Quelle est la taille de l'ensemble des x pour lesquels cette fonction est strictement positive ? Est-ce que l'ensemble $\{x \geq 2 : \sum_{p \leq x} \lambda_f(p) > 0\}$ est « la moitié » de l'ensemble total ?

On montre que si la fonction L satisfait certaines propriétés analytiques qui sont en général attendues dans la théorie des fonctions L, alors on peut commencer à répondre à ces questions. On utilise notamment la notion de distribution logarithmique limite qui est, depuis les travaux de Rubinstein et Sarnak [RS94], la quantité centrale à étudier dans les questions de biais de Chebyshev. Notre premier résultat est le suivant.

Théorème 3. *Soit $L(f, s)$ une fonction L analytique suivant la définition 3.1 et auto-duale. Soit $\beta_{f,0} = \sup\{\mathrm{Re}(\rho) : L(f, \rho) = 0\}$. On pose*

$$E_f(x) = \frac{\log x}{x^{\beta_{f,0}}} \sum_{p \leq x} \lambda_f(p).$$

La fonction $E_f(x)$ admet une distribution logarithmique limite μ_f (selon la définition 3.15).

Ce résultat se démontre par des méthodes d'analyse complexe classiques dans l'étude des fonctions L. Il demande aussi un argument de théorie ergodique : le théorème de Kronecker–Weyl. On donne de plus une expression explicite pour la valeur de la moyenne et de la variance de la mesure μ_f en fonction des zéros de la fonction $L(f, s)$. On peut appliquer ce résultat à tout élément de notre classe de fonctions L analytiques, cela fournit de nouveaux exemples de courses de nombres premiers intéressantes.

Pour répondre plus précisément aux questions posées dans le cadre des biais de Chebyshev, on cherche ensuite à trouver plus de propriétés pour la mesure μ_f. On s'inspire de conjectures classiques sur les répartitions des zéros de fonctions L pour rajouter des hypothèses dans notre cadre.

Théorème 4. *Soit $L(f,s)$ une fonction L analytique suivant la définition 3.1 et auto-duale. Pour tout $T>0$ soit $\mathcal{Z}_f^*(T)=\{\gamma : 0<\gamma\leq T, L(f,\beta_{f,0}+i\gamma)=0\}$.*

1. *Supposons qu'il existe $\epsilon>0$ tel que pour tout T assez grand, il existe $\gamma_T\in\mathcal{Z}_{\mathcal{S}}^*(T^{\frac{1}{2}-\epsilon})$ tel que $\gamma_T\notin\langle\mathcal{Z}_f^*(T)-\{\gamma_T\}\rangle_{\mathbf{Q}}$. Alors l'ensemble $\{x\geq 2:\sum_{p\leq x}\lambda_f(p)>0\}$ admet une densité logarithmique.*
2. *Supposons que pour tout T, pour tout $(k_\gamma)_\gamma\in\mathbf{Z}^{\mathcal{Z}_f(T)}$ tel que $\sum_{\gamma\in\mathcal{Z}_f(T)}k_\gamma\gamma=0$ on a $\sum_{\gamma\in\mathcal{Z}_f(T)}k_\gamma\equiv 0\ [\mathrm{mod}\ 2]$ (conjecture 3.14). Alors la distribution limite μ_f est symétrique par rapport à sa moyenne.*
3. *Supposons que l'hypothèse de Riemann généralisée est satisfaite pour $L(f,s)$ (conjecture 3.6), alors $\operatorname{supp}\mu_f=\mathbf{R}$.*

Les hypothèses des deux premiers points sont inspirées du fait que l'on imagine en général que les zéros des fonctions L ont des parties imaginaires qui sont indépendantes les unes des autres. On utilise des versions affaiblies de l'hypothèse (LI) (conjecture 3.10) qui est notamment utilisée dans les travaux de Rubinstein et Sarnak [RS94]. On montre des résultats similaires à ceux de loc. cit. sous des hypothèses plus faibles. Par exemple le point 2 implique que si la moyenne de la distribution μ_f est non nulle, alors la course associée va être biaisée dans la direction du signe de cette moyenne.

L'hypothèse de Riemann est certainement une des conjectures les plus citées en théorie analytique des nombres. On note qu'une certaine force de nos résultats réside dans le fait qu'on ne l'utilise pas plus tôt (le théorème 3 par exemple est inconditionnel). On remarque qu'une conséquence intéressante du point 3 est que la densité logarithmique de l'ensemble $\{x\geq 2:\sum_{p\leq x}\lambda_f(p)>0\}$ ne peut pas être extrême : sous l'hypothèse de Riemann on a

$$0<\delta_{\inf}\left\{x\geq 2:\sum_{p\leq x}\lambda_f(p)>0\right\}\leq\delta_{\sup}\left\{x\geq 2:\sum_{p\leq x}\lambda_f(p)>0\right\}<1.$$

Les propriétés analytiques que l'on suppose sur la fonction L dans le théorème 3 sont assez générales. Elles sont vérifiées dans de nombreux cas. Cela nous permet d'appliquer le principe des courses de nombres premiers à de nouveaux exemples. On montre notamment le résultat suivant.

Théorème 5. *Soient E_1 et E_2 deux courbes elliptiques définies sur $\mathbf{Q}$ toutes deux sans multiplication complexe, soient f_1 et f_2 les formes automorphes associées. On suppose que les courbes E_1 et E_2 ne sont pas isogènes sur $\mathbf{Q}$ ni sur aucune extension abélienne de $\mathbf{Q}$. Sous l'hypothèse de Riemann pour $L(f_{E_1}\otimes f_{E_2},\cdot)$, la fonction*

$$E(x)=\frac{\log(x)}{\sqrt{x}}\sum_{p\leq x}\frac{a_p(E_1)a_p(E_2)}{p}$$

admet une distribution logarithmique limite d'espérance strictement négative.

L'interprétation de ce résultat est que dans la situation donnée, les coefficients $a_p(E_1)$ et $a_p(E_2)$ ont tendance à être souvent de signes opposés.

Notations

Rappelons quelques notations standard utilisées dans cette thèse. On note $|A|$ le cardinal de l'ensemble A.

On note $\mathcal{P}$ l'ensemble des nombres premiers. En général les notations p et ℓ sont réservées à des nombres premiers distincts. On note (a, b) le plus grand diviseur commun des entiers a et b.

Pour $x \in \mathbf{R}$, on note $[x]$ la partie entière de x.

Pour $z \in \mathbf{C}$, on note $e(z) = \exp(2i\pi z)$.

On utilise les notations $f \ll g$ pour $x \in X$ ou $f = O(g)$ pour $x \in X$, où X est un ensemble sur lequel f et g sont définies, pour dire qu'il existe une constante $C \geq 0$ telle que $|f(x)| \leq Cg(x)$ pour tout $x \in X$. La constante C aussi appelée « constante implicite » peut dépendre de certains paramètres qui seront précisés. On écrit $f \asymp g$ pour $f \ll g$ et $g \ll f$. Enfin $f(x) = o(g(x))$ quand $x \to x_0$ signifie que $f(x)/g(x) \to 0$ quand $x \to x_0$.

Chapitre 1

Classes de congruence modulo des premiers du nombre de points rationnels des variétés

Dans [FK01], Fouvry et Katz introduisent une condition intéressante pour garantir une bonne estimation de certaines sommes exponentielles indexées sur un schéma affine.

Théorème 1.1. *Soient d, n, D des entiers ≥ 1, soit X un sous-schéma fermé de $\mathbb{A}^n_{\mathbf{Z}[1/D]}$, tel que $X/\mathbf{C}$ est irréductible et lisse de dimension d. On suppose qu'il existe un ensemble infini de premiers p pour lesquels il existe un corps fini E_p de caractéristique p tel que $|X(E_p)|$ est premier à p,*

Alors pour tout morphisme $f : X \to \mathbb{A}^1$ il existe une constante C ne dépendant que de X et f, un sous-schéma fermé $X_2 \subset \mathbb{A}^n_{\mathbf{Z}[1/D]}$, de dimension relative $\leq n-2$, tels que pour $h \in \mathbb{A}^n_{\mathbf{Z}[1/D]}(\mathbf{F}_p) - X_2(\mathbf{F}_p)$, tout p premier ne divisant pas D, tout caractère additif non-trivial ψ de $\mathbf{F}_p$, on a

$$\left| \sum_{x \in X(\mathbf{F}_p)} \psi(f(x) + h_1 x_1 + \ldots + h_n x_n) \right| \leq C p^{\frac{d}{2}}.$$

Ce théorème est la concaténation de [FK01, Th. 8.1 et Cor. 4.5] qui traitent en fait du A-nombre de X. On donne plus de détails sur ces résultats et sur le A-nombre dans la section 1.2 de ce chapitre. Notamment sous la même condition, on a aussi une bonne répartition des points rationnels de X sur $\mathbf{F}_p$. Le but de ce chapitre est d'étudier l'hypothèse de ce théorème. On a en effet l'impression que cette hypothèse devrait être satisfaite avec grande probabilité pour un schéma X choisi « au hasard ».

On s'intéresse plus particulièrement au nombre de $\mathbf{F}_p$-points modulo p de schémas définis sur $\mathbf{Z}$ en faisant varier p dans l'ensemble des nombres premiers. Le but est de savoir dans quelle mesure on peut dire que la propriété « p ne divise pas $N_X(p)$ » (le nombre de $\mathbf{F}_p$-points) est typique. Il y a deux façons de comprendre le mot « typique » dans la phrase précédente. La première est : étant donné un schéma X particulier, peut-on minorer la taille de l'ensemble des premiers $\{p : p \nmid N_X(p)\}$? Le but dans l'optique du théorème 1.1 est de garantir qu'il est infini. On répond à cette question en donnant des exemples pour lesquels on sait minorer la densité inférieure (au sens de la définition 1) de cet ensemble, assurant ainsi qu'il est infini et même « assez gros ». C'est le point principal de la partie 1.4. On peut aussi se demander si l'ensemble $\{p : p \nmid N_X(p)\}$ est infini pour beaucoup de schémas dans une famille. Dans ce but on donne dans la sous-section 1.4.4 une condition géométrique sur le schéma étudié pour que cette propriété soit vérifiée. C'est le cas par exemple pour les courbes irréductibles (voir la proposition 1.38).

Ces résultats sont en lien étroit avec un théorème de Serre [Ser12, Th. 6.3]. On utilise en fait une forme un peu plus générale que l'on re-démontre dans la section 1.3.

Comme nous l'a fait remarquer A. Chambert-Loir à propos d'une version préliminaire de [Dev17], les résultats obtenus se généralisent en fait facilement au cas plus général de l'étude d'ensembles :

$$\{p \in \mathcal{P} : p \nmid \prod_{i=1}^{n} (N_X(p) - a_i)\}$$

où X est un schéma de type fini sur $\mathbf{Z}$ (et non plus seulement affine), et $a_1, \ldots, a_n$ sont des entiers fixés.

On verra que la géométrie joue un rôle important dans ce chapitre, on donnera donc tout d'abord quelques éléments de géométrie algébrique sur les schémas de type fini sur $\mathbf{Z}$. On rappellera aussi quelques résultats classiques de géométrie algébrique qui nous permettront de simplifier notre problème.

1.1 Schémas de type fini sur Z

Dans ce chapitre on s'intéresse au nombre de $\mathbf{F}_p$-points de schémas de type fini sur $\mathbf{Z}$. Le but de cette section est de rappeler comment calculer ces nombres avec les outils de la géométrie algébrique.

Notre objet d'étude sera un schéma X séparé réduit de type fini sur $\mathrm{Spec}(\mathbf{Z})$. On pourra voir par exemple [Har77, I] pour des définitions. Étant donné X un tel schéma, pour chaque nombre premier p, on peut associer à X le schéma $X_p = X \times_{\mathbf{Z}} \mathbf{F}_p$ la « réduction modulo p » de X. Le schéma X_p est séparé et de type fini sur $\mathbf{F}_p$. De la même façon, on s'intéresse à la fibre générique du morphisme $X \to \mathrm{Spec}(\mathbf{Z})$. On notera dans la suite $X_0 = X \times_{\mathbf{Z}} \mathbf{Q}$ ce schéma.

Remarque 1.
1. Pour X un schéma sur un anneau A et B un A-module, on prend la convention de noter $X \times_A B$ le produit fibré $X \times_{\mathrm{Spec}\, A} \mathrm{Spec}\, B$ pour alléger les notations (on oublie le symbole « Spec »).
2. Il est à noter que l'on ne suppose pas nos schémas irréductibles ni même connexes.

On peut compter le nombre de points modulo p de X. Plus précisément on s'intéresse à la quantité $N_X(p) := |X_p(\mathbf{F}_p)|$ le nombre de $\mathbf{F}_p$-points rationnels de X_p. Dit autrement $N_X(p)$ est le nombre de points fermés de X_p dont le corps résiduel est de cardinal p. On ne compte pas avec « multiplicité ». Ainsi si $(X_p)^{\mathrm{red}}$ est le schéma réduit associé à X_p, on a $|(X_p)^{\mathrm{red}}(\mathbf{F}_p)| = |X_p(\mathbf{F}_p)|$.

Dans le cas affine, on a $X = \mathrm{Spec}(\mathbf{Z}[T_1, \ldots, T_n]/(f_1, \ldots, f_m))$ où les f_i sont des polynômes à coefficients entiers. La quantité $N_X(p)$ est exactement le nombre de solutions dans $(\mathbf{F}_p)^n$ aux équations polynomiales qui définissent X.

Dans le cas projectif, on a $X = \mathrm{Proj}(\mathbf{Z}[T_1, \ldots, T_n]/(f_1, \ldots, f_m))$ où les f_i sont des polynômes homogènes à coefficients dans $\mathbf{Z}$. Pour p un premier le nombre de points $N_X(p)$ est alors le nombre de solutions dans $(\mathbf{F}_p)^{n+1} - \{0\}$ aux équations qui définissent X à multiplication par un scalaire près dans $\mathbf{F}_p^*$.

On connaît de nombreuses propriétés de $N_X(p)$, notamment par les conjectures de Weil prouvées par Deligne ([Del80]). Pour énoncer ces résultats nous allons avoir besoin de quelques notions de cohomologie ℓ-adique. La plupart des énoncés des sous-sections 1.1.1 et 1.1.2 m'ont été expliqués par G. Laumon, j'ai aussi consulté [Ser12, Chap. 4] et le survol de Katz [Kat94b]. Pour des références plus classiques sur le sujet, on pourra voir [Mil80] ou [Del77]. On cite ensuite quelques conséquences des conjectures de Weil qui nous seront utiles par la suite. La plupart de ces résultats s'expriment mieux dans le cadre des variétés projectives lisses. On commence donc par énoncer un résultat nous permettant de lier notre schéma X à une variété projective lisse sur $\mathbf{Q}$ grâce à la résolution des singularités de Hironaka.

1.1.1 Résolution des singularités

Le cas projectif lisse est souvent le plus facile à traiter : la cohomologie y est mieux connue. On peut remarquer notamment que la dualité de Poincaré est vérifiée dans ce cas. Il est donc séduisant d'essayer de se ramener aussi souvent que possible au cas des schémas projectifs lisses. D'après un résultat de Hironaka (voir par exemple [Kol07, Th. 3.36]), sur un corps de caractéristique 0 on peut résoudre les singularités d'un schéma pour obtenir une variété projective lisse. Dans le cas de notre schéma X sur $\mathbf{Z}$, on pourra donc résoudre les singularités de X_0, le but de cette sous-section est d'étudier les conditions permettant de propager cette résolution de X_0 à X_p.

Commençons par énoncer le théorème de résolution des singularités sur $\mathbf{Q}$. On utilise pour cela l'ouvert lisse du schéma X_0.

Définition 1.2. Soit X_0 une variété sur $\mathbf{Q}$, on définit X_0^{lisse} l'ouvert lisse de de X_0, comme le sous-schéma ouvert de X_0 sur lequel la jacobienne de X_0 a rang maximal.

Théorème 1.3 (Hironaka)**.** *Soit X_0 un schéma projectif réduit sur $\mathbf{Q}$, alors il existe un schéma $\tilde{X}_0$ projectif lisse sur $\mathbf{Q}$ et un morphisme birationnel $\tilde{X}_0 \to X_0$ qui est un isomorphisme au dessus de X_0^{lisse}. De plus $\tilde{X}_0 - X_0^{\mathrm{lisse}}$ est un diviseur à croisement normaux.*

Le théorème de Hironaka donne la résolution des singularités par une série d'éclatements [Kol07, Th. 3.36]. Ces éclatements peuvent être définis dans le corps de base de la variété (ici $\mathbf{Q}$), on obtient ainsi une application birationnelle $\tilde{X}_0 \to X_0$ définie sur $\mathbf{Q}$. Quitte à inverser un nombre fini d'entiers, on peut relever cette résolution à $\mathbf{Z}$. Énonçons ce résultat dans le cas plus simple où X_0 est lisse (quitte à considérer l'ouvert lisse) mais pas forcément projective.

Théorème 1.4. *Soit X un schéma quasi-projectif réduit sur $\mathbf{Z}$ tel que X_0 est lisse sur $\mathbf{Q}$. Il existe un entier $N \geq 1$, un schéma Y projectif lisse sur $\mathbf{Z}[1/N]$ et un sous-schéma fermé $D \subset Y$ tels que*

1. *le sous-schéma D est un diviseur à croisement normaux relatif sur $\mathrm{Spec}(\mathbf{Z}[1/N])$ (voir par exemple [SGA03, XIII 2.1] pour une définition précise), en particulier pour tout premier $p \nmid N$, le sous-schéma D_p est un diviseur à croisement normaux dans Y_p,*
2. *on a $X \times_{\mathbf{Z}} \mathbf{Z}[1/N] \simeq Y - D$.*

1.1.2 Cohomologie à support compact

Fixons $\overline{\mathbf{Q}}$ une clôture algébrique de $\mathbf{Q}$, pour tout premier on va choisir une clôture algébrique de $\mathbf{F}_p$ de façon à avoir des morphismes canoniques (dépendants de ces choix) entre les groupes de Galois que l'on va considérer par la suite.

Pour tout p premier, on fixe $\overline{\mathbf{Q}}_p$ une clôture algébrique de $\mathbf{Q}_p$ et on fait le choix d'un plongement de $\overline{\mathbf{Q}}$ dans $\overline{\mathbf{Q}}_p$. On note $\mathbf{Q}_p^{\mathrm{nr}}$ l'extension maximale non ramifiée de $\mathbf{Q}_p$ dans $\overline{\mathbf{Q}}_p$. Soit $\mathbf{Z}_p^{\mathrm{nr}}$ l'anneau des entiers de $\mathbf{Q}_p^{\mathrm{nr}}$: c'est la clôture intégrale de $\mathbf{Z}_p$ dans $\mathbf{Q}_p^{\mathrm{nr}}$. L'anneau $\mathbf{Z}_p^{\mathrm{nr}}$ est à valuation discrète, son corps résiduel est une clôture algébrique de $\mathbf{F}_p$ que l'on note $\overline{\mathbf{F}}_p$.

On a alors la suite exacte :

$$1 \to \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p^{\mathrm{nr}}) \to \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p) \to \mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p) \to 1. \tag{1.1}$$

Le groupe $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p^{\mathrm{nr}})$ est aussi appelé sous-groupe d'inertie et noté I_p. Le groupe $\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$ est isomorphe à $\sigma_p^{\hat{\mathbf{Z}}}$ où σ_p est l'endomorphisme de Frobenius arithmétique

donné par l'élévation à la puissance p dans $\overline{\mathbf{F}}_p$. Le choix du plongement $\overline{\mathbf{Q}}$ dans $\overline{\mathbf{Q}}_p$ nous donne aussi un morphisme

$$\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p) \to \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}). \tag{1.2}$$

Reprenons notre schéma X séparé réduit de type fini sur $\mathrm{Spec}(\mathbf{Z})$. On définit $\overline{X}_p = X_p \times_{\mathbf{F}_p} \overline{\mathbf{F}}_p$. De la même façon on définit la variété $\overline{X}_0 = X_0 \times_{\mathbf{Q}} \overline{\mathbf{Q}}$.

Soit ℓ un nombre premier (distinct de p la caractéristique du corps). Pour chacun des corps $K = \mathbf{F}_p, \mathbf{Q}_p, \mathbf{Q}$, et pour $i \geq 0$, on définit (voir par exemple [Kat94b]) les groupes de cohomologie étale à support compact

$$H^i_c(X \times_{\mathbf{Z}} \overline{K}, \mathbf{Q}_\ell) = H^i_c(X \times_{\mathbf{Z}} \overline{K}, \mathbf{Z}_\ell) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell.$$

Ce sont des $\mathbf{Q}_\ell$-espaces vectoriels de dimension finie, qui sont triviaux quand $i > 2\dim(X_0)$. L'action du groupe de Galois $\mathrm{Gal}(\overline{K}/K)$ sur $\overline{K}$ induit une action sur $X \times_{\mathbf{Z}} \overline{K}$, donc aussi une action sur les groupes de cohomologie $H^i_c(X \times_{\mathbf{Z}} \overline{K}, \mathbf{Q}_\ell)$.

On veut montrer que pour presque tous les premiers p, l'action du Frobenius σ_p sur $H^i_c(X \times_{\mathbf{Z}} \overline{\mathbf{F}}_p, \mathbf{Q}_\ell)$ peut se relever en une action sur $H^i_c(X \times_{\mathbf{Z}} \overline{\mathbf{Q}}, \mathbf{Q}_\ell)$.

Le plongement $\overline{\mathbf{Q}} \subset \overline{\mathbf{Q}}_p$ donne pour tout $i \geq 0$ un isomorphisme

$$H^i_c(\overline{X}_0, \mathbf{Q}_\ell) \simeq H^i_c(X \times_{\mathbf{Z}} \overline{\mathbf{Q}}_p, \mathbf{Q}_\ell).$$

En effet $X \times_{\mathbf{Z}} \overline{\mathbf{Q}}_p = \overline{X}_0 \times_{\overline{\mathbf{Q}}} \overline{\mathbf{Q}}_p$ et la cohomologie est inchangée par changement de base d'un corps algébriquement clos à un autre. De plus cet isomorphisme est compatible avec le morphisme $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p) \to \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Ainsi il nous suffit maintenant de relever l'action du Frobenius σ_p sur $H^i_c(X \times_{\mathbf{Z}} \overline{\mathbf{Q}}_p, \mathbf{Q}_\ell)$.

Définition 1.5. On appelle élément de Frobenius en p un élément γ_p de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ qui est l'image par le morphisme (1.2) d'un élément de $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ qui a pour image σ_p dans $\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$ par la surjection de (1.1).

D'après la suite exacte (1.1), si le groupe d'inertie I_p agit trivialement sur le groupe $H^i_c(X \times_{\mathbf{Z}} \overline{\mathbf{Q}}_p, \mathbf{Q}_\ell)$, on a un isomorphisme

$$H^i_c(\overline{X}_p, \mathbf{Q}_\ell) \simeq H^i_c(X \times_{\mathbf{Z}} \overline{\mathbf{Q}}_p, \mathbf{Q}_\ell).$$

qui est compatible avec l'action du Frobenius σ_p, ou de son relevé dans $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$.

Dans le cas lisse, si on peut relever la situation du théorème 1.4 à $\mathbf{Z}_p$, on a l'isomorphisme espéré d'après [Del77, p.254, 1.3.3].

Théorème 1.6. *Soit Y un schéma projectif lisse sur $\mathbf{Z}_p$ et D un diviseur à croisements normaux au dessus de $\mathbf{Z}_p$ dans Y. On note $X = Y - D$. Alors pour tout premier $\ell \neq p$, pour tout $i \geq 0$ le groupe d'inertie I_p agit trivialement sur $H^i_c(X \times_{\mathbf{Z}} \overline{\mathbf{Q}}_p, \mathbf{Q}_\ell)$ et il existe un isomorphisme canonique*

$$H^i_c(X \times_{\mathbf{Z}} \overline{\mathbf{Q}}_p, \mathbf{Q}_\ell) \simeq H^i_c(\overline{X}_p, \mathbf{Q}_\ell)$$

compatible avec l'action de $\mathrm{Gal}(\mathbf{Q}_p^{nr}/\mathbf{Q}_p) \simeq \mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$.

En combinant les théorèmes 1.4 et 1.6 on obtient le résultat suivant (voir aussi [Ser12, Th. 4.13]).

Corollaire 1.7. *Soit $X \to \mathbf{Z}$ un schéma séparé réduit de type fini. On peut choisir une partie finie Σ_X de l'ensemble des premiers telle que :*

1. *pour tout premier $p \notin \Sigma_X \cup \{\ell\}$, pour tout $i \geq 0$, l'action du groupe d'inertie I_p sur $H^i_c(X \times_{\mathbf{Z}} \overline{\mathbf{Q}}_p, \mathbf{Q}_\ell)$ est triviale ;*

2. *et pour tout élément de Frobenius γ_p en $p \notin \Sigma_X \cup \{\ell\}$, pour tout $\alpha \in \mathbf{Z}$ et pour tout $i \geq 0$, on a*

$$\mathrm{tr}(\gamma_p^\alpha \mid H_c^i(\overline{X}_0, \mathbf{Q}_\ell)) = \mathrm{tr}(\sigma_p^\alpha \mid H_c^i(\overline{X}_p, \mathbf{Q}_\ell)).$$

Le cas où X_0 est projective lisse est plus simple. D'après [Mil80, p.230, Cor. 4.2], on peut prendre pour l'ensemble Σ_X l'ensemble des « premiers de mauvaise réduction pour X », c'est-à-dire l'ensemble des premiers p tel que X_p n'est pas projective lisse.

Dans le cas où X_0 est lisse, les théorèmes 1.4 et 1.6 permettent de conclure. On prend pour l'ensemble Σ_X l'ensemble des premiers p ne divisant pas l'entier N qui apparaît par le théorème 1.4.

Dans le cas général, on se ramène au cas lisse en utilisant la stratification (voir par exemple [KL85, Sect. 3]). On écrit X_0 comme une réunion ensembliste finie disjointe de sous-schémas réduits localement fermés et lisses : $X_0 = \sqcup_k X^k$. Pour cela on prend $X^0 = X_0^{\mathrm{lisse}}$, et pour $k \geq 0$, X^{k+1} est l'ouvert lisse du schéma réduit du schéma fermé complémentaire de X^k dans $X_0 - \sqcup_{j<k} X^j$. Le processus est fini car le fermé complémentaire perd au moins une dimension à chaque fois. On raisonne par récurrence sur la dimension en utilisant les isomorphismes dans les suites exactes longues pour les groupes de cohomologie associés à cette décomposition. On montre ainsi que l'on peut prendre $\Sigma_X = \cup_k \Sigma_{X^k}$.

Dans la suite pour chaque schéma $X \to \mathbf{Z}$ séparé réduit de type fini, on suppose qu'un choix d'un ensemble Σ_X satisfaisant les conditions du corollaire 1.7 a été fait.

1.1.3 Quelques invariants géométriques

Soit $X \to \mathbf{Z}$ un schéma séparé réduit de type fini. On définit dans cette partie quelques invariants liés à la cohomologie du schéma X.

Définition 1.8. Soit p premier. Les nombres de Betti de X_p sont définis par

$$b_i(X_p) := \dim_{\mathbf{Q}_\ell} H_c^i(\overline{X}_p, \mathbf{Q}_\ell).$$

D'après le corollaire 1.7, sauf éventuellement pour un nombre fini de premiers, on a $b_i(X_p) = b_i(X_0)$. On utilise donc une définition plus globale des nombres de Betti.

Définition 1.9. On définit les nombres de Betti de X : pour tout $i \geq 0$, $b_i(X) := b_i(X_0)$.

Définition 1.10. On définit la caractéristique d'Euler–Poincaré à support compact de X par $\chi_c(X) = \sum_{i=0}^{2\dim(X)} (-1)^i b_i(X)$.

Dans le cas où X_0 est projective lisse, on va aussi se servir des nombres de Hodge. On définit les nombres de Hodge de X_0 grâce à la cohomologie usuelle sur les faisceaux de différentielles $\Omega^i_{X_0}$, voir par exemple [CR12, Sect. 4].

Définition 1.11. On pose $h^{i,m-i}(X) = \dim_{\mathbf{Q}} H^{m-i}(X_0, \Omega^i_{X_0})$.

Remarque 2. Par changement de base plat [Har77, Th. 9.3], on voit qu'on obtient les mêmes nombres de Hodge pour X_0, $X_0 \times_{\mathbf{Q}} \mathbf{C}$ et pour $X_0 \times_{\mathbf{Q}} \mathbf{Q}_p$ (voir [Ill94]) à condition que p soit un premier de bonne réduction pour X.

On peut lier les nombres de Hodge aux nombres de Betti par la relation suivante.

Proposition 1.12 (Décomposition de Hodge)**.** *On a $b_m(X) = \sum_{i=0}^m h^{i,m-i}(X)$.*

1.1.4 Calculer $N_X(p)$

Soit X un schéma séparé réduit de type fini sur $\mathbf{Z}$. La variété X_p est munie d'un $\mathbf{F}_p$-morphisme de Frobenius naturel $\mathrm{Frob}_p : X_p \to X_p$ défini comme suit : sur l'espace topologique X_p c'est l'identité, et son action sur le faisceau structurel $\mathcal{O}_{X_p}$ est donnée par $f \mapsto f^p$. Dans le cas affine, cela revient à mettre les coordonnées à la puissance p. Alors l'ensemble des $\mathbf{F}_p$-points de X_p est exactement l'ensemble des $\overline{\mathbf{F}}_p$-points fixes par l'application Frobenius naturelle Frob_p.

Remarque 3. Nous venons de redéfinir un endomorphisme de Frobenius sur X_p de façon plus géométrique, il est tout de même comparable à l'endomorphisme de Frobenius arithmétique de la sous-section 1.1.2 : on a $\mathrm{Frob}_p = \sigma_p^{-1}$.

Comme dans la sous-section 1.1.2, on a une action de Frob_p sur les groupes de cohomologie $H^i_c(\overline{X}_p, \mathbf{Q}_\ell)$. On a le théorème de Grothendieck–Lefschetz.

Théorème 1.13 (Grothendieck–Lefschetz)**.** *Soit ℓ un nombre premier différent de p, alors*

$$N_X(p) = \sum_i (-1)^i \operatorname{tr}(\mathrm{Frob}_p \mid H^i_c(\overline{X}_p, \mathbf{Q}_\ell)).$$

On va utiliser une variante de ce théorème ([Ser12, Th. 4.13]) qui va nous permettre d'étudier $N_X(p)$ en faisant varier le nombre premier p.

Théorème 1.14. *Pour ℓ premier, pour tout $p \notin \Sigma_X \cup \{\ell\}$*

$$N_X(p) = \sum_i (-1)^i \operatorname{tr}(\mathrm{Frob}_p \mid H^i_c(X \times_{\mathbf{Z}} \overline{\mathbf{Q}}, \mathbf{Q}_\ell)).$$

Ce théorème est une conséquence directe du corollaire 1.7.

1.1.5 Quelques conséquences des conjectures de Weil

En utilisant la formule de Grothendieck–Lefschetz (théorème 1.14), on a maintenant une façon théorique de calculer $N_X(p)$ pour tous les premiers $p \notin \Sigma_X$. Plus on a d'informations sur les groupes de cohomologie à support compact $H^i(X, \ell) := H^i_c(X \times_{\mathbf{Z}} \overline{\mathbf{Q}}, \mathbf{Q}_\ell)$ et sur la façon dont l'endomorphisme de Frobenius agit dessus, plus on peut déduire d'informations sur $N_X(p)$. C'est l'idée des conjectures de Weil, démontrées par Deligne [Del80] (on pourra aussi voir [Kli]). Ce sont des résultats puissants dont on n'utilisera pas toute l'ampleur, on en présente seulement ici deux conséquences dont on se servira par la suite.

Le résultat suivant est une conséquence du résultat principal de [Del80].

Lemme 1.15. *Soit p un nombre premier. Soit X_p un schéma de type fini sur $\mathbf{F}_p$. Soit $i \geq 0$.*

$$\operatorname{tr}(\mathrm{Frob}_p \mid H^i_c(X_p \times_{\mathbf{F}_p} \overline{\mathbf{F}}_p, \mathbf{Q}_\ell)) = \sum_{j=1}^{b_i(X_p)} \alpha_{i,j}$$

où les $\alpha_{i,j}$ sont des nombres complexes satisfaisant $|\alpha_{i,j}| = p^{\frac{m_{i,j}}{2}}$ pour des entiers $m_{i,j} \leq i$. Dans le cas où X_p est projective lisse, on a $m_{i,j} = i$ pour tout j.

On a en particulier le théorème de Lang–Weil (voir par exemple [Kat90]) qui permet d'estimer les nombres de points rationnels.

Lemme 1.16 (Lang–Weil)**.** *Soit $X/\mathbf{Z}$ un schéma de type fini de dimension d. Soit N le nombre de composantes irréductibles de dimension d de $X/\mathbf{C}$. Alors il existe une constante $C(X) > 0$ telle que pour tout premier $p \notin \Sigma_X$, on a*

$$0 \leq N_X(p) \leq Np^d + C(X)p^{d-\frac{1}{2}}. \tag{1.3}$$

Remarque 4. On peut prendre $N = b_{2d}(X)$. Comme on veut que l'inégalité (1.3) soit vérifiée par presque tous les premiers, on ne peut pas espérer une meilleure estimation (en particulier minoration) sans hypothèse sur le corps de définition des composantes irréductibles sur $\mathbf{C}$.

En particulier on a toujours une borne supérieure sur $N_X(p)$.

Le résultat suivant est un corollaire facile de la dualité de Poincaré.

Lemme 1.17. *Soit p un premier et Y_p une variété projective lisse de dimension d définie sur $\mathbf{F}_p$. Pour tout premier $\ell \neq p$, pour tout entier $i \in \{d+1, \dots 2d\}$, on a*

$$\operatorname{tr}(\mathrm{Frob}_p \mid H_c^i(Y_p \times \overline{\mathbf{F}}_p, \mathbf{Q}_\ell)) = p^{i-d} \operatorname{tr}(\mathrm{Frob}_p \mid H_c^{2d-i}(Y_p \times \overline{\mathbf{F}}_p, \mathbf{Q}_\ell)).$$

Démonstration. D'après les résultats de Deligne [Del74] on peut écrire pour chaque i,

$$\operatorname{tr}(\mathrm{Frob}_p \mid H_c^i(Y_p \times \overline{\mathbf{F}}_p, \mathbf{Q}_\ell)) = \sum_{j=1}^{b_i(Y_p)} \alpha_{i,j}$$

où $|\alpha_{i,j}| = p^{\frac{i}{2}}$. La dualité de Poincaré [Del74, (2.4)] assure que $b_i = b_{2d-i}$ et (quitte à changer l'ordre) $\alpha_{i,j} = \frac{p^d}{\alpha_{2d-i,j}}$ pour tout j. Ainsi

$$\begin{aligned}
\sum_{j=1}^{b_i} \alpha_{i,j} &= \sum_{j=1}^{b_i} \frac{p^d}{\alpha_{2d-i,j}} = p^{\frac{i}{2}} \sum_{j=1}^{b_i} \frac{p^{d-\frac{i}{2}}}{\alpha_{2d-i,j}} \\
&= p^{\frac{i}{2}} \sum_{j=1}^{b_i} \overline{\left(\frac{\alpha_{2d-i,j}}{p^{d-\frac{i}{2}}} \right)} \\
&= p^{i-d} \operatorname{tr}(\mathrm{Frob}_p \mid H_c^{2d-i}(Y_p \times \overline{\mathbf{F}}_p, \mathbf{Q}_\ell))
\end{aligned}$$

où $z \mapsto \overline{z}$ est la conjugaison complexe. □

Ce résultat fournit une propriété de divisibilité par p des traces de Frobenius sur les groupes de cohomologies d'ordre strictement supérieur à la dimension du schéma. Si Y_p est un schéma projectif lisse, alors p divise $\operatorname{tr}(\mathrm{Frob}_p \mid H_c^i(Y_p \times \overline{\mathbf{F}}_p, \mathbf{Q}_\ell))$ pour tout $i > \dim Y_p$. On a un autre résultat du même type en utilisant une conjecture de Katz démontrée par Mazur et Ogus (voir par exemple [Ill94, 1.3.9], aussi [Maz72]).

Théorème 1.18 (Mazur–Ogus)**.** *Soit Y un schéma projectif lisse sur $\mathbf{Z}_p$ de dimension d. Soit $m \leq d$ un entier. Soit c le plus petit entier tel que $h^{c,m-c}(Y) \neq 0$. Alors p^c divise* $\operatorname{tr}(\mathrm{Frob}_p \mid H_c^m(Y \times \overline{\mathbf{F}}_p, \mathbf{Q}_\ell))$

C'est un corollaire du Théorème de Mazur-Ogus [BO78, 8.39] : le polygone de Newton de $(H^m(Y/\mathbf{Z}_p)/\text{torsion}, \mathrm{Frob}_p)$ est au dessus du polygone de Hodge de Y en degré m. (Pour plus de détails sur les définitions de ces polygones, voir [Ill94]).

En particulier si $h^{i,m-i}(Y \times_{\mathbf{Z}_p} \mathbf{Q}_p) = 0$ pour tout $i < c$, la plus petite pente du polygone de Hodge de Y en degré m est c. Donc les valeurs propres de l'action du Frobenius sur $H^m(Y_p/\mathbf{Z}_p)/\text{torsion}$ sont des entiers algébriques avec une valuation p-adique supérieure à c. On en déduit que leur somme est divisible par p^c.

Remarque 5. Dans le cas où X est un schéma projectif sur $\mathbf{Z}$ tel que X_0 soit projectif lisse sur $\mathbf{Q}$, on a pour tout $p \notin \Sigma_X$ premier de bonne réduction, le schéma $Y = X \times_{\mathbf{Z}} \mathbf{Z}_p$ est projectif lisse. De plus on a vu que par changement de base plat on a $h^{i,m-i}(X) = h^{i,m-i}(Y)$. On en déduit donc le résultat suivant.

Soit X un schéma projectif sur $\mathbf{Z}$ tel que X_0 soit projectif lisse, supposons que pour un entier m on a $h^{0,m}(X) = 0$. Alors pour tout $p \notin \Sigma_X$, p divise $\operatorname{tr}(\mathrm{Frob}_p \mid H_c^m(\overline{X}_p, \mathbf{Q}_\ell))$.

1.2 A-nombre et nombre de $\mathbf{F}_p$-points modulo p

Revenons au théorème 1.1. Pour comprendre son hypothèse on s'intéresse aux propriétés de divisibilité par p de $N_X(p)$. On s'est intéressé plus particulièrement à l'étude d'ensembles du type :

$$\{p \in \mathcal{P} : p \nmid N_X(p)\} \tag{1.4}$$

avec X un schéma affine sur $\mathbf{Z}$. Fouvry et Katz [FK01] ont montré qu'on peut relier l'estimation de sommes exponentielles indexées sur X à l'étude de l'ensemble (1.4), en passant par le A-nombre de X.

Plus précisément, étant donné un schéma X de type fini affine défini sur $\mathbf{Z}$ tel que $X/\mathbf{C}$ soit lisse, une fonction f sur X (i.e. un morphisme $f : X \to \mathbb{A}^1$), un corps fini k et un caractère additif non-trivial ψ de k, les auteurs définissent $A(X, f, k, \psi)$ comme le rang d'un certain faisceau lisse défini en utilisant la transformée de Fourier ([FK01, Part 4]).

On trouve dans l'introduction de [Kat94a] une bonne façon d'appréhender le A-nombre dans une situation simplifiée. Précisément, pour X un sous-schéma fermé de $\mathbb{A}^n_{\mathbf{Z}}$ de dimension d, Katz introduit le A-nombre pour évaluer la somme « normalisée » :

$$M(p) = p^{-n} \sum_{a \in \mathbb{A}^n(\mathbf{F}_p)} p^{-d/2} \left| \sum_{x \in X(\mathbf{F}_p)} \exp\left(\frac{2i\pi}{p} \sum_{i=1}^{n} a_i x_i\right)\right|.$$

Dans le cas où X est irréductible, on obtient facilement $M(p) \leq 1 + O(p^{-1/2})$. Le A-nombre nous permet de donner plus de précisions sur cette majoration. Il y a deux cas où la connaissance du A-nombre nous permet vraiment d'affiner l'estimation :

— si $A = 0$, alors $M(p) = O(p^{-1/2})$,

— si $A = 1$, alors $|M(p) - 1| = O(p^{-1/2})$.

Plus généralement on a le [FK01, Lem. 4.3] : $A(X, f, k, \psi) = 0$ si et seulement s'il existe un ouvert dense U dans $\mathbb{A}^n_k$ tel que pour toute extension finie E de k et tout $h \in U(E)$ la somme exponentielle

$$\sum_{x \in X(E)} \psi(\mathrm{tr}_{E/k}(f(x) + \sum_i h_i x_i))$$

est nulle.

Dans le cas où le A-nombre est non-nul, [FK01, Cor. 4.5] donne une estimation très précise de ce type de sommes exponentielles.

Théorème 1.19 (Fouvry–Katz)**.** *Soient d, n, D des entiers ≥ 1, soit X un sous-schéma fermé de $\mathbb{A}^n_{\mathbf{Z}[1/D]}$, tel que $X/\mathbf{C}$ est irréductible et lisse de dimension d. Soit f une fonction sur X. On suppose que $A(X, f, k, \psi) \geq 1$, pour tout corps k de caractéristique suffisamment grande et tout caractère additif non-trivial ψ de k à valeurs dans $\mathbf{Q}_\ell^\times$.*

Alors il existe une constante C ne dépendant que de X et f, un sous-schéma fermé $X_2 \subset \mathbb{A}^n_{\mathbf{Z}[1/D]}$, de dimension relative $\leq n-2$, tels que pour tout $h \in \mathbb{A}^n_{\mathbf{Z}[1/D]}(\mathbf{F}_p) - X_2(\mathbf{F}_p)$, pour tout p premier ne divisant pas D, tout caractère additif non-trivial ψ de $\mathbf{F}_p$, on a

$$\left| \sum_{x \in X(\mathbf{F}_p)} \psi(f(x) + h_1 x_1 + \ldots + h_n x_n) \right| \leq C p^{\frac{d}{2}}.$$

Ce théorème améliore un résultat obtenu dans [KL85], sur la dimension du sous-schéma « exceptionnel » X_2 mettant en défaut la majoration ci-dessus. La fonction f peut être très générale, par exemple une fraction rationnelle en les coordonnées.

Par ailleurs, la non-nullité du A-nombre garantit aussi une bonne répartition des $\mathbf{F}_p$-points dans l'espace affine [FK01, Cor. 1.5].

Théorème 1.20 (Fouvry–Katz). *Soient d, n, des entiers ≥ 2, soit X un sous-schéma fermé de $\mathbb{A}^n_{\mathbf{Z}}$, tel que $X/\mathbf{C}$ est irréductible et lisse de dimension d. On suppose que $X/\mathbf{C}$ n'est pas inclus dans un hyperplan de $\mathbb{A}^n_{\mathbf{C}}$. On suppose que $A(X, 0, k, \psi) \geq 1$, pour tout corps k de caractéristique suffisamment grande et tout caractère additif non-trivial ψ de k à valeurs dans $\mathbf{Q}_\ell^\times$.*

Alors pour tout b vérifiant $1 \leq b \leq p$ on a

$$|\{x \in X(\mathbf{F}_p) : \forall i, 0 \leq x_i < b\}| = |X(\mathbf{F}_p)| \left(\frac{b}{p}\right)^n + O\left(p^{d/2}(\log p)^n(1 + b^d p^{-\frac{d+1}{2}}(\log p)^{-d})\right).$$

Ces théorèmes montrent l'intérêt d'établir la non-nullité du A-nombre. Bien qu'il y ait une formule topologique [Kat89, 4.6] pour calculer le A-nombre à l'aide de caractéristiques d'Euler–Poincaré, celle-ci n'est pas très effective et il est difficile de savoir si la valeur est nulle ou non. En utilisant des propriétés géométriques, Katz a calculé les A-nombres dans certains cas particuliers.

Notamment ([Kat80, p. 150]) dans le cas de surfaces S de $\mathbb{A}^3$ définies par : $f(x, y, z) = 0$, pour k un corps de caractéristique première à $\deg(f)$, le A-nombre associé à $(S, 0, k, \psi)$ est $\deg(f)(\deg(f) - 1)^2$. En particulier il est non nul dès que $\deg(f) > 1$.

On peut aussi citer [Kat89, Cor. 6.5] : soit X une hypersurface lisse de $\mathbb{A}^n_{\mathbf{Z}}$ donnée par une équation du type : $F(x_1, \ldots, x_n) = \alpha$ avec $\alpha \neq 0$ et F un polynôme homogène pondéré. Alors le A-nombre associé à $(X, 0, k, \psi)$ est supérieur ou égal à 2.

Enfin on a le Théorème [FK01, Th. 8.1] qui donne un critère pour garantir la non-nullité du A-nombre.

Théorème 1.21 (Fouvry–Katz). *Soit X un sous-schéma fermé de $\mathbb{A}^n_{\mathbf{Z}}$ tel que $X/\mathbf{C}$ est lisse connexe de dimension relative d. Soit D le produit des premiers de mauvaise réduction pour $X/\mathbf{Z}$. Cette donnée fournit un entier N (lié à la stratification).*

S'il existe un ensemble infini de premiers p tels qu'il existe un corps fini E_p de caractéristique p avec $p \nmid |X(E_p)|$. Alors le A nombre associé à (X, f, k, ψ) est non nul pour toute fonction f, pour tout corps fini k de caractéristique première à $DN\ell$ et pour tout caractère additif ψ de k à valeurs dans $\mathbf{Q}_\ell^\times$.

Fouvry et Katz ont utilisé le théorème 1.21 pour exhiber de nouvelles classes d'exemples de schémas affines avec un A-nombre non nul. Ils montrent notamment que pour $n \geq 3$ et $d \geq 1$ impairs, et $a_1, \ldots, a_n$ des entiers premiers entre eux, le sous-schéma affine X de $\mathbb{A}^n_{\mathbf{Z}}$ défini par les équations :

$$\begin{cases} \prod_{i=1}^n x_i & = 1 \\ \sum_{i=1}^n a_i x_i^d & = 0 \end{cases}$$

a un A-nombre non nul pour toutes les situations (X, f, k, ψ) à condition que la caractéristique de k soit assez grande.

L'étude des premiers p qui ne divisent pas $N_X(p)$ s'inscrit dans le cadre général de l'étude des propriétés p-adiques de $N_X(p)$. Une première approche est le Théorème de Chevalley–Warning qui a été successivement amélioré par Ax puis Katz [Kat71].

Théorème 1.22 (Chevalley–Warning–Ax–Katz). *Soit k un corps fini à $q = p^\alpha$ éléments. Soient $f_1, \ldots, f_n$ des polynômes en m variables à coefficients dans k, de degrés respectifs $d_1, \ldots, d_n$. Soit V le sous-schéma affine de $\mathbb{A}^m_k$ défini par l'annulation de $f_1, \ldots, f_n$. Soit μ le plus petit entier supérieur à $\frac{m - \sum_{i=1}^n d_i}{\max(d_i)}$. Alors*

$$|V(k)| \equiv 0 \pmod{q^\mu}.$$

En particulier, si $m \geq \sum_{i=1}^{n} d_i$, p divise le nombre de $\mathbf{F}_p$-points de la variété affine. On est dans un cas où le théorème 1.1 ne s'applique pas, mais cela ne veut pas dire que le A-nombre est nul.

Le cas des surfaces cubiques est assez classique, on a [Man74, 27.1.1] :

Proposition 1.23. *Soit S_p une surface cubique projective lisse sur $\mathbf{F}_p$ alors*

$$|S_p(\mathbf{F}_p)| \equiv 1 \ [\mathrm{mod}\ p].$$

Enfin dans la veine de ces résultats, certaines conditions géométriques garantissent certaines propriétés p-adique de $N_X(p)$. C'est le cas par exemple de [Esn03, Th. 1.1]. Ce résultat garantit que si le groupe de Chow des 0-cycles d'une variété projective lisse $X_p/\mathbf{F}_p$ est égal à $\mathbf{Z}$ alors $N_X(p) \equiv 1 \ [\mathrm{mod}\ p]$.

1.3 Fonctions frobeniennes et généralisation du théorème de Serre

De façon générale, il est assez courant d'avoir à étudier des ensembles du type :

$$\{p \in \mathcal{P} : N_X(p) \in S(p)\}$$

où $S(p)$ est un ensemble qui peut dépendre de p. Par exemple la conjecture de Sato–Tate (qui est maintenant un théorème [CHT08], [HSBT10]) résout complètement et très précisément la question de l'étude d'un tel ensemble dans le cas où X est une courbe elliptique sur $\mathbf{Q}$ et $S(p)$ est un intervalle de la forme $]p+1+a\sqrt{p}, p+1+b\sqrt{p}[$, avec $a, b \in [-2, 2]$ indépendants de p.

Théorème 1.24 (Conjecture de Sato–Tate)**.** *Soit E une courbe elliptique sans multiplication complexe, écrivons*

$$N_E(p) = p - 2\sqrt{p}\cos(\theta_p) + 1,$$

avec $\theta_p \in [0, \pi]$ alors pour tous $0 \leq \alpha < \beta \leq \pi$, on a

$$\mathrm{dens}(\{p \in \mathcal{P} : \alpha \leq \theta_p \leq \beta\}) = \frac{2}{\pi}\int_{\alpha}^{\beta} \sin^2(t)dt.$$

Le cas avec multiplication complexe est aussi connu (voir par exemple [Mur82, p. 198]) mais la distribution dépend de la courbe et peut charger les points.

Toujours dans le cadre des courbes elliptiques, une fois la conjecture de Sato–Tate connue, il est naturel d'étudier des ensembles du type $\{p : a_p(E) = h\}$. C'est l'idée de la conjecture de Lang–Trotter, il est conjecturé que étant donné un « bon » entier h, l'ensemble $\{p : a_p(E) = h\}$ est infini, de plus on conjecture un équivalent asymptotique pour la taille de cet ensemble. On pourra lire l'introduction de [Kat09] pour plus de précisions sur ces conjectures. En général on pense que ces ensembles ont une densité nulle. Citons par exemple un résultat obtenu par Serre [Ser81, Th. 20] :

Théorème 1.25 (Serre)**.** *Soit E une courbe elliptique sur $\mathbf{Q}$. Supposons que E n'ait pas multiplication complexe. On a*

$$|\{p \leq x : a_p(E) = h\}| = O(x/\log(x)^{4/3-\delta})$$

pour tout $\delta > 0$.

L'estimation a été amélioré par Elkies [Elk87] dans le cas $h = 0$. En particulier on sait déjà dans le cas d'une courbe elliptique E sans multiplication complexe que la densité de l'ensemble $\{p : p \nmid (N_E(p) - h)\}$ est 1.

Dans le cadre plus général des variétés abéliennes, Ogus [Ogu81] s'est intéressé à l'ensemble des premiers ordinaires. Étant donné une variété abélienne A sur $\mathbf{Z}$ de dimension g, un premier p est dit ordinaire si p ne divise pas $\mathrm{tr}(\mathrm{Frob}_p \mid H_c^g(A_p \times_{\mathbf{F}_p} \overline{\mathbf{F}_p}, \mathbf{Q}_\ell))$. En particulier si on se donne C une courbe projective irréductible lisse de genre g, sa jacobienne est une variété abélienne A de dimension g. Alors si un premier p est ordinaire pour A, il satisfait $p \nmid (N_C(p) - 1)$. Ogus a montré [Ogu81, Cor. 2.9] dans le cas des variétés abéliennes de dimension plus petite ou égale à 2 que l'ensemble des premiers ordinaires a une densité strictement positive. L'idée de sa démonstration est assez élémentaire une fois connu le lemme 1.15, on reprendra cette idée dans la preuve du résultat principal de ce chapitre (voir la sous-section 1.4.2).

Le cas des courbes irréductibles est assez simple, il suffit de connaître l'action de l'endomorphisme de Frobenius sur le module de Tate ℓ-adique. Dans le cas général, d'après la formule de Grothendieck–Lefschetz (théorème 1.14), l'étude de $N_X(p)$ est liée à l'action de l'endomorphisme de Frobenius en p sur le produit des groupes de cohomologie ℓ-adique à support compact. Comme l'endomorphisme de Frobenius n'est bien défini qu'à conjugaison près, il est naturel d'étudier des ensembles du type :

$$\{p \in \mathcal{P} : \mathrm{Frob}_p \in C\}$$

où C est une réunion de classes de conjugaisons dans G, un groupe de Galois fini (groupe de Galois d'une extension finie de $\mathbf{Q}$). C'est exactement de cela que traite le théorème de Chebotarev (voir par exemple [Ser81, §2]).

Théorème 1.26 (Chebotarev)**.** *Soit G le groupe de Galois d'une extension finie $E/\mathbf{Q}$. Soit C un sous-ensemble de G stable par conjugaison. Alors l'ensemble*

$$\{p \in \mathcal{P} : \text{ non ramifié, } \mathrm{Frob}_p \in C\}$$

admet une densité naturelle (au sens de la définition 1) égale à $\frac{|C|}{|G|}$.

Dans le livre [Ser12], Serre utilise le théorème de Chebotarev pour étudier des ensembles du type

$$\{p \in \mathcal{P} : N_X(p) \equiv a \pmod{m}\}$$

pour tout X schéma de type fini sur $\mathbf{Z}$, et tout a, m entiers fixés. Plus précisément, Serre prouve le théorème suivant.

Théorème 1.27 (Serre)**.** *Soit X un schéma séparé de type fini sur $\mathbf{Z}$, a, m deux entiers fixés ($m \geq 1$). Alors l'ensemble des premiers p tels que $N_X(p) \equiv a \pmod{m}$ admet une densité rationnelle. De plus si $a \equiv \chi_c(X) \pmod{m}$ la caractéristique d'Euler–Poincaré de X à support compact (voir la définition 1.10), alors cette densité est strictement positive.*

En particulier le résultat de Serre porte sur la fonction $p \mapsto N_X(p) \pmod{m}$ pour m un entier fixé non nul, mais sa preuve contient déjà le cas général d'une fonction provenant de traces de Frobenius. Pour montrer ce résultat, Serre a introduit la notion générale de fonctions frobeniennes. Il obtient en fait un résultat semblable pour toutes les fonctions frobeniennes. On montre dans la sous-section 1.3.3 une version généralisée du théorème 1.27 afin de déduire des informations sur $N_X(p) \pmod{p}$ à partir d'informations sur une fonction modulo m. L'idée est en fait de montrer que la fonction qui nous intéresse est frobenienne.

Remarque 6. Il est à noter que cette même idée a été utilisée par Sawin dans [Saw16] pour calculer explicitement les densités des ensembles des premiers ordinaires de surfaces

abéliennes définies sur $\mathbf{Q}$, et ainsi préciser le résultat de Ogus [Ogu81, Cor. 2.9]. Notre résultat est plus général car il traite de schémas de type finis assez généraux de petite dimension ou vérifiant certaines propriétés géométriques. Cependant on ne parvient pas à calculer une borne inférieure strictement positive pour le cas général. Une étude des groupes de Sato–Tate généralisés pour un schéma fixé devrait permettre d'obtenir une telle borne. Cependant les seuls résultats connus portent sur les courbes elliptiques ou les courbes de genre 2 (dans les travaux de Fité, Kedlaya, Rotger et Sutherland [FKRS12]) c'est ce qui permet à Sawin de calculer les densités pour les surfaces abéliennes.

1.3.1 Généralisation du résultat de Serre

On va montrer une légère variante du théorème [Ser12, Th. 6.3]. Soit X un schéma séparé réduit de type fini sur $\mathbf{Z}$. D'après le théorème 1.14 il existe une partie finie Σ_X de $\mathcal{P}$ telle que pour tout $p \notin \Sigma_X$, pour tout $\ell \neq p$ premier,

$$N_X(p) = \sum_{i=0}^{2d} (-1)^i \operatorname{tr}(\mathrm{Frob}_p \mid H^i(X, \ell))$$

où Frob_p est l'isomorphisme de Frobenius géométrique associé à p, c'est un élément (bien défini à conjugaison près) de $\Gamma_{\Sigma_X,\ell} := \mathrm{Gal}(\overline{\mathbf{Q}}_{\Sigma_X \cup \{\ell\}}/\mathbf{Q})$, groupe de Galois de l'extension galoisienne maximale $\mathbf{Q}_{\Sigma_X \cup \{\ell\}}$ de $\mathbf{Q}$ non ramifiée au-dessus de $\Sigma_X \cup \{\ell\}$ (voir la sous-section 1.1.2).

Le théorème [Ser12, Th. 6.3] traite de la fonction $p \mapsto N_X(p)$. Grâce à la formule de Grothendieck–Lefschetz, on voit qu'il suffit de savoir traiter des fonctions du type

$$\begin{aligned} f_{X,i} : \mathcal{P} - (\Sigma_X \cup \{\ell\}) &\to \mathbf{Z} \\ p &\mapsto \operatorname{tr}(\mathrm{Frob}_p \mid H^i(X, \ell)) \end{aligned} \tag{1.5}$$

ainsi que n'importe quelle combinaison linéaire à coefficients entiers de ces fonctions. On peut décomposer ces fonctions :

$$\mathcal{P} - \Sigma_X \cup \{\ell\} \xrightarrow{\mathrm{Frob}} \Gamma_{\Sigma_X,\ell} := \mathrm{Gal}(\overline{\mathbf{Q}}_{\Sigma_X,\ell}/\mathbf{Q}) \xrightarrow{\rho_\ell} GL(H^i(X, \ell)) \xrightarrow{\mathrm{tr}} \mathbf{Q}_\ell.$$

La deuxième flèche correspond à l'action de $\Gamma_{\Sigma_X,\ell}$ sur $H^i(X, \ell)$. Cette action laisse fixe l'image du réseau $H^i_c(X \times \overline{\mathbf{Q}}, \mathbf{Z}_\ell)$ dans $H^i(X, \ell)$. Cela permet de voir l'image $\rho_\ell(\Gamma_{\Sigma_X,\ell})$ comme un sous-groupe de $GL_{b_i(X)}(\mathbf{Z}_\ell)$ où $b_i(X) = \dim H^i(X, \ell)$ est le i-ème nombre de Betti de X (comme dans la définition 1.9). D'après les conjectures de Weil, on sait en fait que l'image de $f_{X,i}$ est dans $\mathbf{Z}$ est indépendante de ℓ.

Il y a une façon naturelle d'étendre les fonctions $f_{X,i}$ en 1. On choisit pour cela la valeur de la fonction $\operatorname{tr} \circ \rho_\ell$ en l'identité (de $\Gamma_{\Sigma_X,\ell}$). On pose

$$f_{X,i}(1) := b_i(X). \tag{1.6}$$

Le résultat clef sur ces fonctions est le théorème suivant, inspiré du théorème de Serre (voir aussi [Dev17, Th. 2.1]).

Théorème 1.28. *Soit $(X_j)_j$ un ensemble fini de schémas séparés réduits de type fini sur $\mathbf{Z}$. Pour chaque j soit Σ_{X_j} l'ensemble fini des « mauvais premiers » associé par le corollaire 1.7. Soit $f : \mathcal{P} - \cup_j \Sigma_{X_j} \to \mathbf{Z}$ une combinaison $\mathbf{Z}$-linéaire de fonctions $f_{X_j,i}$ comme dans (1.5). Alors pour tout $a, m \in \mathbf{Z}$, l'ensemble*

$$E_{a,m}(f) = \{p \in \mathcal{P} - \cup_j \Sigma_{X_j} : p \nmid m, f(p) \equiv a \pmod{m}\} \tag{1.7}$$

vérifie une des deux propriétés :

— *soit* $E_{a,m}(f) = \emptyset$,

— *soit* $\mathrm{dens}(E_{a,m}(f))$ *est un nombre rationnel strictement positif.*

De plus si $f(1) \equiv a \pmod{m}$ *alors* $E_{a,m}(f) \neq \emptyset$.

Remarque 7.

1. Le théorème 1.27 est le cas particulier où $f = N_X$ du théorème 1.28. Il s'agit bien d'une combinaison linéaire à coefficients entiers de fonctions $f_{X,i}$ d'après le théorème 1.14. De plus on a $N_X(1) = \chi_c(X)$ par définition de la caractéristique d'Euler–Poincaré (définition 1.10).
2. Le théorème 1.28 est en fait un résultat sur les « fonctions frobeniennes » de Serre. On montre que pour tout m entier fixé non nul, la fonction $f^{(m)} : p \mapsto f(p) \pmod{m}$ est $\left(\cup_j \Sigma_{X_j} \cup \{p \mid m\}\right)$-frobenienne. Il est alors facile de déduire qu'une intersection ou une réunion finie d'ensembles $E_{a,m}(f)$ est soit un ensemble vide, soit un ensemble qui admet une densité rationnelle strictement positive.
3. En particulier le théorème 1.28 assure que si on trouve un premier dans l'ensemble $E_{a,m}(f)$ alors cet ensemble est infini (et même admet une densité strictement positive). L'idée de garantir qu'une infinité de premiers satisfont la même propriété en ne vérifiant cette propriété que pour un seul peut déjà être trouvée dans [Lub99].

1.3.2 Fonctions frobeniennes

Commençons par donner des résultats généraux sur les « fonctions frobeniennes » de Serre. On verra alors que la preuve du théorème 1.28 en découle naturellement. On va se contenter de définir les fonctions frobeniennes sur l'ensemble des nombres premiers et non en toute généralité sur l'ensemble des places archimédiennes d'un corps de nombre. Pour le cas plus général, on pourra voir [Ser12, Part. 3.3] : les preuves des résultats exposés ci-dessous sont similaires.

Soit S un sous-ensemble fini de $\mathcal{P}$, Ω un ensemble muni de la topologie discrète. Soit $f : \mathcal{P} - S \to \Omega$ une application.

Définition 1.29. On dit que f est une fonction S-frobenienne s'il existe une extension galoisienne finie E de $\mathbf{Q}$ non ramifiée hors de S et une application $\phi : \mathrm{Gal}(E/\mathbf{Q}) \to \Omega$ stable par conjugaison telle que pour tout $p \in \mathcal{P} - S$,

$$f(p) = \phi(\mathrm{Frob}_p).$$

Proposition 1.30. *Soit* $f : \mathcal{P} - S \to \Omega$ *une fonction* S*-frobenienne, alors les images de* f *et* ϕ *sont égales.*

Démonstration. On a clairement $\mathrm{Im}(f) \subset \mathrm{Im}(\phi)$. Pour $g \in \mathrm{Gal}(E/\mathbf{Q})$ le théorème de Chebotarev (théorème 1.26) assure qu'il existe (une infinité de) $p \in \mathcal{P} - S$ tel que Frob_p est dans la classe de conjugaison de g. Donc $\phi(g) = \phi(\mathrm{Frob}_p) \in \mathrm{Im}(f)$. □

Définition 1.31. Un ensemble $\Sigma \subset \mathcal{P} - S$ est dit S-frobenien si sa fonction indicatrice est S-frobenienne, c'est-à-dire s'il existe une extension galoisienne finie E de $\mathbf{Q}$, et un sous-ensemble C de l'ensemble des classes de conjugaison de son groupe de Galois G, tels que $p \in \Sigma$ si et seulement si $\mathrm{Frob}_p \in C$.

Alors d'après le théorème de Chebotarev, Σ a une densité qui est égale à $\frac{|C|}{|G|}$. On en déduit la proposition suivante.

Proposition 1.32. *Un ensemble* S*-frobenien est soit vide soit de densité rationnelle strictement positive.*

Démonstration. Cela découle de la définition associée au théorème de Chebotarev. En effet si l'ensemble Σ est S-frobenien et non vide, alors le sous-ensemble C associé est aussi non vide. □

De façon plus générale, on a la proposition suivante.

Proposition 1.33. *Soit $f : \mathcal{P} - S \to \Omega$ une fonction S-frobenienne, et soit $\omega \in \Omega$. Alors l'ensemble $f^{-1}(\omega)$ est soit vide soit de densité rationnelle strictement positive.*

Démonstration. Il existe une extension galoisienne finie $E/\mathbf{Q}$ de groupe de Galois G, et $\phi : G \to \Omega$ tels que pour tout $p \in \mathcal{P} - S$, on a $f(p) = \phi(\mathrm{Frob}_p)$. Alors $p \in f^{-1}(\omega)$ si et seulement si $\mathrm{Frob}_p \in \phi^{-1}(\omega)$. Cela montre que $f^{-1}(\omega)$ est S-frobenien par stabilité de ϕ par conjugaison. □

Définition 1.34. Si $f : \mathcal{P} - S \to \Omega$ est S-frobenienne, on peut définir $f(1) := \phi_f(1)$ où 1 est l'identité du groupe de Galois $\mathrm{Gal}(E/\mathbf{Q})$.

On remarque que $f(1)$ est dans l'image de f puisqu'il est dans l'image de ϕ_f (par la proposition 1.30), donc la proposition 1.33 assure que l'ensemble

$$\{p \in \mathcal{P} - S : f(p) = f(1)\}$$

est non vide donc de densité rationnelle strictement positive.

1.3.3 Preuve du Théorème 1.28

D'après le théorème des restes chinois on peut supposer que $m = \ell^k$ avec ℓ premier. Une combinaison linéaire entière de fonctions frobeniennes reste frobenienne donc on peut supposer que $f = f_{X,i}$.

Reprenons la décomposition des fonctions de type (1.5), on a vu qu'on peut choisir un $\mathbf{Z}_\ell$-réseau L_i de $H^i(X, \ell)$ stable par l'action de Γ_{S_ℓ} de façon à avoir

$$\mathrm{tr}(\mathrm{Frob}_p \mid H^i(X, \ell)) = \mathrm{tr}(\mathrm{Frob}_p \mid L_i).$$

(Il suffit de prendre pour L_i l'image dans $H^i(X, \ell)$ de $H^i_c(\overline{X}_0, \mathbf{Z}_\ell)$.) On peut alors considérer le groupe $L_i/\ell^k L_i$, c'est un $\mathbf{Z}/\ell^k\mathbf{Z}$-module libre de rang $b_i(X)$. On a la décomposition suivante

$$\begin{array}{ccccccc}
\mathcal{P} - S_\ell & \xrightarrow{\mathrm{Frob}} & \Gamma_{S_\ell} & \longrightarrow & GL(L_i) & & \\
 & & \downarrow & \overset{\phi_{\ell^k}}{\searrow} & \downarrow & & \\
 & & G_{\ell^k} & \hookrightarrow & GL_{b_i(X)}(\mathbf{Z}/\ell^k\mathbf{Z}) & \xrightarrow{\mathrm{tr}} & \mathbf{Z}/\ell^k\mathbf{Z}
\end{array}$$

où on a factorisé ϕ_{ℓ^k} par son noyau. Ainsi, $f_{X,i}(p)$ ne dépend que de l'image de Frob_p dans

$$GL(L_i/\ell^k L_i) \simeq GL_{b_i(X)}(\mathbf{Z}/\ell^k\mathbf{Z})$$

qui est un groupe fini. Donc il suffit de connaître l'image de Γ_{S_ℓ} dans un groupe fini : un quotient fini de Γ_{S_ℓ} qui correspond à une extension galoisienne finie K_{ℓ^k} de $\mathbf{Q}$, avec

$$G_{\ell^k} = \mathrm{Gal}(K_{\ell^k}/\mathbf{Q}) \hookrightarrow GL_{b_i(X)}(\mathbf{Z}/\ell^k\mathbf{Z}).$$

Finalement $f_{X,i}$ est S_ℓ-frobenienne pour $\phi : g \mapsto \mathrm{tr}(g \mid L_i/\ell^k L_i)$.

On a défini $f_{X,i}(1)$ dans (1.6) de façon compatible avec la définition 1.34. Ainsi la proposition 1.33 permet de conclure la preuve du théorème 1.28.

1.4 Ensemble des premiers p tels que $N_X(p)$ évite certaines classes de congruence modulo p

Dans cette section on cherche des conditions pour garantir que l'ensemble des premiers $\{p \notin \Sigma_X : p \nmid \prod_{i=1}^n (N_X(p) - a_i)\}$ est infini. De plus on montre que si cet ensemble est infini, alors il a une densité inférieure strictement positive.

Plus précisément on donne deux énoncés. Le cas projectif lisse est habituellement plus accessible. On a un résultat assez général dans ce cas.

Théorème 1.35. *Soit X un schéma projectif sur $\mathbf{Z}$, tel que $X \times_{\mathbf{Z}} \mathbf{Q}$ est une variété projective lisse de dimension d. Supposons que $h^{0,m}(X) = 0$ pour tout $3 \leq m \leq d$. Alors pour tout $a_1, \ldots, a_n \in \mathbf{Z}$, soit l'ensemble $\{p \notin \Sigma_X : p \nmid \prod_{i=1}^n (N_X(p) - a_i)\}$ est vide, soit il admet une densité inférieure strictement positive.*

Dans cet énoncé, on utilise la notation $h^{i,j}(X)$ pour les nombres de Hodge de X (voir la définition 1.11), et l'ensemble Σ_X est l'ensemble des premiers de mauvaise réduction pour X (voir le corollaire 1.7).

Plus généralement, d'après le théorème 1.3 une variété sur $\mathbf{Q}$ est toujours birationnelle à une variété projective lisse. Dans certains cas, on ne perd pas trop d'informations en considérant le nombre de $\mathbf{F}_p$-points de la variété projective lisse.

Définition 1.36. Soit X un schéma séparé réduit de type fini sur $\mathbf{Z}$, on suppose donné un morphisme birationnel $Y_0 \to X_0$. On définit $\Sigma'_{X,Y}$ comme l'ensemble des premiers de mauvaise réduction associé à cette situation. On a $\Sigma'_{X,Y} \supset \Sigma_X \cup \Sigma_Y$ et il faut encore éventuellement rajouter un nombre fini de premiers que l'on a besoin d'inverser pour effectuer le morphisme.

On déduit le corollaire suivant qui s'applique par exemple aux variétés affines (voir aussi une version un peu plus faible [Dev17, Th. 1.1]).

Corollaire 1.37. *Soit X un schéma séparé réduit de type fini sur $\mathbf{Z}$. On suppose que $X \times_{\mathbf{Z}} \mathbf{Q}$ est birationnelle à une variété projective lisse Y_0 satisfaisant :*

- $\dim(Y_0) \leq 3$ *et*
- $h^{0,3}(Y_0) = 0$.

Alors pour tout $a_1, \ldots, a_n \in \mathbf{Z}$, soit l'ensemble $\{p \notin \Sigma'_{X,Y} : p \nmid \prod_{i=1}^n (N_X(p) - a_i)\}$ est vide, soit il admet une densité inférieure strictement positive.

Remarque 8. Dans le cas où le schéma X est de dimension au plus 2, la condition sur le nombre de Hodge est satisfaite automatiquement pour tout choix de Y_0. En particulier on peut prendre $\Sigma'_{X,Y} = \Sigma_X$.

Le théorème 1.35 est une conséquence du théorème 1.28. Pour en déduire le théorème 1.35, il nous suffira de construire la bonne fonction auxiliaire combinée à des arguments élémentaires. En évaluant la fonction auxiliaire en 1, on pourra déduire des conditions géométriques pour garantir que notre ensemble de premiers est infini. Notamment, dans le cas des courbes irréductibles, on montre le résultat suivant.

Proposition 1.38. *Soit C un schéma de type fini sur $\mathbf{Z}$ tel que $C \times_{\mathbf{Z}} \mathbf{Q}$ est une courbe géométriquement irréductible. Alors pour tout $a \in \mathbf{Z} - \{\chi_c(C) - 1\}$, on a*

$$\mathrm{dens}_{\mathrm{inf}}\{p \in \mathcal{P} - \Sigma_C, p \nmid (N_C(p) - a)\} > 0.$$

On a un résultat du même type pour les surfaces $K3$. Pour rappel les surfaces $K3$ sont les surfaces S qui ont un faisceau canonique trivial et un premier nombre de Betti $b_1(S)$ nul, on pourra voir par exemple [BPVdV84, VIII] pour plus de détails sur les propriétés de telles surfaces.

Proposition 1.39. *Soit S un schéma projectif sur $\mathbf{Z}$ tel que $S \times_{\mathbf{Z}} \mathbf{Q}$ est une surface $K3$. Alors pour tout $a \in \mathbf{Z} - \{1,2,3,4,5\}$, on a*

$$\mathrm{dens}_{\inf}\{p \in \mathcal{P} - \Sigma_S : p \nmid (N_S(p) - a)\} > 0.$$

Remarque 9. On sait juste dire dans les résultats ci-dessus que la densité inférieure est strictement positive mais on ne sait ni montrer l'existence de la densité, ni minorer la densité par une borne strictement positive dans le cas général. On détaille un peu plus ce qu'on pourrait faire dans la sous-section 1.4.5.

1.4.1 Simplification du problème

Dans cette section on prouve parallèlement le théorème 1.35 et le corollaire 1.37. L'idée est que pour prouver le corollaire 1.37, on se ramène au cas projectif lisse puis on évalue la différence entre le nombre de points de la variété de départ et le nombre de points de son modèle lisse. Ainsi, on va prouver le théorème 1.35 dans le processus.

Pour cela on se sert du théorème 1.28 qui traite de classes de congruences modulo un entier m d'une certaine fonction définie avec des traces de Frobenius. On va construire une fonction auxiliaire M_X suffisamment proche de la fonction N_X, qui soit aussi une combinaison linéaire entière de traces de Frobenius, mais pour laquelle l'information sur sa classe de congruence modulo certains entiers m nous permette de déduire des informations sur la classe de congruence de $M_X(p)$ [mod p]. Précisément, on prouve le résultat suivant.

Théorème 1.40. *Soit X un schéma de type fini sur $\mathbf{Z}$ satisfaisant les hypothèses du théorème 1.35 (resp. du corollaire 1.37). Alors pour tout $a \in \mathbf{Z}$, il existe une fonction $M_{X,a}$ définie sur $\mathcal{P} - \Sigma_X$ (resp. sur $\mathcal{P} - \Sigma'_{X,Y}$) telle que*

1. *la fonction $M_{X,a}$ est une combinaison $\mathbf{Z}$-linéaire de fonctions $f_{U,i}$ de type (1.5) pour des schémas U et des entiers i,*
2. *pour tout $p \in \mathcal{P} - \Sigma_X$ (resp. $p \in \mathcal{P} - \Sigma'_{X,Y}$), on a $M_{X,a}(p) \equiv N_X(p) - a$ [mod p],*
3. *il existe des entiers $b_-(X)$, $b_+(X)$ tels que pour tout $\epsilon > 0$ il existe $A = A(X,a,\epsilon) > 0$ satisfaisant pour tout $p \in \mathcal{P} - \Sigma_X$ (resp. $p \in \mathcal{P} - \Sigma'_{X,Y}$), $p \geq A$:*

$$(b_-(X) - \epsilon)p < M_{X,a}(p) < (b_+(X) + \epsilon)p.$$

On prouve ce résultat dans la sous-section 1.4.3. On peut alors en déduire le théorème 1.35 et le corollaire 1.37. Ce sont en effet des conséquences immédiates du résultat suivant :

Proposition 1.41. *Soit X un schéma de type fini sur $\mathbf{Z}$ satisfaisant les hypothèses du théorème 1.35 ou du corollaire 1.37. Soient $a_1, \ldots, a_n \in \mathbf{Z}$, et soient $M_{X,a_1}, \ldots, M_{X,a_n}$ des fonctions associées par le théorème 1.40. Alors soit l'ensemble $\{p \notin \Sigma'_{X,Y} : p \nmid \prod_{i=1}^n (M_{X,a_i}(p))\}$ est vide, soit il admet une densité inférieure strictement positive.*

De plus, l'évaluation en 1 des fonctions $M_{X,a}$ nous donne d'autres conditions pour assurer la non-vacuité de tels ensembles. On a ainsi le résultat suivant.

Théorème 1.42. *Soit X un schéma de type fini sur $\mathbf{Z}$ satisfaisant les hypothèses du théorème 1.35 ou du corollaire 1.37. Soient $a_1, \ldots, a_n \in \mathbf{Z}$. Soient $M_{X,a_1}, \ldots, M_{X,a_n}$ et $b_\pm(X)$ des fonctions et bornes associées par le théorème 1.40. Supposons que pour tout i on ait*

$$\max(|M_{X,a_i}(1) - b_-(X) + 1|, |M_{X,a_i}(1) - b_+(X) - 1|) \geq 2 + b_+(X) - b_-(X). \qquad (1.8)$$

Alors

$$\mathrm{dens}_{\inf}\{p \notin \Sigma'_{X,Y} : p \nmid \prod_{i=1}^n (N_X(p) - a_i)\} > 0.$$

On cherche alors à minimiser ou au moins évaluer la quantité $b_+(X) - b_-(X)$. On donne des valeurs de ces bornes dans la preuve du théorème 1.40. On en déduit notamment les propositions 1.38 et 1.39.

1.4.2 Conséquences du théorème 1.40

Commençons par prouver la proposition 1.41, en supposant le théorème 1.40 vrai.

Démonstation de la proposition 1.41. Soit X comme dans le théorème et $a_1, \dots, a_n \in \mathbf{Z}$, alors le théorème 1.40 nous fournit des fonctions M_{X,a_i} et des bornes $b_\pm(X) \in \mathbf{Z}$, $A_i = A(X, a_i, 1) > 0$ telles que pour tout $p \notin \Sigma'_{X,Y}$, $p > A_i$, on a pour tout $k \in \mathbf{Z}$:

$$(b_-(X) - 1 + k)p < M_{X,a_i}(p) + kf_{\mathbb{A}^1}(p) < (b_+(X) + 1 + k)p.$$

Supposons que l'ensemble $\{p \notin \Sigma'_{X,Y} : p \nmid \prod_{i=1}^n (M_{X,a_i}(p))\}$ est non vide. Soit p_0 un premier dans cet ensemble. Posons $m_i = M_{X,a_i}(p_0)$. D'après le théorème 1.40.2, pour tout $k \in \mathbf{Z}$ on a, en utilisant la notation (1.7),

$$p_0 \in \bigcap_{i=1}^n E_{0,m_i+kp_0}(M_{X,a_i} + kf_{\mathbb{A}^1}). \tag{1.9}$$

On a donc des ensembles frobeniens d'intersection non vide. Comme les fonctions $M_{X,a_i} + kf_{\mathbb{A}^1}$ sont des combinaisons linéaires entières de traces de Frobenius (théorème 1.40.1), on peut leur appliquer le théorème 1.28. On en déduit que l'intersection (1.9) admet une densité qui est un nombre rationnel strictement positif.

Prenons maintenant $A = \max_i(A_i)$. Alors pour k assez grand, on a

$$\bigcap_{i=1}^n E_{0,m_i+kp_0}(M_{X,a_i} + kf_{\mathbb{A}^1}) \cap [A, \infty) \subset \bigcap_{i=1}^n \{p \in \mathcal{P}, N_X(p) \not\equiv a_i \pmod p\}. \tag{1.10}$$

En effet, puisque $p_0 \geq 2$, on peut prendre $k \geq -b_-(X) + 1$ tel que pour tout i on a $m_i + kp_0 \geq b_+(X) + 1 + k$. Alors pour $p \in E_{0,m_i+kp_0}(M_{X,a_i} + kf_{\mathbb{A}^1}) \cap [A, \infty)$, on a

$$0 < M_{X,a_i}(p) + kf_{\mathbb{A}^1}(p) < (b_+(X) + 1 + k)p$$

et

$$M_{X,a_i}(p) + kf_{\mathbb{A}^1}(p) \equiv 0 \pmod{m_i + kp_0}.$$

Donc p ne divise pas $M_{X,a_i}(p) + kf_{\mathbb{A}^1}(p)$. On a ainsi la proposition 1.41. □

On peut aussi garantir que des intersections

$$\bigcap_{i=1}^n E_{0,m_{i,k_i}}(M_{X,a_i} + k_i f_{\mathbb{A}^1})$$

sont non vides grâce à la valeur en 1. Alors si on peut choisir les k_i pour que les m_{i,k_i} soient assez grand on aura de nouveau l'inclusion (1.10), cela permet de déduire le théorème 1.42.

Démonstration du théorème 1.42. Fixons un $i \in \{1, \dots, n\}$. Supposons que

$$|M_{X,a_i}(1) - b_-(X) + 1| \geq 2 + b_+(X) - b_-(X). \tag{1.11}$$

On pose $k_i = -b_-(X) + 1$. Alors on a pour tout p assez grand,

$$0 < M_{X,a_i}(p) - (b_-(X) - 1)f_{\mathbb{A}^1}(p) < (b_+(X) - b_-(X) + 2)p.$$

Choisissons

$$m_i := |M_{X,a_i}(1) - (b_-(X) - 1)f_{\mathbb{A}^1}(1)|$$

Alors d'après le théorème 1.28, l'ensemble $E_{0,m_i}(M_{X,a_i} + k_i f_{\mathbb{A}^1})$ est non vide. De plus la condition (1.11) permet de garantir que pour tout p assez grand dans $E_{0,m_i}(M_{X,a_i}+k_i f_{\mathbb{A}^1})$:

$$p \nmid (N_X(p) - a_i).$$

Si la condition (1.11) n'est pas satisfaite, alors d'après l'hypothèse (1.8), on a

$$|M_{X,a_i}(1) - b_+(X) - 1| \geq 2 + b_+(X) - b_-(X).$$

Dans ce cas on prend $k_i = -b_+(X) - 1$ et $m_i = |M_{X,a_i}(1) - b_+(X) - 1|$.

L'intersection $\cap_{i=1}^n E_{0,m_i}(M_{X,a_i} + k_i f_{\mathbb{A}^1})$ contient 1, elle a donc une densité qui est strictement positive. □

On donne des applications de ce résultat dans la sous-section 1.4.4, après la preuve du théorème 1.40 dans lequel on donne plus de détails sur les valeurs des bornes $b_\pm(X)$.

1.4.3 Construction de la fonction auxiliaire — Démonstration du Théorème 1.40

Nous avons montré dans la partie précédente l'utilité des fonctions auxiliaires $M_{X,a}$. Prouvons maintenant leur existence. On peut se réduire au cas où $a = 0$, en effet une fois construite une fonction M_X satisfaisant le théorème 1.40 pour $a = 0$, il nous suffit de définir $M_{X,a} := M_X - a f_{\bullet,0}$ où $\bullet$ est le point affine : $f_{\bullet,0}(p) = 1$ pour tout p.

Commençons par le cas projectif lisse qui permet de déduire le théorème 1.35.

Proposition 1.43. *Soit X un schéma projectif sur $\mathbf{Z}$, tel que $X \times_{\mathbf{Z}} \mathbf{Q}$ est une variété projective lisse de dimension d. Supposons que $h^{0,m}(X) = 0$ pour tout $3 \leq m \leq d$. Alors la fonction $M_X := \sum_{i=0}^{2}(-1)^i f_{X,i}$ satisfait le théorème 1.40 pour $a = 0$. On peut prendre $b_-(X) = -b_2(X)$ et $b_+(X) = b_2(X)$.*

Ici $b_2(X)$ est le deuxième nombre de Betti de X, comme dans la définition 1.9.

Démonstration. Soit d la dimension de X sur $\mathbf{Z}$. D'après le théorème 1.14, pour tout $p \notin \Sigma_X$ on a

$$N_X(p) = \sum_{i=0}^{2d} f_{X,i}(p).$$

On utilise alors le lemme 1.17 conséquence de la dualité de Poincaré : on a pour tout $i \in \{d+1, \dots 2d\}$, pour tout $p \notin \Sigma_X$,

$$f_{X,i}(p) = p^{i-d} f_{X,2d-i}(p).$$

En particulier, comme $f_{X,2d-i}(p)$ est un entier,

$$N_X(p) \equiv \sum_{i=1}^{d} (-1)^i f_{X,i}(p) \text{ [mod } p].$$

On utilise maintenant le théorème 1.18 (« corollaire de divisibilité » de Mazur–Ogus). D'après l'hypothèse, $h^{0,m}(X) = 0$ pour tout $3 \leq m \leq d$, donc tout $p \notin \Sigma_X$ divise $f_{X,m}(p)$ pour tout $m \geq 3$. Finalement on a obtenu

$$N_X(p) \equiv \sum_{i=1}^{2} (-1)^i f_{X,i}(p) \text{ [mod } p].$$

La condition 3 ainsi que les valeurs des bornes $b_\pm(X)$ sont conséquences directes du lemme 1.15. □

Pour la preuve dans le cadre du corollaire 1.37, on fait la preuve par récurrence sur la dimension. Le cas de la dimension 1 est une initialisation facile.

Proposition 1.44. *Soit X un schéma de type fini sur $\mathbf{Z}$, tel que $X \times_{\mathbf{Z}} \mathbf{Q}$ est une courbe. Alors la fonction $M_X := N_X$ satisfait le théorème 1.40 pour $a = 0$. On peut prendre $b_-(X) = 0$ et $b_+(X) = b_2(X)$.*

Démonstration. C'est une conséquence directe du lemme 1.16. □

Pour la dimension 2 et 3 on se ramène au cas projectif lisse grâce au théorème de Hironaka (théorème 1.3) et on utilise la proposition 1.43.

Proposition 1.45. *Soit X un schéma de type fini sur $\mathbf{Z}$ de dimension 2 ou 3. Supposons que la variété $X \times_{\mathbf{Z}} \mathbf{Q}$ est birationnelle à une variété Y_0 satisfaisant les hypothèses de la proposition 1.43. Soit D le produit des éléments de $\Sigma'_{X,Y}$. Soit Y le schéma sur $\mathbf{Z}[1/D]$ correspondant à Y_0, et U le sous-schéma ouvert de $X \times_{\mathbf{Z}} \mathbf{Z}[1/D]$ tel que l'application birationnelle est un isomorphisme sur U. Alors la fonction*

$$M_X := M_Y - M_{Y-U} + M_{X-U}$$

satisfait le théorème 1.40 pour $a = 0$. On peut prendre

$$\begin{aligned} b_-(X) &= -b_2(Y) - b_+(Y-U) + b_-(X-U) \\ \text{et } b_+(X) &= b_2(Y) - b_-(Y-U) + b_+(X-U). \end{aligned}$$

Démonstration. Pour tout $p \notin \Sigma'_{X,Y}$ on a clairement $N_U(p) = N_U(p)$, où U est vu comme sous-schéma de $X \times_{\mathbf{Z}} \mathbf{Z}[1/D]$ ou de Y, autrement dit

$$N_X(p) = N_Y(p) - N_{Y-U}(p) + N_{X-U}(p).$$

On utilise la proposition 1.43 pour Y. Comme U_0 est un ouvert dense de X_0 on a $\dim(X_0 - U_0) < \dim(X_0)$, et de même $\dim(Y_0 - U_0) < \dim(X_0)$. Ainsi dans le cas où X est de dimension 2, les sous-schémas $Y_0 - U_0$ et $X_0 - U_0$ sont des courbes, on peut donc leur appliquer la proposition 1.44. On construit de cette façon les fonctions M_{Y-U} et M_{X-U}. Dans le cas où X est de dimension 3, les sous-schémas $Y_0 - U_0$ et $X_0 - U_0$ sont au plus de dimension 2, et satisfont les hypothèses de la proposition 1.45 que l'on a déjà prouvé dans le cas de la dimension 2. On obtient ainsi la fonction M_X annoncée. □

1.4.4 Retour sur l'évaluation en 1

On a donné dans les propositions 1.43, 1.44 et 1.45 des formules explicites pour les fonctions M_X et pour les bornes $b_\pm(X)$. On peut dans certains cas calculer leurs valeurs et donc en déduire des applications du théorème 1.42.

On a notamment dans le cas des courbes irréductibles le résultat suivant (déjà énoncé à la proposition 1.38).

Proposition 1.46. *Soit C un schéma de type fini sur $\mathbf{Z}$ tel que $C \times_{\mathbf{Z}} \mathbf{Q}$ est une courbe géométriquement irréductible. Alors pour tout $a \in \mathbf{Z} - \{\chi_c(C) - 1\}$, on a*

$$\mathrm{dens}_{\inf}\{p \in \mathcal{P} - \Sigma_C, p \nmid (N_C(p) - a)\} > 0.$$

Démonstration. D'après la proposition 1.44, on peut prendre $M_C = N_C$ et dans le cas irréductible, $b_+(C) = b_-(C) = 1$. Donc la condition (1.8) du théorème 1.42 devient

$$\max(|\chi_c(C) - a|, |\chi_c(C) - a - 2|) \geq 2. \tag{1.12}$$

La seule valeur exclue pour a entier est $a = \chi_c(C) - 1$. □

Remarque 10. 1. On peut se demander s'il est naturel d'exclure une valeur. Dans le cas de la droite affine, on a $N_{\mathbb{A}^1}(p) = p$, il est évident qu'il faut enlever la valeur $a = 0 = \chi_c(\mathbb{A}^1) - 1$. De même pour la droite projective, $\chi_c(\mathbb{P}^1) - 1 = 1$. Dans le cas des courbes elliptiques la valeur exclue est $a = -1$, on remarque qu'elle correspond à la valeur $h = -2$ du théorème 1.25 pour laquelle Serre donne une meilleure borne [Ser81, Th. 20].

2. On sait déjà beaucoup plus de choses dans ce cadre, notamment pour les courbes de genre ≤ 1. En effet dans le cas des morceaux de droites ou de coniques (de genre nul), on a souvent une formule explicite pour le nombre de $\mathbf{F}_p$-points, et la quantité $N_X(p) \pmod p$ ne prend que quelques valeurs qui dépendent de la classe de congruence de p modulo un certain entier. Dans le cas des morceaux de courbes elliptiques, la conjecture de Sato–Tate (théorème 1.24) règle complètement la question.

Pour appliquer le théorème 1.42 à des surfaces, cherchons des surfaces S pour lesquelles l'action de l'endomorphisme de Frobenius sur le groupe de cohomologie $H^2(S, \ell)$ est assez bien connue. Une première idée est de regarder les surfaces cubiques.

Soit S un schéma projectif sur $\mathbf{Z}$ tel que S_0 est une surface cubique projective lisse. Alors on a $h^{0,2}(S) = 0$ (voir par exemple [BPVdV84, V.2]) donc $p \mid f_{S,2}(p)$ pour tout $p \notin \Sigma_S$. De plus $b_1(S) = 0$. En particulier on peut prendre $M_S = f_{S,0}$ et $b_+(S) = b_-(S) = 0$. En fait le cas des cubiques projectives lisse est déjà connu (voir la proposition 1.23). On peut s'intéresser à l'intersection d'une telle surface avec un ouvert affine, alors on se ramène à étudier le nombre de points de la courbe à l'infini. Soit f un polynôme de degré 3 dans $\mathbf{Z}[x, y, z]$. On note f_3 sa composante homogène de degré 3. Soit X la surface affine donnée par $f(x, y, z) = 0$. On suppose que

— la surface projective S définie par l'équation $t^3 f(\frac{x}{t}, \frac{y}{t}, \frac{z}{t}) = 0$ est lisse sur $\mathbf{C}$, et

— la courbe projective C « à l'infini » définie par l'équation $f_3(x, y, z) = 0$ est une courbe irréductible sur $\mathbf{C}$.

Alors $N_X(p) \equiv 1 - N_C(p) \pmod p$. Donc d'après la proposition 1.38, pour tout $a \neq 2 - \chi_c(C)$ on a

$$\mathrm{dens}_{\inf}(\{p \notin \Sigma_X : p \nmid (N_X(p) - a)\}) > 0.$$

Exemple 1. On peut donner un exemple concret. La courbe projective donnée par l'équation $x^3 + y^3 + z^3 = 0$ est une courbe elliptique sur $\mathbf{C}$ et la surface projective donnée par l'équation $Y : x^3 + y^3 + z^3 + t^2(x + y + z) = 0$ est lisse sur $\mathbf{C}$. On peut donc appliquer le raisonnement ci-dessus à la surface affine $X : x^3 + y^3 + z^3 + x + y + z = 0$, on a pour tout $a \neq 2$,

$$\mathrm{dens}_{\inf}(\{p \notin \Sigma_X : p \nmid (N_X(p) - a)\}) > 0.$$

Un deuxième cas de surfaces pour lesquelles l'endomorphisme de Frobenius est assez simple est celui des surfaces $K3$. En effet, une propriété remarquable des surfaces $K3$ est que le deuxième groupe de cohomologie $H^2(S, \mathbf{Z})$ se décompose en une somme directe $\mathrm{Pic}(S) \oplus H^2_{tr}(S, \mathbf{Z})$ où $\mathrm{Pic}(S)$ est le groupe de Picard de la surface et $H^2_{tr}(S, \mathbf{Z})$ est un sous-module dit « transcendantal » de rang 2 (voir par exemple [BPVdV84, VIII.3]). De plus pour tout premier p de bonne réduction, p divise $\mathrm{tr}(\mathrm{Frob}_p \mid \mathrm{Pic}(S))$, il ne reste donc plus que l'action sur le groupe transcendantal. Par ailleurs on a $b_1(S) = 0$. On peut alors prendre comme fonction auxiliaire $M_S(p) = \mathrm{tr}(\mathrm{Frob}_p \mid H^2_{tr}(S, \ell)) + f_{S,0}(p)$, et les bornes sont $b_+(S) = 2$, $b_-(S) = -2$. L'application du théorème 1.42 nous donne donc le résultat suivant (déjà énoncé à la proposition 1.39).

Proposition 1.47. *Soit S un schéma projectif sur $\mathbf{Z}$ tel que $S \times_{\mathbf{Z}} \mathbf{Q}$ est une surface $K3$. Alors pour tout $a \in \mathbf{Z} - \{1, 2, 3, 4, 5\}$, on a*

$$\mathrm{dens}_{\inf}\{p \in \mathcal{P} - \Sigma_S : p \nmid (N_S(p) - a)\} > 0.$$

Démonstration. On applique le théorème 1.42 dans la situation comme expliquée plus haut. On a $M_S(1) = 2 + 1 = 3$. Alors la condition(1.8) devient

$$\max(|6 - a|, |-a|) \geq 6. \tag{1.13}$$

Il nous faut donc exclure toutes les valeurs de a comprises strictement entre 0 et 6. □

1.4.5 Tentatives d'estimation de la densité inférieure

Dans le cas des courbes elliptiques sans multiplication complexe, le résultat de Serre (théorème 1.25) garantit que la densité de l'ensemble $\{p \in \mathcal{P} - \Sigma_E : p \nmid (N_E(p) - a)\}$ existe et vaut 1. On pourrait se demander s'il y a d'autres cas où l'on sait assurer que la densité existe. Faute de savoir assurer l'existence de la densité, il semble naturel de vouloir donner une borne inférieure strictement positive pour la densité inférieure.

En fait ces questions sont assez difficiles. Une façon d'y répondre est de tenter de calculer la densité d'un ensemble $E_{0,m}(M_{X,a})$ comme défini au (1.7). D'après le théorème 1.28, on sait que la densité est un nombre rationnel. En suivant la preuve du théorème 1.28 on a une façon théorique de calculer la valeur de cette densité.

En effet, supposons que $m = \ell$ est un nombre premier pour simplifier. Réduisons pour le moment au cas où on s'intéresse juste à une fonction frobenienne élémentaire de type $f_{X,i}$ comme dans (1.5). Alors la densité de l'ensemble $E_{a,\ell}(f_{X,i})$ vaut $\frac{|C_a \cap G_\ell(X,i)|}{|G_\ell(X,i)|}$ où $G_\ell(X, i)$ est l'image du groupe de Galois $\Gamma_{\Sigma_{X,\ell}}$ donnée par l'action de l'endomorphisme de Frobenius sur $H^i(X, \ell)$, et C_a est le sous-ensemble (stable par conjugaison) des matrices de trace valant a dans ce groupe.

On peut estimer cette densité si on connaît le groupe $G_\ell(X, i)$. Le problème est que ce groupe n'est pas bien connu en général, mais on peut avoir des idées sur ce qu'il devrait être.

Par exemple dans le cas d'une courbe C irréductible projective lisse on sait que pour $p \notin \Sigma_{C,\ell}$, Frob_p agit sur $H^0(C, \ell) \times H^1(C, \ell) \times H^2(C, \ell)$ comme un élément $(1, M, p)$ de $\{1\} \times CSp(2g, \mathbf{F}_\ell) \times \mathbf{F}_\ell^*$ avec de plus le multiplicateur de M égal à p. Donc on peut s'attendre dans un cadre « générique » à ce que le groupe qui nous intéresse soit $G_\ell = \bigcup_{\alpha \in \mathbf{F}_\ell^*} \{1\} \times \alpha Sp(2g, \mathbf{F}_\ell) \times \{\alpha\}$. On a alors

$$\begin{aligned} \mathrm{dens}(E_{0,\ell}(N_{C,a})) &= \sum_{\alpha \in \mathbf{F}_\ell^*} \frac{|\{M \in \alpha Sp(2g, \mathbf{F}_\ell) : \ \mathrm{tr}(M) \equiv 1 - a + \alpha \ [\mathrm{mod}\ \ell]\}|}{|CSp(2g, \mathbf{F}_\ell)|} \\ &\sim \frac{1}{\ell} \end{aligned}$$

par [Kow08a, App. B.2]. On a donc trouvé une borne inférieure strictement positive dans ce cas.

Le cas des courbes irréductibles projectives lisses est particulièrement simple, car pour p assez grand il y a une seule valeur modulo p qui ne convient pas. On a

$$\{p \notin \Sigma_{C,\ell} : p \nmid (N_C(p) - a)\} \simeq \{p \notin \Sigma_{C,\ell} : f_{C,1}(p) \neq 1 - a\}$$

où le symbole $\simeq$ signifie que les ensembles coïncident à un nombre fini de premiers près.

Donc à ℓ fixé, on fait une réunion finie d'ensembles $E_{\ell,b}(f_{C,1})$. On a

$$\begin{aligned}\mathrm{dens}_{\inf}(\{p \notin \Sigma_{C,\ell}, p \nmid (N_C(p)-a)\}) &\\ \geq &\sum_{b\in\mathbf{F}_\ell^*} \frac{|\{M \in CSp(2g,\mathbf{F}_\ell) : \mathrm{tr}(M) \equiv 1-a+b \ [\mathrm{mod}\ \ell]\}|}{|CSp(2g,\mathbf{F}_\ell)|}\\ \geq &\frac{(\ell-1)(\ell-1)}{\ell(\ell-1)}\left(\frac{\ell}{\ell+1}\right)^{2g^2+g+1}\\ = &\frac{\ell-1}{\ell}\left(\frac{\ell}{\ell+1}\right)^{2g^2+g+1}\end{aligned}$$

où la deuxième minoration découle de [Kow08a, App. B.2].

Comme $\sup_{\ell\in\mathcal{P}} \frac{\ell-1}{\ell}\left(\frac{\ell}{\ell+1}\right)^{2g^2+g+1} = 1$ on en déduit que dans ce cas l'ensemble des premiers $\{p \notin \Sigma_C : p \nmid (N_C(p)-a)\}$ est de densité 1.

Finalement, pour répondre à la question posée dans cette sous-section, une bonne idée est de chercher plus d'informations sur l'action de l'endomorphisme de Frobenius. Cependant cette recherche n'a pas été poussée plus loin dans cette thèse. On pourra voir par exemple l'article [FKRS12] où les auteurs cherchent à déterminer plus précisément les groupes de Sato–Tate qui entrent en jeu pour les courbes de genre 2.

1.5 Exemples de schémas avec un A-nombre non nul

Les résultats de la section 1.4, et notamment le corollaire 1.37 nous permettent de revenir à la question de départ : trouver des schémas affines qui satisfont l'hypothèse du théorème 1.1. Dans cette section on exhibe de nouveaux exemples de schémas affines dont le A-nombre est non-nul, en utilisant le théorème 1.21 dû à Fouvry et Katz et notre corollaire 1.37 qui permet de simplifier l'hypothèse de Fouvry et Katz. On déduit en effet le résultat suivant.

Corollaire 1.48. *Soit X un sous-schéma fermé de $\mathbb{A}^n_{\mathbf{Z}}$ tel que $X/\mathbf{C}$ est lisse connexe de dimension relative d. On suppose que $X \times_{\mathbf{Z}} \mathbf{Q}$ est birationnelle à une variété projective lisse Y_0 satisfaisant :*

- $\dim(Y_0) \leq 3$ *et*
- $h^{0,3}(Y_0) = 0$.

Soit D le produit des premiers de mauvaise réduction associés à cette situation (éléments de $\Sigma'_{X,Y}$). S'il existe un premier $p_0 \notin \Sigma'_{X,Y}$ tel que $p_0 \nmid N_X(p_0)$. Alors le A nombre associé à (X, f, k, ψ) est non nul pour toute fonction f, pour tout corps fini k de caractéristique première à $D\ell$ et pour tout caractère additif ψ de k à valeurs dans $\mathbf{Q}_\ell^\times$.

Notre résultat ne s'applique qu'à des schémas de dimension plus petite que 3. On présente des exemples et contre-exemples de chaque dimension.

1.5.1 Exemples de courbes

Le cas des courbes irréductibles a déjà été réglé par la proposition 1.38. En particulier on a

Proposition 1.49. *Soit C un schéma affine sur $\mathbf{Z}$ tel que C_0 soit une courbe irréductible. Alors si $\chi_c(C) \neq 1$, l'ensemble $\{p : p \nmid N_C(p)\}$ a densité inférieure strictement positive.*

On s'intéresse donc à la caractéristique d'Euler–Poincaré des courbes irréductibles pour voir lesquelles sont exclues de ce résultat. Pour calculer le genre d'une courbe qui peut avoir

des points singuliers, on peut chercher un modèle projectif lisse puis utiliser le théorème de Hurwitz (voir par exemple [Har77, IV.2]).

Soit C une courbe affine sur $\mathbf{Z}$, on peut compléter $C/\mathbf{C}$ en une courbe projective $\overline{C}/\mathbf{C}$ en lui ajoutant un nombre fini $N \geq 1$ de points. Alors par additivité de la caractéristique d'Euler-Poincaré,

$$\chi_c(C) = \chi_c(\overline{C}) - N.$$

Par une suite d'éclatement, on obtient un modèle projectif lisse $\tilde{C}/\mathbf{C}$ de $\overline{C}/\mathbf{C}$. On a donc un morphisme séparé $\tilde{C} \to \overline{C}$ de courbes de degré 1. Le théorème de Hurwitz [Har77, IV. Cor. 2.4] garantit que

$$\chi_c(\tilde{C}) = \chi_c(\overline{C}) - \deg R$$

où $\deg R$ est une quantité positive qui compte la ramification. Or $\chi_c(\tilde{C}) = 2 - 2g(\tilde{C})$ Ainsi on a

$$\chi_c(C) \leq \chi_c(\tilde{C}) - 1 \leq 1$$

et l'égalité n'est vérifié que dans le cas où $\tilde{C}$ est une courbe de genre nul et $N = 1$. Par exemple les droites affines ne satisfont pas la propriété 1.49. Dès que $\tilde{C}$ est de genre $g \geq 1$ ou qu'il faut rajouter plus d'un point à $C/\mathbf{C}$ pour la compléter, on est dans le cadre de la propriété 1.49.

1.5.2 Exemples de surfaces

Le contre-exemple des surfaces elliptiques

Soit $f(x,t)$ un polynôme à coefficients dans $\mathbf{Z}$ de degré exactement 3 en la première variable, alors on peut définir la surface elliptique affine associée par $S : y^2 = f(x,t)$ dans $\mathbb{A}^3$. Ces surfaces ne vérifient pas toujours les hypothèses du corollaire 1.48, précisément on a le résultat suivant.

Proposition 1.50. *Supposons que l'on puisse écrire $f(x,t) = ax^3 + b(t)x^2 + c(t)x + d(t)$ avec $a \in \mathbf{Z} - \{0\}$, $b, c, d \in \mathbf{Z}[T]$ de degrés respectivement bornés par $1, 3, 5$. Alors pour p premier différent de 2, on a*

$$N_S(p) = 0 \ [\text{mod } p].$$

Démonstration. Soit p un nombre premier, on a

$$N_S(p) = \sum_{(x,t) \in \mathbf{F}_p^2} 1 + \chi_p(f(x,t))$$

où χ_p est le caractère de Legendre modulo p. On s'intéresse à la valeur de $N_S(p)$ [mod p], donc on va étudier la somme

$$\sum_{(x,t) \in \mathbf{F}_p^2} \chi_p(f(x,t)).$$

On s'inspire de la preuve de [Hua82, Th. 8.2].

Lemme 1.51. *Soit p premier impair, soit c entier non divisible par $p-1$, alors*

$$\sum_{x \in \mathbf{F}_p} x^c = 0 \ [\text{mod } p].$$

En particulier si P est un polynôme de degré au plus $p-2$,

$$\sum_{x \in \mathbf{F}_p} P(x) = 0 \ [\text{mod } p].$$

Démonstration. C'est immédiat en utilisant la cyclicité de $\mathbf{F}_p^\times$. □

On peut maintenant prouver la proposition. Pour tout $(x,t) \in \mathbf{F}_p^2$, on a

$$\chi_p(f(x,t)) = f(x,t)^{\frac{p-1}{2}} \text{ [mod } p]$$
$$= \sum_{k=0}^{\frac{p-1}{2}} \sum_{\ell=0}^{k} \sum_{m=0}^{\ell} \binom{\frac{p-1}{2}}{k} \binom{k}{\ell} \binom{\ell}{m} a^{\frac{p-1}{2}-k} x^{3(\frac{p-1}{2}-k)+2(k-\ell)+(\ell-m)} b(t)^{k-\ell} c(t)^{\ell-m} d(t)^m \text{ [mod } p]$$

Pour k, ℓ, m fixés, en sommant d'abord sur x, on obtient la somme

$$\sum_{x \in \mathbf{F}_p} x^{3(\frac{p-1}{2}-k)+2(k-\ell)+(\ell-m)} = \sum_{x \in \mathbf{F}_p} x^{\frac{3(p-1)}{2}-k-\ell-m}$$

d'après le lemme 1.51, cette somme est nulle modulo p sauf si $\frac{3(p-1)}{2} - k - \ell - m$ est un multiple (non nul) de $p-1$. Comme $k, \ell, m \geq 0$,

$$\frac{3(p-1)}{2} - k - \ell - m < 2(p-1),$$

donc la somme est non nulle seulement dans le cas $k + \ell + m = \frac{p-1}{2}$.

Dans le cas où $k + \ell + m = \frac{p-1}{2}$, faisons d'abord la somme sur t,

$$\sum_{t \in \mathbf{F}_p} b(t)^{k-\ell} c(t)^{\ell-m} d(t)^m = \sum_{t \in \mathbf{F}_p} P(t)$$

où P est un polynôme à coefficients entiers de degré au plus

$$(k-\ell) + 3(\ell - m) + 5m = k + 2\ell + 2m < 2(k + \ell + m) = p - 1$$

car $k > 0$. Donc P est de degré au plus $p-2$. Le lemme 1.51 permet d'affirmer que cette somme est nulle modulo p.

On a donc montré que pour tout triplet (k, ℓ, m),

$$\sum_{x \in \mathbf{F}_p} \sum_{t \in \mathbf{F}_p} x^{3(\frac{p-1}{2}-k)+2(k-\ell)+(\ell-m)} b(t)^{k-\ell} c(t)^{\ell-m} d(t)^m = 0 \text{ [mod } p]$$

donc

$$\sum_{x \in \mathbf{F}_p} \sum_{t \in \mathbf{F}_p} \chi_p(f(x,t)) = 0 \text{ [mod } p].$$

□

Remarque 11.
1. Si on suppose que le degré total de f est majoré par 3 on est dans le cadre des hypothèses de la proposition 1.50, et la surface S est une surface cubique, ce résultat est alors un corollaire du résultat déjà énoncé sur les surfaces cubiques projectives lisse (proposition 1.23, voir aussi le paragraphe correspondant dans la sous-section 1.4.4). En effet, dans ce cas la courbe à l'infini C est une réunion de droites $\{[\alpha : Y : \beta], Y \in \mathbf{F}_p\} \cup \{[0:1:0]\}$ avec $f_3(\alpha, \beta) = 0$, où f_3 est la composante homogène de degré 3 de f. Ce qui fait $N_C(p) \equiv 1 \text{ [mod } p]$, donc $N_S(p) \equiv 0 \text{ [mod } p]$.
2. Les surfaces cubiques de cette forme fournissent un exemple de surfaces qui ont un A-nombre non nul d'après le résultat de Katz [Kat80, p. 150] (voir aussi le paragraphe correspondant dans la section 1.2), mais qui ne satisfont pas l'hypothèse du corollaire 1.48. En effet, pour tout premier $p \mid N_S(p)$.

Remarque 12. On ne peut pas affaiblir l'hypothèse sur le degré de b, en effet pour $p > 2$,

$$\sum_{x \in \mathbf{F}_p} \sum_{t \in \mathbf{F}_p} \chi_p(x(x-1)(x-t^2)) = \chi_p(-1) \text{ [mod } p].$$

Le calcul se fait en utilisant [Hua82, Th. 8.2]

Proposition 1.52. *Soit $p > 2$ premier, $a, b \in \mathbf{Z}$, alors*

$$\sum_{x \in \mathbf{F}_p} \chi_p(x^2 + ax + b) = -1 \text{ [mod } p].$$

On a en sommant d'abord sur t,

$$\sum_{t \in \mathbf{F}_p} \chi_p(x - t^2) = -\chi_p(-1) \text{ [mod } p],$$

puis en sommant sur x,

$$\sum_{x \in \mathbf{F}_p} (-\chi_p(x^2 - x)\chi_p(-1)) = \chi_p(-1) \text{ [mod } p]$$

c'est le résultat voulu.

Surfaces affines dont le modèle projectif lisse est une surface $K3$

On a vu dans la proposition 1.39 que pour les surfaces $K3$ il faut éviter seulement 5 valeurs de a pour assurer que l'ensemble $\{p \in \mathcal{P} - \Sigma_S : p \nmid (N_S(p) - a)\}$ est infini. On peut aussi calculer le nombre de $\mathbf{F}_{p_0}$-points de S pour un certain $p_0 \notin \Sigma_S$ pour garantir que cet ensemble est infini.

Pour appliquer le corollaire 1.48, on s'intéresse à des schémas affines. Regardons ici des schémas affines dont le modèle projectif lisse est une surface $K3$. Alors si on veut appliquer la proposition 1.39, il faut savoir évaluer la différence de points entre la surface $K3$ projective et une surface affine associée. On peut aussi appliquer directement le corollaire 1.37 à condition de comprendre l'ensemble de mauvaise réduction associé à la surface.

Exemple 2. On traite ici l'exemple d'une surface affine inspiré de l'article [PTvdV92]. La surface X est définie sur $\mathbf{Z}$ par les équations :

$$\begin{cases} 1 + x + y + z + t = 0 \\ xyzt + xyz + xyt + xzt + yzt = 0 \end{cases}$$

Pour compléter X en une surface projective on peut rajouter les 4 droites à l'infini mais la surface projective ainsi obtenue n'est pas lisse, elle a 10 points singuliers (trois coordonnées nulles et les deux autres opposées). On nomme Y le schéma obtenu après éclatement en ces 10 points. La surface Y est une surface projective lisse qui est même une surface $K3$ (voir [PTvdV92]). La surface X n'a qu'un nombre fini de points singuliers donc on peut supposer $\dim(X - U) = 0$. Le complémentaire de U dans Y est composé de diviseurs lisses à croisements normaux. Donc $\Sigma'_{X,Y} \subset \Sigma_Y \subset \{2, 3, 5\}$. Il nous suffit de calculer le nombre de $\mathbf{F}_7$-points de X pour conclure. En utilisant `SageMath` [SD16], on trouve $N_7(X) = 94 \equiv 3$ [mod 7]. Donc on peut déduire que

$$\text{dens}_{\text{inf}}\{p : p \nmid N_p(X)\} > 0.$$

Dans l'article [Wen06], l'auteur s'intéresse à des surfaces quartiques de l'espace projectif $\mathbb{P}^3$ données sous la forme

$$Y = Y(f_1, f_2) : f_1(x_0, x_1) + f_2(x_2, x_3) = 0$$

où f_1 etf_2 sont des polynômes homogènes de degré 4 que l'on supposera à coefficients entiers, sans racines doubles, de façon à ce que pour $k = 1, 2$,

$$E_k : y_0^2 = f_k(y_1, y_2)$$

soient des courbes elliptiques dans $\mathbb{P}(2, 1, 1)$ l'espace projectif pondéré. On suppose de plus que $Y(f_1, f_2)$ est lisse. D'après le théorème de Lefschetz faible [Mil80, Prop. 7], $Y(f_1, f_2)$ admet donc un H^1 trivial, D'après [Ino76, p. 552] c'est même une surface $K3$.

Exemple 3. La quartique de Fermat est définie par :

$$\mathcal{F} : x_0^4 + x_1^4 + x_2^4 + x_3^4 = 0.$$

On s'intéresse au nombre de $\mathbf{F}_p$-points rationnels d'une surface affine associée à $\mathcal{F}$, par exemple

$$X_{\mathcal{F}} : 1 + x_1^4 + x_2^4 + x_3^4 = 0.$$

D'après le corollaire 1.37, il suffit de trouver un premier de bonne réduction vérifiant $p \nmid N_{X_{\mathcal{F}}}(p)$ pour savoir qu'il en existe un ensemble de densité inférieure strictement positive. Le schéma $\mathcal{F}$ est un modèle projectif lisse de $X_{\mathcal{F}}$ (lui même lisse), et on a juste rajouté une courbe (quartique) lisse pour l'obtenir. Donc il nous faut juste éviter le premier 2 qui est de mauvaise réduction. Un calcul avec le logiciel `SageMath` [SD16] donne

$$N_{X_{\mathcal{F}}}(3) = 12 \equiv 0 \text{ [mod 3]}$$

ce qui ne permet pas de conclure. On teste les premiers suivants pour finalement trouver

$$N_{X_{\mathcal{F}}}(13) = 96 \equiv 5 \text{ [mod 13]}$$

On conclut donc que

$$\text{dens}_{\text{inf}}\{p : p \nmid N_p(X_{\mathcal{F}})\} > 0$$

et on a donc le corollaire 1.48.

De façon un peu plus générale, étudions

$$X = X(f_1, f_2) : f_1(x, y) + f_2(z, 1) = 0.$$

On a alors pour p premier,

$$N_X(p) = N_Y(p) - N_C(p)$$

où C est la courbe quartique dans $\mathbb{P}^2$ définie par

$$C : f_1(x_0, x_1) + f_2(x_2, 0) = 0.$$

Supposons $f_2(1, 0) \neq 0$, comme E_1 est une courbe elliptique, C est une courbe lisse géométriquement irréductible. C'est une courbe projective de genre 3, donc de caractéristique d'Euler–Poincaré égale à -4. En particulier on peut utiliser les propositions 1.38 et 1.39 pour $a = 0$. On déduit le résultat suivant :

Proposition 1.53. *Si $f_2(1, 0) \neq 0$ alors l'ensemble $\{p \notin \Sigma_X : p \nmid N_X(p)\}$ est de densité inférieure strictement positive.*

Remarque 13. Le cas où $f_2(1, 0) = 0$, est moins aisé. Si f_1 est scindé dans $\mathbf{F}_p$, $C(\mathbf{F}_p)$ est l'union de 4 droites données par $x_0 b_i = y_0 a_i$ où $[a_i : b_i]$ sont les quatre racines de f_1 dans $\mathbb{P}^1(\mathbf{F}_p)$. Ces droites sont concourantes au point $[0 : 0 : 1]$ donc sous ces conditions

$$N_C(p) = 4(p + 1) - 3 = 4p + 1.$$

Ainsi sous ces conditions,

$$N_X(p) \equiv N_Y(p) - 1 \text{ [mod } p].$$

Or $a = 1$ est une valeur exclue dans la proposition 1.39, on ne peut donc pas conclure automatiquement, il faudra calculer le nombre de points pour un premier de bonne réduction pour chaque exemple.

1.5.3 Exemples en dimension trois

On veut un exemple de schéma affine de dimension 3 qui soit birationnel à un schéma projectif lisse avec un nombre de Hodge $h^{0,3}$ nul.

On pourrait d'abord penser à l'exemple le plus simple : une hypersurface de l'espace affine $\mathbb{P}^4$. Soit $Y \subseteq \mathbb{P}^4$ une hypersurface projective lisse définie sur $\mathbf{Z}$ par une équation de degré d. Alors ses nombres de Hodge sont tous connus (voir par exemple [CR12, Sec. 4]). On a $h^{0,3}(Y) = \binom{d-1}{4}$. En particulier les hypersurfaces lisses de degré inférieur ou égal à 4 satisfont les hypothèses du théorème 1.35.

Remarque 14. Une façon de garantir que le nombre de Hodge $h^{0,3}(Y)$ est nul est d'avoir plus que cela, le nombre de Betti $b_3(Y) = 0$. D'après [Dim92, Chap. 5 §3], dans le cas d'une hypersurface de degré d on a $b_3(Y) = \frac{(d-1)^5+1}{d} - 1$ ce qui est nul seulement si $d = 1$ ou 2 (strictement positif si $d > 2$).

Construction d'exemples avec troisième nombre de Betti nul

Reprenons l'idée de la remarque 14, on cherche à construire des exemples pour lesquels le troisième nombre de Betti b_3 nul. En suivant une idée qui nous a été proposée par O. Benoist, on va construire des schémas affines de dimension 3 dont un modèle projectif lisse vérifie $b_3 = 0$.

On a vu que les hypersurfaces non rationnelles ne conviennent pas. Donnons maintenant une construction non triviale de tels exemples. On se donne une surface projective S définie sur $\mathbf{Z}$, lisse sur $\mathbf{C}$ avec $b_1(S) = 0$ (on peut par exemple prendre pour S une surface $K3$). Alors on construit un schéma lisse Y muni d'un morphisme $g : Y \to S$ tel que pour tout $s \in S$, la fibre Y_s est isomorphe $\mathbb{P}^1$. Le calcul des nombres de Betti de Y se fait en utilisant la suite spectrale de Leray (voir par exemple [Voi02, Chap. 16]) pour $g : Y \to S$. La suite est donnée par $E_2^{i,j} := H^i(S, R^j g_* \mathbf{Q}) \Rightarrow H^{i+j}(Y, \mathbf{Q})$. Cela signifie en particulier ([Voi02, Th. 8.21]) qu'on a une suite exacte :

$$\ldots \to \operatorname{coker}\left(H^0(S_0, R^2 g_* \mathbf{Q}) \to H^3(S_0, R^0 g_* \mathbf{Q})\right) \to H^3(Y_0, \mathbf{Q}) \\ \to \ker\left(H^1(S_0, R^2 g_* \mathbf{Q}) \to H^4(S_0, R^0 g_* \mathbf{Q})\right) \to \ldots.$$

Or $R^0 g_* \mathbf{Q} \simeq \mathbf{Q} \simeq R^2 g_* \mathbf{Q}$ car les fibres de g sont toutes isomorphes à la droite $\mathbb{P}^1$, et $H^0(\mathbb{P}^1, \mathbf{Q}) \simeq H^2(\mathbb{P}^1, \mathbf{Q}) \simeq \mathbf{Q}$. Comme $H^3(S_0, \mathbf{Q}) \simeq H^1(S_0, \mathbf{Q}) \simeq 0$ par hypothèse sur S, cela permet de déduire que $b_3(Y) = 0$.

Remarque 15. Le premier exemple de tel schéma auquel on pense est le produit fibré $S \times \mathbb{P}^1$. Cependant connaître le nombre de $\mathbf{F}_p$-points de cette variété ne nécessite pas un théorème propre à la dimension 3. On va donc chercher des exemples plus intéressants.

Les schémas que l'on vient de décrire sont connus et étudiés sous le nom de « schémas de Severi-Brauer sur S d'ordre relatif 2 ». Dans notre cas (S est une surface projective lisse sur $\mathbf{C}$), [Gro68, Part. 8] assure que Les « schémas de Severi-Brauer sur S d'ordre relatif 2 » sont classifiés par la 2-torsion du groupe de Brauer de S, que l'on note $Br(S)[2]$.

Notons $K = \mathbf{C}(S)$ le corps des fonctions de S. Alors $Br(S)[2]$ est le sous-groupe de $Br(K)[2]$ constitué des classes non ramifiées sur S. On peut interpréter $Br(K)[2]$ comme l'ensemble des algèbres de quaternions sur K. En particulier les éléments de $Br(S)[2]$ peuvent se décrire grâce à des fonctions rationnelles définies sur un ouvert affine.

De plus dans le cas où S est une surface complexe projective lisse, on a une description de ce groupe :

$$Br(S)[2] = (\mathbf{Z}/2\mathbf{Z})^{b_2(S)-r} \oplus H^3(S, \mathbf{Z})[2],$$

où r est le rang du groupe de Picard de S. Dans le cas où $Br(S)[2]$ est non-trivial (c'est le cas quand S est une surface $K3$ par exemple), alors un élément non trivial de $Br(S)[2]$

fournit une équation pour un schéma de Severi-Brauer sur S d'ordre relatif 2 qui n'est pas $S \times \mathbb{P}^1$. La seule condition pour donner des équations explicites de telles variétés sera de savoir expliciter un élément non-trivial de $Br(S)[2]$.

Plus concrètement, on fixe S une surface $K3$ dans l'espace projectif pondéré $\mathbb{P}(1,1,1,3)$ donnée par une équation $f(x,y,z) = w^2$ où f est un polynôme homogène de degré 6. Un élément non-trivial de $Br(S)[2]$ peut être donné sur un ouvert affine O de S comme un couple (a,b) où a et b sont des fonctions rationnelles en la variable $s = (x,y,z) \in O$. On définit le schéma $\overline{U}(a,b)$ dans $O \times \mathbb{P}^2$par les équations :

$$\overline{U}(a,b) : a(s)u^2 + b(s)v^2 = t^2.$$

Alors $\overline{U}(a,b)$ est birationnel à un schéma de Severi-Brauer sur S d'ordre relatif 2, c'est-à-dire qu'il admet une complétion projective lisse $Y(a,b)$ satisfaisant $b_3(Y(a,b)) = 0$. Écrivons $a = \alpha/d$, $b = \beta/d$ avec α, β, d des polynômes, on peut alors définir une variété plus grande $\overline{X}(a,b)$ dans $\mathbb{P}(1,1,1,3) \times \mathbb{P}^2$ par les équations :

$$\overline{X}(a,b) : \left\{ \begin{array}{rcl} f(x,y,z) & = & w^2 \\ \alpha(x,y,z)u^2 + \beta(x,y,z)v^2 & = & d(x,y,z)t^2 \end{array} \right.$$

avec les variables $[x:y:z:w] \in \mathbb{P}(1,1,1,3)$, $[t:u:v] \in \mathbb{P}^2$. Alors $\overline{U}(a,b)$ est ouvert dense dans $\overline{X}(a,b)$ donc $\overline{X}(a,b)$ est aussi birationnel à $Y(a,b)$. Comme on cherche un exemple affine, on retire au schéma $\overline{X}(a,b)$ une intersection avec un hyperplan à l'infini : le schéma affine dans $\mathbb{A}^5$ donné par les équations

$$X(a,b) : \left\{ \begin{array}{rcl} f(x,y,1) & = & w^2 \\ \alpha(x,y,1)u^2 + \beta(x,y,1)v^2 & = & d(x,y,1) \end{array} \right.$$

admet $Y(a,b)$ comme modèle projectif lisse.

Comme on peut s'y attendre, on ne sait pas en général décrire un élément non-trivial du groupe $Br(S)[2]$, mais on peut trouver des études de surfaces $K3$ dans la littérature.

Exemple 4. Dans l'article [ABBVA14] les auteurs s'intéressent à une surface $K3$ que l'on notera S et que l'on peut définir par une équation $w^2 = f(x,y,z)$ avec

$$\begin{aligned} f(x,y,z) = {} & x^6 + 6x^5y + 12x^5z + x^4y^2 + 22x^4yz + 28x^3y^3 - 38x^3y^2z + 46x^3yz^2 \\ & + 4x^3z^3 + 24x^2y^4 - 4x^2y^3z - 37x^2y^2z^2 - 36x^2yz^3 - 4x^2z^4 + 48xy^4z - 24xy^3z^2 \\ & + 34xy^2z^3 + 4xyz^4 + 20y^5z + 20y^4z^2 - 8y^3z^3 - 11y^2z^4 - 4yz^5. \end{aligned}$$

D'après [ABBVA14, Th. 9 (iv)], la surface $K3$ a un groupe de Picard de rang 2, donc $Br(S)[2]$ n'est pas trivial. Alors [ABBVA14, Prop. 11] fournit un élément non-trivial du groupe $Br(S)[2]$ sous la forme d'une algèbre de quaternions de paramètre (a,b) avec

$$a = x^2 + 14xy - 23y^2 - 8yz$$

et

$$b = b_1b_2 = (x - 4y - z)(3x^3 + 2x^2y - 4x^2z + 8xyz + 3xz^2 - 16y^3 - 11y^2z - 8yz^2 - z^3).$$

Soit X le schéma de dimension 3 dans $\mathbb{A}^5$ donné par les équations

$$X : \left\{ \begin{array}{rcl} f(x,y,1) & = & w^2 \\ a(x,y,1)u^2 + b(x,y,1)v^2 & = & 1 \end{array} \right. .$$

D'après le raisonnement que l'on vient de suivre, le schéma X admet un modèle projectif lisse Y satisfaisant $b_3(Y) = 0$. On peut donc lui appliquer le corollaire 1.37. On connaît les

premiers de mauvaise réduction pour la surface S, ils sont donnés dans [ABBVA14, Rk. 12]. Supposons que la construction de X ne crée pas d'autres premiers de mauvaise réduction. Alors on peut calculer le nombre de $\mathbf{F}_7$-points de X. En utilisant `SageMath` [SD16], on obtient

$$N_X(7) = 584 \neq 0 \text{ [mod 7]}.$$

On déduit (sous l'hypothèse que $7 \notin \Sigma'_{X,Y}$)

$$\mathrm{dens}_{\mathrm{inf}}(\{p : p \nmid N_X(p)\}) > 0.$$

Chapitre 2

Méthodes de crible et plus petit premier dans un ensemble frobenien

On a vu dans la proposition 1.38 au chapitre précédent que pour une courbe irréductible C sur $\mathbf{Z}$, pour des entiers $a_1, \ldots, a_n \neq \chi_c(C) - 1$, l'ensemble $\{p : p \nmid \prod_{i=1}^{n}(N_C(p) - a_i)\}$ est infini et même admet une densité inférieure strictement positive. L'idée générale pour les résultats du chapitre précédent est de trouver un premier de bonne réduction dans l'ensemble $\{p : p \nmid \prod_{i=1}^{n}(N_C(p) - a_i)\}$ afin de garantir qu'il n'est pas vide. Dans ce chapitre on cherche à savoir s'il est difficile de trouver ce premier : on se pose la question d'estimer la taille du plus petit élément de l'ensemble $\{p : p \nmid \prod_{i=1}^{n}(N_C(p) - a_i)\}$. Au vu de la proposition 1.38 l'ensemble a une densité inférieure strictement positive, donc on s'attend à ce que ce premier soit « assez petit » en fonction des paramètres qui permettent de définir la courbe. Cependant on parvient dans la section 2.3 à construire des exemples de courbes pour lesquelles le plus petit premier de l'ensemble $\{p : p \nmid N_C(p)\}$ est arbitrairement grand.

Remarque 16.

1. On pourrait se poser la question dans un cadre plus général pour un schéma X de type fini sur $\mathbf{Z}$ vérifiant les hypothèses du corollaire 1.37 par exemple. Comme on en a déjà fait la remarque plus tôt, le cas des courbes irréductibles est assez facile à traiter, tandis que le cas général est beaucoup plus délicat. On se contente donc ici de traiter le cas plus simple des courbes.

2. Dans le cas des surfaces, on a vu dans la proposition 1.50 des exemples de surfaces pour lesquelles l'ensemble $\{p : p \nmid N_C(p)\}$ est vide. Il n'y a donc pas de plus petit premier dans cet ensemble.

L'idée que l'on va suivre dans ce chapitre est de majorer pour presque toutes les courbes irréductibles C_u dans une famille indexée par un paramètre u, le plus petit élément $p_0(C_u)$ de l'ensemble $\{p : p \nmid \prod_{i=1}^{n}(N_{C_u}(p) - a_i)\}$. Pour cela on va utiliser deux méthodes de crible imbriquées suivant l'idée de [EEHK09]. On veut estimer la taille de l'ensemble des u dans l'espace de paramètres U sur $\mathbf{Z}$ pour lesquels $p_0(C_u)$ est plus grand qu'une certaine valeur Q. Il faudra choisir cette valeur Q pour que l'ensemble $\{u \in U : p_0(C_u) > Q(U)\}$ soit « petit ». Pour estimer la taille de tels ensembles on aura recours à des méthodes de grands cribles différentes selon l'espace des paramètres U. On estimera en particulier la taille de l'image de tels ensembles par la réduction modulo p. Pour cela on utilisera à nouveau une méthode de grand crible pour les classes de conjugaison du Frobenius tel que présenté dans [Kow08a, Chap. 8]. On commence dans la section 2.1 par rappeler le principe du grand crible tel que présenté dans [Kow08a], ainsi que diverses manières de l'appréhender qui permettent d'obtenir différents résultats que l'on comparera.

2.1 Inégalités de grand crible

La notion de crible en théorie analytique des nombres regroupe diverses méthodes dont le but est d'estimer asymptotiquement des fonctions définies par des propriétés arithmétiques contraintes par des relations de congruences modulo un ensemble de nombre premier. Le plus souvent cette fonction est l'indicatrice d'un ensemble dont l'image modulo divers premiers p évite des ensembles criblants Ω_p. Dans ce chapitre on utilise le principe du « grand crible » de Linnik, dans le sens où les tailles des ensembles criblants Ω_p sont des fonctions croissantes de p, (par opposition au « petit crible » où les ensembles criblants sont de taille bornée). On renvoie au livre de Kowalski sur le grand crible [Kow08a] pour la plupart des preuves de cette section.

Commençons par redonner le cadre général du grand crible tel qu'énoncé dans [Kow08a, Chap. 2] (voir aussi [Jou07, Chap. 6]). Un *cadre de crible* est la donnée d'un triplet $(Y, \Lambda, (\rho_\ell)_{\ell\in\Lambda})$ où Y est un ensemble, Λ est un ensemble d'indices et pour chaque $\ell \in \Lambda$ l'application $\rho_\ell : Y \to Y_\ell$ est surjective vers un ensemble fini Y_ℓ. Dans les applications Λ sera toujours un ensemble de nombres premiers. Souvent l'application ρ_ℓ est une réduction modulo ℓ de l'ensemble Y (cela a du sens quand Y est défini sur $\mathbf{Z}$). On définit aussi un *ensemble à cribler* associé à un cadre de crible $(Y, \Lambda, (\rho_\ell)_{\ell\in\Lambda})$ comme la donnée d'un triplet (X, μ, F) où (X, μ) est un espace mesuré et $F : X \to Y$ est une application telle que pour tout ℓ, $\rho_\ell \circ F$ est mesurable. On se donne aussi un *support premier de crible* $\mathcal{L}^*$: une partie finie de Λ. Enfin pour tout $\ell \in \mathcal{L}^*$, on a une famille d'*ensembles criblants* $\Omega_\ell \subset Y_\ell$.

A toutes ces données on associe un problème de crible qui est de majorer la mesure de l'ensemble

$$S(X, (\Omega_\ell)_\ell, \mathcal{L}^*) := \{x \in X : \forall \ell \in \mathcal{L}^*, \rho_\ell(F(x)) \notin \Omega_\ell\}.$$

L'idée générale est que plus les ensembles Ω_ℓ sont gros, plus l'ensemble $S(X, (\Omega_\ell)_\ell, \mathcal{L}^*)$ devrait être petit et devrait donc représenter un ensemble d'exceptions à une règle générale qui serait d'avoir son image dans au moins un des Ω_ℓ.

Pour majorer la mesure de l'ensemble $S(X, (\Omega_\ell)_\ell, \mathcal{L}^*)$ la méthode consiste à couper le problème en deux. D'une part, on utilise une estimation de la taille des ensembles criblants Ω_ℓ. D'autre part on majore une *constante de grand crible* Δ qui va dépendre du cadre de crible mais pas des ensembles criblants. On peut donner une formule explicite pour Δ et l'utiliser dans divers problèmes de crible, on donnera notamment des bornes supérieures dans trois cadres de cribles différents aux sous-sections 2.1.1, 2.1.2, et 2.1.3.

Pour définir la constante de grand crible, on a besoin de quelques données supplémentaires. On utilise pour tout ℓ une densité de probabilité ν_ℓ sur l'ensemble Y_ℓ à valeurs dans $]0, 1]$. Cette densité permet de choisir une structure hermitienne sur l'ensemble des fonctions sur Y_ℓ à valeurs dans $\mathbf{C}$ en définissant le produit scalaire :

$$\langle f, g\rangle = \sum_{y\in Y_\ell} \nu_\ell(y) f(y)\overline{g(y)}.$$

On va utiliser une base de l'espace des fonctions définies sur les Y_ℓ. Pour $\ell \in \mathcal{L}^*$ soit $\mathcal{B}_\ell^* \cup \{\mathbf{1}\}$ une base orthonormée de l'espace $L^2(Y_\ell, \langle , \rangle_{\nu_\ell})$ où $\mathbf{1}$ est la fonction constante égale à 1.

On peut énoncer la première inégalité de grand crible formulée par Montgomery (voir [Kow08a, Prop. 2.3]).

Théorème 2.1 (Montgomery)**.** *Étant donné une situation de crible comme définie plus haut, soit $\Delta = \Delta(X, \mathcal{L}^*)$ la constante de grand crible associée définie comme la plus petite valeur réelle positive satisfaisant*

$$\sum_{\ell\in\mathcal{L}^*} \sum_{\phi\in\mathcal{B}_\ell^*} \left| \int_X \alpha(x)\phi(\rho_\ell(F(x)))d\mu(x) \right| \leq \Delta \int_X |\alpha(x)|^2 d\mu(x)$$

pour tout $\alpha \in L^2(X)$. Alors on a pour toute famille d'ensembles criblants $(\Omega_\ell)_{\ell\in\mathcal{L}^*}$ l'inégalité

$$\mu(S(X,(\Omega_\ell)_\ell,\mathcal{L}^*)) \leq \Delta H^{-1}$$

où

$$H := \sum_{\ell\in\mathcal{L}^*} \frac{\nu_\ell(\Omega_\ell)}{\nu_\ell(Y_\ell - \Omega_\ell)}.$$

La définition de Δ n'est pas utilisable directement. Grâce au principe de dualité on parvient à majorer la constante de grand crible par des sommes exponentielles que l'on sait en général mieux traiter. Pour cela on a besoin d'une hypothèse supplémentaire sur les surjections ρ_ℓ. Pour tout $\ell \neq \ell' \in \mathcal{L}^*$ on a l'application $\rho_{\ell,\ell'} : Y \to Y_\ell \times Y_{\ell'}$ définie comme le produit de ρ_ℓ et $\rho_{\ell'}$. Cette application n'est pas a priori surjective mais on va avoir besoin qu'elle le soit dans les applications que l'on développe.

Définition 2.2. On dit que le système $(\rho_\ell)_{\ell\in\Lambda}$ est linéairement indépendant si pour tout $\ell \neq \ell' \in \Lambda$, l'application $\rho_{\ell,\ell'} : Y \to Y_\ell \times Y_{\ell'}$ est surjective.

Sous l'hypothèse de linéaire indépendance du système, on peut donner une majoration de Δ. C'est le contenu de [Kow08a, Prop. 2.9].

Théorème 2.3. *On se place dans la situation ci-dessus. Soient $\ell, \ell' \in \mathcal{L}^*$, et $\phi \in \mathcal{B}_\ell^*$, $\phi' \in \mathcal{B}_{\ell'}^*$, on définit*

$$W(\phi,\phi') := \int_X \phi(\rho_\ell(F(x)))\overline{\phi'(\rho_{\ell'}(F(x)))}d\mu(x).$$

On a

$$\Delta(X,\mathcal{L}^*) \leq \max_{\ell\in\mathcal{L}*}\max_{\phi\in\mathcal{B}_\ell^*} \sum_{\ell'\in\mathcal{L}^*}\sum_{\phi'\in\mathcal{B}_{\ell'}^*} |W(\phi,\phi')|.$$

Cette borne est souvent calculable, on va donner des exemples de ce calcul dans les sections suivantes. En général dans les applications on utilise la borne du membre de droite à la place de Δ.

Remarque 17. On a donné les théorèmes 2.1 et 2.3 dans le cadre du crible à support premier. Dans [Kow08a] ces résultats sont présentés sous une forme plus générale en faisant un crible sur un ensemble plus grand de nombres sans facteurs carrés. Prendre un support de crible plus grand permet en général d'affiner la majoration, on utilise ainsi dans la sous-section 2.1.2 une version du crible due à Kowalski où le support de crible est un ensemble d'entiers sans facteurs carrés dont les facteurs premiers sont assez grands. Cependant, prendre comme support de crible tous les entiers sans facteurs carrés ne donne pas toujours la meilleure borne, on montre dans la sous-section 2.1.3 une version améliorée d'un résultat de Bellaïche en prenant comme support de crible seulement un ensemble de nombres premiers.

On utilisera régulièrement le résultat suivant,

Lemme 2.4. *Soient $Q > 0$, $a > -1$ et $b \in \mathbf{R}$ alors $\sum_{\ell<Q} \ell^a(\log\ell)^b \asymp_a Q^{a+1}(\log Q)^{b-1}$.*

C'est un résultat classique que l'on obtient grâce à une sommation d'Abel et le théorème des nombres premiers.

2.1.1 Crible pour la mesure de comptage sur $\mathbf{Z}^d$

Commençons par présenter la situation simple du crible sur $\mathbf{Z}^d$ avec la mesure de comptage. On pourra voir [Gal73] pour une première utilisation de ce crible. Le cadre du crible est $(\mathbf{Z}^d, \mathcal{P}, (\rho_p)_{p\in\mathcal{P}})$ où ρ_p est la réduction modulo $p : \mathbf{Z}^d \to \mathbf{F}_p^d$. C'est une généralisation du grand crible classique (voir [Kow08a, 4.2]). Le résultat utilisé par Gallagher [Gal73, Sect. 1] est obtenu avec un crible supporté sur les entiers sans facteurs carrés. On donne ici une preuve élémentaire d'un résultat un peu plus faible dans le cas où le support de crible est le support premier.

Soit $T > 1$ assez grand fixé, on choisit comme ensemble à cribler $X(T) := \mathbf{Z}^d \cap [-T, T]^d$ muni de la mesure de comptage et de l'inclusion naturelle dans $\mathbf{Z}^d$. Prenons pour $\mathcal{L}^* = \mathcal{L}^*(Q)$ l'ensemble des premiers plus petits qu'une borne Q.

Majorons la constante de grand crible $\Delta(T, Q)$. D'après le théorème 2.3, il nous faut d'abord chercher une base orthonormée de l'espace des fonctions sur $\mathbf{F}_p^d$ pour le produit scalaire usuel. On pose pour $a \in \mathbf{F}_p^d$,

$$\phi_{a,p} : x \mapsto e\left(\frac{a \cdot x}{p}\right)$$

où $\cdot$ est le produit scalaire usuel de $\mathbf{F}_p^d$. Les $(\phi_{a,p})_{a\in\mathbf{F}_p^d}$ forment une base orthonormée de $L^2(\mathbf{F}_p^d)$. On a donc

$$\Delta(T, Q) \leq \max_{p\leq Q} \max_{a\in\mathbf{F}_p^d-\{\underline{0}\}} \sum_{p'\leq Q} \sum_{b\in\mathbf{F}_{p'}^d-\{\underline{0}\}} |W(\phi_{a,p}, \phi_{b,p'})|.$$

Calculons la valeur de $W(\phi_{a,p}, \phi_{b,p'})$.

$$\begin{aligned} W(\phi_{a,p}, \phi_{b,p'}) &= \sum_{|u|\leq T} \phi_{a,p}(u)\overline{\phi_{b,p'}(u)} \\ &= \prod_{j=1}^{d} \sum_{u_j=-T}^{T} e\left(\frac{a_j p' - b_j p}{pp'} u_j\right). \end{aligned}$$

Donc

— si $p = p'$ et $a = b$, on obtient

$$W(\phi_{a,p}, \phi_{a,p}) = (2T + 1)^d.$$

— Si $p = p'$ et $a \neq b$, soit k le nombre de coefficients identiques entre a et b (on a $0 \leq k \leq d - 1$), alors quitte à réordonner pour que les coefficients identiques soient les k premiers,

$$W(\phi_{a,p}, \phi_{b,p}) \leq (2T + 1)^k \prod_{j=k+1}^{d} \min\left(2T + 1, \frac{1}{2\|\frac{a_j - b_j}{p}\|}\right).$$

où $\|x\|$ est la distance de x à $\mathbf{Z}$. Comme $p \nmid a_j - b_j$, on a $\left\|\frac{a_j-b_j}{p}\right\| \geq \frac{1}{p}$. Ainsi,

$$|W(\phi_{a,p}, \phi_{b,p})| \leq (2T + 1)^k \left(\frac{p}{2}\right)^{d-k}$$

et cette majoration est non triviale à condition que $p \ll T$. Si on fixe a dans $\mathbf{F}_p^d$, il y a $\binom{d}{k} p^{d-k}$ éléments b dans $\mathbf{F}_p^d$ avec exactement k coordonnées semblables.

— Si $p \neq p'$, on a $a_j p' - b_j p \neq 0$ pour tout j sauf dans le cas $a_j = b_j = 0$ ce qui peut arriver pour au plus $d-1$ indices j. Soit k le nombre de coefficients nuls en commun à a et b on trouve, quitte à réordonner

$$|W(\phi_{a,p}, \phi_{b,p'})| \leq (2T+1)^k \prod_{j=k+1}^{d} \min\left(2T+1, \frac{1}{2\|\frac{a_j p' - b_j p}{pp'}\|}\right).$$

D'où

$$|W(\phi_{a,p}, \phi_{b,p'})| \leq (2T+1)^k \left(\frac{pp'}{2}\right)^{d-k}.$$

Et cette majoration n'est pas triviale si $p, p' \leq \sqrt{T}$. Pour a fixé dans $\mathbf{F}_p^d$ avec k_a coefficients nuls, il y a $\binom{k_a}{k} p'^{d-k}$ éléments b dans $\mathbf{F}_{p'}^d$ avec exactement k zéros communs.

On obtient donc la majoration de $\Delta(T, Q)$,

$$\begin{aligned}
\Delta(T,Q) \leq & \max_{p \leq Q} \left\{ (2T+1)^d + \sum_{k=0}^{d-1} \binom{d}{k} (2T+1)^k \left(\frac{p}{2}\right)^{d-k} p^{d-k} \right. \\
& \left. + \max_{a \in \mathbf{F}_p - \{\underline{0}\}} \sum_{p' \leq Q} \sum_{k=0}^{k_a} \binom{k_a}{k} p'^{d-k} (2T+1)^k \left(\frac{pp'}{2}\right)^{d-k} \right\} \\
\ll & (T+Q^2)^d + \frac{Q}{\log Q} \max_{p \leq Q} \max_{a \in \mathbf{F}_p - \{\underline{0}\}} \left\{ \sum_{k=0}^{k_a} \binom{k_a}{k} (2T+1)^k \left(\frac{pQ^2}{2}\right)^{d-k} \right\} \\
\ll & (T+Q^2)^d + \frac{Q}{\log Q} (T+Q^3)^{d-1}
\end{aligned}$$

et la constante implicite ne dépend que de d.

Remarque 18. Cette majoration est triviale si $Q > \sqrt{T}$.

Finalement on a obtenu le résultat suivant.

Proposition 2.5. *Dans le cadre du grand crible sur $\mathbf{Z}^d$, on a*

$$\Delta(T,Q) \ll (T+Q^2)^d + \frac{Q}{\log Q}(T+Q^3)^{d-1}.$$

2.1.2 Crible pour les classes de conjugaison de Frobenius

Dans [Kow08a, Chap. 8], Kowalski utilise un crible pour les classes de conjugaison de l'endomorphisme de Frobenius pour donner une version quantitative d'un résultat de Chavdarov [Cha97] en réponse à une question de Katz sur la fonction zêta d'une courbe sur un corps fini. On se demande si typiquement le numérateur de la fonction zêta d'une courbe irréductible vérifie certaines propriétés comme : être irréductible sur $\mathbf{Q}$ ou avoir un corps de décomposition dont le groupe de Galois sur $\mathbf{Q}$ est maximal. Ces questions avaient déjà été abordées dans [Kow06a] mais les bornes ont été améliorées et précisées dans [Kow08a].

On se place dans le cadre d'une famille de courbes $C \to U$ sur un corps fini. Plus précisément, soit q une puissance d'un nombre premier p, et soit $U/\mathbf{F}_q$ une variété algébrique affine lisse géométriquement connexe de dimension $d \geq 1$ sur $\mathbf{F}_q$. Fixons un second premier $\ell \neq p$. Au revêtement étale $C \to U$ on associe la représentation ℓ-adique continue du groupe fondamental étale arithmétique de U :

$$\rho_\ell : \pi_1(U, \overline{\eta}) \to GL(2g, \mathbb{Q}_\ell)$$

correspondant à l'action de l'endomorphisme de Frobenius Frob_u sur $H^1_c(C_u, \ell)$. En particulier pour tout $u \in U(\mathbb{F}_p)$, le numérateur de la fonction zêta de C_u est

$$\det(1 - T\rho_\ell(\mathrm{Frob}_u)).$$

C'est un polynôme à coefficients dans $\mathbf{Z}_\ell$. La représentation ne dépend en fait pas vraiment de ℓ, et les coefficients sont dans $\mathbf{Z}$, on dit que le système est compatible (voir [Kow08a, Def. 8.7]).

D'après la dualité de Poincaré, l'image $\rho_\ell(\pi_1(U, \overline{\eta}))$ réduite modulo ℓ est un sous-groupe G_ℓ du groupe des similitudes symplectiques $CSp(2g, \mathbf{F}_\ell)$. Dans le cas où on connaît précisément ces sous-groupes quand ℓ varie, on peut utiliser le crible pour les classes de conjugaison sur ce groupe pour évaluer la taille d'ensembles du type $\{u \in U(\mathbf{F}_p) : \mathrm{Frob}_u \in A\}$. En particulier on peut évaluer la taille d'ensembles pour lesquels le polynôme caractéristique du Frobenius satisfait certaines propriétés.

Le principe du crible pour les classes de conjugaison du Frobenius est de prendre comme cadre de crible $Y = G^\sharp$ l'ensemble des classes de conjugaison du groupe $G = \pi_1(U, \overline{\eta})$. Soit Λ un ensemble de premier différents de p et pour chaque $\ell \in \Lambda$ la surjection $\tilde{\rho}_\ell : G \to G_\ell$ est la restriction à son image de la réduction modulo ℓ de l'application ρ_ℓ. Dans le cas où la dimension de U est supérieure à 2 on a besoin d'une condition supplémentaire de non-ramification sur $\Lambda = \Lambda_d$. On pose $\Lambda_1 = \mathcal{P} - \{p\}$ et pour $d \geq 2$, Λ_d est l'ensemble des premiers ℓ différents de p tels que $p \nmid |G_\ell|$.

Remarque 19. La condition que l'on impose ici sur Λ_d pour $d \geq 2$ est trop forte, on pourrait prendre un ensemble de premiers plus grand. En effet comme remarqué dans [Kow08b, Sect. 4], il suffit que les morphismes $\tilde{\rho}_\ell$ soient modérément ramifiés (on pourra voir l'énoncé de [Kow08b, Th. 4.1] pour plus de détails). Ces deux ensembles de premiers ont une densité positive donc ils donnent des majorations du même ordre à la constante près.

L'ensemble à cribler que l'on considère est $X = U(\mathbf{F}_p)$ qui est fini. On lui associe la mesure de comptage et l'application $u \mapsto \mathrm{Frob}_u$ qui donne bien un élément dans $G^\sharp$.

Dans le cas maximal — c'est-à-dire que l'image par $\tilde{\rho}_\ell$ du groupe fondamental étale géométrique $\pi_1^g(U, \overline{\eta})$ est le groupe symplectique $Sp(2g, \mathbf{F}_\ell)$ — Kowalski obtient des bornes pour la constante de grand crible associée à cette situation [Kow08a, Cor. 8.10].

Théorème 2.6 (Kowalski)**.** *Dans la situation de crible donnée plus haut, on suppose que le système $(\rho_\ell)_{\ell \in \Lambda}$ est linéairement indépendant (selon la définition 2.2). Pour tout $\ell \in \Lambda_d$ on se donne un sous-ensemble $\Omega_\ell \subset G_\ell$ stable par conjugaison. Alors pour tout L entier,*

$$|\{u \in U(\mathbf{F}_p) : \forall \ell \in \Lambda_d, \ell \leq L, \tilde{\rho}_\ell(\mathrm{Frob}_u) \notin \Omega_\ell\}| \leq (q^d + Cq^{d-1/2}(L+1)^A)H^{-1}$$

où l'on peut prendre

— $A = 2g^2 + g + 2$ *si* $d = 1$,

— $A = 6g^2 + 3g + 4$ *si* $d \geq 2$ *et que* $p \nmid |G_\ell|$ *pour tout* $\ell \in \Lambda_d$,

et

$$H := \sum_{m \in \mathcal{L}} \prod_{\ell | m} \frac{\nu_\ell(\Omega_\ell)}{\nu_\ell(Y_\ell - \Omega_\ell)},$$

le support de crible $\mathcal{L}$ est ici

$$\mathcal{L} = \{m \text{ sans facteur carré } : \ell \mid m \Rightarrow \ell \in \Lambda_d, \prod_{\ell | m}(\ell + 1) \leq L + 1\}.$$

La constante C ne dépend que de U.

Remarque 20. Ici le support de crible n'est pas seulement le support premier $\mathcal{L}^*$. On prend un ensemble de nombres sans facteurs carrés dont les diviseurs premiers sont dans $\mathcal{L}^*$. L'idée d'enlever les nombres sans facteurs carrés qui ont des petits facteurs premiers est due à Zywina, cela permet de gagner un facteur d'ordre une puissance de $\log \log L$.

2.1.3 Méthode de Bellaïche

En général dans le cadre du grand crible, seule la taille des ensembles cribants Ω_ℓ compte. L'idée de Bellaïche dans [Bel16] est de modifier légèrement le principe du grand crible pour prendre en compte la structure des ensembles Ω_ℓ notamment dans le cadre du crible pour Frobenius de la section 2.1.2.

Le résultat que nous allons présenter dans cette section est une légère amélioration dans un cadre général de [Bel16, Th. 14]. Il suppose qu'on connaît un bon terme d'erreur dans le théorème de Chebotarev généralisé associé à la situation. Nous avons déjà énoncé le théorème de Chebotarev dans le chapitre précédent (théorème 1.26), on appelle théorème de Chebotarev effectif un résultat qui donne une estimation du terme d'erreur obtenu dans le calcul de la densité. De tels résultats sont souvent conditionnels. L'article de Bellaïche se base notamment sur une version effective du théorème de Chebotarev due à Lagarias et Odlyzko [LO77, Th. 1.1] (voir aussi [Bel16, Th. 2]), ce résultat est conditionnel à l'hypothèse de Riemann généralisée et à la conjecture d'Artin. Dans ce résultat apparaît un invariant numérique qu'il nomme *complexité de Littlewood*.

Définition 2.7. Soit $E/\mathbf{Q}$ une extension finie galoisienne de degré d et de groupe de Galois $G := \mathrm{Gal}(E/\mathbf{Q})$. Soit M le produit des nombres premiers ramifiés dans E. On définit la *complexité de Littlewood* de f une fonction centrale sur G à valeurs complexes par

$$\lambda_G(f) = \sum_{\pi} \frac{1}{|G|} \left| \sum_{g \in G} \mathrm{tr}(f(g)\pi(g^{-1})) \right| \dim \pi$$

où la première somme est indexée par un ensemble de représentants des classes d'isomorphismes de représentations complexes irréductibles de G.

Pour $C \subset G$ un sous-ensemble stable par conjugaison, on note $\lambda_G(C) = \lambda_G(\mathbf{1}_C)$ la complexité de Littlewood de sa fonction indicatrice.

On peut alors énoncer le théorème de Chebotarev effectif [Bel16, Th. 1] (voir aussi [IK04, Sect. 5.13]).

Théorème 2.8 (Chebotarev effectif)**.** *Soit $E/\mathbf{Q}$ une extension finie galoisienne de groupe de Galois G. Soit M le produit des nombres premiers ramifiés dans E. Soit f une fonction centrale sur G à valeurs complexes et $\pi(x, f) := \sum_{p<x} f(\mathrm{Frob}_p)$. Supposons vraies l'hypothèse de Riemann généralisée et la conjecture d'Artin pour les fonctions L associées aux représentations irréductibles de G. Pour $x \geq 3$ on a*

$$|\pi(x, f) - \mu_G(f)\,\mathrm{Li}(x)| \ll \sqrt{x}\lambda_G(f)(\log x + \log M + \log|G|),$$

où la constante implicite est absolue et $\mu_G(f) = \frac{1}{|G|}\sum_{g\in G} f(g)$ est la valeur moyenne de f.

Remarque 21. Dans le cas où $f = \mathbf{1}_C$ la fonction indicatrice d'un ensemble stable par conjugaison, on a $\mu_G(f) = \frac{|C|}{|G|}$. On retrouve donc bien un énoncé classique du théorème de Chebotarev.

En utilisant une nouvelle version de grand crible et le théorème 2.8, Bellaïche montre le résultat suivant [Bel16, Th. 14].

Théorème 2.9 (Bellaïche)**.** *On se donne deux entiers, M et N. Soit Λ l'ensemble des nombres premiers ne divisant pas N, à chaque $\ell \in \Lambda$ on associe L_ℓ une extension galoisienne finie de $\mathbf{Q}$ non-ramifiée en dehors des nombres premiers divisant M. On note G_ℓ son groupe de Galois. On se donne également une famille $(D_\ell)_{\ell\in\Lambda}$ de sous-ensembles stables par conjugaison des G_ℓ. Pour $x > 0$, on note*

$$\pi(D, x) = |\{p \leq x : p \nmid M \text{ et } \forall \ell \in \Lambda, \mathrm{Frob}_{p,G_\ell} \in D_\ell\}|.$$

Supposons qu'il existe deux réels $0 < \alpha < 1$, $0 \leq \beta$, et des constantes $P, P', R > 0$ tels que

- *on a $\log |G_\ell| = O(\log \ell)$,*
- *pour tout $\ell \in \Lambda$, $P\ell^\alpha \leq \frac{|G_\ell|}{|D_\ell|} \leq P'\ell^\alpha$,*
- *pour tout $\ell \in \Lambda$, $\lambda_{G_\ell}(D_\ell) \leq R\ell^\beta$,*
- *pour tous $\ell \neq \ell'$ dans Λ, l'application naturelle $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to G_\ell \times G_{\ell'}$ est surjective.*

En supposant vraies l'hypothèse de Riemann généralisée et la conjecture d'Artin pour toutes les fonctions L d'Artin des représentations irréductibles des $(G_\ell)_{\ell\in\Lambda}$, on a

$$\pi(D, x) = O\left(x^{\frac{\alpha+4\beta+1}{2\alpha+4\beta+2}} (\log x)^{\frac{\alpha+1}{\alpha+2\beta+1}}\right).$$

Remarque 22. Le théorème 2.9 n'est pas exactement celui énoncé par Bellaïche. L'amélioration que l'on apporte est un gain dans l'exposant du logarithme. Elle est obtenue en choisissant comme support de crible le support premier au lieu de l'ensemble de tous les nombres sans facteur carré.

On va prouver le théorème 2.9 comme corollaire d'un résultat un peu plus général.

Théorème 2.10. *Soit X un ensemble fini muni d'une application $x \mapsto F_x$ vers un groupe Γ.*

On se donne une famille de représentations qui forme un système linéairement indépendant $\rho_\ell : \Gamma \to G_\ell$, $\ell \in \Lambda$ vers des groupes finis. On se donne également une famille $(D_\ell)_{\ell\in\Lambda}$ de sous-ensembles stables par conjugaison des G_ℓ, on veut majorer

$$\pi(X, D) = |\{x \in X : \forall \ell \in \Lambda, \rho_\ell(F_x) \in D_\ell\}|.$$

On suppose que pour chacune des représentations finies $\rho : \Gamma \to G$ avec $G = G_\ell$ ou $G = G_\ell \times G_{\ell'}$, on a un théorème de Chebotarev effectif : pour toute fonction f centrale sur G, on a

$$|\pi(X, f) - |X|\mu(f)| \leq CA(|X|)B(|G|)\lambda_G(f) \tag{2.1}$$

où $\pi(X, f) = \sum_{x\in X} f(\rho(F_x))$, $\mu(f)$ est la moyenne de f sur G et λ_G est une norme sur l'espace des fonctions centrales satisfaisant $\lambda_G(1) = 1$ et $\lambda_{G_1\times G_2}(f_1 \otimes f_2) = \lambda_{G_1}(f_1)\lambda_{G_2}(f_2)$. Supposons de plus que $A(T) \sim T^r(\log T)^s$ et $B(T) = O(T^t(\log T)^u)$ (avec $r < 1$, $t, u \geq 0$).

Supposons qu'il existe des réels $0 \leq \alpha, \alpha', \beta, \delta$, et des constantes $M, P, P', R > 0$ (avec $P > 1$ si $\alpha = 0$) tels que

- *on a pour tout $\ell \in \Lambda$, $|G_\ell| \leq M\ell^\delta$,*
- *pour tout $\ell \in \Lambda$, $P\ell^\alpha \leq \frac{|G_\ell|}{|D_\ell|} \leq P'\ell^{\alpha'}$,*
- *pour tout $\ell \in \Lambda$, $\lambda_{G_\ell}(D_\ell) \leq R\ell^\beta$.*

Alors

$$\pi(X, D) = O\left(|X|^{1-\frac{(\alpha+1)(1-r)}{\alpha'+2\beta+2t\delta+1}} (\log |X|)^{\frac{\alpha'-\alpha+(\alpha+1)(s+u)+2(\beta+t\delta)}{\alpha'+2\beta+2t\delta+1}}\right).$$

Remarque 23.

1. Dans les applications, Γ sera souvent un groupe de Galois d'extension séparable d'un corps de nombre ou du type $\pi_1(U, \overline{\eta})$ pour U une variété algébrique, alors l'application $x \mapsto F_x$ sera l'application Frobenius.
2. Pour Bellaïche [Bel16], λ_G est la complexité de Littlewood vue à la définition 2.7. Cependant la preuve fonctionne avec n'importe quelle norme satisfaisant les hypothèses citées.

Démonstration. On se place dans le même cadre que dans l'article [Bel16], et on utilise les notations de [Kow08a, § 2.1] (voir aussi l'introduction de cette section). Pour tout $\ell \in \Lambda$ on a une application $X \to G_\ell$ qui à un élément x associe $\rho_\ell(F_x)$. Prenons $Y_\ell = \{0,1\}$, alors on a pour tout ℓ une application surjective π_ℓ de X dans Y_ℓ donnée par $x \mapsto \mathbf{1}_{D_\ell}(\rho_\ell(F_x))$. On munit Y_ℓ d'une mesure de probabilité, $\mu_\ell(\{0\}) = \frac{|G_\ell|-|D_\ell|}{|G_\ell|}$, $\mu_\ell(\{1\}) = \frac{|D_\ell|}{|G_\ell|}$.

On prend pour $\mathcal{L}^*$ un sous-ensemble fini de Λ, $\mathcal{L}^* \subset \Lambda \cap [0,Q]$ que l'on optimisera plus tard. Pour $\ell \in \Lambda$, $\Omega_\ell = \{0\} \subset Y_\ell$.

Alors l'ensemble criblé est

$$S(X,\Omega,\mathcal{L}^*) = \{x \in X : \forall \ell \in \mathcal{L}^*, \rho_\ell(F_x) \in D_\ell\}.$$

En particulier, $\pi(X,D) \leq |S(X,\Omega,\mathcal{L}^*)|$.

Pour $\ell \in \Lambda$, soit ϕ_ℓ la fonction de $L^2(Y_\ell,\mu_\ell,\mathbf{C})$ positive en 1, qui complète $\{\mathbf{1}\}$ en une base orthonormée. On a $\phi_\ell(1) = \sqrt{\frac{|G_\ell|-|D_\ell|}{|D_\ell|}}$, $\phi_\ell(0) = -\sqrt{\frac{|D_\ell|}{|G_\ell|-|D_\ell|}}$. Selon les notations de l'introduction, $B_\ell^* = \{\phi_\ell\}$, et on a d'après les théorèmes 2.1 et 2.3

$$|S(X,\Omega,\mathcal{L}^*)| \leq \Delta H^{-1}$$

où $\Delta \leq \max_{\ell\in\mathcal{L}^*} \sum_{\ell'\in\mathcal{L}^*} |W(\phi_\ell,\phi_{\ell'})|$ et $H = \sum_{\ell\in\mathcal{L}^*} \frac{\mu_\ell(\Omega_\ell)}{\mu_\ell(Y_\ell-\Omega_\ell)}$.

On veut majorer $\max_{\ell\in\mathcal{L}^*} \sum_{\ell'\in\mathcal{L}^*} |W(\phi_\ell,\phi_{\ell'})|$ où pour $\ell,\ell' \in \mathcal{L}^*$,

$$\begin{aligned} W(\phi_\ell,\phi_{\ell'}) &= \sum_{x\in X} \phi_\ell(\pi_\ell(x))\overline{\phi_{\ell'}(\pi_{\ell'}(x))} \\ &= \sum_{x\in X} \phi_\ell(\mathbf{1}_{D_\ell}(\rho_\ell(F_x)))\phi_{\ell'}(\mathbf{1}_{D_{\ell'}}(\rho_{\ell'}(F_x))) \end{aligned}$$

(les ϕ_ℓ étant à valeurs réelles). Donc $W(\phi_\ell,\phi_{\ell'}) = \pi(X, f_{\ell,\ell'})$ suivant les notations du théorème 2.10, où $f_{\ell,\ell'} = \phi_\ell \circ \mathbf{1}_{D_\ell} \otimes \phi_{\ell'} \circ \mathbf{1}_{D_{\ell'}}$ sur $G_\ell \times G_{\ell'}$ si $\ell \neq \ell'$, et $f_{\ell,\ell} = \phi_\ell^2 \circ \mathbf{1}_{D_\ell}$ sur G_ℓ. Dans les deux cas, $f_{\ell,\ell'}$ est une fonction centrale, donc par le théorème de Chebotarev effectif de l'hypothèse (2.1),

$$|W(\phi_\ell,\phi_{\ell'}) - \mu(f_{\ell,\ell'})|X|| \leq CA(|X|)B(|G_{\ell,\ell'}|)\lambda(f_{\ell,\ell'}).$$

On a par définition de $\phi_\ell, \phi_{\ell'}$,

$$\begin{aligned} \mu(f_{\ell,\ell'}) &= 0, \text{ si } \ell \neq \ell' \\ \mu(f_{\ell,\ell}) &= 1. \end{aligned}$$

Par inégalité triangulaire,

$$\lambda(\phi_\ell^2 \circ \mathbf{1}_{D_\ell}) \leq \frac{|G_\ell|-|D_\ell|}{|D_\ell|}\lambda(D_\ell) + \frac{|D_\ell|}{|G_\ell|-|D_\ell|}\lambda(G_\ell - D_\ell).$$

Comme par inégalité triangulaire $\lambda(G_\ell - D_\ell) \leq \lambda(D_\ell) + 1 \leq cR\ell^\beta$, pour c assez grand, D_ℓ étant non vide, en utilisant les majorations et minorations des hypothèses, on obtient

$$\begin{aligned} \lambda(\phi_\ell^2 \circ \mathbf{1}_{D_\ell}) &\leq \left(P'\ell^{\alpha'} - 1 + \frac{c}{P\ell^\alpha - 1}\right) R\ell^\beta \\ &\leq P'R\ell^{\alpha'+\beta} \end{aligned}$$

pour ℓ suffisamment grand (comme $\alpha > 0$, on remarque que si $\alpha = 0$ et $P > 1$ alors on a une majoration du même type quitte à faire croître la constante).

De la même façon,

$$\begin{aligned}\lambda(\phi_\ell \circ \mathbf{1}_{D_\ell}) &\leq \sqrt{\frac{|G_\ell|-|D_\ell|}{|D_\ell|}}\lambda(D_\ell) + \sqrt{\frac{|D_\ell|}{|G_\ell|-|D_\ell|}}\lambda(G_\ell - D_\ell)\\ &\leq \sqrt{\frac{|G_\ell|}{|D_\ell|} + 2c - 1 + \frac{c^2}{\frac{|G_\ell|}{|D_\ell|}-1}}R\ell^\beta\\ &\leq \sqrt{P'\ell^{\alpha'} + 2c - 1 + \frac{c^2}{P\ell^\alpha - 1}}R\ell^\beta\\ &\leq R\sqrt{P'+2c}\ell^{\frac{\alpha'}{2}+\beta}.\end{aligned}$$

pour ℓ suffisamment grand (comme précédemment, si $\alpha > 0$ c'est immédiat, si $\alpha = 0$ et $P > 1$ on a un résultat similaire quitte à changer la constante).

Comme par hypothèse sur λ, $\lambda(\phi_\ell \circ \mathbf{1}_{D_\ell} \otimes \phi_{\ell'} \circ \mathbf{1}_{D_{\ell'}}) = \lambda(\phi_\ell \circ \mathbf{1}_{D_\ell})\lambda(\phi_{\ell'} \circ \mathbf{1}_{D_{\ell'}})$, on a une majoration de tous les termes apparaissant dans Δ à condition de prendre pour $\mathcal{L}^*$ un sous-ensemble de Λ du type $\Lambda \cap [N, Q]$, pour N suffisamment grand fixé.

On a par le lemme 2.4,

$$\begin{aligned}\Delta &\leq \max_{\ell\in\mathcal{L}^*}\left\{|X| + CA(|X|)\left(B(|G_\ell|)P'R\ell^{\alpha'+\beta} + \sum_{\ell'\neq\ell} R^2(P'+4)\ell'^{\frac{\alpha'}{2}+\beta}B(|G_{\ell,\ell'}|)\ell^{\frac{\alpha'}{2}+\beta}\right)\right\}\\ &\leq |X| + C'Q^{\alpha'+2\beta+2t\delta+1}(\log Q)^{u-1}A(|X|)\end{aligned}$$

On veut minorer $H = \sum_{\ell\in\mathcal{L}^*}\frac{|G_\ell|-|D_\ell|}{|D_\ell|}$, c'est-à-dire $\sum_{\ell\in\mathcal{L}^*}\left(\frac{|G_\ell|}{|D_\ell|} - 1\right)$. Par hypothèse,

$$\begin{aligned}H &\geq \sum_{\ell\in\mathcal{L}^*}(P\ell^\alpha - 1)\\ &\geq \frac{P}{2}\sum_{N\leq\ell\leq Q}\ell^\alpha\\ &\geq C_2\frac{Q^{\alpha+1}}{\log Q},\end{aligned}$$

en utilisant le lemme 2.4. A nouveau si $\alpha = 0$ et $P > 1$, la minoration reste du même type. Donc $H^{-1} \leq \frac{1}{C_2}Q^{-\alpha-1}\log Q$.

On a finalement,

$$\pi(X, D) \leq \Delta H^{-1} \leq (|X| + C'Q^{\alpha'+2\beta+2t\delta+1}A(|X|)(\log Q)^{u-1})\frac{1}{C_2}Q^{-\alpha-1}\log Q,$$

donc

$$\pi(X, D) \leq C_3|X|Q^{-\alpha-1}\log Q + C_4|X|^r(\log|X|)^sQ^{\alpha'-\alpha+2(\beta+t\delta)}(\log Q)^u.$$

On cherche Q sous la forme $|X|^a(\log|X|)^b$ pour que les deux termes soient de même ordre, sachant que si on trouve $a > 0$ alors $\log Q$ sera du même ordre que $\log|X|$.

$$\begin{aligned}1 - (1+\alpha)a &= r + (\alpha' - \alpha + 2(\beta + t\delta))a\\ \Leftrightarrow a &= \frac{1-r}{\alpha' + 2\beta + 2t\delta + 1}\end{aligned}$$

comme $r < 1$, $a > 0$. On a alors une équation pour b :

$$\begin{aligned}1 - (1+\alpha)b &= s + u + (\alpha' - \alpha + 2(\beta + t\delta))b\\ \Leftrightarrow b &= \frac{1-s-u}{\alpha' + 2\beta + 2t\delta + 1}.\end{aligned}$$

On pose donc

$$Q = |X|^{\frac{1-r}{\alpha'+2\beta+2t\delta+1}} (\log |X|)^{\frac{1-s-u}{\alpha'+2\beta+2t\delta+1}}, \tag{2.2}$$

Q croît vers l'infini avec $|X|$ donc peut-être supérieur à N pour $|X|$ assez grand. On obtient alors pour $|X|$ assez grand,

$$\pi(X, D) \leq C_5 |X|^{\frac{\alpha'-\alpha+r\alpha+2\beta+2t\delta+r}{\alpha'+2\beta+2t\delta+1}} \log(|X|)^{\frac{(\alpha+1)(s+u)+\alpha'-\alpha+2(\beta+t\delta)}{\alpha'+2\beta+2t\delta+1}}.$$

□

Remarque 24.

1. Contrairement au résultat de la sous-section 2.1.2, il est ici évident de calculer la taille des $\Omega_p = \{0\}$. Cependant la constante de grand crible Δ est plus compliquée à évaluer, elle prend compte de la structure des ensembles criblants, ce qui n'est pas le cas dans le grand crible usuel. Ainsi, avec une bonne connaissance des groupes impliqués et pour de bons ensembles criblants, on peut imaginer obtenir de meilleures majorations par cette méthode que par la méthode usuelle.
2. Par équivalence des normes sur les espaces de dimension finie, $\lambda_G(D) \leq C_G \|\mathbf{1}_D\|_2 = C_G\sqrt{|D|}$. Cette majoration donne en général des résultats moins bons que ceux connus, mais si on a une estimation de C_{G_ℓ} qui tend vers 0 quand ℓ tend vers l'infini, le résultat devient plus intéressant.
3. On peut avoir $\alpha' \neq \alpha$ mais il faut tout de même maîtriser α' car si on le laisse être arbitrairement grand, la borne obtenue sur $\pi(X, D)$ est triviale. Il faut donc savoir minorer les tailles des ensembles D_ℓ. On n'a pas besoin d'une telle minoration dans le cadre du grand crible usuel, c'est une difficulté supplémentaire.

On déduit du théorème 2.10 la preuve du théorème 2.9.

Démonstration du théorème 2.9. On utilise de le théorème de Chebotarev effectif 2.8 et le théorème 2.10, avec $X = \{p < x : p \nmid M\}$ de cardinal de l'ordre de $\mathrm{Li}(x)$, on a

$$A(|X|) = \sqrt{x}\log x \sim \sqrt{\mathrm{Li}(x)}(\log \mathrm{Li}(x))^{\frac{3}{2}}$$

donc $r = \frac{1}{2}$, $s = \frac{3}{2}$, et $B(|G|) = 1$ car $\log |G| = O(\log x)$. Les propriétés demandées pour λ sont prouvées dans [Bel16, Part. 2]. □

2.1.4 « Plus grand crible », méthode de Gallagher

Dans le cadre d'un sous-ensemble de $\mathbf{Z}^d$, Nous utiliserons une autre méthode de grand crible basée sur le « plus grand crible » (larger sieve) de Gallagher tel que généralisé par Zywina [Zyw10, Sec. 3]. Ce résultat est déjà utilisé dans le cadre du double crible [EEHK09, Prop. 17].

On redonne ici la preuve dans un cadre un peu plus général que nécessaire. En particulier on donne le résultat [Zyw10, Th. 3.1] dans le cas où on veut étudier la taille d'une partie finie de K^d où K est un corps de nombres. On verra cependant que le cas $d \geq 2$ ne permet pas d'obtenir des résultats très satisfaisants dans notre situation.

Définition 2.11. Soit K un corps de nombres. Soit M_K l'ensemble des places de K. Pour $v \in M_k$, on note $|\cdot|_v$ la valeur absolue associée à v, et on note $n_v = [K_v : \mathbf{Q}_v]$ le degré local en v. Pour $a = (a_1, \ldots, a_d) \in K^d$ on définit la hauteur de a par

$$h_d(a) = \max_{1\leq i\leq d} \prod_{v\in M_K} \max(1, |a_i|_v^{n_v}).$$

Définition 2.12. Soit K un corps de nombres. Soit $\mathfrak{p}$ un idéal premier de l'anneau des entiers $\mathbf{Z}_K$, on note $\mathbf{F}_\mathfrak{p}$ le corps résiduel en $\mathfrak{p}$. On définit une application naturelle de réduction modulo $\mathfrak{p}$, $\pi_\mathfrak{p} : K^d \to \mathbb{P}^d(\mathbf{F}_\mathfrak{p})$ par :

— si $a = (a_1, \dots, a_d)$, avec $v_\mathfrak{p}(a_i) \geq 0$ pour tout i, on pose $\pi_\mathfrak{p}(a) = [a_1 \pmod{\mathfrak{p}} : \dots : a_d \pmod{\mathfrak{p}} : 1]$.

— sinon, il existe une représentation $(\tilde{a}_1, \dots, \tilde{a}_d, \tilde{a}_{d+1})$ de l'élément $[a_1 : \dots : a_d : 1] \in \mathbb{P}^d(K)$, avec $v_\mathfrak{p}(\tilde{a}_i) \geq 0$ pour tout i, et pour au moins un i, on a $v_\mathfrak{p}(\tilde{a}_i) = 0$. On pose alors $\pi_\mathfrak{p}(a) = [\tilde{a}_1 \pmod{\mathfrak{p}} : \dots : \tilde{a}_d \pmod{\mathfrak{p}} : \tilde{a}_{d+1} \pmod{\mathfrak{p}}]$.

Théorème 2.13 (Zywina)**.** *Soit $K/\mathbf{Q}$ un corps de nombres, soit $d > 0$ un entier, soit $T > 0$ une constante et soit $\mathcal{A}$ un ensemble fini d'éléments de K^d tel que $h_d(a) \leq T$ pour tout $a \in \mathcal{A}$. Soit S un ensemble fini d'idéaux premiers dans $\mathbf{Z}_K$. Supposons que la taille de l'image de $\mathcal{A}$ par l'application de réduction $\pi_\mathfrak{p} : K \to \mathbb{P}^d(\mathbf{F}_\mathfrak{p})$ est $\leq \nu(\mathfrak{p})$ pour tout $\mathfrak{p} \in S$. Alors on a*

$$|\mathcal{A}| \leq \frac{\sum_{\mathfrak{p}\in S} \log(N\mathfrak{p}) - \log(2^{[K:\mathbf{Q}]}T^2)}{\sum_{\mathfrak{p}\in S} \frac{\log(N\mathfrak{p})}{\nu(\mathfrak{p})} - \log(2^{[K:\mathbf{Q}]}T^2)}$$

si le dénominateur de cette expression est positif, dans le cas contraire l'inégalité est dans l'autre sens.

Démonstration. On pose $\Delta = \prod_{a\neq b\in\mathcal{A}} h(a-b)$, c'est un nombre réel supérieur ou égal à 1.

Pour tout $a \neq b$, on a $h(a-b) \leq 2^{[K:\mathbf{Q}]}h(a)h(b)$ donc

$$\Delta \leq (2^{[K:\mathbf{Q}]}T^2)^{|\mathcal{A}|(|\mathcal{A}|-1)}. \tag{2.3}$$

On peut aussi minorer Δ : on a $\Delta = \prod_{a\neq b\in\mathcal{A}} h((a-b)^{-1})$ (où les opérations se font coefficient par coefficient). D'où

$$\Delta \geq \prod_{a\neq b\in\mathcal{A}} \prod_{\mathfrak{p}\in S} (N\mathfrak{p})^{\min_i v_\mathfrak{p}(a_i-b_i)}.$$

On peut restreindre le produit intérieur aux $\mathfrak{p}$ tels que $\min_i v_\mathfrak{p}(a_i - b_i) > 0$, c'est à dire que $a \equiv b \pmod{\mathfrak{p}}$. Ainsi

$$\begin{aligned}\log(\Delta) &\geq \sum_{a\neq b\in\mathcal{A},} \sum_{\substack{\mathfrak{p}\in S \\ a\equiv b \pmod{\mathfrak{p}}}} \log(N\mathfrak{p}) \\ &\geq \sum_{\mathfrak{p}\in S,\, a\equiv b \pmod{\mathfrak{p}}} \log(N\mathfrak{p}) - |\mathcal{A}| \sum_{\mathfrak{p}\in S} \log(N\mathfrak{p}).\end{aligned} \tag{2.4}$$

Or $\sum_{a\equiv b \pmod{\mathfrak{p}}} 1 \geq \frac{|\mathcal{A}|^2}{\nu(\mathfrak{p})}$ d'après l'inégalité de Cauchy–Schwarz. Finalement en réunissant (2.3) et (2.4) on a obtenu

$$\sum_{\mathfrak{p}\in S} \log(N\mathfrak{p}) \left(\frac{|\mathcal{A}|^2}{\nu(\mathfrak{p})} - |\mathcal{A}| \right) \leq \log(\Delta) \leq |\mathcal{A}|(|\mathcal{A}|-1)\log(2^{[K:\mathbf{Q}]}T^2).$$

Il suffit alors de diviser par $|\mathcal{A}|$ et de réorganiser les termes pour avoir le résultat annoncé. □

Remarque 25. On remarque que ce crible donne de bons résultats quand $\nu(\mathfrak{p})$ est petit par rapport à $\log N\mathfrak{p}$, c'est-à-dire que la proportion $\frac{|\Omega_\mathfrak{p}|}{|Y_\mathfrak{p}|}$ doit être très proche de 1. Dans le cadre du grand crible classique, on a juste besoin que cette proportion soit positive et bornée inférieurement par une constante, c'est la raison pour laquelle on appelle cette méthode le *plus grand crible*.

2.2 Applications : majorer le plus petit premier dans un ensemble frobenien

Dans cette section on utilise les méthodes de cribles énoncées à la section précédentes pour répondre à notre question : majorer pour la plupart des courbes C hyperelliptiques dans une certaine famille le plus petit premier dans l'ensemble $\{p : p \nmid \prod_{i=1}^{n}(N_C(p) - a_i)\}$.

On va pour cela utiliser des familles à un ou plusieurs paramètres de courbes hyperelliptiques. Suivant l'idée de [Kow08a], quand on réduit ces familles modulo des nombres premiers p, on peut majorer la taille de l'image de l'ensemble des « mauvais » paramètres modulo p grâce à un crible pour les classes de conjugaison de Frobenius tel que présenté dans la sous-section 2.1.2. Alors suivant une idée de [EEHK09], on peut utiliser cette majoration pour borner la taille de l'ensemble des « mauvais » paramètres grâce à un second crible.

Le plus grand crible tel que présenté dans la sous-section 2.1.4 donne une majoration très forte dans le cas où l'espace des paramètres est de dimension 1, cependant il ne donne rien dans les cas de dimension supérieures. On utilise alors soit le crible pour la mesure de comptage (comme vu à la sous-section 2.1.1) soit une adaptation du crible de Bellaïche (comme vu à la sous-section 2.1.3). On verra que ces deux techniques donnent des résultats comparables.

2.2.1 Mise en place du problème

Fixons un ensemble de paramètres $U \subset \mathbf{Z}^d$, on veut étudier une famille de courbes paramétrée par U. Plus précisément, soit U un ouvert de $\mathbb{A}^d_{\mathbf{Z}}$. On se donne une famille de courbes sur U, c'est-à-dire un morphisme $\mathcal{C} \to U$ dont toutes les fibres sont des courbes sur $\mathbf{Z}$, on va rajouter l'hypothèse qu'elles sont toutes projectives lisses sur $\mathbf{Q}$ de genre fixé g.

Prenons un nombre premier p, notre famille de courbes $\mathcal{C}$ sur $\mathbf{Z}$, se réduit modulo p en une famille de courbes $\mathcal{C}_p \to U_p$ sur $\mathbf{F}_p$ via le changement de base $\mathbf{Z} \to \mathbf{F}_p$. Modulo chaque premier p on est donc dans la situation de la sous-section 2.1.2. En particulier, pour chaque premier p on peut considérer la situation de crible pour les classes de conjugaison du Frobenius déduite de l'action ρ_ℓ de Frob_u sur $H^1_c(C_u, \ell)$. Pour tout $u \in U$, on peut considérer sa réduction modulo p coefficients par coefficients, alors si $C_u/\mathbf{F}_p$ est lisse, on a

$$a(C_u, p) := p + 1 - N_{C_u}(p) = \mathrm{tr}(\rho_\ell(\mathrm{Frob}_u)).$$

On dit que p est un premier ordinaire pour la courbe C_u, ou que la courbe $C_u/\mathbf{F}_p$ est ordinaire, si $a(C_u, p) \neq 0$.

L'idée de cette partie est d'évaluer la taille de l'ensemble des paramètres $u \in U$ pour lesquels la courbe C_u a un plus petit premier ordinaire anormalement grand. On étudiera pour cela la réduction modulo p de l'ensemble des paramètres $u \in U$, pour voir que modulo un premier p fixé, l'ensemble des $u \in U(\mathbf{F}_p)$ pour lesquels C_u n'est pas ordinaire est assez petit. Alors par une méthode de crible on en déduira un majorant pour la taille de l'ensemble de ces paramètres. Plus généralement, dans cette section on s'intéresse à des ensembles du type

$$S(U, T, Q, \underline{a}) = \{u \in U : \|u\| \leq T, \forall p \leq Q, p \mid \prod_{i=1}^{n}(N_{C_u}(p) - a_i)\} \tag{2.5}$$

pour un n-uplet d'entiers $\underline{a} = (a_1, \ldots, a_n)$, où $\|.\|$ est la norme infinie sur $\mathbf{Z}^d$. On veut minimiser la valeur de Q tout en garantissant que cet ensemble est un ensemble d'exceptions (de taille petite par rapport à T^d). Ainsi on pourra conclure que pour la plupart des courbes dans la famille, le plus petit premier de l'ensemble $\{p : p \nmid \prod_{i=1}^{n}(N_C(p) - a_i)\}$ est inférieur à Q.

En utilisant la réduction modulo p, on peut écrire l'ensemble (2.5) sous la forme

$$S(U,T,Q,\underline{a}) = \{u \in U : \|u\| \leq T, \forall p \leq Q, \pi_p(u) \in D_p(\underline{a})\},$$

où π_p est la réduction modulo p coefficients par coefficients et

$$D_p(\underline{a}) := \{u \in U_p(\mathbf{F}_p) : a(C_u,p) \in \{1-a_1,\dots,1-a_n\}\}.$$

Dans la sous-section 2.2.2, sous une hypothèse de grande monodromie, on va estimer la taille des ensembles $D_p(\underline{a})$ grâce à la technique de grand crible pour les classes de conjugaison de Frobenius présentée à la sous-section 2.1.2. Cela fait on pourra utiliser diverses méthodes de grand crible ou de plus grand crible pour trouver une majoration de la taille des ensembles $S(U,T,Q,\underline{a})$. C'est le point des sous-sections 2.2.3, 2.2.4 et 2.2.5.

Donnons d'abord deux exemples de situations auxquelles on imagine pouvoir appliquer un tel résultat.

Exemple 5. Soit $g \geq 2$ un entier et soit $f \in \mathbf{Z}[T]$ un polynôme séparable de degré $2g$ on considère les courbes de modèle affine

$$C_u : y^2 = f(t)(t-u)$$

où $u \in \mathbf{Z}$.

Si le polynôme $f(t)(t-u)$ est séparable, la courbe $C_u/\mathbf{Q}$ est une courbe affine hyperelliptique. On note $\widetilde{C_u}$ la courbe projective lisse dont les points en dehors de l'infini sont donnés par le modèle ci-dessus. La réduction de $\widetilde{C_u}$ en un premier p qui ne divise pas son discriminant est une courbe hyperelliptique sur $\mathbf{F}_p$. On a

$$N_{\widetilde{C_u}}(p) = p - a(C_u,p) + 1$$

ou comme $\deg(f(t)(t-u))$ est impair, la courbe n'a qu'un point à l'infini donc

$$N_{C_u}(p) = p - a(C_u,p).$$

On déduit que pour $p \geq 4g^2$ premier de bonne réduction, $p \nmid N_{C_u}(p)$ si $a(C_u,p) \neq 0$.

Dans ce cas, U est l'ensemble des paramètres u tels que $f(t)(t-u)$ est séparable. Notre famille de courbes $\mathcal{C} \to U$ a pour fibre au dessus de u la courbe $\widetilde{C_u}$. Un théorème de Yu (voir par exemple [Kow08a, Prop. 8.13]) assure que l'image par ρ_ℓ du groupe fondamental étale géométrique $\pi_1^g(U_p)$ est le groupe symplectique $Sp(2g,\mathbf{F}_\ell)$: on est dans le cas maximal de la sous-section 2.1.2.

Par application des résultats de la sous-section 2.2.3, on obtient le résultat suivant (voir aussi [Dev17, Th. 1.3]).

Proposition 2.14. *On se place dans la situation évoquée dans l'exemple 5, en particulier la famille de courbes est*

$$C_u : y^2 = f(t)(t-u)$$

où $u \in \mathbf{Z}$ et f est un polynôme séparable de degré $2g$. Alors

$$\frac{1}{T}|\{u \in \mathbf{Z} : |u| \leq T, p \mid \prod_{i=1}^{n}(N_{C_u}(p)-a_i), \forall p < Q_{g,1}(T) \text{ de bonne réduction }\}| \ll \frac{Q_{g,1}(T)}{T\log T}$$

avec $Q_{g,1}(T) = (2K_g\gamma\log T)^{\gamma/2}\left(\log(2K_g\gamma\log T)\right)^{\frac{\gamma}{2}(1-\frac{2}{\gamma+2n-2})}$ pour une constante K_g ne dépendant que de g et $\gamma = 4g^2+2g+4$.

Exemple 6. On peut aussi regarder la famille de courbes hyperelliptiques $C_f : y^2 = f(x)$ pour f parcourant l'ensemble des polynômes unitaires séparables de degré $2g+1 > 1$ dans $\mathbf{Z}[X]$.

Dans ce cas U est un sous-schéma ouvert de $\mathbb{A}^{2g+1}_{\mathbf{Z}}$. La famille $\mathcal{C} \to U$ a pour fibre au dessus de f le modèle projectif lisse de C_f, elle contient la famille de l'exemple 5 donc le théorème de Yu s'applique encore. En utilisant les résultats de la sous-section 2.2.4 on obtient le résultat suivant.

Proposition 2.15. *On se place dans la situation de l'exemple 6, la famille de courbes qu'on étudie est indexée par les polynômes unitaires séparables de degré* $2g+1$, $f(x) = x^{2g+1} + u_{2g}x^{2g} + \ldots + u_1 x + u_0$. *Alors*

$$\frac{1}{T^{2g+1}}|\{u \in \mathbf{Z}^{2g+1} : \|u\| \leq T, p \mid \prod_{i=1}^{n}(N_{C_u}(p) - a_i), \forall p < Q'_{g,2g+1}(T) \text{ de bonne réduction }\}| \ll T^{-\frac{2g+1}{6g+1}(1+\frac{1}{6g^2+3g+4})}(\log T)^2$$

avec $Q'_{g,2g+1}(T) = T^{\frac{2g+1}{6g+1}}$.

Remarque 26. Yu n'a pas publié la preuve de son théorème. Cependant on peut trouver une preuve par Hall dans [Hal08].

2.2.2 Majoration de la taille des ensembles $D_p(\underline{a})$ grâce au crible pour les Frobenius

On va utiliser le résultat de la sous-section 2.1.2 pour estimer la taille de l'ensemble

$$D_p(\underline{a}) := \cup_{i=1}^{n}\{u \in U_p, a(C_u, p) = a_i\}. \tag{2.6}$$

On va prouver le résultat suivant.

Proposition 2.16. *Soit* p *un nombre premier. On se place dans la situation décrite dans la sous-section 2.1.2. On suppose que pour tout* $\ell \in \Lambda_d$ *l'image par* $\tilde{\rho}_\ell$ *du groupe fondamental étale géométrique* $\pi_1^g(U, \overline{\eta})$ *est le groupe symplectique* $Sp(2g, \mathbf{F}_\ell)$. *Soit* $D_p(\underline{a})$ *défini comme en (2.6), alors*

1. *si* $d = 1$, *on a*
$$|D_p(\underline{a})| \ll p^{1-2/\gamma}(\log p)^{1-2/(\gamma+2n-2)},$$
où $\gamma = 4g^2 + 2g + 4$ *et la constante implicite ne dépend que de* g.
2. *si* $d \geq 2$, *et* $p > 2g+1$, *on a*
$$|D_p(\underline{a})| \ll \frac{\phi(p)}{\phi(p) - r(g,p)} p^{d-1/(6g^2+3g+4)} \log p,$$
où $r(g,p)$ *est le nombre de racines de l'unité modulo* p *d'ordre inférieur ou égal à* g, $\phi(p) = p-1$ *est le nombre de classes inversibles modulo* p *et la constante implicite ne dépend que de* g *et de* n.

Démonstration. Par une variante du lemme de Goursat [Cha97, Prop. 5.1] (voir aussi [Kow08a, Lem. 8.12]), dans le cas maximal le système (ρ_ℓ) est linéairement indépendant. Ainsi d'après le théorème 2.6, il existe une constante $C \geq 0$ telle que

$$|D_p| \leq (p^d + Cp^{d-\frac{1}{2}}(L+1)^A)H^{-1}, \tag{2.7}$$

avec

1. $A = 2g^2 + g + 2$ si $d = 1$,
2. $A = 6g^2 + 3g + 4$ si $d \geq 2$ et $p \nmid |G_\ell|$ pour tout $\ell \in \Lambda_d$,

ici

$$H = \sum_{m \in \mathcal{L}_d} \prod_{\ell | m} \frac{|\Omega_\ell|}{|Sp_{2g}(\mathbf{F}_\ell)| - |\Omega_\ell|}$$

et $\mathcal{L}_d$ est l'ensemble des nombres m sans facteur carré à facteurs premiers dans l'ensemble Λ_d vérifiant $\prod_{\ell|m}(\ell+1) \leq L+1$. On optimisera le paramètre L plus tard.

1. Dans le cas $d = 1$, l'ensemble Λ_1 est l'ensemble de tous les premiers différents de p.
2. Si $d \geq 2$, comme on l'a déjà vu, on ajoute l'hypothèse $p \nmid |G_\ell|$ pour chaque $\ell \in \Lambda_d$. Le groupe $G_\ell \subset CSp(2g, \mathbf{F}_\ell)$ est un sous-groupe de $GL(2g, \mathbf{F}_\ell)$ donc son ordre divise $\ell^{g(2g-1)} \prod_{k=1}^{2g}(\ell^k - 1)$. Il suffit donc que p ne divise pas $\prod_{k=1}^{2g}(\ell^k - 1)$ pour que p ne divise pas $|G_\ell|$. Donc il suffit que $\ell \neq p$ ne soit pas une racine de l'unité modulo p d'ordre plus petit que $2g$. Cette condition est possible si $p > 2g+1$, on prend alors $\Lambda_{\geq 2} = \{\ell \neq p, \prod_{k=1}^{2g}(\ell^k - 1) \neq 0 \pmod p\}$, on exclut un nombre borné $r(g,p)$ de classes modulo p.

On veut minorer H. Dans notre situation, on a

$$\Omega_\ell = \cap_{i=1}^n \{g \in GSp_{2g}(\mathbf{F}_\ell), m(g) = p, \mathrm{tr}(g) \neq a_i\}.$$

Écrivons la condition sur les traces à l'aide d'un polynôme caractéristique :

$$|\Omega_\ell| = \sum_{f \in \mathbf{F}_\ell[T], f'(0) \neq a_1, \ldots, a_n} |\{g \in GSp_{2g}(\mathbf{F}_\ell), m(g) = p, \det(T - g) = f\}|.$$

On trouve dans [Kow08a, Lem. B.5] une minoration du nombre de matrices à polynôme caractéristique donné, cela permet de déduire que le cardinal de l'ensemble Ω_ℓ est supérieur à la quantité

$$|\cap_{i=1}^n \{f \in \mathbf{F}_\ell[T], p\text{-symplectique de degré } 2g, f'(0) \neq a_i\}| \frac{|Sp_{2g}(\mathbf{F}_\ell)|}{\ell^g} \left(\frac{\ell}{\ell+1}\right)^{2g^2+g+1}.$$

On rappelle qu'un polynôme f de degré $2g$ est dit p-symplectique si c'est un polynôme unitaire vérifiant $T^{2g} f(\frac{p}{T}) = p^g f(T)$. On dénombre les polynômes symplectiques avec le second coefficient évitant au plus n valeurs :

$$\frac{|\Omega_\ell|}{|Sp_{2g}(\mathbf{F}_\ell)|} \geq \delta(\ell) := \frac{\ell - n}{\ell} \left(\frac{\ell}{\ell+1}\right)^{2g^2+g+1} = 1 - \frac{2g^2 + g + 1 + n}{\ell} + O_g\left(\frac{1}{\ell^2}\right).$$

Comme la fonction $x \mapsto \frac{x}{1-x}$ est croissante, on en déduit que

$$\frac{|\Omega_\ell|}{|Sp_{2g}(\mathbf{F}_\ell)| - |\Omega_\ell|} \geq \frac{\delta(\ell)}{1 - \delta(\ell)}.$$

1. Dans le cas $d = 1$, l'ensemble Λ_1 recouvre presque tous les premiers. On suit le même raisonnement que pour la preuve de [Kow08a, Th. 8.15] : on applique le théorème de Lau–Wu ([LW02], voir aussi [Kow08a, Th. G.2]). Posons pour m dans $\mathcal{L}_1$, $f(m) := \frac{1}{m} \prod_{\ell|m} \frac{\delta(\ell)}{1-\delta(\ell)}$. On a

$$H \geq \sum_{m \in \mathcal{L}_1} m f(m) \geq \frac{L}{2} \sum_{m \in \mathcal{L}_1, m \geq L/2} f(m).$$

De plus pour tout premier $\ell \in \Lambda_1$ on a

$$f(\ell) = \frac{1}{\ell} \frac{1 - \frac{2g^2+g+1+n}{\ell} + O\left(\frac{1}{\ell^2}\right)}{1 - \left(1 - \frac{2g^2+g+1+n}{\ell} + O\left(\frac{1}{\ell^2}\right)\right)} = \frac{1}{2g^2+g+1+n} + O_g\left(\frac{1}{\ell}\right).$$

Le théorème de Lau–Wu assure que

$$H \gg L^2 (\log L)^{-1+1/(2g^2+g+1+n)}$$

avec une constante implicite ne dépendant que de g.

2. Dans le cas $d \geq 2$, il faudrait traiter une somme sur les nombres avec des facteurs premiers dans certaines classes de congruence. On évite la difficulté en écrivant que la somme sur les nombres sans facteurs carrés est supérieure à la somme sur les premiers.

$$H \gg \sum_{\ell \in \Lambda_{\geq 2}, \ell \leq L} \ell \gg \left(1 - \frac{r(g,p)}{\phi(p)}\right) L^2 (\log L)^{-1}$$

avec une constante implicite ne dépendant que de g et n.

Finalement, on choisit $L = p^{1/2A}$ pour que les deux termes dans la parenthèse de (2.7) soient de même ordre de grandeur.

1. Dans le cas $d = 1$, on obtient :

$$|D_p(\underline{a})| \ll p^{1-2/\gamma} (\log p)^{1-2/(\gamma+2n-2)},$$

avec $\gamma = 4g^2 + 2g + 4$. La constante implicite ne dépend que de g.

2. Dans le cas $d \geq 2$, cela donne :

$$|D_p(\underline{a})| \ll \frac{\phi(p)}{\phi(p) - r(g,p)} p^{d-1/(6g^2+3g+4)} \log p,$$

la constante implicite ne dépendant que de g et n.

□

Remarque 27.

1. Dans la situation de la proposition 2.16, la densité de l'ensemble Ω_ℓ se rapproche de 1 quand ℓ tend vers l'infini. C'est légèrement mieux que ce qu'on attend d'habitude dans le grand crible. Il nous suffit en général de montrer que la densité est minorée par une constante. On a donc une minoration de H meilleure que dans les cas classiques de grand crible. On pourrait vouloir utiliser un plus grand crible dans cette situation. A ma connaissance une telle méthode n'a pas été développée pour les cribles de classes de conjugaison de Frobenius.
2. La minoration de H dans le cas $d \geq 2$ est peut-être un peu brutale. On pourrait estimer mieux la somme d'entiers sans facteurs carrés dont les facteurs premiers sont dans certaines classes de congruences. Cependant une meilleure estimation ne pourrait nous faire gagner au mieux qu'une puissance de $\log L$.
3. On pourrait imaginer tenter de trouver une meilleure majoration en utilisant la technique de Bellaïche de la sous-section 2.1.3, mais il y a assez peu d'espoir : dans [Bel16, §2.3.2], Bellaïche montre que la borne de Cauchy est à peu près optimale dans les sous-ensembles de trace fixé de GL_n.

2.2.3 Cas d'un espace de paramètres de dimension 1 — Utilisation du plus grand crible

Commençons par appliquer le plus grand crible de la sous-section 2.1.4. On peut utiliser la majoration de la taille de l'ensemble $D_p(\underline{a})$ obtenue à la proposition 2.16 pour donner une majoration de la taille de l'ensemble $S(U,T,Q,\underline{a})$ défini en (2.5), on obtient alors le résultat suivant.

Théorème 2.17. *Soit g un entier positif fixé. Soit $U \subset \mathbb{A}_{\mathbf{Z}}$ un sous-schéma ouvert dense. On se donne une famille $\mathcal{C} \to U$ de courbes projectives sur $\mathbf{Z}$ dont la fibre générique est lisse de genre g. On suppose que pour tout premier p et tout premier $\ell \neq p$, on a $\rho_\ell(\pi_1^g(U_p)) = Sp(2g, \mathbf{F}_\ell)$. Alors il existe une constante K_g qui ne dépend que de g telle que pour « la plupart » des $u \in U$, $|u| \leq T$, le plus petit p vérifiant $p \nmid \prod_{i=1}^n (N_{C_u}(p) + a_i - 1)$ est majoré par $Q_{g,1}(T) := (2K_g\gamma \log T)^{\gamma/2} \left(\log(2K_g\gamma \log T)\right)^{\frac{\gamma}{2}(1-\frac{2}{\gamma+2n-2})}$, où $\gamma = 4g^2+2g+4$.*

Précisément, on a

$$\frac{1}{T}|\{u \in \mathbf{Z} : |u| \leq T, a(C_u,p) \in \{a_1, \dots a_n\}, \forall p < Q_{g,1}(T)\}| \ll \frac{Q_{g,1}(T)}{T \log T}$$

où la constante implicite est absolue.

Démonstration. On a

$$S(U,T,Q,\underline{a}) = \{u \in \mathbf{Z}^d, h_1(u) \leq T, \forall p < Q, u \ [\mathrm{mod}\ p] \in D_p(\underline{a})\},$$

où la hauteur h_1 est comme dans la définition 2.11. L'ensemble $S(U,T,Q,\underline{a})$ est un sous-ensemble fini de $\mathbf{Q}$ qui vérifie les hypothèses du théorème 2.13. D'après la proposition 2.16 il existe une constante K_g telle que $\nu(p) = K_g p^{1-2/\gamma}(\log p)^{1-2/(\gamma+2n-2)}$ convient.

Le théorème 2.13 assure alors que

$$|S(U,T,Q,\underline{a})| \leq \frac{\sum_{p \leq Q} \log p}{\sum_{p \leq Q} \frac{\log p}{\nu(p)} - \log(2T^2)}$$

si le dénominateur est positif.

En utilisant le lemme 2.4 on peut minorer la somme au dénominateur :

$$\sum_{p \leq Q} \frac{\log p}{\nu(p)} \gg \frac{\gamma}{2K_g} Q^{2/\gamma} (\log Q)^{-1+2/(\gamma+2n-2)}$$

avec une constante implicite absolue. De la même façon, on majore le numérateur :

$$\sum_{p \leq Q} \log p \ll Q$$

avec une constante implicite absolue.

Prenons $Q = Q_{g,1}(T) = (2K_g\gamma \log T)^{\gamma/2} \left(\log(2K_g\gamma \log T)\right)^{\frac{\gamma}{2}(1-\frac{2}{\gamma+2n-2})}$ alors le dénominateur est de taille

$$\left(\gamma \left(\frac{\gamma}{2}\right)^{-1+2/(\gamma+2n-2)} - 1\right) \log T > (\sqrt{2}-1) \log T.$$

Il est en particulier positif : on obtient

$$|S(U,T,Q_{g,1}(T),\underline{a})| \ll \frac{Q_{g,1}(T)}{\log T}$$

la constante implicite est toujours absolue.

□

On peut tout de même suivre le raisonnement dans le cas où U est un sous-schéma ouvert de dimension $d \geq 2$. On obtient alors le résultat (moins intéressant) suivant.

Proposition 2.18. *Soit g un entier positif fixé. Soit $U \subset \mathbb{A}^d_{\mathbf{Z}}$ un sous-schéma ouvert dense de dimension $d \geq 2$. On se donne une famille $\mathcal{C} \to U$ de courbes projectives sur $\mathbf{Z}$ dont la fibre générique est lisse de genre g. On suppose que pour tout premier p et tout premier $\ell \neq p$, on a $\rho_\ell(\pi_1^g(U_p)) = Sp(2g, \mathbf{F}_\ell)$. Alors pour tout $a \in \mathbf{Z}$, il existe $T > 0$ et $u \in U(\mathbf{Z})$, $\|u\| \leq T$ satisfaisant $a(C_u, p) = a$ pour tout $p \leq \frac{1}{2}\log(2T^2)$.*

Démonstration. Dans le cas $d \geq 2$, d'après la proposition 2.16 on a

$$\nu(p) = K_{g,n} p^{d-1/(6g^2+3g+4)} \log p.$$

On applique le théorème 2.13. Le dénominateur est donc

$$\sum_{p \leq Q} \frac{\log p}{\nu(p)} - \log(2T^2) = K_{g,n}^{-1} \sum_{p \leq Q} p^{-d+1/(6g^2+3g+4)} - \log(2T^2).$$

Pour $d \geq 2$, la somme sur les premiers est convergente, donc si on prend T assez grand, le dénominateur sera négatif. Dans ce cas, le théorème 2.13 assure que

$$|S(U, T, Q, \underline{a})| \gg \frac{\log(2T^2) - Q}{\log(2T^2) - K_{g,n}^{-1} \sum_{p \leq Q} p^{-d+1/(6g^2+3g+4)}}.$$

Prenons $Q(T) = \frac{1}{2}\log(2T^2)$ alors on a

$$|S(U, T, Q(T), \underline{a})| \gg 1.$$

En particulier, pour T assez grand, l'ensemble $S(U, T, \frac{1}{2}\log(2T^2), \underline{a})$ est non vide, c'est-à-dire qu'il existe une courbe C_u, $|u| \leq T$, telle que pour tout $p \leq \frac{1}{2}\log(2T^2)$, on ait $a(C_u, p) \in \{a_1, \ldots, a_n\}$. □

2.2.4 Cas d'un espace de paramètres de dimension supérieure — Utilisation de la mesure de comptage sur $\mathbf{Z}^d$

Pour $d \geq 2$, le plus grand crible ne permet pas de donner un majorant de la taille du plus petit premier de l'ensemble $\{p : p \nmid \prod_{i=1}^n (N_C(p) - a_i)\}$ pour la plupart des courbes C d'une famille à d paramètres. Dans cette situation, on utilise le grand crible sur $\mathbf{Z}^d$ comme vu dans la sous-section 2.1.1. Cela permet d'obtenir le résultat suivant.

Théorème 2.19. *Soient g et $d \geq 1$ des entiers positifs. Soit $U \subset \mathbb{A}^d_{\mathbf{Z}}$ un sous-schéma ouvert. On se donne une famille $\mathcal{C} \to U$ de courbes projectives sur $\mathbf{Z}$ dont la fibre générique est lisse de genre g. On suppose que pour tout premier p et tout premier $\ell \neq p$, on a $\rho_\ell(\pi_1^g(U_p)) = Sp(2g, \mathbf{F}_\ell)$. Alors pour « la plupart » des $u \in U$, $\|u\| \leq T$, le plus petit p vérifiant $p \nmid \prod_{i=1}^n (N_{C_u}(p) + a_i - 1)$ est majoré par $\sqrt{T}$ si $d = 1$ et par $Q'_{g,d}(T) := T^{\frac{d}{3d-2}}$ si $d \geq 2$.*

Précisément,

1. *si $d = 1$, on a*

$$\frac{1}{T}|\{u \in \mathbf{Z} : \|u\| \leq T, \pi_p(u) \in D_p(\underline{a}), \forall p < \sqrt{T}\}| \ll_g T^{-\frac{1}{2}-1/\gamma} (\log T)^{2-2/(\gamma+2n-2)},$$

où $\gamma = 4g^2 + 2g + 4$ et la constante implicite ne dépendent que de g,

2. si $d \geq 2$, on a

$$\frac{1}{T^d}|\{u \in \mathbf{Z}^d : \|u\| \leq T, a(C_u, p) \in \{a_1, \dots a_n\}, \forall p < Q'_{g,d}(T)\}| \\ \ll_{g,n} T^{-\frac{d}{3d-2}(1+1/(6g^2+3g+4))}(\log T)^2$$

où la constante implicite ne dépend que de g et n.

Démonstration. On applique le théorème 2.1 avec la borne obtenue à la proposition 2.5 pour Δ. On a pour $T, Q > 0$

$$|\{u \in \mathbf{Z}^d : \|u\| \leq T, \pi_p(u) \in D_p(\underline{a}), \forall p < Q\}| \ll \left((T+Q^2)^d + \frac{Q}{\log Q}(T+Q^3)^{d-1}\right) H^{-1},$$

avec $H = \sum_{p \leq Q} \frac{p^d - |D_p(\underline{a})|}{|D_p(\underline{a})|}$.

La proposition 2.16 jointe au lemme 2.4 permet de minorer H.

1. si $d = 1$, on a
$$|D_p(\underline{a})| \ll p^{1-2/\gamma}(\log p)^{1-2/(\gamma+2n-2)},$$
où $\gamma = 4g^2 + 2g + 4$ et la constante implicite ne dépendent que de g. Donc
$$H \gg \sum_{p \leq Q} p^{2/\gamma}(\log p)^{-1+2/(\gamma+2n-2)} \\ \gg Q^{1+2/\gamma}(\log Q)^{-2+2/(\gamma+2n-2)}$$
la constante implicite ne dépend que de g.
2. si $d \geq 2$, et $p > 2g+1$, on a
$$|D_p(\underline{a})| \ll p^{d-1/(6g^2+3g+4)} \log p,$$
la constante implicite ne dépend que de g et de n. Donc
$$H \gg \sum_{p \leq Q} p^{1/(6g^2+3g+4)}(\log p)^{-1} \\ \gg Q^{1+1/(6g^2+3g+4)}(\log Q)^{-2}$$
la constante implicite ne dépend que de g et de n.

On choisit Q de façon à avoir $\Delta(T, Q) \ll T^d$, cela permet de conclure.

1. Dans le cas $d = 1$, prenons $Q = Q'_{g,1}(T) = \sqrt{T}$, alors on obtient
$$|\{u \in \mathbf{Z} : \|u\| \leq T, \pi_p(u) \in D_p(\underline{a}), \forall p < \sqrt{T}\}| \ll T^{\frac{1}{2}-1/\gamma}(\log T)^{2-2/(\gamma+2n-2)}.$$
2. Dans le cas $d \geq 2$, prenons $Q = Q'_{g,d}(T) = T^{\frac{d}{3d-2}}$, alors on obtient
$$|\{u \in \mathbf{Z}^d : \|u\| \leq T, \pi_p(u) \in D_p(\underline{a}), \forall p < Q'_{g,d}(T)\}| \\ \ll T^{d-\frac{d}{3d-2}(1+1/(6g^2+3g+4))}(\log T)^2.$$

□

Remarque 28. Dans le cas $d = 1$, on trouve un majorant de l'ordre de $\sqrt{T}$, c'est beaucoup moins bien que le résultat obtenu par la méthode de plus grand crible au théorème 2.17.

2.2.5 Cas d'un espace de paramètres de dimension supérieure — Utilisation de la méthode de grand crible de Bellaïche

En utilisant la sous-section 2.1.3, on a une autre façon de trouver un majorant pour le plus petit premier de l'ensemble $\{p : p \nmid \prod_{i=1}^{n}(N_C(p) - a_i)\}$.

Proposition 2.20. *Supposons qu'il existe $\alpha' > 0$ tel que pour tout premier p on ait*

$$|D_p(\underline{a})| \gg p^{d-\alpha'}.$$

Alors pour « la plupart » des $u \in U$, $\|u\| \leq T$, le plus petit p vérifiant $p \nmid \prod_{i=1}^{n}(N_{C_u}(p) + a_i - 1)$ est majoré par

$$Q_{g,d}(T) := T^{\frac{1}{2d+\alpha'+1}} (\log T)^{\frac{1}{2d+\alpha'+1}}.$$

Précisément, on a

$$\frac{1}{T^d}|\{u \in U : \|u\| \leq T, a(C_u, p) \in \{a_1, \ldots, a_n\}, \forall p < Q_{g,d}(T)\}| \ll T^{-\frac{1+1/\gamma(d)+\epsilon}{(2d+\alpha'+1)}}$$

pour tout $\epsilon > 0$, où $\gamma(1) = 2g^2 + g + 2$, et $\gamma(d) = 6g^2 + 3g + 4$ si $d \geq 2$ et la constante implicite ne dépend que de ϵ, g et d.

Remarque 29. Dans le cas $d = 1$ le très grand crible (théorème 2.17) donne encore la meilleure majoration pour le plus petit premier de l'ensemble $\{p : p \nmid \prod_{i=1}^{n}(N_C(p) - a_i)\}$. Dans le cas $d \geq 2$, la borne $Q'_{g,d}(T)$ obtenue dans le théorème 2.19 est moins bonne que celle de la proposition 2.20. Ce qu'on gagne dans la proposition 2.20 par rapport au théorème 2.19 pour la borne $Q_{g,d}(T)$ est perdu dans la majoration de la taille de l'ensemble exceptionnel.

Démonstration. On cherche à appliquer le théorème 2.10 à notre situation. Pour T entier assez grand fixé, on prend $X = [-T, T]^d \cap \mathbf{Z}^d$, alors $|X| = (2T+1)^d$. L'application naturelle à associer est l'inclusion dans $\mathbf{Z}^d$. On regarde alors pour tout premier p la projection $\rho_p : \mathbf{Z}^d \to (\mathbf{Z}/p\mathbf{Z})^d$, le système (ρ_p) est bien linéairement indépendant selon la définition 2.2. Comme précédemment

$$D_p(\underline{a}) = \{u \in U_p : a(C_u, p) \in \{a_1, \ldots, a_n\}\}$$

est bien un sous ensemble de $(\mathbf{Z}/p\mathbf{Z})^d$ stable par conjugaison.

Commençons par vérifier le théorème de Chebotarev effectif.

Lemme 2.21. *Soit m un entier, et $f : (\mathbf{Z}/m\mathbf{Z})^d \to \mathbf{C}$ une fonction. On a*

$$\left| \sum_{x \in [-T,T]^d \cap \mathbf{Z}^d} f(x \ [\mathrm{mod}\ m]) - (2T+1)^d \mu(f) \right| = O(T^{d-1} m^d \mu(|f|))$$

la constante implicite ne dépend que de d.

Démonstration. On évalue la somme

$$\sum_{x \in [-T,T]^d \cap \mathbf{Z}^d} f(x \ [\mathrm{mod}\ m])$$

en découpant le grand cube $[-T, T]^d$ en petits cubes de coté m. On peut mettre $\left[\frac{2T}{m}\right]^d$ cubes de coté m entiers. La somme sur chacun de ces cubes est $m^d \mu(f)$. Il reste alors une somme sur moins de m^d valeurs de f, on peut la majorer par $m^d \mu(|f|)$. Donc

$$\sum_{x \in [-T,T]^d \cap \mathbf{Z}^d} f(x \ [\mathrm{mod}\ m]) = \left[\frac{2T}{m}\right]^d m^d \mu(f) + O(m^d \mu(|f|)).$$

Il nous reste à estimer la différence avec $(2T+1)^d\mu(f)$. On a

$$\begin{aligned}\left[\frac{2T}{m}\right]^d m^d &= \left(\frac{2T}{m}+O(1)\right)^d m^d \\ &= (2T)^d + O(d(2T)^{d-1}m^d).\end{aligned}$$

On peut conclure. □

Donc on a bien un théorème de Chebotarev effectif avec $\lambda_G = \mu_G|\cdot|$ c'est une norme sur les fonctions $f : G \to \mathbf{C}$, on a bien $\mu_G(1) = 1$ et la propriété de multiplicativité pour les produits tensoriels de fonctions sur les produits de groupes. Suivant les notations du théorème 2.10,

— on a $A(T^d) = T^{d-1}$ donc $r = \frac{d-1}{d}$, $s = 0$,

— on a $B(m^d) = m^d$ donc $t = 1$, $u = 0$,

— pour p premier, $|(\mathbf{Z}/p\mathbf{Z})^d| = p^d$, donc $\delta = d$,

— grâce à la proposition 2.16, on sait minorer $\frac{p^d}{|D_p(\underline{a})|}$, on peut prendre $\alpha = \frac{1}{\gamma(d)} - \epsilon$ pour n'importe quel $\epsilon > 0$, avec $\gamma(1) = 2g^2+g+2$ et $\gamma(d) = 6g^2+3g+4$ si $d \geq 2$.

— par hypothèse, $\alpha' = \alpha'$,

— on a $\lambda(D_p(\underline{a})) = \frac{|D_p(\underline{a})|}{p^d}$, mais pour le théorème 2.10, il faut $\beta \geq 0$, on prend donc $\beta = 0$.

On utilise la formule (2.2) : la valeur optimale pour Q est :

$$\begin{aligned}Q_{g,d}(T) &= T^{d\frac{1-(d-1)/d}{\alpha'+2d+1}}(\log T)^{\frac{1}{\alpha'+2d+1}} \\ &= T^{\frac{1}{2d+\alpha'+1}}(\log T)^{\frac{1}{2d+\alpha'+1}}.\end{aligned}$$

Le théorème 2.10 assure que

$$|S(U,T,Q_{g,d}(T),\underline{a})| \ll T^{d\left(1-\frac{1+1/\gamma(d)+\epsilon}{d(2d+\alpha'+1)}\right)}(\log T)^{\frac{2d+\alpha'-1/\gamma(d)+\epsilon}{2d+\alpha'+1}},$$

pour tout $\epsilon > 0$ assez petit. On a donc le résultat annoncé. □

On n'a pas spécifié la valeur de α' dans l'énoncé de la proposition 2.20, pour cela on a besoin de minorer la taille de $D_p(\underline{a})$. Dans l'idée, la majoration devrait être optimale, donc $\alpha' \approx \alpha$ devrait convenir (c'est la solution qui donne la meilleure majoration possible de $|S(U,T,Q,\underline{a})|$ mais pas pour la borne sur le plus petit premier). Dans tous les cas, il est raisonnable de penser qu'on va avoir $\alpha \leq \alpha' \leq d$.

En effet, on peut espérer que $|D_p(\underline{a})| \geq 1$ pour tout p. Sinon, $D_{p_0}(\underline{a})$ est vide pour un certain premier p_0. Alors $S(U,T,p_0,\underline{a})$ est vide indépendamment de T. Or $p_0 \ll T^{\frac{1}{3d}}$, donc $\alpha' = d$ convient encore.

2.3 Courbes avec un grand plus petit premier

Soit C une courbe affine lisse qui admet un modèle projectif lisse de genre plus grand que 2. On soupçonne que le plus petit élément de $\{p \in \mathcal{P} : p \nmid N_C(p)\}$ n'est pas très grand. On cherche ici des courbes hyperelliptiques pour lesquelles ce plus petit premier va être assez grand. Comme on l'a vu dans la section 2.2, il est naturel de penser que ces familles de courbes vont soit avoir un genre non borné, soit avoir un conducteur non borné.

2.3.1 Courbes avec un grand genre

Une première idée est donc de faire tendre le genre vers l'infini. Soit q un nombre premier, on définit C_q la courbe hyperelliptique affine par l'équation :

$$C_q : y^2 = x^q + 1.$$

Alors pour tout premier $p \notin \{2, q\}$, la courbe $C_q/\mathbf{F}_p$ est lisse. De plus, si $p \not\equiv 1 \pmod{q}$ alors l'application $x \mapsto x^q + 1$ est une bijection de $\mathbf{F}_p$. On en déduit $N_{C_q}(p) = p$. Ainsi pour tout premier $p < 2q + 1$, on a $N_{C_q}(p) = p$.

La borne $2q + 1$ n'est intéressante que si $2q + 1$ est premier. Il pourrait être composé. Dans ce cas on a $N_{C_q}(p) = p$ pour tout premier $p < 4q + 1$, et on peut continuer si $4q + 1$ est aussi composé. On cherche donc des premiers q pour lesquels le plus petit premier $p \equiv 1 \pmod{q}$ est grand. Plus précisément, pour un entier N fixé, on cherche le plus petit premier q possible satisfaisant : le plus petit premier $p \equiv 1 \pmod{q}$ est supérieur à N.

Exemple 7. On cherche une courbe du type C_q pour laquelle le plus petit premier $p \nmid N_{C_q}(p)$ est supérieur à 100. Le plus petit premier congru à 1 modulo 17 est $6 \times 17 + 1 = 103$, et on a $N_{C_{17}}(103) = 87$. Donc pour tout premier $p < 103$ de bonne réduction pour C_{17} on a $N_{C_{17}}(p) = p$.

Exemple 8. Pour $N = 10000$, le premier $q = 457$ convient, en effet $457 \times 30 + 1 = 13711$ est le plus petit premier dans la classe de congruence 1 [mod q]. On a $N_{C_{457}}(13711) = 13255$. Alors pour tout premier $p < 13711$, on a $N_{C_{457}}(p) = p$.

2.3.2 Courbes de genre fixé

D. Lombardo m'a proposé une façon de construire une famille de courbes hyperelliptiques de genre 2, mais avec des coefficients potentiellement très grands. Fixons un grand entier N. Pour tout premier $p \leq N$, il est possible de trouver un polynôme $f_p \in \mathbf{F}_p[X]$ de degré 5, tel que la courbe affine dans $\mathbf{F}_p$ donnée par l'équation $y^2 = f_p(x)$ soit lisse et ait exactement p points dans $\mathbf{F}_p$. L'existence d'une courbe projective hyperelliptique sur $\mathbf{F}_p$ avec $p + 1$ points est donnée par [HNR09, Th. 1.2], on choisit alors un ouvert affine pour avoir exactement un point à l'infini. Grâce au théorème des restes chinois, on déduit l'existence d'un polynôme $f \in \mathbf{Z}[X]$ de degré 5 qui satisfait pour tout $p < N$, $f \equiv f_p \pmod{p}$. Alors le plus petit premier p vérifiant $p \nmid N_C(p)$ pour la courbe $C : y^2 = f(x)$ est supérieur à N.

Exemple 9. Soient C_1 et C_2 les courbes hyperelliptiques affines de genre 2 données par les équations : $C_1 : y^2 = x^5 + 5x^3 + 5x$ et $C_2 : y^2 = x^5 + x$. En utilisant `SageMath` [SD16] on trouve que pour tout $p < 401$, on a $N_{C_1}(p) = p$ ou $N_{C_2}(p) = p$. Donc on peut en déduire une courbe C sur $\mathbf{Z}$ telle que $N_C(p) = p$ pour tout $p < 401$, et C_0 a un modèle projectif lisse de genre 2.

En fait, pour tout $p \equiv \pm 2 \pmod{5}$, on a $N_{C_1}(p) = p$. L'idée est qu'alors les racines de $x^4 + 5x^2 + 5$ ne sont pas dans $\mathbf{F}_p$, et elles sont échangées par l'action de l'endomorphisme de Frobenius.

On peut aussi compter le nombre de points d'une courbe hyperelliptique par un calcul direct. Si C est donnée sur $\mathbf{Z}$ par l'équation $y^2 = f(x)$ alors $N_X(p) = p + \sum_{x \in \mathbf{F}_p} \chi_p(f(x))$. On peut simplifier cette expression en utilisant le lemme 1.51.

Exemple 10. Soit C_b la courbe hyperelliptique affine donnée par l'équation $C_b : y^2 = x^5 + bx$. On a

$$N_X(p) \equiv \sum_{x \in \mathbf{F}_p} \sum_{k+\ell = \frac{p-1}{2}} \binom{(p-1)/2}{k} b^\ell x^{5k+\ell} \pmod{p}.$$

On intervertit les sommes et on utilise le lemme 1.51. On a $0 \leq 5k+\ell \leq \frac{5}{2}(p-1)$ donc les seuls termes qui comptent sont ceux où $5k+\ell = p-1$ ou $5k+\ell = 2(p-1)$. Dans le premier cas, $k+\ell = \frac{p-1}{2}$ et $5k+\ell = p-1$, on trouve $k = \frac{p-1}{8}$. Dans le second cas, on trouve $k = \frac{3(p-1)}{8}$. Finalement

— si $p \not\equiv 1 \pmod 8$, on déduit que $N_{C_b}(p) \equiv 0 \pmod p$,

— si $p \equiv 1 \pmod 8$, on a $N_{C_b}(p) \equiv -\binom{(p-1)/2}{(p-1)/8}(b^{\frac{3(p-1)}{8}} + b^{\frac{p-1}{8}}) \pmod p$, donc si $b^{\frac{p-1}{4}} \equiv -1 \pmod p$, on trouve $N_{C_b}(p) \equiv 0 \pmod p$.

On peut donc construire une famille de courbes hyperelliptiques C_N de genre 2, avec le plus petit premier $p \nmid N_{C_N}(p)$ arbitrairement grand et avec des coefficients qui croissent de manière raisonnable.

Par exemple 2 est une racine 4-ème de -1 modulo 17, c'est aussi une racine 10-ème de -1 modulo 41, par contre $2^{18} \equiv 1 \pmod{73}$. Donc pour la courbe $C_2 : y^2 = x^5 + 2x$, on a $N_{C_2}(p) = p$ pour tout $p < 73$.

En utilisant `SageMath` [SD16], on trouve que pour la courbe $C = C_{-36284789135} : y^2 = x^5 - 36284789135x$, on a $N_C(p) = p$ pour tout $p < 113$.

2.4 Autres applications de la méthode de grand crible de Bellaïche

On souhaite voir d'autres exemples d'applications de la nouvelle méthode de Bellaïche pour le grand crible (théorème 2.10), pour cela il nous faut un théorème de Chebotarev effectif. On a un tel théorème démontré par Kowalski [Kow06b] dans le cadre des variétés sur les corps finis.

On considère les données suivantes : $U/\mathbf{F}_q$ est une courbe affine lisse, géométriquement irréductible, réalisée comme ouvert dense d'une courbe projective lisse $C/\mathbf{F}_q$ de genre g, soit $n_\infty = |(C-U)(\overline{\mathbf{F}}_q)|$ le nombre de points à l'infini. Pour tout ℓ premier différent de la caractéristique du corps on se donne une application surjective vers un groupe fini $\rho_\ell : \pi_1(U, \overline{\eta}) \to G_\ell$ qui résulte de la réduction modulo ℓ d'un faisceau $\mathbf{Z}_\ell$-adique modérément ramifié lisse et sans torsion. On suppose de plus que le système formé des représentations ρ_ℓ est linéairement indépendant. On note dans la suite $\rho = \rho_\ell$ (resp. $\rho = \rho_\ell \times \rho_{\ell'}$ pour $\ell \neq \ell'$), et $G = G_\ell$ (resp. $G = G_\ell \times G_{\ell'}$). On note $G_\ell^g = \rho_\ell(\pi_1(\overline{U}, \overline{\eta}))$ (resp. $G^g = G_\ell^g \times G_{\ell'}^g$. On a une suite exacte

$$1 \to G^g \to G \xrightarrow{\mathrm{m}} \Gamma \to 1$$

avec Γ abélien. Pour $u \in U(\mathbf{F}_q)$ on note Frob_u la classe de conjugaison du Frobenius géométrique en u dans $\pi_1(U, \overline{\eta})$. Il existe $\gamma \in G$ tel que pour tout u, $\rho(\mathrm{Frob}_u) \in \gamma G^g$. On transforme [Kow06b, Th. 3] en théorème de Chebotarev effectif avec constante de Littlewood à la façon de Bellaïche.

Théorème 2.22 (Kowalski)**.** *Dans le cadre ci-dessus pour toute fonction centrale $f : G \to \mathbf{C}$ dont le support est inclus dans la classe à gauche γG^g, on a*

$$\pi(f, q) = \mu_{G^g}(f)|U(\mathbf{F}_q)| + O((n_\infty + g)\sqrt{q}\lambda_G(f))$$

avec une constante implicite absolue, où

$$\mu_{G^g}(f) = \frac{1}{|G^g|}\sum_{g \in \gamma G^g} f(g) \text{ et } \lambda_G(f) = \sum_{\chi \in \widehat{G}} \frac{1}{|G|}\left|\sum_{g \in G} f(g)\overline{\chi(g)}\right|\chi(1).$$

Remarque 30. On note que contrairement au théorème 2.8, ce théorème est inconditionnel.

Démonstration. On reprend la preuve de [Kow06b, Th. 3] sans la dernière majoration par inégalité de Cauchy–Schwarz. Comme f est centrale sur G, on peut écrire

$$f = \sum_{\chi \in \widehat{G}} \langle f, \chi \rangle \chi.$$

Les caractères χ de représentations triviales sur G^g, correspondent exactement aux caractères ψ (de degré 1) de Γ avec $\chi(g) = \psi(\mathrm{m}(g))$ pour tout $g \in G$. On a

$$\begin{aligned}\sum_{\psi \in \widehat{\Gamma}} \langle f, \psi \rangle \psi(\rho(\mathrm{Frob}_u)) &= \sum_{\psi \in \widehat{\Gamma}} \frac{1}{|G|} \sum_{g \in \gamma G^g} f(g) \overline{\psi(\mathrm{m}(\gamma))} \psi(\mathrm{m}(\gamma)) \\ &= \frac{|\Gamma|}{|G|} \sum_{g \in \gamma G^g} f(g) = \mu_{G^g}(f).\end{aligned}$$

Ainsi,

$$\pi(f, q) = \mu_{G^g}(f) |U(\mathbf{F}_q)| + \sum_{\chi \text{ non trivial sur } G^g} \langle f, \chi \rangle \sum_{u \in U(\mathbf{F}_q)} \chi(\rho(\mathrm{Frob}_u)).$$

Il nous reste à majorer le second terme, en utilisant la formule des traces de Grothendieck–Lefschetz, on écrit

$$\sum_{u \in U(\mathbf{F}_q)} \chi_\pi(\rho(\mathrm{Frob}_u)) = \sum_{i=0}^{2} (-1)^i \operatorname{tr}(\mathrm{Frob}_q \mid H_c^i(\overline{U}, \pi(\rho)))$$

où si χ_π est le caractère associé à la représentation irréductible π, on note aussi $\pi(\rho)$ le faisceau correspondant à la représentation $\pi \circ \rho$. On a $H_c^2(\overline{U}, \pi(\rho)) = 0$, cela découle de l'hypothèse sur la forme de ρ (voir [Kow06a, preuve de la Prop. 5.1]). Dans le cas $G = G_\ell$ on remarque qu'on a déjà écarté la situation où π est la représentation triviale. Donc d'après le théorème de Deligne,

$$\left| \sum_{u \in U(\mathbf{F}_q)} \chi(\rho(\mathrm{Frob}_u)) \right| \leq \sqrt{q} \sigma_c'(\overline{U}, \pi(\rho))$$

où

$$\sigma_c'(\overline{U}, \pi(\rho)) = \dim H^0(\overline{U}, \pi(\rho)) + \dim H^1(\overline{U}, \pi(\rho)) \leq (n_\infty + 2g - 1) \dim(\pi)$$

Suivant la preuve de Kowalski [Kow06b, Th. 3], le faisceau est modérément ramifié donc le terme supplémentaire dû aux conducteur de Swan dans le cas général est ici nul. Finalement on majore le second terme par

$$(n_\infty + 2g - 1) \sum_{\chi \in \widehat{G}} |\langle f, \chi \rangle| \chi(1)$$

□

Remarque 31. Comme f est à support dans un γG^g, on pourrait vouloir plutôt utiliser une constante de Littlewood sur le groupe G^g mais la fonction $f(\gamma\,.\,)$ sur G^g n'est pas forcément centrale donc on ne peut pas l'écrire comme combinaison linéaire de caractères sur G^g. Cependant, si γ est dans le centre de G, la fonction $f(\gamma\,.\,)$ est centrale et

$$\lambda_G(f) = \lambda_{G^g}(f(\gamma\,.\,)).$$

En effet on a alors $G = \langle \gamma \rangle \times G^g$ car G est le groupe engendré par les images de Frobenius par le théorème de Chebotarev. Donc $\widehat{G} = \widehat{\langle \gamma \rangle} \times \widehat{G^g}$, et les caractères de $\langle \gamma \rangle$ sont constants sur le support de f.

Remarque 32. On peut penser que la majoration de la somme sur les caractères non triviaux sur G^g par la somme sur tous les caractères est un peu grossière, mais le terme alors ajouté est

$$(n_\infty + 2g - 1) \sum_{\psi \in \widehat{\Gamma}} |\langle f, \psi \circ m \rangle| \psi(m(1)) = (n_\infty + 2g - 1) \mu_{G^g}(f)$$

qui est négligeable devant le premier terme quand q est grand.

Proposition 2.23. *Soit $U/\mathbf{F}_q$ comme dans le théorème 2.22, Λ un sous-ensemble de l'ensemble des nombres premiers, $(\rho_\ell : \pi_1(U, \overline{\eta}) \to G_\ell)_{\ell \in \Lambda}$ une famille de représentations continues qui forment un système linéairement indépendant. Pour tout $\ell \in \Lambda$ on se donne un ensemble $D_\ell \subset G_\ell$ stable par conjugaison, inclus la classe à gauche γG_ℓ^g. Supposons qu'il existe deux réels $0 \leq \alpha, \beta$, et des constantes $P, P', R > 0$ tels que*

— *pour tout $\ell \in \Lambda$, $P\ell^\alpha \leq \frac{|G_\ell^g|}{|D_\ell|} \leq P'\ell^\alpha$, (si $\alpha = 0$, alors $P > 1$),*

— *pour tout $\ell \in \Lambda$, $\lambda_{G_\ell}(D_\ell) \leq R\ell^\beta$,*

alors

$$|\{u \in U(\mathbf{F}_q), \forall \ell \in \Lambda, \rho_\ell(\mathrm{Frob}_u) \in D_\ell\}| \ll q^{\frac{\alpha+4\beta+1}{2\alpha+4\beta+1}} \log(q)^{\frac{2\beta}{\alpha+2\beta+1}}.$$

Démonstration. On est presque dans le cadre du Théorème 2.10, avec $X = U(\mathbf{F}_q)$, $|X| \sim q$, $A(T) = \sqrt{T}$ donc $r = \frac{1}{2}, s = 0$, et $B(T) = 1$ ainsi $t = u = 0$. La différence est que notre théorème de Chebotarev effectif fait apparaître μ_{G^g} au lieu de μ_G. On peut cependant suivre la preuve de la même façon : l'application Frobenius est $X \to \gamma G_\ell^g$ pour tout $\ell \in \Lambda$. Donc on remplace G_ℓ par γG_ℓ^g dans la preuve (quand on n'utilise pas le fait que c'est un groupe). On prend désormais $\mu_\ell(\{1\}) = \frac{|D_\ell|}{|G_\ell^g|}$ et $\mu_\ell(\{0\}) = \frac{|G_\ell^g| - |D_\ell|}{|G_\ell^g|}$. Alors $\phi_\ell(1) = \sqrt{\frac{|G_\ell^g| - |D_\ell|}{|D_\ell|}}$, $\phi_\ell(0) = -\sqrt{\frac{|D_\ell|}{|G_\ell^g| - |D_\ell|}}$.

Les fonctions $f_{\ell,\ell'}$ sont définies sur $\gamma_\ell G_\ell^g \times \gamma_{\ell'} G_{\ell'}^g$ (ou $\gamma_\ell G_\ell^g$), on peut les prolonger au groupe entier en leur donnant pour valeur 0 sur le complémentaire. Ce sont alors des fonctions centrales (car γG_ℓ^g est stable par conjugaison) qui vérifient les hypothèses du théorème 2.22.

Il apparaît donc un facteur $\lambda_{G_{\ell,\ell'}}(f_{\ell,\ell'})$ que l'on majore par

$$C \sqrt{\frac{|G_\ell^g|}{|D_\ell|}} \lambda_{G_\ell}(D_\ell) \sqrt{\frac{|G_{\ell'}^g|}{|D_{\ell'}|}} \lambda_{G_{\ell'}}(D_{\ell'}).$$

Par hypothèse, on sait majorer ce terme. Finalement on trouve

$$\pi(U(\mathbf{F}_q), D) \ll q^{\frac{\alpha+4\beta+1}{2\alpha+4\beta+2}} \log(q)^{\frac{2\beta}{\alpha+2\beta+1}}.$$

□

Remarque 33. Dans l'article de Kowalski utilisé [Kow06b] on trouve un théorème plus général avec X de dimension quelconque, on pourrait aussi tirer un résultat de crible de ce théorème.

Exemple 11. Traitons un exemple d'application en supposant que pour tout $\ell \in \Lambda$, $G_\ell^g = SL_2(\mathbf{F}_\ell)$. Par exemple on regarde une famille à un paramètre de courbes elliptiques C_t, $t \in U(\mathbf{F}_q)$ (sous ensemble de $\mathbf{F}_q$). On a pour tout premier ℓ différent de p, une application $t \mapsto \mathrm{Frob}_t | H^1(\overline{C}, \ell)$ qui induit une représentation de degré 2 du groupe fondamental étale arithmétique de U. On peut s'intéresser au nombre de t tels que P_t est réductible, où P_t est le polynôme caractéristique de $\mathrm{Frob}_t | H^1(\overline{C}, \ell)$. On étudie $D_\ell = \{M \in G_\ell, \det(T - M)$ est réductible$\}$.

Si pour tout ℓ l'image du Frobenius est dans une classe à gauche qui peut être représentée par une homothétie (ou un élément du centre) modulo G_ℓ^g, alors la connaissance de G_ℓ^g pour tout ℓ suffit. Ici l'image du Frobenius est la classe à gauche modulo $SL(2, \mathbf{F}_\ell)$ des matrices de déterminant q. Donc si $q = p^{2r}$ est un carré, l'homothétie de rapport p^r est dans la classe de conjugaison de l'image du Frobenius et dans le centre du groupe G_ℓ pour tout $\ell \neq p$. Appelons γ cette homothétie (ou son image dans G_ℓ).

On a

$$\frac{|G_\ell^g|}{|D_\ell|} = \frac{|G_\ell^g|}{|\gamma^{-1} D_\ell|} \sim 2$$

quand $\ell \to +\infty$, donc on peut prendre $\alpha = 0$, $P > 1$. En utilisant la table des caractères de $SL_2(\mathbf{F}_\ell)$, [Kow08a, p. 230], on calcule

$$\lambda_{G_\ell}(D_\ell) = \lambda_{G_\ell^g}(\gamma^{-1} D_\ell) = O(\ell)$$

donc on peut prendre $\beta = 1$.

Le résultat précédent donne

$$|\{t \in \mathbf{F}_q, P_t \text{ est réductible dans } \mathbf{Z}[T]\}| \ll p^{\frac{5}{6}} \log(p)^{\frac{2}{3}}.$$

Remarque 34. Une estimation intéressante de la constante de Littlewood dépend de la connaissance de la table des caractères des groupes G_ℓ^g, il faut donc non seulement connaître le groupe (ce qui n'est pas toujours facile) mais aussi sa table des caractères (ce qui devient difficile quand l'ordre grandit).

Chapitre 3

Courses de nombres premiers pour les coefficients de certaines fonctions L

Dans ce chapitre on s'intéresse à la généralisation de la notion de biais de Chebyshev dans les courses de nombres premiers. L'idée vient d'une lettre de Chebyshev à Fuss [Che99] dans laquelle celui-ci affirme avoir montré que pour beaucoup d'entiers x il y a plus de premiers inférieurs à x qui sont congrus à 3 $[\bmod 4]$ qu'à 1 $[\bmod 4]$. L'appellation « course de nombres premiers » souligne le fait que l'on compare deux ensembles de nombres premiers. Pour poursuivre la métaphore, on dit qu'un concurrent est en tête au moment x s'il y a plus de premiers inférieurs à x dans son équipe que dans l'autre. On se pose alors la question de savoir si chacun des concurrents est une infinité de fois en tête, et si on peut estimer précisément la taille des ensembles des $x \geq 2$ tels qu'un concurrent donné est en tête.

L'observation de Chebyshev peut se traduire par le fait que la fonction $x \mapsto \sum_{p \leq x} \left(\frac{-1}{p}\right)$ est beaucoup plus souvent négative que positive. L'approche standard pour étudier cette question est d'utiliser la fonction L de Dirichlet associée au caractère de Lengendre $\left(\frac{-1}{\cdot}\right)$. On donne plus de détails sur l'historique des courses de nombres premiers dans la section 3.2.

Plus généralement, étant donné une fonction $L(s) = \sum_{n \geq 1} a_n n^{-s}$, on peut chercher à comprendre le signe de la fonction $x \mapsto \sum_{p \leq x} a_p$. On parlera de la course de nombres premiers associée à la fonction L. On considère cette fois la course entre les premiers pour lesquels les coefficients a_p sont positifs et ceux pour lesquels les coefficients a_p sont négatifs, en pondérant par leur valeur. On peut alors se poser les mêmes questions que pour la course originelle de Chebyshev.

Le but principal de ce chapitre est de définir les propriétés que doit satisfaire la fonction L pour que la course associée soit bien définie, et soit éventuellement intéressante. On définit pour cela dans la section 3.1 une notion de fonctions L *analytiques* pour lesquelles les preuves de résultats antérieurs sur les courses de nombres premiers s'adaptent bien. On énonce notamment quelques résultats et conjectures classiques liés aux propriétés des zéros de telles fonctions. On démontre alors dans la section 3.3 que l'on peut étudier les courses associées aux fonctions L de cette classe, grâce à l'idée introduite par Wintner [Win41] d'étudier la distribution logarithmique limite associée à une « fonction de course » normalisée (voir la définition 3.15).

On verra que notre notion de fonction L analytique regroupe des hypothèses assez naturelles qui sont connues ou au moins supposées vraies pour la plupart des « fonctions L » habituellement utilisées en théorie des nombres. Cela nous permet de donner dans la section 3.4 diverses courses de nombres premiers associées à des fonctions L d'origines diverses. On retrouve notamment les résultats obtenus pour les courses à deux concurrents

dans les classes de congruences modulo un entier fixé qui est un cas particulier de [RS94]. Nos raisonnements sont une généralisation de certains des résultats de [Sar07], [Fio14a] sur les courses pour les coefficients a_p de courbes elliptiques sur $\mathbf{Q}$.

La plupart des résultats obtenus antérieurement sont conditionnels à de fortes hypothèses telles que l'hypothèse de Riemann généralisée et des hypothèses sur l'indépendance linéaire des zéros ou sur leur multiplicité. Dans la section 3.5, on montre des résultats conditionnels à ces hypothèses ainsi qu'à des versions affaiblies de celles-ci. On s'intéresse à la régularité, la symétrie et au support de la distribution logarithmique limite dont l'existence est garantie par le théorème 3.19. On montre notamment conditionnellement à une hypothèse d'indépendance linéaire assez faible, que l'ensemble $\{x > 2 : \sum_{p \leq x} a_p \geq 0\}$ admet une densité logarithmique.

3.1 Une classe analytique de fonctions L

3.1.1 Définition des fonctions L analytiques

Dans ce chapitre on utilise une définition de fonction L *analytique* inspirée de [IK04, Chap. 5] et de la classe de Selberg. On ne définit de telles fonctions que par des propriétés analytiques, que l'on utilisera pour étudier la course de nombres premiers associée.

Définition 3.1 (Fonction L analytique)**.** Soit $L(f,s)$ une fonction en la variable $s \in \mathbf{C}$, associée à un paramètre auxiliaire f auquel on peut associer un entier $q(f)$ (souvent f est d'origine arithmétique et $q(f)$ est son conducteur). Alors $L(f,s)$ est une fonction L analytique si les conditions suivantes sont satisfaites :

1. La fonction s'écrit comme une série de Dirichlet qui se factorise en produit eulérien de degré $d \geq 1$:

$$L(f,s) = \sum_{n \geq 1} \lambda_f(n) n^{-s} = \prod_p \prod_{j=1}^{d} \left(1 - \alpha_{f,j}(p) p^{-s}\right)^{-1}$$

   avec $\lambda_f(1) = 1$ et $\alpha_{f,j}(p) \in \mathbf{C}$, vérifiant $|\alpha_{f,j}(p)| = 1$ pour tout j et $p \nmid q(f)$. En particulier la série de Dirichlet et le produit eulérien sont absolument convergents sur $\mathrm{Re}(s) > 1$. On appelle d le *degré* de la fonction L.

2. On peut associer à la fonction un facteur gamma de paramètres locaux $\kappa_j \in \mathbf{C}$, $\mathrm{Re}(\kappa_j) > -1$:

$$\gamma(f,s) = \pi^{-ds/2} \prod_{j=1}^{d} \Gamma\left(\frac{s + \kappa_j}{2}\right).$$

   On définit le *conducteur analytique* de f par :

$$\mathfrak{q}(f) = q(f) \prod_{j=1}^{d} \left(|\kappa_j| + 3\right),$$

   et on définit la fonction L complétée

$$\Lambda(f,s) = q(f)^{s/2} \gamma(f,s) L(f,s).$$

   La fonction $\Lambda(f,s)$ se prolonge de façon holomorphe à tout le plan complexe ; on obtient une fonction entière d'ordre 1. De plus on a une équation fonctionnelle

$$\Lambda(f,s) = \epsilon(f) \Lambda(\overline{f}, 1-s), \tag{3.1}$$

   avec $\epsilon(f) = \pm 1$. On a noté dans l'équation précédente $\Lambda(\overline{f}, \cdot)$ la fonction L complétée associée à la fonction $L(\overline{f}, s) := \sum_{n \geq 1} \overline{\lambda_f(n)} n^{-s}$.

3. La fonction
$$L(f^{(2)},s)=\prod_p\prod_{j=1}^{d}\left(1-\alpha_{f,j}(p)^2p^{-s}\right)^{-1}$$
est définie sur $\mathrm{Re}(s)>1$. On fait l'hypothèse qu'il existe un ouvert $U\supset\{\mathrm{Re}(s)\geq 1\}$ tel que la fonction $L(f^{(2)},\cdot)$ se prolonge en une fonction méromorphe sur U. De plus on suppose que le prolongement sur $U-\{1\}$ n'a ni zéro ni pôle.

Remarque 35.
1. Les hypothèses que l'on fait ici sont plus fortes que celles habituellement données pour définir la classe de Selberg [KP99], elles sont aussi plus fortes que celles proposées par Iwaniec et Kowalski [IK04, Chap. 5]. On note par exemple qu'on suppose que les zéros locaux sont presque tous de norme 1, c'est une version très forte de la conjecture de Ramanujan–Petersson. Il est plus classique de supposer seulement pour tout $\epsilon>0$, $\lambda_f(n)=O(n^\epsilon)$. Notre hypothèse permet d'avoir $|\lambda_f(n)|\leq\tau_d(n)$ où $\tau_d(n)$ est le nombre de représentations de n comme produit de d nombres entiers. En particulier, pour p premier, on a $|\lambda_f(p)|\leq d$.
2. On suppose aussi que le prolongement analytique de notre fonction L est holomorphe, en particulier la fonction ζ de Riemann n'est pas une fonction L analytique dans le sens de notre définition 3.1.
3. Une fonction Λ holomorphe sur $\mathbf{C}$ est dite d'ordre 1 si elle vérifie pour tout $\beta>1$ (et pour aucun $\beta<1$) :
$$\Lambda(s)\ll\exp(|s|^\beta).$$
Cela implique des propriétés sur la répartition des zéros (voir proposition 3.4) et donc sur une borne pour la dérivée logarithmique (voir proposition 3.5).
4. L'hypothèse 3, n'est peut-être pas très habituelle. On peut écrire la fonction $L(f^{(2)},s)$ sous la forme
$$L(f^{(2)},s)=L(\mathrm{Sym}^2 f,s)L(\wedge^2 f,s)^{-1}$$
(voir la définition 3.2). Donc on pourrait remplacer l'hypothèse sur $L(f^{(2)},s)$ en une hypothèse similaire sur ces deux fonctions. Alternativement, comme l'a proposé F. Brumley, on pourrait demander une propriété de la fonction $L(f\otimes\overline{f},s)$.

Définition 3.2. Soit $L(f,s)$ une fonction L analytique de degré d et de zéros locaux $\alpha_{f,j}(p)$. On définit pour $\mathrm{Re}(s)>1$, la fonction L carré symétrique
$$L(\mathrm{Sym}^2 f,s)=\prod_p\prod_{1\leq j\leq k\leq d}\left(1-\alpha_{f,j}(p)\alpha_{f,k}(p)p^{-s}\right)^{-1}$$
et la fonction L carré alterné
$$L(\wedge^2 f,s)=\prod_p\prod_{1\leq j<k\leq d}\left(1-\alpha_{f,j}(p)\alpha_{f,k}(p)p^{-s}\right)^{-1}.$$

Remarque 36. Ces fonctions ne sont pas forcément des fonctions L analytiques suivant la définition 3.1, en fait on verra dans les exemples que souvent l'une des deux se prolonge avec un pôle en 1.

Exemple 12. On a plusieurs exemples de fonctions usuelles qui satisfont les hypothèses de la définition 3.1.
1. Les fonctions L de Dirichlet pour les caractères non triviaux sont analytiques dans le sens de la définition 3.1. En particulier on pourra retrouver les résultats de [RS94] à partir de nos résultats plus généraux (voir la sous-section 3.4.1).

2. Les fonctions L provenant de formes modulaires primitives holomorphes cuspidales de niveau $q \in \mathbf{N}$, caractère χ, poids $k \geq 1$ satisfont aussi toutes les hypothèses de la définition 3.1. Ce sont des fonctions L analytiques de degré 2 (voir par exemple [IK04, 5.11]). La conjecture de Ramanujan–Petersson est satisfaite selon [Del74, Th. 8.2] et [DS74]. En particulier d'après les travaux sur la modularité ([Wil95], [TW95], [BCDT01]), si E est une courbe elliptique sur $\mathbf{Q}$ alors la fonction de Hasse–Weil associée $L(E, s)$ satisfait la définition 3.1. Cette propriété a déjà été utilisée par Fiorilli dans [Fio14a]. La preuve dans le cas général des fonctions L analytiques va en fait fonctionner de la même façon que la preuve des résultats de Fiorilli.

3. Étant donné $L(f, s)$ et $L(g, s)$ deux fonctions L provenant de formes modulaires comme dans le point 2, on peut définir le produit de Rankin–Selberg $L(f \otimes g, s)$ comme la fonction L dont les zéros locaux sont les produits des zéros locaux de $L(f, s)$ et $L(g, s)$. Si $f \neq \overline{g}$, la fonction $L(f \otimes g, s)$ est une fonction L de degré 4 qui satisfait aussi la définition 3.1 (voir [IK04, Chap. 5.1]). Il nous reste à vérifier l'hypothèse 3. On a

$$L((f \otimes g)^{(2)}, s) = \frac{L(\mathrm{Sym}^2 f \otimes \mathrm{Sym}^2 g, s) L(\chi_f \chi_g, s)}{L((\mathrm{Sym}^2 f) \otimes \chi_g, s) L((\mathrm{Sym}^2 g) \otimes \chi_f, s)}$$

où χ_f, χ_g sont les caractères respectivement associés à f et g. Toutes les fonctions dans cette expression se prolongent à un ouvert contenant $\mathrm{Re}(s) = 1$ sans zéro ni pôle ailleurs qu'en 1. On utilise cette propriété dans la sous-section 3.4.4 dans le cas où f et g sont associés à des courbes elliptiques non isogènes.

4. Si on suppose vérifiée la conjecture de Ramanujan–Petersson pour les fonctions L de représentations automorphes cuspidales unitaires de $GL(m)$, $m \geq 1$, on obtient de nouveaux exemples de fonctions L analytiques. En effet l'hypothèse 1 est alors garantie par la conjecture de Ramanujan–Petersson. L'hypothèse 2 est connue dans ce cas : voir [GJ72], [Cog04]. Enfin on peut écrire la fonction $L(\pi^{(2)}, s)$ sous la forme

$$L(\pi^{(2)}, s) = L(\mathrm{Sym}^2 \pi, s) L(\wedge^2 \pi, s)^{-1}.$$

Les deux facteurs du produit sont des fonctions L automorphes comme composées de représentations [Sha97]. De plus [Sha97, Th. 1.1] garantit qu'aucune de ces deux fonctions ne s'annule sur la droite $\mathrm{Re}(s) = 1$. On obtient donc l'hypothèse 3. On revient sur ces exemples généraux dans la sous-section 3.4.3.

Soit $L(f, s)$ une fonction L analytique de degré d selon la définition 3.1. On a pour tout p premier, $\lambda_f(p) = \sum_{j=1}^{d} \alpha_{f,j}(p)$. Si on sait de plus que $L(f, s) = L(\overline{f}, s)$, alors $\lambda_f(p)$ est un nombre réel pour tout p. La conjecture de Sato–Tate généralisée dans ce cadre dit qu'on s'attend à ce que les $(\lambda_f(p))_p$ s'équirépartissent dans l'intervalle $[-d, d]$ suivant une certaine loi définie par un groupe de Sato–Tate associé. Dans ce chapitre on s'intéresse au signe de la fonction $\sum_{p \leq x} \lambda_f(p)$. Cette question a plus d'intérêt si la loi de répartition des $(\lambda_f(p))_p$ est symétrique par rapport à 0, ou au moins si elle a une moyenne nulle. On fait l'hypothèse que la conjecture générale suivante est satisfaite.

Conjecture 3.3 (Sato–Tate généralisée)**.** *Soit $\mathcal{S}$ un ensemble fini stable par conjugaison de fonctions L analytiques au sens de la définition 3.1. On se donne aussi des poids complexes $(a_f)_{f \in \mathcal{S}}$ tels que $a_{\overline{f}} = \overline{a_f}$. Alors la suite $\left(\sum_{f \in \mathcal{S}} a_f \lambda_f(p)\right)_p$ est équirépartie dans un intervalle de $\mathbf{R}$ suivant une loi de Sato–Tate.*

Remarque 37. Dans le cas d'une fonction L de Hasse–Weil associée à une courbe elliptique, la conjecture 3.3 est une version faible de la conjecture de Sato–Tate originelle qui est désormais prouvée ([CHT08], [HSBT10]).

Sous la conjecture 3.3 pour l'ensemble $\mathcal{S}$ avec les poids $(a_f)_{f\in\mathcal{S}}$, et dans le cas où la loi de Sato–Tate a une moyenne nulle, on est naturellement amené à étudier le signe de la fonction

$$x \mapsto \sum_{p\leq x}\sum_{f\in\mathcal{S}} a_f\lambda_f(p).$$

Le but de la section 3.3 est d'utiliser les propriétés des fonctions L analytiques pour étudier ce type de fonctions.

3.1.2 Propriétés des fonctions L analytiques

Présentons quelques conséquences de la définition 3.1, notamment sur les zéros des fonctions L analytiques. Soit $L(f,s)$ une fonction L analytique de degré d. Dans la définition 3.1.2, on associe à $L(f,s)$ un facteur

$$\gamma(f,s) = \pi^{-ds/2}\prod_{j=1}^{d}\Gamma\left(\frac{s+\kappa_j}{2}\right)$$

où les κ_j sont des nombres complexes de partie réelle > -1. Cette hypothèse garantit que la fonction $\gamma(f,s)$ ne s'annule pas sur $\mathbf{C}$ et n'a pas de pôle sur $\mathrm{Re}(s)\geq 1$. Comme la fonction complétée $\Lambda(f,s)$ est supposée holomorphe, les pôles de la fonction $\gamma(f,s)$ sont des zéros de la fonction $L(f,s)$. On appelle ces zéros les « zéros triviaux » de $L(f,s)$, ils sont situés aux points $-2m-\kappa_j$ pour $1\leq j\leq d$ et $m\in\mathbf{N}$.

Les autres zéros de la fonction $L(f,s)$ sont appelés « zéros non-triviaux », ils sont tous situés dans la bande critique $0\leq \mathrm{Re}(s)\leq 1$. L'équation fonctionnelle (3.1) induit des propriétés de symétrie entre les zéros de $L(f,s)$ et ceux de $L(\overline{f},s)$. Précisément si ρ est un zéro de $L(f,s)$, alors $1-\rho$ et $\overline{\rho}$ sont des zéros de $L(\overline{f},s)$. En particulier si $L(\overline{f},s)=L(f,s)$, alors il y a une symétrie centrale de centre $\frac{1}{2}$ ainsi qu'une symétrie par rapport à la droite réelle dans l'ensemble des zéros de $L(f,s)$.

Proposition 3.4. *Soit $L(f,s)$ une fonction L analytique de degré d au sens de la définition 3.1. On a pour tout $\epsilon>0$,*

$$\sum_{\rho,\Lambda(f,\rho)=0}|\rho|^{-1-\epsilon} < +\infty.$$

Plus précisément, on a pour $T\geq 1$,

$$|\{\rho=\beta+i\gamma : L(f,\rho)=0, 0\leq\beta\leq 1, |\gamma|\leq T\}| = \frac{T}{\pi}\log\frac{q(f)T^d}{(2\pi e)^d} + O\left(\log\left(\mathfrak{q}(f)(T+3)^d\right)\right)$$

et

$$|\{\rho=\beta+i\gamma : \Lambda(f,\rho)=0, |T-\gamma|\leq 1\}| \ll \log\left(\mathfrak{q}(f)(T+3)^d\right). \tag{3.2}$$

En particulier on a une borne sur la multiplicité des zéros en fonction de leur partie imaginaire. Les constantes implicites sont absolues.

Démonstration. La première assertion est une conséquence du fait que $\Lambda(f,s)$ est entière d'ordre 1, on applique alors la formule de Jensen (voir par exemple [Rud80, 15.20]) pour obtenir le résultat. Les preuves sont détaillées dans [IK04, 5.3]. □

Grâce aux propriétés de distribution des zéros, on peut déduire une borne sur la dérivée logarithmique d'une fonction L analytique quand on reste à une certaine distance des zéros.

Proposition 3.5. *Soit $L(f,\cdot)$ une fonction L analytique selon la définition 3.1. Pour tout $\delta > 0$, et pour tout $s \in \mathbf{C}$, vérifiant $\mathrm{Re}(s) \leq 2$ et $|s-\rho| > \delta$, pour tout ρ zéro de la fonction L complétée $\Lambda(f,\cdot)$ (voir la défintion 3.1.2) on a*

$$\left|\frac{L'(f,s)}{L(f,s)}\right| \ll \log\left(\mathfrak{q}(f)(|s|+3)^d\right)(|\mathrm{Re}(s)| + d\delta^{-1})$$

où $\mathfrak{q}(f)$ est le conduteur analytique de $L(f,s)$ tel que défini dans la définition 3.1.2 et la constante implicite est absolue.

Démonstration. D'après la définition 3.1.2, la fonction L complétée $\Lambda(f,\cdot)$ est une fonction holomorphe sur $\mathbf{C}$ d'ordre 1. Par le théorème de factorisation de Hadamard [IK04, Th. 5.6], on a

$$-\frac{L'(f,s)}{L(f,s)} = \frac{\gamma'(f,s)}{\gamma(f,s)} - \sum_\rho \frac{1}{s-\rho} + O(\log \mathfrak{q}(f))$$

où la somme est sur l'ensemble des zéros ρ de $\Lambda(f,\cdot)$ et le facteur γ est tel que donné dans la définition 3.1.2 : $\gamma(f,s) = \prod_{j=1}^d \Gamma(\frac{s+\kappa_j}{2})$. Donc on a

$$\frac{\gamma'(f,s)}{\gamma(f,s)} = \sum_{j=1}^d \frac{\Gamma'(\frac{s+\kappa_j}{2})}{2\Gamma(\frac{s+\kappa_j}{2})}.$$

Or la fonction Γ satisfait l'équation fonctionnelle $\Gamma(s+1) = s\Gamma(s)$ en dérivant on obtient $\frac{\Gamma'(s+1)}{\Gamma(s+1)} = \frac{1}{s} + \frac{\Gamma'(s)}{\Gamma(s)}$. On peut donc se ramener à étudier $\frac{\Gamma'(s)}{\Gamma(s)}$ pour $1 < \mathrm{Re}(s) \leq 2$. En effet en itérant le procédé, dans le cas où $\mathrm{Re}\left(\frac{s+\kappa_j}{2}\right) \geq 1$ pour tout j on écrit

$$\frac{\gamma'(f,s)}{\gamma(f,s)} = \sum_{j=1}^d \left(\sum_{k=1}^{\left[\mathrm{Re}\left(\frac{s+\kappa_j}{2}\right)\right]-1} \frac{1}{2}\frac{1}{\frac{s+\kappa_j}{2}-k} + \frac{\Gamma'}{2\Gamma}\left(\frac{s+\kappa_i}{2} - \left[\mathrm{Re}\left(\frac{s+\kappa_j}{2}\right)\right]+1\right)\right)$$

si pour un j on a plutôt $\mathrm{Re}\left(\frac{s+\kappa_j}{2}\right) < 1$, alors on remplace la somme intérieure par $-\sum_{k=\left[\mathrm{Re}\left(\frac{s+\kappa_j}{2}\right)\right]-2}^{0}$. Pour $\mathrm{Re}(z) > 1$ on a $\frac{\Gamma'(z)}{\Gamma(z)} \ll \log|z|$. Donc on en déduit

$$\frac{\gamma'(f,s)}{\gamma(f,s)} \ll d\delta^{-1} + \log\left(\mathfrak{q}(f)(|s|+3)^d\right).$$

Il nous reste à estimer la somme $\sum_\rho \frac{1}{s-\rho}$. On suit pour cela l'idée de la preuve de [IK04, (5.28)]. Soit $s = \sigma + it$ satisfaisant les hypothèses de la proposition 3.5. On a

$$\begin{aligned}\sum_\rho \frac{1}{s-\rho} &= \sum_\rho \left(\frac{1}{s-\rho} - \frac{1}{3+it-\rho}\right) + \sum_\rho \frac{1}{3+it-\rho} \\ &= \sum_\rho \left(\frac{1}{s-\rho} - \frac{1}{3+it-\rho}\right) + O(\log(\mathfrak{q}(f)(|t|+3)^d))\end{aligned}$$

d'après [IK04, (5.32)]. De plus pour chaque $\rho = \beta + i\gamma$ zéro de $\Lambda(f,\cdot)$, on a

$$\begin{aligned}\left|\frac{1}{s-\rho} - \frac{1}{3+it-\rho}\right| &\leq \left|\frac{3-\sigma}{(3-\beta)(\sigma-\beta) - (t-\gamma)^2 + i(3+\sigma-2\beta)(t-\gamma)}\right| \\ &\ll \frac{|\sigma|+1}{|2(\sigma-\beta)-(t-\gamma)^2|}\end{aligned}$$

avec une constante implicite absolue. Si $\sigma < -1/2$, on en déduit

$$|2(\sigma-\beta)-(t-\gamma)^2| \geq 1+(t-\gamma)^2.$$

En utilisant de nouveau [IK04, (5.32)], on obtient

$$\sum_{\rho} \frac{1}{s-\rho} \ll (|\mathrm{Re}(s)|+1)\log(\mathfrak{q}(f)(|t|+3)^d)$$

avec une constante implicite absolue. Dans le cas où $-1/2 \leq \sigma < 2$, on a

$$\left|\frac{1}{s-\rho}-\frac{1}{3+it-\rho}\right| \ll \frac{1}{\delta+(t-\gamma)^2}.$$

On coupe la somme en deux selon si $|t-\gamma|$ est ≤ 1 ou > 1 et on utilise (3.2). On obtient

$$\sum_{\rho} \frac{1}{s-\rho} \ll \delta^{-1}\log(\mathfrak{q}(f)(|t|+3)^d)$$

avec une constante implicite absolue. On a donc le résultat annoncé.

□

3.1.3 Hypothèses supplémentaires sur les zéros non triviaux

Dans le cas des fonctions L de l'exemple 12, on rajoute souvent des hypothèses sur les zéros non triviaux pour obtenir des résultats plus forts. Nous présentons dans cette partie quelques conjectures usuelles dans des versions plus ou moins faibles.

Hypothèse de Riemann

L'hypothèse la plus souvent faite sur les zéros des fonctions L est l'hypothèse de Riemann généralisée. On pense que les zéros non triviaux d'une fonction L devraient tous se trouver sur la droite $\mathrm{Re}(s) = 1/2$.

Conjecture 3.6 (GRH)**.** *Soit $L(f,s)$ une fonction L analytique, alors si ρ est un zéro non trivial de $L(f,s)$ on a $\mathrm{Re}(\rho) = \frac{1}{2}$.*

Dans ce chapitre, on ne suppose pas en général que l'hypothèse de Riemann est vérifiée. On introduit alors la notation

$$\beta_{f,0} = \sup\{\mathrm{Re}(\rho) : L(f,\rho) = 0\}$$

et plus généralement dans le cas d'un ensemble fini $\mathcal{S}$ de fonctions L analytiques

$$\beta_{\mathcal{S},0} = \sup\{\mathrm{Re}(\rho) : \exists f \in \mathcal{S}, L(f,\rho) = 0\}.$$

Alors on a $\frac{1}{2} \leq \beta_{f,0} \leq 1$ et le fait que l'hypothèse de Riemann est satisfaite pour la fonction $L(f,s)$ est équivalent à $\beta_{f,0} = \frac{1}{2}$.

Remarque 38. On pense que si l'hypothèse de Riemann n'est pas satisfaite pour $L(f,s)$, alors $\beta_{f,0} = 1$ et la borne supérieure n'est pas atteinte. Cependant cette situation n'est pas satisfaisante pour les calculs que l'on veut faire : notre objet d'étude se réduit à l'ensemble vide. En général, on imaginera que $\beta_{f,0}$ est atteint (i.e. que la borne supérieure est un maximum), comme le suppose Fiorilli [Fio14a, Hyp. LI(E)].

On utilisera alors dans la suite une notation pour l'ensemble des zéros de partie réelle maximale. Dans le cas d'un ensemble fini $\mathcal{S}$ de fonctions L analytiques, on note

$$\mathcal{Z}_{\mathcal{S}} = \{\gamma > 0 : \exists f \in \mathcal{S}, L(f, \beta_{\mathcal{S},0} + i\gamma) = 0\}, \qquad \mathcal{Z}_{\mathcal{S}}(T) = \mathcal{Z}_{\mathcal{S}} \cap]0, T],$$

les multi-ensembles de zéros de partie réelle maximale comptés avec multiplicités. Dans le cas où on ne veut pas prendre en compte les multiplicités, on rajoute une $*$ en exposant. On note $\mathcal{Z}_{\mathcal{S}}^*$ et $\mathcal{Z}_{\mathcal{S}}^*(T)$ les ensembles associés aux multi-ensembles ci-dessus. De la même façon que précédemment, quand l'ensemble $\mathcal{S}$ est un singleton $\{f\}$, on notera seulement un f en indice au lieu de $\{f\}$. Suivant l'idée de la remarque 38, on imagine que ces ensembles ne sont pas vides même si $\beta_0 > 1/2$. D'après la discussion sur la symétrie de l'ensemble des zéros, il suffit de connaître les zéros de partie imaginaire positive pour connaître tous les zéros de partie réelle maximale.

Dans le cas où l'on ne veut pas supposer l'hypothèse de Riemann, on peut supposer des résultats plus faibles. On imagine que les zéros hors de la droite $\mathrm{Re}(s) = \frac{1}{2}$ sont très peu nombreux. On formalise cette idée grâce à des théorèmes de type « théorème de densité zéro ».

Définition 3.7. Soit $L(f, s)$ une fonction L analytique. On appelle un théorème de densité zéro (Zero Density Theorem) pour $L(f, s)$, un résultat qui garantit que les zéros de $L(f, s)$ hors de la droite $\mathrm{Re}(s) = 1/2$ forment un ensemble de densité nulle dans l'ensemble des zéros de $L(f, s)$, pour une notion de densité choisie (voir les définitions 1 et 2).

On utilisera la conjecture suivante qui ne traite que des zéros de partie réelle maximale.

Conjecture 3.8 (ZD)**.** *Soit $L(f, s)$ une fonction L analytique. Dans le cas où $\beta_{f,0} > \frac{1}{2}$, on a pour tout $\epsilon > 0$*

$$|\mathcal{Z}_f(T)| \ll_\epsilon T^{1-\epsilon}.$$

En particulier la somme $\sum_{\gamma \in \mathcal{Z}_f} \frac{1}{|\beta_0 + i\gamma|}$ est finie.

Remarque 39. En comparant la conjecture 3.8 à la proposition 3.4, on déduit bien que l'ensemble des zéros de partie réelle maximale doit être de densité zéro si l'hypothèse de Riemann n'est pas satisfaite.

Pour plus de détails et de précisions sur les théorèmes de densité zéro pour la fonction ζ de Riemann ainsi que pour les fonctions L de Dirichlet on pourra voir le chapitre consacré dans le livre de Iwaniec et Kowalski [IK04, chap. 10]. Citons tout de même dans le cas de la classe de Selberg le résultat suivant [KP03, Lem. 3].

Théorème 3.9 (Kaczorowski–Perelli)**.** *Soit $L(f, s)$ une fonction de la classe de Selberg de degré d. Soit $\epsilon > 0$. On a*

$$|\{\rho = \beta + i\gamma : L(f, \rho) = 0, \beta \geq \sigma, |\gamma| \leq T\}| \ll_\epsilon T^{4(d+3)(1-\sigma)+\epsilon}$$

quand $T \to \infty$ uniformément pour $\frac{1}{2} \leq \sigma \leq 1$.

En particulier, si $\beta_{f,0} \geq 1 - \frac{1}{4(d+3)}$ alors la conjecture 3.8 est satisfaite pour $L(f, s)$.

Indépendance linéaire

Il est courant (suivant le travail de Rubinstein–Sarnak) quand il est question de biais de Chebyshev de faire des hypothèses d'indépendance linéaire entre les zéros des fonctions L utilisées. Dans le cas de [RS94], cette hypothèse prend la forme forte suivante.

Conjecture 3.10 (LI)**.** *Soit $\mathcal{S}$ un ensemble fini de fonctions L analytiques. Le multi-ensemble $\mathcal{Z}_{\mathcal{S}}$ est linéairement indépendant sur $\mathbf{Q}$.*

Remarque 40. Cette conjecture suit la philosophie suivant laquelle les zéros d'une fonction L devraient être des nombres réels « au hasard ». On remarque que cette conjecture implique que les zéros de chaque $L(f,s), f \in \mathcal{S}$ sont tous simples.

On peut affaiblir cette conjecture en autorisant des multiplicités.

Conjecture 3.11 (LI*)**.** *Soit $\mathcal{S}$ un ensemble fini de fonctions L analytiques. L'ensemble $\mathcal{Z}_{\mathcal{S}}^*$ est linéairement indépendant sur* $\mathbf{Q}$*.*

Dans l'optique d'affaiblir ces hypothèses, nous utiliserons la notion de zéros « autonomes » (self-sufficient) telle qu'introduite par Martin et Ng dans leur travail en cours [MN]. Ainsi qu'une version un peu plus faible dépendante de certains paramètres.

Définition 3.12.
1. Soit $\gamma \in \mathcal{Z}_{\mathcal{S}}^*$, on dit que γ est autonome s'il n'est pas dans le $\mathbf{Q}$-espace vectoriel engendré par les combinaisons linéaires finies de $\mathcal{Z}_{\mathcal{S}}^* - \{\gamma\}$.
2. Soient $U, V > 0$, alors $\gamma \in \mathcal{Z}_{\mathcal{S}}^*(U)$ est (U,V)-autonome s'il n'est pas dans le $\mathbf{Q}$-espace vectoriel engendré par $\mathcal{Z}_{\mathcal{S}}^*(V) - \{\gamma\}$.

Remarque 41. Un zéro autonome est clairement (U,V)-autonome pour tous U, V assez grands.

La conjecture 3.11 revient à dire que tous les zéros sont autonomes. Une version un peu plus faible de cette conjecture pourrait donc être la conjecture suivante.

Conjecture 3.13. *Soit $\mathcal{S}$ un ensemble fini de fonctions L analytiques. On a*

$$\sum_{\substack{\gamma \in \mathcal{Z}_{\mathcal{S}}^* \\ \gamma \text{ autonome}}} \frac{1}{\gamma} = +\infty.$$

Remarque 42.
1. Martin et Ng ont utilisé la notion de zéro autonome pour énoncer la conjecture 3.13. Sous cette hypothèse ils parviennent à montrer que chaque concurrent est en tête de la course une infinité de fois dans le cadre des courses dans les classes de congruences modulo un entier.
2. Cette conjecture n'est pas compatible avec la conjecture 3.8 dans le cas où l'hypothèse de Riemann n'est pas vérifiée.

On utilisera aussi dans ce chapitre l'hypothèse plus faible que la conjecture 3.11 suivante.

Conjecture 3.14. *Soit $\mathcal{S}$ un ensemble fini de fonctions L analytiques. On a pour toute combinaison linéaire finie à coefficients dans* $\mathbf{Z}$ *:*

$$\sum_{\gamma \in \mathcal{Z}_{\mathcal{S}}} k_\gamma \gamma = 0 \Rightarrow \sum_{\gamma \in \mathcal{Z}_{\mathcal{S}}} k_\gamma \equiv 0 \ [\mathrm{mod}\ 2].$$

3.2 Le biais de Chebyshev et les premières généralisations

3.2.1 Courses de nombres premiers dans les classes de congruences modulo un entier

L'idée des biais de Chebyschev remonte à la lettre [Che99] écrite par Chebyshev à Fuss dans laquelle il remarque qu'il semble y avoir souvent plus de premiers congrus à 3 [mod 4] qu'à 1 [mod 4] dans les intervalles d'entiers $[2,x]$. Une telle remarque peut se vérifier en étudiant le signe de la fonction $x \mapsto \sum_{p \leq x} \left(\frac{-1}{p}\right)$, où $\left(\frac{-1}{p}\right)$ est le symbole de Legendre.

Cette étude a été généralisée et approfondie par Rubinstein et Sarnak. Dans [RS94] les auteurs étudient le cas général de courses à plusieurs participants dans les classes de

congruences modulo un entier q fixé. Restons dans la situation à deux concurrents. Étant donné a, b deux classes inversibles modulo q, on veut savoir si pour les premiers dans l'intervalle $[2, x]$ une classe est favorisée par rapport à l'autre. Une façon de répondre à cette question est d'étudier les ensembles $\{x : \pi(x; q, a) > \pi(x; q, b)\}$ où pour c une classe inversible modulo q, on note $\pi(x; q, c) := |\{p \leq x : p \equiv c \ [\text{mod } q]\}|$.

De façon générale, on veut étudier l'ensemble des x pour lesquels une certaine fonction $E(x)$ est positive. Une première question est de savoir si cet ensemble est non-vide, si c'est le cas on se demande s'il est infini, puis s'il a une densité positive. Suivant les travaux de Wintner sur le terme de reste dans le théorème des nombres premiers [Win35], [Win41], l'objet naturel à étudier ici est la distribution logarithmique limite de la fonction normalisée $E(x)$. Cette notion a été reprise par Rubinstein et Sarnak pour étudier le biais dans le cas des courses de premiers dans les classes de congruences modulo q, elle a ensuite été beaucoup réutilisée dans des versions plus générales de courses de nombres premiers.

Définition 3.15. Soit E une fonction sur $\mathbf{R}$ à valeurs réelles, on dit que E admet une distribution logarithmique limite μ si pour toute fonction g continue bornée et lipschitzienne sur $\mathbf{R}$ on a

$$\lim_{Y\to\infty} \frac{1}{Y} \int_2^Y g(E(e^y))dy = \int_{\mathbf{R}} g(t)d\mu(t). \tag{3.3}$$

Kaczorowski a prouvé par des calculs numériques [Kac95] que l'ensemble

$$\{x : \pi(x; 4, 3) > \pi(x; 4, 1)\}$$

n'a pas de densité naturelle (au sens de la définition 1). On peut tout de même chercher si de tels ensembles ont une densité logarithmique. En effet, on sait par exemple que l'ensemble des premiers dont le premier chiffre est 1 admet une densité logarithmique mais pas de densité naturelle, cet exemple est cité dans [Ser70] comme communiqué par Bombieri (on pourra aussi voir [FL96]). Rappelons la définition de densité logarithmique que l'on utilise dans ce chapitre.

Définition 3.16. On reprend les notations de la définition 3.15. Soit

$$\overline{\delta}(E) = \limsup_{Y\to\infty} \frac{1}{Y} \int_2^Y \mathbf{1}_{\geq 0}(E(e^y))dy$$

et

$$\underline{\delta}(E) = \liminf_{Y\to\infty} \frac{1}{Y} \int_2^Y \mathbf{1}_{\geq 0}(E(e^y))dy.$$

Si ces deux densités sont égales, on note $\delta(E)$ leur valeur commune. Ces quantités permettent de mesurer le biais de $E(x)$ vers les valeurs positives.

Cette définition est une version continue de la définition 2, il suffit de faire le changement de variable $x = e^y$, $X = e^Y$.

Définition 3.17. Si $\delta(E)$ existe et est $> \frac{1}{2}$ on dit qu'il y a un biais vers les valeurs positives. Si on a $\delta(E) < \frac{1}{2}$ on dit qu'il y a un biais vers les valeurs négatives.

Remarque 43. On remarque que si E admet une distribution limite μ qui a de bonnes propriétés de régularité — par exemple si μ est absolument continue par rapport à la mesure de Lebesgue — alors $\delta(E)$ existe et vaut $\mu(0, +\infty)$.

Remarque 44. Rubinstein et Sarnak donnent en fait des définitions plus générales dans le cas de fonctions à valeurs dans $\mathbf{R}^r$, mais nous n'étudierons ici que le cas de courses à deux concurrents. Dans ce cas, on peut comparer les deux concurrents directement donc les fonctions à valeurs dans $\mathbf{R}$ suffisent.

Dans ce cadre et conditionnellement à GRH (conjecture 3.6) et LI (conjecture 3.10) pour les fonctions L de Dirichlet de caractères modulo q, Rubistein et Sarnak montrent [RS94, Th. 1.4] que les courses de nombres premiers dans les classes de congruences modulo q sont toujours biaisées sauf dans deux cas particuliers : la course à deux concurrents qui ont le même nombre de racines carrées modulo q, et la course à trois concurrents a_1, a_2, a_3 qui vérifient $a_2 = \rho a_1 \pmod q$, $a_3 = \rho^2 a_1 \pmod q$ pour $\rho \neq 1 \pmod q$ vérifiant $\rho^3 = 1 \pmod q$. Ils prouvent sous les mêmes hypothèses que le biais se dissipe lorsque q tend vers $+\infty$ [RS94, Th. 1.5]. En particulier, dans le cas des courses à deux concurrents, ils montrent que la course est biaisée en direction de la classe qui n'est pas un carré modulo q. Cela confirme et explique l'observation de Chebyshev, pour laquelle ils font le calcul numérique de la densité logarithmique.

Ces résultats se basent sur une version générale du théorème de Kronecker-Weyl (voir par exemple [Hum]).

Théorème 3.18 (Kronecker–Weyl)**.** *Soient $t_1, \dots, t_N$ des nombres réels quelconques. Soit A l'adhérence topologique du groupe à 1 paramètre $\{y(t_1, \dots, t_N), y \in \mathbf{R}\}/\mathbf{Z}^N$ dans le tore $\mathbf{T}^N$. Pour tout fonction continue $h : \mathbf{T}^N \to \mathbf{R}$, on a*

$$\lim_{Y\to\infty} \frac{1}{Y} \int_0^Y h(yt_1, \dots, yt_N)dy = \int_A h(a)d\omega_A \tag{3.4}$$

où ω_A est la mesure de Haar normalisée sur A.

On peut trouver dans [FM13] plus de précisions sur le biais obtenu dans le cas général d'une course à deux concurrents dans les classes de congruences modulo un entier q toujours sous GRH et LI. À propos des courses dans les classes de congruences modulo q avec plusieurs concurrents, on pourra aussi voir le survol [GM06]. Inconditionnellement à GRH, Ford et Konyagin ont montré ([FK02]) que certains zéros des fonctions L de Dirichlet hors de la droite critique $\mathrm{Re}(s) = \frac{1}{2}$ pouvaient créer des courses avec un biais extrême (égal à 0 ou à 1). Martin et Ng travaillent actuellement ([MN]) sur le support de la distribution limite associée à une course à plusieurs concurrents modulo q sous des hypothèses plus faibles que LI. Ils ont notamment des résultats conditionnels à la conjecture 3.13.

En restant dans le cadre des courses de premiers dans les classes de congruences modulo q, on peut faire des courses à deux concurrents dont les concurrents sont des ensembles de classes de congruence. On étudie alors le signe d'une fonction

$$x \mapsto \frac{1}{|A|}\pi(x; q, A) - \frac{1}{|B|}\pi(x; q, B)$$

où A et B sont des sous-ensembles de $(\mathbf{Z}/q\mathbf{Z})^*$. Un cas classique étudié par Rubinstein et Sarnak est celui de la course entre les résidus quadratiques $R = \{a \pmod q : \exists x \pmod q, x^2 \equiv a \pmod q\}$ et les non-résidus quadratiques $NR = \{a \pmod q : \forall x \pmod q, x^2 \not\equiv a \pmod q\}$ modulo q. Cette étude a été poursuivie par Fiorilli dans [Fio14b] où sont exhibées des courses dont le biais est arbitrairement proche de 1.

3.2.2 Généralisations à l'étude d'autres termes d'erreur

L'étude du biais de Chebyshev dans sa version originelle repose sur le second terme dans le théorème de Dirichlet sur l'équirépartition des nombres premiers dans les progressions arithmétiques. Dans le cas où on a des données arithmétiques avec un théorème d'équirépartition — par exemple du type de la conjecture 3.3 — on peut aussi étudier le biais associé.

Cette idée a été proposée par Mazur dans son article de survol sur les termes d'erreurs en arithmétique [Maz08]. Il y propose d'étudier la questions des courses de nombres premiers pour les nombres de $\mathbf{F}_p$-points de courbes elliptiques ou plus généralement pour

les coefficients de formes modulaires. Plus précisément il trace les graphes de fonctions du type

$$x \mapsto |\{p \leq x, a_p(E) > 0\}| - |\{p \leq x, a_p(E) < 0\}|$$

où $a_p(E) = p + 1 - |E(\mathbf{F}_p)|$, pour diverses courbes elliptiques E sur $\mathbf{Q}$. Il observe alors une possible corrélation entre le rang algébrique de la courbe elliptique et le biais de la course entre les premiers pour lesquels $a_p(E) > 0$ et ceux pour lesquels $a_p(E) < 0$. Il semble que plus le rang algébrique est grand, plus la course est biaisée vers les valeurs négatives.

Cependant une telle observation est difficile à justifier théoriquement. En effet Sarnak a proposé un cadre pour justifier l'observation de Mazur dans sa lettre [Sar07]. Pour cela il est nécessaire d'étudier les zéros de toutes les puissances symétriques $L(\mathrm{Sym}^n E, s)$ $(n \geq 1)$ de la fonction de Hasse–Weil de la courbe elliptique $E/\mathbf{Q}$, en supposant l'hypothèse LI dans toute la famille (infinie).

Sarnak propose d'étudier une fonction plus simple : $\sum_{p \leq x} \frac{a_p(E)}{\sqrt{p}}$. Le signe de cette fonction peut être étudié en ne connaissant que des propriétés de la fonction de Hasse–Weil $L(E, s)$. Pour cette course, Sarnak a expliqué l'observation de Mazur sur le lien entre le biais et le rang analytique de la courbe elliptique conditionnellement à GRH et LI (en supposant aussi la conjecture de Birch et Swinnerton-Dyer, on a donc le lien entre le biais et le rang algébrique de la courbe elliptique).

Les idées de la lettre de Sarnak on été reprises par Fiorilli dans [Fio14a]. Fiorilli exhibe des courses pour les courbes elliptiques arbitrairement biaisées sous des hypothèses plus faibles que GRH et LI. Les raisonnements ne dépendent pas du fait que la fonction étudiée vient d'une courbe elliptique sur $\mathbf{Q}$, mais seulement des propriétés analytiques que cela induit sur la fonction L associée. On peut généraliser ces résultats à des fonctions L satisfaisant des propriétés similaires. C'est ce qui motive notre définition 3.1.

3.3 Une course pour des coefficients de fonctions L générales

Dans cette section on se fixe un ensemble fini stable par conjugaison $\mathcal{S}$ de fonctions L analytiques selon la définition 3.1, ainsi que des poids complexes $(a_f)_{f \in \mathcal{S}}$ vérifiant pour tout $f \in \mathcal{S}$, $a_{\overline{f}} = \overline{a_f}$. On veut étudier le signe de la fonction

$$x \mapsto \frac{\log x}{x^{\beta_{\mathcal{S},0}}} \sum_{p \leq x} \sum_{f \in \mathcal{S}} a_f \lambda_f(p).$$

On va montrer qu'une bonne normalisation de cette fonction admet une distribution limite dont on sait calculer la moyenne et la variance en fonction des zéros des fonctions L de l'ensemble $\mathcal{S}$.

Commençons par introduire une notation pour les multiplicités des zéros et pôles. Soit L une fonction méromorphe au voisinage d'un point ρ. On note $m(L, \rho)$ la multiplicité du zéro de L au point $s = \rho$. (On a $m(L, \rho) = 0$ si $L(\rho) \neq 0$, $m(L, \rho) > 0$ si $L(\rho) = 0$ et $m(L, \rho) < 0$ si L a un pôle en $s = \rho$.)

Le résultat principal de cette section est le théorème suivant qui est une généralisation de [Fio14a, Lem. 3.4].

Théorème 3.19. *Soit $\mathcal{S}$ un ensemble fini de fonctions L analytiques vérifiant $\overline{\mathcal{S}} = \mathcal{S}$, et soit $(a_f)_{f \in \mathcal{S}}$ un ensemble de nombres complexes vérifiant $a_{\overline{f}} = \overline{a_f}$. On pose*

$$E_{\mathcal{S}}(x) = \frac{\log x}{x^{\beta_{\mathcal{S},0}}} \sum_{p \leq x} \sum_{f \in \mathcal{S}} a_f \lambda_f(p).$$

La fonction $E_{\mathcal{S}}(x)$ admet une distribution logarithmique limite $\mu_{\mathcal{S}}$ (voir définition 3.15).

Il existe C une constante positive (dépendante de $\mathcal{S}$) telle que pour tout A, on a

$$\mu_{\mathcal{S}}(\mathbf{R} - [-A, A]) \ll \exp(-C\sqrt{A}).$$

De plus soit $X_{\mathcal{S}}$ une variable aléatoire de loi $\mu_{\mathcal{S}}$, alors on connaît l'espérance et la variance de $X_{\mathcal{S}}$: on a

$$\mathbb{E}(X_{\mathcal{S}}) = m_{\mathcal{S}} := \sum_{f\in\mathcal{S}} a_f \left(m(L(f^{(2)}, \cdot), 1)\delta_{\beta_{\mathcal{S},0}=1/2} - \beta_{\mathcal{S},0}^{-1} m(L(f, \cdot), \beta_{\mathcal{S},0}) \right),$$

et

$$\mathrm{Var}(X_{\mathcal{S}}) = 2 \sum_{\gamma\in\mathcal{Z}_{\mathcal{S}}^*} \frac{|M_{\mathcal{S}}(\gamma)|^2}{(\beta_{\mathcal{S},0}^2 + \gamma^2)}$$

où on note $M_{\mathcal{S}}(\gamma) := \sum_{f\in\mathcal{S}} a_f m(L(f, \cdot), \beta_{\mathcal{S},0} + i\gamma)$, pour $\gamma \in \mathcal{Z}_{\mathcal{S}}^*$.

Remarque 45. La valeur de la moyenne donne une idée de la direction du biais. Il est naturel de penser (quand la variance n'est pas trop grande) que si la moyenne est non nulle alors la distribution est concentrée autour de sa moyenne. Cette idée est fausse en toute généralité. Il faut bien sur préciser la taille de la variance ; cela pourra se faire à l'aide d'une inégalité de Chebyshev. On note aussi que si la distribution est symétrique par rapport à sa moyenne (voir la sous-section 3.5.2) ou si la distribution admet une densité qui ne s'annule pas sur des ouverts (voir le théorème 3.36.4) alors ce principe est plus proche de la vérité. On a tout de même tendance à penser que si le biais existe, il est en faveur des valeurs du même signe que la moyenne.

On prouvera ce théorème grâce à la proposition suivante qui lie plus directement la distribution $\mu_{\mathcal{S}}$ aux zéros des fonctions L de l'ensemble $\mathcal{S}$.

Proposition 3.20. *Soit $T > 2$ et*

$$G_{\mathcal{S},T}(x) = m_{\mathcal{S}} - \sum_{\gamma\in\mathcal{Z}_{\mathcal{S}}^*(T)} 2\,\mathrm{Re}\left(M_{\mathcal{S}}(\gamma) \frac{x^{i\gamma}}{\beta_{\mathcal{S},0} + i\gamma} \right).$$

La fonction $G_{\mathcal{S},T}(x)$ a une distribution logarithmique limite $\mu_{\mathcal{S},T}$. De plus pour toute fonction g continue bornée et lipschitzienne, on a

$$\lim_{T\to\infty} \int_{\mathbf{R}} g(t) d\mu_{\mathcal{S},T}(t) = \int_{\mathbf{R}} g(t) d\mu_{\mathcal{S}}(t).$$

On verra la preuve de l'existence de $\mu_{\mathcal{S},T}$ dans la sous-section 3.3.6. C'est une conséquence du théorème de Kronecker–Weyl (théorème 3.18).

Remarque 46.

1. Dans la situation où l'ensemble $\mathcal{Z}_{\mathcal{S}}$ est vide (voir la remarque 38 à ce sujet), les fonctions $G_{\mathcal{S},T}(x)$ sont constantes et ne dépendent pas de T. La proposition 3.20 et le théorème 3.19 deviennent assez peu intéressants dans ce cas. Les distributions logarithmiques limites $\mu_{\mathcal{S},T}$ et $\mu_{\mathcal{S}}$ sont égales au poids de Dirac $\delta_{m_{\mathcal{S}}}$.
2. En particulier dans le cas où $\beta_{\mathcal{S},0} = 1$ et n'est pas atteint, l'ensemble $\mathcal{Z}_{\mathcal{S}}$ est vide et la distribution logarithmique limite est δ_0. Donc l'information que nous donne le théorème 3.19 est $E_{\mathcal{S}}(x) = o(1)$ ce qui est correct mais déjà connu.
3. Un résultat similaire a déjà été obtenu dans [ANS14]. L'idée est de voir les fonctions $G_{\mathcal{S},T}(e^y)$ comme des polynômes trigonométriques qui approchent la fonction $E_{\mathcal{S}}(e^y)$ lorsque $T \to \infty$. Cependant le résultat de [ANS14] est conditionnel à GRH, tandis que dans notre situation les parties réelles des zéros peuvent varier.

Commençons la preuve du théorème 3.19. On remarque que mis à part le cas de la variance, les assertions que l'on veut démontrer sont stables par linéarité. On ne prouve donc ces assertions que dans le cas où $\mathcal{S}$ est un singleton $\{f\}$ et $a_f = 1$. On reviendra au cas général pour le calcul de la variance dans la sous-section 3.3.7. La preuve suit essentiellement les idées de Fiorilli pour la preuve de [Fio14a, Lem. 3.4]. On ne donne donc pas toujours tous les détails classiques. On tente de garder la dépendance en f pour chacune des bornes car on a dans l'idée de faire varier la fonction L. On donne plus de détails là-dessus dans la sous-section 3.3.8.

3.3.1 Approximation de $\psi(f, x)$

Le résultat que l'on veut prouver est lié au second terme du développement asymptotique dans un résultat du type théorème des nombres premiers pour une fonction L générale. Il est classique dans le cadre de tels résultats de commencer par étudier la fonction associée

$$\psi(f, x) = \sum_{k=1}^{\infty} \sum_{p^k \leq x} \left(\sum_{j=1}^{d} \alpha_j(p)^k \right) \log p.$$

Cette fonction est liée à la dérivée logarithmique de $L(f, s)$. Pour $\mathrm{Re}(s) > 1$, on a

$$-\frac{L'(f, s)}{L(f, s)} = \sum_{k=1}^{\infty} \sum_{p} \left(\sum_{j=1}^{d} \alpha_j(p)^k \right) p^{-ks} \log p =: \sum_{n=1}^{\infty} \Lambda_f(n) n^{-s}.$$

La formule de Perron et le théorème des résidus après intégration sur un chemin entourant certains zéros nous fournissent une formule explicite pour $\psi(f, x)$.

Lemme 3.21. *Soit $L(f, \cdot)$ une fonction L analytique, alors*

$$\psi(f, x) = - \sum_{\substack{L(f,\rho)=0 \\ |\mathrm{Im}(\rho)| \leq T}} \frac{x^\rho}{\rho} + R(f, x, T)$$

où

$$R(f, x, T) = O\left(d \log x + d \frac{x}{T} (\log x)^2 + d x^{-1/4} \log x \left(\log(\mathfrak{q}(f) T^d) \right)^2 + \frac{d \log(\mathfrak{q}(f) T^d)}{T} x \right),$$

avec une constante implicite absolue.

Démonstration. D'après la formule de Perron (voir par exemple [MV07, Cor. 5.3]), on a pour terme principal

$$\frac{1}{2i\pi} \int_{c-iT}^{c+iT} -\frac{L'(f, s)}{L(f, s)} x^s \frac{ds}{s}$$

pour $c > 1$. On choisit $c = 1 + \frac{1}{\log x}$. Le terme d'erreur est

$$O\left(\sum_{x/2 < n < 2x} |\Lambda_f(n)| \min\left(1, \frac{x}{T|x - n|}\right) + \frac{(4x)^c}{T} \sum_{n=1}^{\infty} \frac{|\Lambda_f(n)|}{n^c} \right).$$

Commençons par simplifier le terme d'erreur. D'après la définition 3.1.1, la conjecture de Ramanujan–Petersson est vérifiée pour $L(f, s)$ donc, pour tout n, on a $|\Lambda_f(n)| \leq d\Lambda(n)$

où Λ est la fonction de von Mangoldt habituelle. En particulier pour $x/2 < n < 2x$, on a $\Lambda_f(n) \leq d \log 2x$. D'où pour $x \geq 2$,

$$\sum_{x/2<n<2x} |\Lambda_f(n)| \min\left(1, \frac{x}{T|x-n|}\right) \ll d \log x \left(1 + \sum_{k<x} \frac{x}{Tk}\right)$$
$$\ll d \log x + d\frac{x}{T}(\log x)^2.$$

Pour le second terme on utilise la même majoration grâce à la fonction de von Mangoldt. On majore la somme du second terme par $d\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^c} = d\frac{\zeta'(c)}{\zeta(c)}$ où ζ est la fonction zêta de Riemann. Comme celle-ci a un pôle simple en 1 on trouve $\frac{\zeta'(c)}{\zeta(c)} \ll \frac{1}{c-1}$ pour $c > 1$. Comme $c = 1 + \frac{1}{\log x}$, on a

$$\frac{(4x)^c}{T} \sum_{n=1}^{\infty} \frac{|\Lambda_f(n)|}{n^c} \ll d\frac{x}{T} \log x.$$

On a ainsi obtenu pour $x \geq 2$,

$$\psi(f,x) = \frac{1}{2i\pi} \int_{c-iT}^{c+iT} -\frac{L'(f,s)}{L(f,s)} x^s \frac{ds}{s} + O\left(d \log x + d\frac{x}{T}(\log x)^2\right). \tag{3.5}$$

Revenons au terme principal, on calcule l'intégrale en utilisant le théorème des résidus le long du chemin rectangulaire formé par les droites $\mathrm{Re}(s) = c$, $\mathrm{Im}(s) = \pm T$, $\mathrm{Re}(s) = -\frac{1}{4}$ parcouru en sens trigonométrique et qui évite les zéros à distance au moins $(\log x)^{-1}$ (quitte à déplacer légèrement le chemin). On a donc une somme sur les zéros (non-triviaux) de partie imaginaire inférieure à T en valeur absolue et une intégrale que l'on peut borner grâce à la proposition 3.5. Plus précisément, l'intégrale sur le segment vertical entre $-\frac{1}{4} - iT$ et $-\frac{1}{4} + iT$ est majorée par

$$\frac{1}{2\pi} \int_{-\frac{1}{4}-iT}^{-\frac{1}{4}+iT} \left|\frac{L'(f,s)}{L(f,s)} x^{-\frac{1}{4}} \frac{ds}{s}\right| \ll x^{-\frac{1}{4}} \int_{-T}^{T} \log\left(\mathfrak{q}(f)(|t|+3)^d\right) \left(\frac{1}{4} + d\log x\right) \frac{dt}{|t| + \frac{1}{4}}$$
$$\ll dx^{-\frac{1}{4}} \log x \left(\log\left(\mathfrak{q}(f)T^d\right)\right)^2.$$

Sur les segments horizontaux entre $-\frac{1}{4} \pm iT$ et $c \pm iT$ on a

$$\frac{1}{2\pi} \int_{-\frac{1}{4}\pm iT}^{c\pm iT} \left|\frac{L'(f,s)}{L(f,s)} x^s \frac{ds}{s}\right| \ll \frac{1}{T} \int_{-\frac{1}{4}}^{c} \log\left(\mathfrak{q}(f)(|\sigma|+T)^d\right) (|\sigma| + d\log x) x^\sigma d\sigma$$
$$\ll d\frac{x \log x \log\left(\mathfrak{q}(f)T^d\right)}{T \log x}.$$

Cela permet de conclure. (On peut aussi voir [IK04, Chap. 5, Ex. 7].) □

Remarque 47. Le lemme 3.21 n'est intéressant que dans le cas où T n'est pas trop grand par rapport à x. Le choix $T = x$ nous donne

$$\psi(f,x) = -\sum_{\substack{L(f,\rho)=0 \\ |\mathrm{Im}(\rho)|\leq x}} \frac{x^\rho}{\rho} + O\left(d\left(\log(\mathfrak{q}(f)x^d)\right)^2\right). \tag{3.6}$$

Donnons une forme plus générale. Soient x et T fixés quelconques. On sépare la somme sur les zéros de l'expression (3.6) de la façon suivante :

$$\sum_{\substack{L(f,\rho)=0 \\ |\mathrm{Im}(\rho)|\leq x}} = \sum_{\substack{L(f,\rho)=0 \\ |\mathrm{Im}(\rho)|\leq T}} + \sum_{\substack{L(f,\rho)=0 \\ |\mathrm{Im}(\rho)|> T}} - \sum_{\substack{L(f,\rho)=0 \\ |\mathrm{Im}(\rho)|> x}} =: \Sigma_1 + \Sigma_2 - \Sigma_3. \tag{3.7}$$

On va alors étudier chacune de ces sommes séparément dans la suite afin de déterminer le terme principal et évaluer les termes d'erreurs.

3.3.2 Majoration de Σ_3

On généralise [Fio14a, Lem. 2.1].

Lemme 3.22. *Soit $L(f,s)$ une fonction L analytique et soit $x \geq 2$. On a*

$$\left| \sum_{\substack{L(f,\rho)=0 \\ |\mathrm{Im}(\rho)|>x}} \frac{x^\rho}{\rho} \right| \ll d\left(\log(\mathfrak{q}(f)x)\right)^2.$$

Démonstration. On utilise de nouveau le théorème des résidus pour montrer que

$$\sum_{\substack{L(f,\rho)=0 \\ \mathrm{Im}(\rho)>T}} \frac{x^\rho}{\rho} = \lim_{R_2\to\infty} \lim_{R_1\to\infty} \frac{1}{2i\pi} \int_{C(R_1,R_2,T)} \frac{L'(f,s)}{L(f,s)} x^s \frac{ds}{s}$$

où $C(R_1,R_2,T)$ est le chemin rectangulaire de sommets $c+iT$, $c+iR_2$, $-R_1+iR_2$, $-R_1+iT$ parcouru dans le sens trigonométrique, avec $c = 1+\frac{1}{\log x}$, on admet que l'on peut légèrement déplacer le chemin pour passer toujours à distance au moins $(\log x)^{-1}$ des zéros de $L(f,s)$.

L'intégrale sur le segment vertical $\mathrm{Re}(s) = c$ est estimée grâce à la différence des formules de Perron obtenues en (3.5). On obtient alors une borne en

$$O\left(d\log x + dx(\log x)^2\left(\frac{1}{T}+\frac{1}{R_2}\right)\right).$$

L'intégrale sur les autres segments est bornée grâce à la proposition 3.5. Sur les segments de droites horizontaux, on écrit

$$\left|\int_{-R_1+iR}^{c+iR} \frac{L'(f,s)}{L(f,s)} x^s \frac{ds}{s}\right| \ll \int_{-R_1}^{c} \log\left(\mathfrak{q}(f)(|\sigma+iR|+3)^d\right)(|\sigma|+d\log x)\frac{x^\sigma}{|\sigma+iR|}d\sigma$$

où $R = T$ ou R_2. On obtient un terme majoré par

$$\frac{1}{R\log x}\left(\log(\mathfrak{q}(f)R^d)(1+\log x)x + \log(\mathfrak{q}(f)(R+R_1)^d)(R_1+\log x)x^{-R_1})\right).$$

Pour le segment vertical $(\mathrm{Re}(s) = -R_1)$, on a

$$\begin{aligned}\left|\int_{-R_1+iT}^{-R_1+iR_2} \frac{L'(f,s)}{L(f,s)} x^s \frac{ds}{s}\right| &\ll \int_{T}^{R_2} \log\left(\mathfrak{q}(f)(|-R_1+it|+3)^d\right)(R_1+\log x)\frac{x^{-R_1}}{|R_1+it|}dt \\ &\ll (R_1+\log x)x^{-R_1}\left(\log(\mathfrak{q}(f)(R_1+R_2)^d)\right)^2.\end{aligned}$$

Si on fait tendre $R_1 \to \infty$ puis $R_2 \to \infty$, on obtient

$$\left|\sum_{\substack{L(f,\rho)=0 \\ |\mathrm{Im}(\rho)|>T}} \frac{x^\rho}{\rho}\right| \ll d\log x + d\frac{x}{T}(\log x)^2 + \frac{x\log(\mathfrak{q}(f)T^d)}{T}. \tag{3.8}$$

Le résultat annoncé s'en déduit en prenant $T = x$. □

3.3.3 Majoration en norme L^2 pour Σ_2

Suivant l'idée de [Fio14a, Lem. 3.3] et [RS94, Lem. 2.2], on donne une borne de la norme L^2 du deuxième terme.

Lemme 3.23. *Soit $L(f,s)$ une fonction L analytique, et soient $T, Y > 2$. On pose*

$$\epsilon_f(x,T) := x^{-\beta_{f,0}} \sum_{\substack{\rho=\beta+i\gamma \\ L(f,\rho)=0 \\ |\gamma|\geq T}} \frac{x^{\beta+i\gamma}}{\beta+i\gamma}. \tag{3.9}$$

Alors on a

$$\int_2^Y |\epsilon_f(e^y,T)|^2 dy \ll Y\frac{d^2\log(\mathfrak{q}(f)T)^2}{T} + \frac{d^2\log(\mathfrak{q}(f)T)^3}{T},$$

la constante implicite est absolue.

Démonstration. On suit l'idée de la preuve de [RS94, Lem. 2.2]. On calcule

$$\begin{aligned}\int_2^Y |\epsilon(e^y,T)|^2 dy &\ll \sum_{\substack{\rho_1,\rho_2 \\ |\mathrm{Im}|>T}} \int_2^Y \frac{e^{y(\rho_1+\overline{\rho_2}-2\beta_{f,0})}}{\rho_1\overline{\rho_2}} dy \\ &\ll \sum_{\substack{\rho_1,\rho_2 \\ |\mathrm{Im}|>T}} \frac{1}{|\mathrm{Im}(\rho_1)||\mathrm{Im}(\rho_2)|} \min(Y, |\rho_1+\overline{\rho_2}-2\beta_{f,0}|^{-1}) \\ &\ll \sum_{\substack{\rho_1,\rho_2 \\ |\mathrm{Im}|>T}} \frac{1}{|\mathrm{Im}(\rho_1)||\mathrm{Im}(\rho_2)|} \min(Y, |\mathrm{Im}(\rho_1)-\mathrm{Im}(\rho_2)|^{-1}).\end{aligned}$$

Le terme diagonal $|\mathrm{Im}(\rho_1)-\mathrm{Im}(\rho_2)| \leq Y^{-1}$ est borné par

$$Y\sum_{|\gamma|>T} \frac{d\log(\mathfrak{q}(f)|\gamma|)}{|\gamma|^2} \ll Y\frac{d^2\log(\mathfrak{q}(f)T)^2}{T}.$$

Pour le second terme, d'après les propriétés des zéros (proposition 3.4) on peut comparer la somme à l'intégrale

$$\int_T^\infty \int_T^{x-\frac{1}{Y}} d^2\frac{\log(\mathfrak{q}(f)x)\log(\mathfrak{q}(f)y)}{xy(x-y)} dydx \ll d^2\frac{\log(\mathfrak{q}(f)T)^3}{T} + d^2\frac{\log(\mathfrak{q}(f)T)^2}{T}\log(\mathfrak{q}(f)Y),$$

la constante implicite est absolue. □

3.3.4 Étude de Σ_1

On montre que le terme Σ_1 est très proche de la fonction $G_{\mathcal{S},T}$ introduite dans la proposition 3.20.

Lemme 3.24. *Soit $L(f,s)$ une fonction L analytique, et soit $T > 2$. On pose*

$$\beta_{f,T} := \sup\{\mathrm{Re}(\rho), L(f,\rho)=0, |\mathrm{Im}(\rho)| \leq T, \mathrm{Re}(\rho) < \beta_{f,0}\}.$$

On a

$$x^{-\beta_{f,0}} \sum_{\substack{\rho \\ L(f,\rho)=0 \\ |\mathrm{Im}(\rho)|\leq T}} \frac{x^\rho}{\rho} = \sum_{\substack{|\gamma|\leq T \\ L(f,\beta_{f,0}+i\gamma)=0}} \frac{x^{i\gamma}}{\beta_{f,0}+i\gamma} + O\left(x^{\beta_{f,T}-\beta_{f,0}}\log(\mathfrak{q}(f)T)^2\right).$$

Remarque 48. Si on suppose l'hypothèse de Riemann, on a $\beta_{f,T} = -\infty$ pour tout T et ce terme de reste est bien nul.

Démonstration. D'après la proposition 3.4, on a

$$\begin{aligned} x^{-\beta_{f,0}} \sum_{\substack{\mathrm{Re}(\rho)<\beta_{f,0} \\ |\mathrm{Im}(\rho)|\leq T}} \frac{x^\rho}{\rho} &\ll x^{\beta_{f,T}-\beta_{f,0}} \sum_{\substack{\mathrm{Re}(\rho)<\beta_{f,0} \\ |\mathrm{Im}(\rho)|\leq T}} \frac{1}{|\rho|} \\ &\ll x^{\beta_{f,T}-\beta_{f,0}} \log(\mathfrak{q}(f)T)^2, \end{aligned}$$

avec une constante implicite absolue. □

3.3.5 Retour à $E_f(x)$

Revenons à la fonction $E_f(x)$ en étudiant la différence avec la fonction $\psi(f,x)$. On montre que dans certains cas la différence n'est pas un terme de reste. Il faut prendre en compte un terme supplémentaire dans le terme principal.

Lemme 3.25. *Soit $L(f,s)$ une fonction L analytique, on a*

$$\log x \sum_{p\leq x} \lambda_f(p) = \psi(f,x) + m(L(f^{(2)}),1)x^{\frac{1}{2}} + o_f(x^{\frac{1}{2}}). \tag{3.10}$$

Démonstration. D'après la conjecture de Ramanujan–Petersson (définition 3.1.1) et le théorème des nombres premiers classique, on a

$$\log x \sum_{p\leq x} \lambda_f(p) = \psi(f,x) - \sum_{p^2\leq x} \left(\sum_{j=1}^{d} \alpha_j(p)^2 \right) \log p + O(dx^{1/3}).$$

Pour évaluer le second terme on utilise un théorème taubérien de Wiener–Ikehara (voir par exemple [Ten15, II.7.5]) pour la fonction $\frac{L'(f^{(2)},s)}{L(f^{(2)},s)}$. D'après la définition 3.1.3, cette fonction a un prolongement méromorphe sur un ouvert contenant $\mathrm{Re}(s) \geq 1$, qui ne s'annule pas sur la droite $\mathrm{Re}(s) = 1$ et qui n'a pas de pôle excepté éventuellement un pôle simple en $s = 1$ de résidu $-m(L(f^{(2)},\cdot),1)$. On obtient

$$\sum_{p^2\leq x} \left(\sum_{j=1}^{d} \alpha_j(p)^2 \right) \log p = -m(L(f^{(2)},\cdot),1)\sqrt{x} + o_f(\sqrt{x}).$$

□

3.3.6 Existence de la distribution limite

On utilise la fonction $G_{f,T}$ de la proposition 3.20,

$$\begin{aligned} G_{f,T}(x) = \frac{m(L(f,\cdot),\beta_{f,0})}{\beta_{f,0}} + m(L(f^{(2)},\cdot),1)\delta_{\beta_{f,0}=\frac{1}{2}} \\ - \sum_{\gamma\in\mathcal{Z}_f^*(T)} 2\,\mathrm{Re}\left(m(L(f,\cdot),\beta_{f,0}+i\gamma)\frac{x^{i\gamma}}{\beta_{f,0}+i\gamma} \right). \end{aligned}$$

On reprend le résultat du lemme 3.25 où on évalue $\psi(f,x)x^{-\beta_0}$ grâce à l'expression (3.6) que l'on coupe selon l'expression (3.7). Alors on peut évaluer chacun des termes. Le lemme 3.24

permet de séparer le terme Σ_1 en la fonction $G_{f,T}(x)$ avec un terme de reste. On utilise ensuite l'expression (3.9) et la borne pour Σ_3 venant du lemme 3.22. On a donc

$$E_f(x) = G_{f,T}(x) + O_f\left(x^{\beta_{f,T}-\beta_{f,0}}(\log T)^2\right) - \epsilon_f(x,T) + o_f(1) \tag{3.11}$$

où le second terme disparaît si on suppose l'hypothèse de Riemann vérifiée. Commençons par montrer que la fonction $G_{f,T}$ a une distribution logarithmique limite.

Lemme 3.26. *Soit $T > 2$. La fonction $G_{f,T}$ a une distribution logarithmique limite $\mu_{f,T}$.*

Démonstration. La preuve est une conséquence du théorème de Kronecker–Weyl (théorème 3.18) et suit l'idée de la preuve de [RS94, Lem. 2.3] (voir aussi [ANS14, Prop. 2.4]).

Ordonnons l'ensemble des zéros de partie imaginaire inférieure à T : on écrit $\mathcal{Z}_f^*(T) = \{\gamma_1, \dots, \gamma_{N(T)}\}$. Fixons une fonction $g : \mathbf{R} \to \mathbf{R}$ continue bornée et lipschitzienne. On peut associer à g la fonction de $N(T)$ variables suivante

$$\tilde{g}(t) = g\left(m_f - 2\,\mathrm{Re}\left(\sum_{k=1}^{N(T)} \frac{e^{2i\pi t_k}}{\beta_{f,0} + i\gamma_k}\right)\right), \tag{3.12}$$

cette fonction est continue sur le tore $\mathbf{T}^{N(T)}$. On a

$$\int_2^Y g(G_{f,T}(e^y))dy = \int_2^Y \tilde{g}\left(\frac{\gamma_1}{2\pi}y, \dots, \frac{\gamma_{N(T)}}{2\pi}y\right)dy.$$

Le théorème de Kronecker–Weyl permet de conclure : la distribution $\mu_{f,T}$ est la tirée en arrière de la mesure de Haar normalisée sur l'adhérence du groupe à un paramètre $\{(\frac{\gamma_1}{2\pi}y, \dots, \frac{\gamma_{N(T)}}{2\pi}y), y \in \mathbf{R}\}/\mathbf{Z}^{N(T)}$ dans $\mathbf{T}^{N(T)}$. □

On peut maintenant utiliser l'expression (3.11) pour montrer que la fonction E_f a une distribution logarithmique limite. Soit g une fonction continue bornée C_g-lipschitzienne, on a

$$\begin{aligned}\int_2^Y g(E_f(e^y))dy = \int_2^Y g(G_{f,T}(e^y)dy + O_f\left(C_g\int_2^Y e^{y(\beta_{f,T}-\beta_{f,0})}dy\right) \\ + O_f\left(C_g\int_2^Y |\epsilon_f(e^y,T)|dy\right) + o_f(C_gY)\end{aligned} \tag{3.13}$$

On divise l'expression par Y, et on prend les limites inférieures et supérieures quand $Y \to \infty$. On peut borner ces limites en utilisant le lemme 3.26 pour remplacer la limite pour $G_{f,T}$ par la distribution logarithmique limite, et le lemme 3.23 avec l'inégalité de Cauchy–Schwarz pour borner le terme venant de ϵ_f. On obtient

$$\begin{aligned}\int_{\mathbf{R}} g(t)d\mu_{f,T} + O_f\left(C_g\frac{\log T}{\sqrt{T}}\right) &\le \liminf_{Y\to\infty}\frac{1}{Y}\int_2^Y g(E_f(e^y))dy \\ &\le \limsup_{Y\to\infty}\frac{1}{Y}\int_2^Y g(E_f(e^y))dy \le \int_{\mathbf{R}} g(t)d\mu_{f,T} + O_f\left(C_g\frac{\log T}{\sqrt{T}}\right).\end{aligned} \tag{3.14}$$

Comme on peut prendre T arbitrairement grand, les limites inférieures et supérieures coïncident, donc la limite existe.

On applique enfin le théorème de Helly à la suite des mesures de probabilité $(\mu_{f,T})_{T\ge1}$, de la même façon que dans la preuve de [ANS14, Th. 2.9]. Cela assure que la limite obtenue est bien une mesure.

3.3.7 Calcul de la moyenne et de la variance

Commençons par montrer que la distribution μ_f a une décroissance exponentielle à l'infini.

Lemme 3.27. *On a*

$$\mu_f(\mathbf{R} - [m_f - R, m_f + R]) \ll_f e^{-c_3(f)\sqrt{R}}.$$

Démonstration. D'après les propriétés de répartition des zéros des fonctions L analytiques (proposition 3.4) on a

$$\begin{aligned}\left|\sum_{\gamma\in\mathcal{Z}_f^*(T)} 2\operatorname{Re}\left(m(L(f,\cdot),\beta_{f,0}+i\gamma)\frac{x^{i\gamma}}{\beta_{f,0}+i\gamma}\right)\right| &\leq \sum_{\gamma\in\mathcal{Z}_f(T)} 2\frac{1}{|\beta_{f,0}+i\gamma|}\\ &\ll_f (\log T)^2.\end{aligned}$$

On en déduit que pour tout T, la fonction $G_{f,T}(e^y)$ est bornée. Donc la mesure $\mu_{f,T}$ a un support compact inclus dans un intervalle $[m_f - c(\log T)^2, m_f + c(\log T)^2]$ où c ne dépend que de f. D'après l'expression (3.14), on a

$$\mu_f(\mathbf{R} - [m_f - c(\log T)^2, m_f + c(\log T)^2]) = O_f\left(\frac{\log T}{\sqrt{T}}\right).$$

Prenons $R = c(\log T)^2$, on obtient le résultat annoncé. □

La distribution μ_f a une décroissance exponentielle, elle a donc des moments finis. On calcule la moyenne et la variance pour conclure la preuve du théorème 3.19. Ces calculs se font en étudiant d'abord la même question pour $\mu_{f,T}$ puis en faisant tendre T vers l'infini. Fixons d'abord $T \geq 2$, on a

$$\begin{aligned}\int_{\mathbf{R}} t d\mu_{f,T} &= \lim_{Y\to\infty}\frac{1}{Y}\int_2^Y G_{f,T}(e^y)dy\\ &= \lim_{Y\to\infty}\frac{1}{Y}\int_2^Y \left(m_f - \sum_{\gamma\in\mathcal{Z}_f^*(T)} 2\operatorname{Re}\left(m(L(f,\cdot),\beta_{f,0}+i\gamma)\frac{e^{iy\gamma}}{\beta_{f,0}+i\gamma}\right)\right)dy\\ &= m_f - \lim_{Y\to\infty}\frac{1}{Y}O\left(\sum_{\gamma\in\mathcal{Z}_f^*(T)} 2m(L(f,\cdot),\beta_{f,0}+i\gamma)\frac{1}{|\beta_{f,0}+i\gamma||\gamma|}\right)\\ &= m_f\end{aligned}$$

car la somme est finie. La limite quand $T \to +\infty$ est donc

$$\int_{\mathbf{R}} t d\mu_f = m_f.$$

Pour le calcul de la variance, on ne peut plus utiliser la linéarité. On revient au cas général. Pour $T \geq 2$ fixé, on utilise la fonction

$$G_{\mathcal{S},T}(x) = m_{\mathcal{S}} - \sum_{\gamma\in\mathcal{Z}_{\mathcal{S}}^*(T)} 2\operatorname{Re}\left(M_{\mathcal{S}}(\gamma)\frac{x^{i\gamma}}{\beta_{\mathcal{S},0}+i\gamma}\right)$$

où, pour $\gamma \in \mathcal{Z}_{\mathcal{S}}^*$, on note comme dans l'énoncé du théorème 3.19,

$$M_{\mathcal{S}}(\gamma) = \sum_{f\in\mathcal{S}} a_f m(L(f,\cdot),\beta_{\mathcal{S},0}+i\gamma).$$

Calculons la variance pour la distribution $\mu_{\mathcal{S},T}$. On a

$$\begin{aligned}\int_{\mathbf{R}} |t-m_{\mathcal{S}}|^2 d\mu_{\mathcal{S},T} &= \lim_{Y\to\infty} \frac{1}{Y}\int_2^Y \left|\sum_{\gamma\in\mathcal{Z}_{\mathcal{S}}^*(T)} \left(\frac{M_{\mathcal{S}}(\gamma)e^{iy\gamma}}{\beta_0+i\gamma}+\frac{M_{\mathcal{S}}(-\gamma)e^{-iy\gamma}}{\beta_0-i\gamma}\right)\right|^2 dy \\ &= \lim_{Y\to\infty}\frac{1}{Y}\sum_{\gamma,\lambda}^{*}\frac{M_{\mathcal{S}}(\gamma)\overline{M_{\mathcal{S}}(\lambda)}}{(\beta_0+i\gamma)(\beta_0-i\lambda)}\int_2^Y e^{i(\gamma-\lambda)y}dy\end{aligned}$$

où la somme porte sur les γ, λ dans $\mathcal{Z}_{\mathcal{S}}^*(T)\cup(-\mathcal{Z}_{\mathcal{S}}^*(T))$. Le terme diagonal $\lambda=\gamma$ est le terme principal égal à

$$\sum_{\gamma\in\mathcal{Z}_{\mathcal{S}}^*(T)}\frac{2|M_{\mathcal{S}}(\gamma)|^2}{|\beta_{\mathcal{S},0}+i\gamma|^2}.$$

L'autre terme tend vers zéro quand $Y\to\infty$ et T est fixé. Suivant le raisonnement de [Fio14a, Lem. 2.6], on obtient

$$\int_{\mathbf{R}}|t-m_{\mathcal{S}}|^2 d\mu_{\mathcal{S}} = \sum_{\gamma\in\mathcal{Z}_{\mathcal{S}}^*}\frac{2|M_{\mathcal{S}}(\gamma)|^2}{|\beta_{\mathcal{S},0}+i\gamma|^2}.$$

3.3.8 Question de la dépendance en le paramètre f

On se demande ce qui se passe si on ne fixe pas f mais qu'on le fait varier dans une famille, ou que l'on fait varier le degré de la fonction L. On reprend (3.13) en faisant plus attention à la dépendance en f. Pour toute fonction g continue bornée lipschitzienne, on a

$$\begin{aligned}\frac{1}{Y}\int_2^Y g(E_f(e^y))dy &= \frac{1}{Y}\int_2^Y g(G_{f,T}(e^y))dy + O_g\left(\frac{\log(\mathfrak{q}(f)T)^2}{Y}\int_2^Y e^{y(\beta_{f,T}-\beta_{f,0})}dy\right) \\ &\quad + O_g\left(d\frac{\log(\mathfrak{q}(f)T)}{\sqrt{T}}+d\frac{\log(\mathfrak{q}(f)T)^{3/2}}{\sqrt{TY}}\right) \\ &\quad + O_g\left(\frac{1}{Y}\int_2^Y d(\log\mathfrak{q}(f)+dy)^2e^{-y\beta_{f,0}}+r(f,e^y)e^{y(\frac{1}{2}-\beta_{f,0})}dy\right).\end{aligned}$$

De nouveau dans cette expression, le deuxième terme disparaît si on suppose l'hypothèse de Riemann généralisée pour les fonctions L de la famille. Le facteur $r(f,x)$ vient du lemme 3.25 où on n'a pas explicité la dépendance en f. On a $r(f,x)\to 0$ quand $x\to+\infty$. Ignorons ce terme pour le moment, alors le troisième terme est

$$O\left(\frac{d^2(\log\mathfrak{q}(f)+d)^2}{Y}\right).$$

On a donc une condition liant Y et f si l'on veut faire varier les deux en même temps. Cependant on voit avec le troisième terme que si l'on fait varier f de façon à ce que $\mathfrak{q}(f)\to+\infty$ ou $d\to+\infty$, le paramètre T devra varier aussi pour que le terme obtenu soit encore un terme de reste. Le problème est qu'alors tous les termes dépendent de f. Le fait de faire tendre f vers une limite ne permet donc pas de déduire que la suite des distributions limites μ_f admet une limite. Dans le cas précédent dans l'expression (3.14), les limites inférieures et supérieures ne dépendaient pas de T et ils donnaient donc une information fixe quand T tendait vers l'infini. Un tel raisonnement semble difficile lorsque f varie.

Cependant si on sait par un autre moyen que la suite des μ_f converge, alors la limite sera la distribution limite de la limite des E_f.

3.4 Exemples d'applications

3.4.1 Courses entre classes de congruences modulo un entier

On peut retrouver les résultats [RS94, Th. 1.1, Th. 1.2] dans le cas d'une course de nombres premiers entre deux classes de congruences a et b modulo un entier q. On applique le théorème 3.19 à l'ensemble des fonctions L de Dirichlet associées aux caractères non triviaux modulo q :

$$\mathcal{S} = \{L(\chi, \cdot) : \chi \bmod q, \chi \neq \chi_0\}$$

avec les poids $a_\chi = \frac{1}{\phi(q)}(\overline{\chi}(a) - \overline{\chi}(b))$. En particulier, on a certains de ces résultats inconditionnellement à GRH.

Théorème 3.28. *Soit $q \geq 3$ un entier et $a \not\equiv b$ deux classes inversibles modulo q. Posons*

$$\beta_{q,0} = \sup\{\mathrm{Re}(\rho), \exists \chi \bmod q, \chi \neq \chi_0, L(\chi, \rho) = 0\}.$$

La fonction

$$E_{q;a,b}(x) = \frac{\log(x)}{x^{\beta_{q,0}}}(\pi(x; q, a) - \pi(x; q, b))$$

admet une distribution logarithmique limite $\mu_{q;a,b}$ sur $\mathbf{R}$. Il existe C une constante positive (dépendante de q) telle qu'on ait

$$\mu_{q;a,b}(\mathbf{R} - [-A, A]) \ll \exp(-C\sqrt{A}).$$

De plus si GRH est vérifiée pour les fonctions L de Dirichlet de caractères modulo q (i.e. $\beta_{0,q} = 1/2$) et si $L(\chi, 1/2) \neq 0$ pour tout $\chi \bmod q$, $\chi \neq \chi_0$. Alors la distribution $\mu_{q;a,b}$ a pour moyenne

$$m_{q;a,b} = \sum_{\substack{\chi \bmod q \\ \chi^2 = \chi_0}} (\chi(b) - \chi(a)).$$

En particulier on a prouvé [RS94, Th. 1.1] inconditionnellement. En suivant l'idée de la remarque 45, on déduit du calcul de la moyenne sous GRH que si le biais existe (voir la sous-section 3.5.1) alors

1. si ab^{-1} est un carré, le biais est égal à $\frac{1}{2}$ (il n'y a pas de biais),
2. sinon le biais est en direction de la classe qui n'est pas un carré modulo q.

Ce qui est bien le résultat de Rubinstein et Sarnak [RS94, Th. 1.4] dans le cas des courses à deux concurrents. On a ainsi ce résultat conditionnellement à GRH et à l'une des conjectures permettant de garantir que le biais est dans la direction du signe de la moyenne (voir la remarque 45), par exemple la conjecture 3.13 ou la conjecture 3.14 qui sont toutes deux plus faibles que LI.

Poursuivant l'idée de [RS94] et [Fio14b], on peut aussi s'intéresser à la course entre résidus quadratiques et non résidus quadratiques modulo un entier q. On prend cette fois

$$\mathcal{S} = \{L(\chi, \cdot) : \chi \bmod q, \chi \neq \chi_0, \chi^2 = \chi_0\}$$

avec pour tout χ, $a_\chi = \frac{1}{\rho(q)} := [(\mathbf{Z}/q\mathbf{Z})^\times : (\mathbf{Z}/q\mathbf{Z})^{\times(2)}]^{-1}$. On obtient ainsi le résultat suivant.

Théorème 3.29. *Soit $q \geq 3$ un entier. Posons*

$$\beta_{q,0}^{(2)} = \sup\{\mathrm{Re}(\rho), \exists \chi \bmod q, \chi \neq \chi_0, \chi^2 = \chi_0, L(\chi, \rho) = 0\}.$$

La fonction

$$E_{q;R,NR}(x) = \frac{\log(x)}{\rho(q)x^{\beta_{q,0}^{(2)}}}((\rho(q) - 1)\pi(x; q, R) - \pi(x; q, NR))$$

admet une distribution logarithmique limite $\mu_{q;R,NR}$ sur $\mathbf{R}$. Supposons de plus que GRH est vérifiée pour les fonctions L de Dirichlet de caractères réels modulo q et si $L(\chi, 1/2) \neq 0$ pour tout $\chi \bmod q$, $\chi \neq \chi_0$, $\chi^2 = \chi_0$. Alors la distribution $\mu_{q;R,NR}$ a pour moyenne

$$m_{q;a,b} = \frac{1 - \rho(q)}{\rho(q)}.$$

On retrouve notamment [RS94, Th. 1.1] dans ce cadre (voir aussi [Fio14b, Lem. 2.2]) inconditionnellement. On remarque que la moyenne obtenue conditionnellement à GRH est toujours négative, elle s'éloigne de zéro quand il y a peu de carrés modulo q. On retrouve donc bien l'idée de [Fio14b] qui est de chercher des courses avec un biais arbitrairement proche de 1 dans les courses entre résidus quadratiques et non résidus quadratiques modulo les entiers qui ont beaucoup de facteurs premiers.

On peut généraliser ces résultats à des courses du genre

$$\sum_{\substack{p \equiv a \ [\bmod \ q] \\ p \leq x}} \lambda_f(p) - \sum_{\substack{p \equiv b \ [\bmod \ q] \\ p \leq x}} \lambda_f(p)$$

ou

$$(\rho(q) - 1) \sum_{\substack{p \equiv \square \ [\bmod \ q] \\ p \leq x}} \lambda_f(p) - \sum_{\substack{p \not\equiv \square \ [\bmod \ q] \\ p \leq x}} \lambda_f(p)$$

où f est une forme modulaire primitive holomorphe cuspidale et pour tout premier p, $\lambda_f(p)$ est son coefficient de Fourier en p. En effet la famille des tordues $L(f \otimes \chi, s)$ pour χ parcourant les caractères modulo un entier q est bien une famille de fonctions L analytiques selon la définition 3.1 (voir par exemple [Cog04]). On peut donc appliquer le théorème 3.19 à l'ensemble de fonctions $\mathcal{S} = \{L(f \otimes \chi, s) : \chi \text{ caractère modulo } q\}$ ou $\mathcal{S} = \{L(f \otimes \chi, s) : \chi \text{ caractère modulo } q, \chi^2 = \chi_0\}$ avec les poids a_χ comme précédemment. On aura de nouveau l'existence d'une distribution logarithmique limite associée aux fonctions normalisées. Pour en déduire des informations sur le biais, il nous faudrait cependant plus de connaissances sur les zéros des fonctions L tordues.

3.4.2 Biais de Chebyshev et nombres premiers de la forme $a^2 + Db^2$

Dans l'article [SB85], les auteurs donnent plusieurs exemples de fonctions L de degré 2 qui ne viennent pas directement de courbes elliptiques mais de surfaces $K3$. On définit les trois fonctions L suivantes :

$$L_D(s) = \prod_{p \nmid 2D} \left(1 - a_p p^{-s} + \left(\frac{-D}{p}\right) p^{-2s}\right)^{-1}$$

pour $D = 4$, 2 et 3, avec

$$a_p = \begin{cases} 0 & \text{si } \left(\frac{-D}{p}\right) = 0 \text{ ou } -1, \\ 2\frac{a^2 - Db^2}{p} & \text{si } p \text{ s'écrit sous la forme } a^2 + Db^2. \end{cases}$$

D'après [SB85, Th. 14.2], ces trois fonctions L coïncident avec des fonctions L de formes paraboliques de poids 3, de niveau $4D$. En particulier ce sont des fonctions L analytiques qui satisfont la définition 3.1.

Remarque 49. Dans le cas $D = 4$, ce résultat était déjà connu de Schoeneberg [Sch53].

Ainsi, on peut étudier le signe des fonctions

$$E_D(x) = \frac{\log(x)}{x^{\beta_{D,0}}} \sum_{p=a^2+Db^2\leq x} 2\frac{a^2-Db^2}{a^2+Db^2}.$$

On a alors le résultat suivant.

Théorème 3.30. *Pour $D = 4$, 2 et 3, la fonction E_D admet une distribution logarithmique limite dont la moyenne est $-\frac{m(L_D,\beta_0)}{\beta_0} - \delta_{\frac{1}{2},\beta_0} \leq 0$.*

Démonstration. Pour tout p, on a $\alpha_1(p)\alpha_2(p) = \left(\frac{-D}{p}\right)$ donc la fonction L donnée par le carré alterné est

$$L(\wedge^2 f_D, s) = \prod_p \left(1 - \left(\frac{-D}{p}\right) p^{-s}\right)^{-1}.$$

qui est holomorphe et ne s'annule pas en $s = 1$. De plus d'après [MW89, App.], la fonction $L(f_D \otimes f_D, s) = L(\wedge^2 f_D, s)L(\mathrm{Sym}^2 f_D, s)$ a un pôle simple en $s = 1$. On en déduit que la fonction $L(f_D^{(2)}, s) = L(\wedge^2 f_D, s)^{-1}L(\mathrm{Sym}^2 f_D, s)$ a un pôle d'ordre 1 en $s = 1$. Le théorème 3.19 permet de conclure. □

En particulier sous GRH pour la fonction $L_D(s)$, suivant l'idée de la remarque 45, si le biais existe pour la course définie par E_D alors il est en direction des valeurs négatives. Ce résultat laisse imaginer que dans la décomposition $p = a^2 + Db^2$, le terme Db^2 est souvent plus grand que le terme a^2. On a tracé les figures 3.1, 3.2 et 3.3 qui correspondent respectivement aux courses entre a^2 et $-Db^2$ pour $D = 4, 2, 3$. On a utilisé pour cela l'algorithme de Cornacchia implémenté dans `SageMath` [SD16] pour obtenir les valeurs des fonctions

$$S_D(x) := \sum_{p=a^2+Db^2\leq x} \frac{a^2-Db^2}{a^2+Db^2}$$

pour x variant de 0 à 2.10^7. Les graphes obtenus rendent assez crédible le fait que les courses sont biaisées vers les valeurs négatives.

Remarque 50. Dans le cas $D = 4$, le résultat est lié à la répartition des angles des premiers de Gauss. Une telle étude utilisant les caractères de Hecke sera approfondie dans un article à venir.

3.4.3 Formes automorphes sur $GL(m)$

On a évoqué dans l'exemple 12.4 le cas des fonctions L associées à des représentations automorphes cuspidales unitaires irréductibles de $GL(m)$ avec $m \geq 2$. Supposons la conjecture de Ramanujan–Petersson vérifiée pour ces fonctions, alors on est dans le cadre de la définition 3.1. Si la représentation π est auto-duale, on peut appliquer le théorème 3.19 à la fonction $L(\pi, s)$. On peut donc définir la course de nombres premiers associée à cette fonction. La fonction $E_\pi(x) = \frac{\log x}{x^{\beta_{\pi,0}}} \sum_{p\leq x} \lambda_\pi(p)$ admet une distribution logarithmique limite μ_π dont on a une formule pour l'espérance.

Si on suppose que l'hypothèse de Riemann est satisfaite, on s'intéresse au comportement en $s = 1$ de la fonction $L(\pi^{(2)}, s) = L(\mathrm{Sym}^2 \pi, s)L(\wedge^2\pi, s)^{-1}$ pour estimer l'espérance. Dans le cas où la représentation π est irréductible et non triviale, [Sha97, Th. 1.1] assure qu'aucune des deux fonctions $L(\mathrm{Sym}^2 \pi, s)$, $L(\wedge^2\pi, s)$ ne s'annule en $s = 1$. Suivant la discussion dans l'introduction de [BG92], on a $L(\pi \otimes \pi, s) = L(\mathrm{Sym}^2 \pi, s)L(\wedge^2\pi, s)$ et quand π est auto-duale, cette fonction a un pôle simple en $s = 1$ [MW89, App.]. Donc il ne reste pas beaucoup de choix :

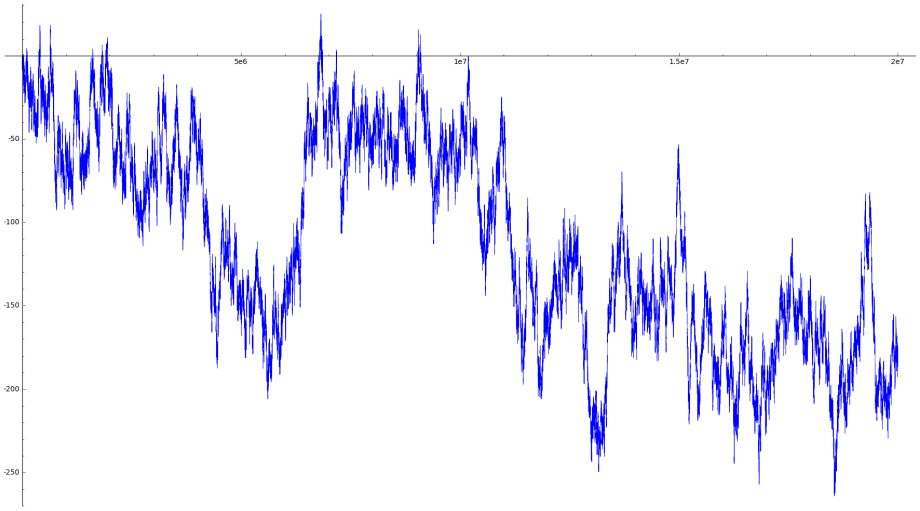

FIGURE 3.1 – Valeurs de $S_4(x)$ dans l'intervalle $[0; 2.10^7]$

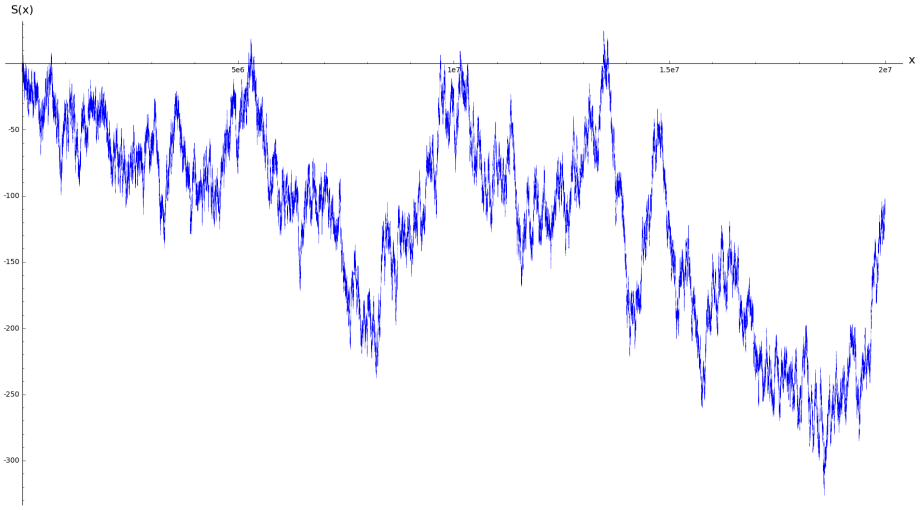

FIGURE 3.2 – Valeurs de $S_2(x)$ dans l'intervalle $[0; 2.10^7]$

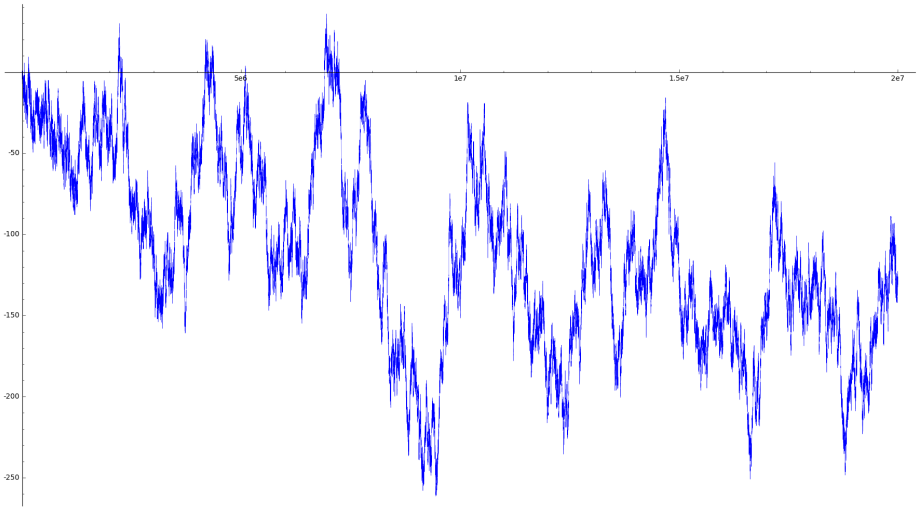

FIGURE 3.3 – Valeurs de $S_3(x)$ dans l'intervalle $[0; 2.10^7]$

— soit $L(\mathrm{Sym}^2\,\pi, s)$ a un pôle simple en $s=1$ et $m(L(f^{(2)},\cdot),1)=-1$,

— soit $L(\wedge^2\pi, s)$ a un pôle simple en $s=1$ et $m(L(f^{(2)},\cdot),1)=1$.

De plus il y a un critère (donné dans [BG92] par exemple) qui permet de déterminer dans quelle situation on est. On a ainsi montré le résultat suivant.

Proposition 3.31. *Soit $L(\pi,s)$ une fonction L associée à une représentation automorphe cuspidale unitaire irréductible de $GL(m)$ avec $m\geq 2$. On suppose vérifiée la conjecture de Ramanujan–Petersson. Alors la fonction $E_\pi(x)=\frac{\log x}{x^{\beta_{\pi,0}}}\sum_{p\leq x}\lambda_\pi(p)$ admet une distribution logarithmique limite μ_π. Sous l'hypothèse de Riemann l'espérance de cette distribution est $m_\pi=\pm 1-2m(L(\pi,\cdot),1/2)$. En particulier $m_\pi\neq 0$.*

Suivant les idées de la remarque 45, un tel résultat laisse penser qu'une course associée à une représentation irréductible va toujours avoir un biais différent de $\frac{1}{2}$.

Dans le cas $m=2$, on retrouve les fonctions L associées aux formes modulaires cuspidales classiques. En particulier on peut traiter le cas des fonctions L de Hasse-Weil associées aux courbes elliptiques sur $\mathbf{Q}$. C'est le sujet de l'article [Fio14a]. Étant donné une courbe elliptique $E/\mathbf{Q}$. On étudie le signe de la fonction

$$E_E(x)=\frac{\log(x)}{x^{\beta_{E,0}}}\sum_{p\leq x}\frac{a_p}{\sqrt{p}},$$

où $a_p=p+1-N_E(p)$. D'après le théorème 3.19 (ou la proposition 3.31), la fonction $E_E(x)$ admet une distribution limite μ_E, de plus une variable aléatoire de loi μ_E a pour espérance $-\frac{m(L(E),\beta_0)}{\beta_0}+\delta_{\frac{1}{2},\beta_{E,0}}$. En effet, la fonction $L(\mathrm{Sym}^2,E,s)$ est holomorphe, et on a $L(\wedge^2,E,s)=\zeta(s)$. donc $m(L(f^{(2)}),1)=1$. On retrouve donc bien de la même façon que Sarnak et sous l'hypothèse de Riemann la dichotomie de comportement déjà remarquée dans [Maz08] entre le cas où le rang analytique est nul est celui où il est non nul.

3.4.4 Corrélation des signes des coefficients a_p pour deux courbes elliptiques

Poursuivons l'étude des termes d'erreur dans les nombres de points de courbes elliptiques. On se donne deux courbes elliptiques E_1 et E_2 définies sur $\mathbf{Q}$ toutes deux sans multiplication complexe. On suppose que les courbes E_1 et E_2 ne sont pas isogènes sur $\mathbf{Q}$ ni sur aucune extension abélienne de $\mathbf{Q}$. En particulier on ne peut pas obtenir une courbe comme une tordue quadratique de l'autre. Il suffit par exemple d'étudier deux courbes elliptiques sur $\mathbf{Q}$ de rangs algébriques différents. Pour les applications numériques on prendra les courbes dont le modèle affine est

$$E_1: y^2+y=x^3-x \text{ et } E_2: y^2+y=x^3+x^2-2x. \tag{3.15}$$

La courbe E_1 est de rang 1, et la courbe E_2 est de rang 2.

D'après les résultats sur la modularité ([Wil95], [TW95], [BCDT01]) on peut associer à E_1 et E_2 des formes modulaires cuspidales de poids 2, f_{E_1} et f_{E_2}. Comme on l'a déjà remarqué dans l'exemple 12.3 on peut faire le produit de Rankin-Selberg des fonctions L associées. La fonction $L(f_{E_1}\otimes f_{E_2},\cdot)$ vérifie pour tout p premier $\lambda(p)=a_p(E_1)a_p(E_2)/p$ et c'est une fonction L analytique selon la définition 3.1.

Cela découle de [Ram00, Th. M]. En effet le fait que E_1 et E_2 sont non isogènes garantit que $f_{E_1}\neq f_{E_2}$, et comme par hypothèse, E_1 et E_2 ne deviennent pas isogènes sur une extension quadratique de $\mathbf{Q}$ la fonction $L(f_{E_1}\otimes f_{E_2},\cdot)$ est associée à une forme automorphe cuspidale sur $GL(4)$. On en déduit les points 1 et 2 de la définition 3.1, le

point 3 a déjà été évoqué dans l'exemple 12.3, on pourra aussi voir la preuve du lemme 3.32. On peut donc appliquer le théorème 3.19, pour étudier la quantité

$$E(x) = \frac{\log(x)}{x^{\beta_0}} \sum_{p \leq x} \frac{a_p(E_1)a_p(E_2)}{p}.$$

Autrement dit on étudie les corrélations entre les signes des a_p des deux courbes elliptiques.

Remarque 51. Dans cette situation — on suppose que E_1 et E_2 ne sont isogènes sur aucune extension abélienne de $\mathbf{Q}$ — une version plus forte de la conjecture 3.3 pour la fonction $L(f_{E_1} \otimes f_{E_2})$ est démontrée (voir [Har09, Th. 5.4]).

Pour calculer la moyenne de la distribution limite il nous faut connaître l'ordre d'annulation de $L(f_{E_1} \otimes f_{E_2}, s)$ en $s = \beta_0$ (ou en $1/2$ sous l'hypothèse de Riemann). Cela peut-il dépendre des ordres d'annulations correspondants aux fonctions de Hasse–Weil de E_1 et E_2 ?

Sous l'hypothèse de Riemann, il faut aussi étudier la fonction $L((f_{E_1} \otimes f_{E_2})^{(2)}, s)$ associée (voir la définition 3.1.3). On sait calculer l'ordre du zéro en $s = 1$ de cette fonction.

Lemme 3.32. *On suppose que E_1 et E_2 ne sont isogènes sur aucune extension abélienne de $\mathbf{Q}$. Alors, la fonction $L(\wedge^2(f_{E_1} \otimes f_{E_2}), \cdot)$ est holomorphe et la fonction $L(\mathrm{Sym}^2(f_{E_1} \otimes f_{E_2}), \cdot)$ a un pôle d'ordre 1 en $s = 1$.*

Démonstration. On écrit pour $i = 1, 2$,

$$L(f_{E_i}, s) = \prod_p (1 - \pi_i p^{-s})^{-1}(1 - \overline{\pi_i} p^{-s})^{-1}.$$

Donc d'après la définition 3.2 on a

$$\begin{aligned} L(\wedge^2(f_{E_1} \otimes f_{E_2}), s) &= \prod_p \prod_{i=1,2} (1 - \pi_i^2 p^{-s})^{-1}(1 - \overline{\pi_i}^2 p^{-s})^{-1}(1 - p^{-s})^{-1} \\ &= L(\mathrm{Sym}^2 f_{E_1}, s) L(\mathrm{Sym}^2 f_{E_2}, s). \end{aligned}$$

Comme on l'a déjà vu dans la sous-section 3.4.3, pour $i = 1, 2$ la fonction $L(\mathrm{Sym}^2 f_{E_i}, \cdot)$ est holomorphe. De la même façon

$$L(\mathrm{Sym}^2(f_{E_1} \otimes f_{E_2}), s) = L(\mathrm{Sym}^2 f_{E_1} \otimes \mathrm{Sym}^2 f_{E_2}, s)\zeta(s).$$

Or comme les courbes E_1 et E_2 ne deviennent pas isogènes sur une extension quadratique de $\mathbf{Q}$, on a (e.g. [Ram00, Th. 4.1.2]) $\mathrm{Sym}^2 f_{E_1} \not\sim \mathrm{Sym}^2 f_{E_2}$ comme représentations. Ainsi d'après [MW89, App.], $L(\mathrm{Sym}^2 f_{E_1} \otimes \mathrm{Sym}^2 f_{E_2}, s)$ est holomorphe et ne s'annule pas en 1. □

On peut donc conclure sous l'hypothèse de Riemann.

Proposition 3.33. *Soient E_1 et E_2 deux courbes elliptiques sur $\mathbf{Q}$ sans multiplication complexe. On suppose que les courbes ne sont isogènes sur aucune extension abélienne de $\mathbf{Q}$. Sous l'hypothèse de Riemann pour $L(f_{E_1} \otimes f_{E_2}, \cdot)$, la fonction*

$$E(x) = \frac{\log(x)}{\sqrt{x}} \sum_{p \leq x} \frac{a_p(E_1)a_p(E_2)}{p}$$

admet une distribution logarithmique limite d'espérance strictement négative.

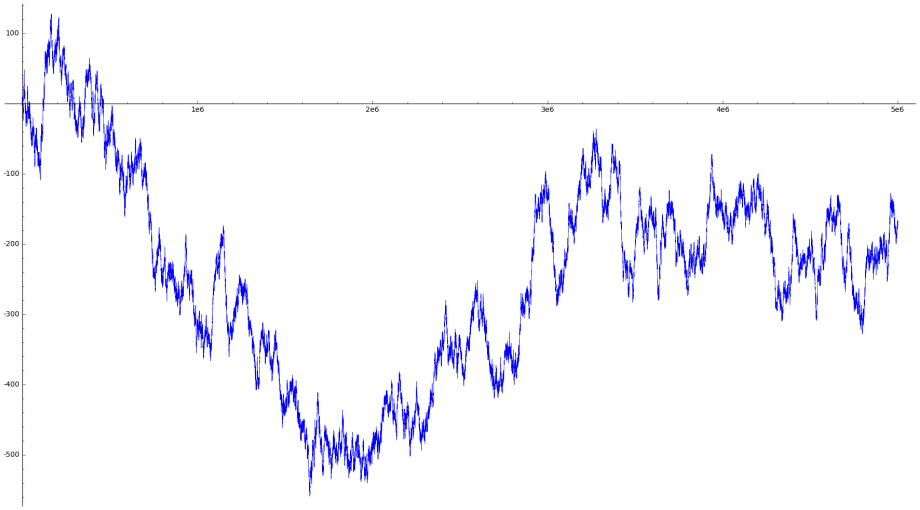

FIGURE 3.4 – Valeurs de $S_{E_1,E_2}(x)$ dans l'intervalle $[0; 5.10^6]$

Démonstration. D'après le théorème 3.19 et le lemme 3.32, sous l'hypothèse de Riemann, la fonction $E(x)$ admet une distribution logarithmique limite d'espérance égale à

$$-2m(L(f_{E_1} \otimes f_{E_2}, \cdot), \frac{1}{2}) - 1 < 0.$$

On peut aussi appliquer directement la proposition 3.31, en effet la représentation associée à $f_{E_1} \otimes f_{E_2}$ par [Ram00] est bien irréductible. □

On déduit de ce résultat que pour deux courbes elliptiques sans multiplication complexe non isogènes (au sens fort ci-dessus) E_1 et E_2, les coefficients $a_p(E_1)$ et $a_p(E_2)$ ont tendance à être de signes opposés. La figure 3.4 correspond à la course entre les signes des $a_p(E_1)a_p(E_2)$ pour E_1 et E_2 comme dans l'exemple (3.15). On a tracé le graphe de la fonction $S_{E_1,E_2}(x) = \sum_{p \leq x} \frac{a_p(E_1)a_p(E_2)}{p}$ pour x variant de 2 à 5.10^6 grâce à l'algorithme de comptage de points des courbes elliptiques implémenté dans `SageMath` [SD16] (et utilisant `pari`) par J. Cremona.

3.4.5 Jacobienne de courbes modulaires

Soit q un nombre premier. On étudie la course de nombres premiers pour les sommes de coefficients de toutes les fonctions L modulaires de formes primitives cuspidales de poids 2 et de niveau q. La fonction L associée à cette course est le produit fini

$$\prod_{f \in S_2(q)^*} L(f, s) = L(J_0(q), s),$$

où $J_0(q)$ est la variété jacobienne de la courbe modulaire $X_0(q)$. La factorisation de la fonction L de $J_0(q)$ est un résultat de Shimura [Shi94]. On a déjà vu que les fonctions $L(f, s)$ pour f parcourant l'ensemble des formes modulaires cuspidales classiques sont analytiques selon la définition 3.1, donc la fonction $L(J_0(q), \cdot)$ qui est un produit de telles fonctions est aussi une fonction L analytique. On peut lui appliquer le théorème 3.19 : la fonction

$$E_{J_0(q)}(x) = \frac{\log(x)}{x^{\beta_{J_0(q),0}}} \sum_{p \leq x} \sum_{f \in S_2(q)^*} \lambda_f(p)$$

admet une distribution logarithmique limite $\mu_{J_0(q)}$ et on a une formule explicite pour son espérance. Sous l'hypothèse de Riemann la valeur de l'espérance dépend de la multiplicité

du zéro en $s = \frac{1}{2}$ de $L(J_0(q), s)$. Comme il est classique de penser que les fonctions L de formes cuspidales sont « toutes »de rang 0 ou 1 et qu'il y en a autant de chaque, en supposant la conjecture de Birch et Swinnerton-Dyer, on ([Bru95]) fait la conjecture suivante.

Conjecture 3.34. *Supposons l'hypothèse de Riemann vérifiée pour $L(J_0(q), s)$, pour tout q premier. On a*

$$m\left(L(J_0(q), \cdot), \frac{1}{2}\right) \sim \frac{1}{2}|S_2(q)^*|$$

lorsque $q \to \infty$.

Des résultats dans cette direction ont été prouvés par Kowalski et Michel ([KM00a] et [KM00b]). Les auteurs montrent inconditionnellement qu'il existe deux constantes explicites $c < \frac{1}{2} < C$ telles que

$$c|S_2(q)^*| \leq m(L(J_0(q), \cdot), 1/2) \leq C|S_2(q)^*|,$$

pour tous les premiers q suffisamment grands.

La conjecture 3.34 nous laisse imaginer un rang très grand, donc potentiellement une moyenne loin de zéro. Cependant on va voir que cette valeur se compense bien avec la multiplicité du zéro en 1 de la fonction $L(J_0(q)^{(2)}, \cdot)$. L'idée est que si l'on considère toutes les formes primitives de poids 2 et de niveau q en même temps, et en supposant que la moitié a rang 0 et l'autre moitié rang 1, on pense que la moitié va donner un course biaisée vers les valeurs positives et l'autre moitié une course biaisée vers les valeurs négatives. Plus précisément on a le résultat suivant.

Théorème 3.35. *Supposons que pour tout premier q assez grand, l'hypothèse de Riemann est satisfaite pour la fonction $L(J_0(q), \cdot)$. Alors la fonction*

$$E_{J_0(q)}(x) = \frac{\log(x)}{\sqrt{x}} \sum_{p \leq x} \sum_{f \in S_2(q)^*} \lambda_f(p)$$

admet une distribution logarithmique limite. Si on suppose vérifiée la conjecture 3.34, son espérance est $o_{q\to\infty}(|S_2(q)^*|)$ et sa variance est $\gg |S_2(q)^*|$.

Remarque 52.

1. Cette fonction L ne provient pas d'une représentation irréductible comme à la sous-section 3.4.3, on peut avoir un $m(L(f^{(2)}, 1) \neq \pm 1$.
2. On est dans la situation où la variance est assez grande par rapport à l'espérance. Cela laisse penser à une possible dissipation du biais quand $q \to +\infty$. Cependant le rapport n'est pas assez petit pour pouvoir prouver la dissipation : il nous faudrait $\frac{m_q}{\sqrt{\mathrm{Var}_q}} \to 0$ pour cela, c'est-à-dire un meilleur terme d'erreur dans la conjecture 3.34.

Démonstration. Commençons par calculer la multiplicité du zéro en $s = 1$ pour la fonction $L(J_0(q)^{(2)}, s)$. On regarde pour cela les zéros locaux des fonctions $L(\wedge^2(J_0(q)), \cdot)$ et $L(\mathrm{Sym}^2(J_0(q)), \cdot)$ pour les factoriser sous une forme plus simple.

Fixons $f \in S_2(q)^*$ et notons $\alpha_f(p)$, $\overline{\alpha_f(p)}$ ses zéros locaux. On a $\alpha_f(p)\overline{\alpha_f(p)} = 1$ si $p \nmid q$. Donc

$$L(\wedge^2(J_0(q)), s) = \zeta_q(s)^{|S_2(q)^*|} \prod_{f \neq f'} L(f \otimes f', s)$$

et

$$L(\mathrm{Sym}^2(J_0(q)), s) = \prod_f L(\mathrm{Sym}^2 f, s) \prod_{f \neq f'} L(f \otimes f', s).$$

Ainsi, la fonction $L(\wedge^2(J_0(q)),\cdot)$ a un pôle d'ordre $|S_2(q)^*|$ en $s=1$, et la fonction $L(\mathrm{Sym}^2(J_0(q)),\cdot)$ est holomorphe au voisinage de $s=1$ et ne s'y annule pas. Finalement la fonction $L(J_0(q)^{(2)},\cdot)$ a un zéro de multiplicité $m(L(J_0(q)^{(2)},\cdot),1)=|S_2(q)^*|$ en $s=1$.

Le théorème 3.35 est donc une conséquence du théorème 3.19, en supposant l'hypothèse de Riemann généralisée et la conjecture 3.34. Dans cette situation l'espérance de la distribution logarithmique limite est

$$2m\left(L(J_0(q),\cdot),\frac{1}{2}\right)-|S_2(q)^*|=o(|S_2(q)^*|).$$

Enfin la variance est

$$\sum_{\substack{L(J_0(q),\frac{1}{2}+i\gamma)=0\\ \gamma\neq 0}}^{*}\frac{m(L(J_0(q),\cdot),\frac{1}{2}+i\gamma)^2}{(\frac{1}{4}+\gamma^2)}\gg\sum_{\substack{L(J_0(q),\frac{1}{2}+i\gamma)=0\\ \gamma\neq 0}}^{*}\frac{1}{(\frac{1}{4}+\gamma^2)}$$
$$\gg\log(\mathfrak{q}(J_0(q))\gg|S_2(q)^*|.$$

□

3.5 Propriétés supplémentaires de la distribution limite

D'après le théorème 3.19, étant donné un ensemble fini $\mathcal{S}$ de fonctions L analytiques stable par conjugaison et des poids a_f, la fonction $E_{\mathcal{S}}(x)=\sum_{p\leq x}\sum_{f\in\mathcal{S}}a_f\lambda_f(p)$ admet une distribution logarithmique limite $\mu_{\mathcal{S}}$. Dans cette section, on cherche des propriétés supplémentaires de la distribution $\mu_{\mathcal{S}}$. Pour cela on va faire des hypothèses supplémentaires classiques sur les zéros non-triviaux des fonctions L de l'ensemble $\mathcal{S}$, en s'inspirant de celles énoncées dans la sous-section 3.1.3.

3.5.1 Existence du biais

On a évoqué à la remarque 43 le fait que si la distribution $\mu_{\mathcal{S}}$ est suffisamment régulière alors, on peut montrer l'existence du biais. On voudrait pouvoir appliquer la formule (3.3) à la fonction $g=\mathbf{1}_{(0,+\infty)}$, cependant cette fonction n'est pas continue. L'idée heuristique de cette partie est que si la mesure $\mu_{\mathcal{S}}$ n'a pas d'accumulation de masse en 0, on ne devrait pas voir le saut de l'indicatrice. Grâce à la transformation de Fourier, on transforme cette idée en une hypothèse sur les zéros des fonctions L de $\mathcal{S}$, en utilisant la notion de zéros autonomes de la définition 3.12. On obtient alors le résultat suivant.

Théorème 3.36. *Soit $\mathcal{S}$ un ensemble fini de fonctions L analytiques vérifiant $\overline{\mathcal{S}}=\mathcal{S}$, et soit $(a_f)_{f\in\mathcal{S}}$ un ensemble de nombres complexes vérifiant $a_{\overline{f}}=\overline{a_f}$.*

1. *Supposons qu'il existe $\epsilon>0$ tel que pour tout T assez grand, il existe $\gamma_T\in\mathcal{Z}_{\mathcal{S}}^*(T^{\frac{1}{2}-\epsilon})$, un zéro $(T^{\frac{1}{2}-\epsilon},T)$-autonome. Alors $\delta(E_{\mathcal{S}})$ existe.*
2. *Supposons que $\mathcal{Z}_{\mathcal{S}}^*$ contient au moins un zéro autonome. Alors la distribution $\mu_{\mathcal{S}}$ est continue (i.e. $\mu_{\mathcal{S}}$ a une masse nulle sur les ensembles finis).*
3. *Supposons que $\mathcal{Z}_{\mathcal{S}}^*$ contient au moins trois zéros autonomes. Alors la distribution $\mu_{\mathcal{S}}$ a une densité $\phi\in L^1$ (i.e. $d\mu_{\mathcal{S}}(x)=\phi(x)dx$).*
4. *Supposons que la somme*
$$\sum_{\substack{\gamma\in\mathcal{Z}_{\mathcal{S}}^*\\ \gamma\ autonome}}\frac{1}{\gamma}$$
est divergente (conjecture 3.13). Alors la distribution $\mu_{\mathcal{S}}$ a une densité lisse $\phi\in C^\infty$ à décroissance rapide.

Remarque 53. 1. Les hypothèses faites ici sont de force croissante, mais elles sont toutes plus faibles que l'hypothèse LI (conjecture 3.10) utilisée dans [RS94] pour montrer l'existence du biais.

2. On rappelle que l'existence de $\delta(E_{\mathcal{S}})$ implique que l'ensemble $\{x \geq 2 : E_{\mathcal{S}}(x) \geq 0\}$ admet une densité logarithmique. Nous avons donc prouvé l'existence de la densité logarithmique pour de tels ensembles sous une condition assez faible.

3. Dans la situation 4, selon [MN] on peut aussi déduire que la distribution $\mu_{\mathcal{S}}$ est supportée dans tout $\mathbf{R}$. En particulier il n'y a pas de biais extrême, chacun des concurrents prend la tête de la course une densité positive de fois. On revient sur le support de la distribution $\mu_{\mathcal{S}}$ dans la sous-section 3.5.3 en faisant d'autres hypothèses.

Démonstration. La preuve de ces résultats part de la même idée que [RS94, Part. 3.1] : on commence par calculer la transformée de Fourier des distributions limites $\mu_{\mathcal{S},T}$. On a

$$\begin{aligned}\hat{\mu}_{\mathcal{S},T}(\xi) &= \int_{A_T} \exp\left(-i\xi\left(m_{\mathcal{S}} - 2\operatorname{Re}\left(\sum_{\gamma\in\mathcal{Z}_{\mathcal{S}}^*(T)} \frac{M(\gamma)e^{2i\pi t_\gamma}}{\beta_{\mathcal{S},0}+i\gamma}\right)\right)\right) dt \\ &= e^{-im_{\mathcal{S}}\xi}\int_{A_T}\prod_{\gamma\in\mathcal{Z}_{\mathcal{S}}^*(T)} \exp\left(i\xi 2\operatorname{Re}\left(M(\gamma)\frac{e^{2i\pi t_\gamma}}{\beta_{\mathcal{S},0}+i\gamma}\right)\right) dt\end{aligned}$$

où A_T est l'adhérence topologique du groupe à un paramètre $\{(\frac{\gamma_1}{2\pi}y,\dots,\frac{\gamma_{N(T)}}{2\pi}y), y \in \mathbf{R}\}/\mathbf{Z}^{N(T)}$ dans $\mathbf{T}^{N(T)}$.

Dans la situation 1, pour T assez grand, on a un élément $\gamma_T \in \mathcal{Z}_{\mathcal{S}}^*(T^{\frac{1}{2}-\epsilon})$, $(T^{\frac{1}{2}-\epsilon},T)$-autonome. On peut traiter différemment l'intégrale selon cette direction en écrivant $A_T = \mathbf{T}\times A'_T$, on sépare l'intégrale :

$$\begin{aligned}\hat{\mu}_{\mathcal{S},T}(\xi) = e^{-im_{\mathcal{S}}\xi}\int_{A'_T}\prod_{\gamma\in\mathcal{Z}_{\mathcal{S}}^*(T)-\{\gamma_T\}} \exp\left(i\xi 2\operatorname{Re}\left(M(\gamma)\frac{e^{2i\pi t_\gamma}}{\beta_{\mathcal{S},0}+i\gamma}\right)\right) dt\times \\ \int_{\mathbf{T}} \exp\left(i\xi 2\operatorname{Re}\left(M(\gamma_T)\frac{e^{2i\pi\theta}}{\beta_{\mathcal{S},0}+i\gamma_T}\right)\right) d\theta. \quad (3.16)\end{aligned}$$

On reconnaît que l'intégrale sur $\mathbf{T}$ est la 0-ème fonction de Bessel du premier type :

$$\int_{\mathbf{T}} \exp\left(i\xi 2\operatorname{Re}\left(M(\gamma_T)\frac{e^{2i\pi\theta}}{\beta_{\mathcal{S},0}+i\gamma_T}\right)\right) d\theta = J_0\left(\left|\frac{2\xi M(\gamma_T)}{\beta_{\mathcal{S},0}+i\gamma_T}\right|\right).$$

On a une estimation des valeurs des fonctions de Bessel (voir par exemple [Wat95]) : pour $x \in \mathbf{R}$,

$$|J_0(x)| \leq \min\left(1, \sqrt{\frac{2}{\pi x}}\right).$$

En bornant trivialement l'intégrale sur A'_T par 1, on obtient une borne pour la transformée de Fourier de $\mu_{\mathcal{S},T}$ pour T assez grand :

$$\begin{aligned}|\hat{\mu}_{\mathcal{S},T}(\xi)| &\leq \left|J_0\left(\left|\frac{2\xi M(\gamma_T)}{\beta_{\mathcal{S},0}+i\gamma_T}\right|\right)\right| \\ &\leq \min\left(1, \sqrt{\left|\frac{\beta_{\mathcal{S},0}+i\gamma_T}{\pi\xi M(\gamma_T)}\right|}\right). \quad (3.17)\end{aligned}$$

Revenons à l'existence du biais, on veut montrer que les limites

$$\limsup_{Y\to\infty}\frac{1}{Y}\int_2^Y \mathbf{1}_{\geq 0}(E_{\mathcal{S}}(e^y))dy$$

et

$$\liminf_{Y\to\infty}\frac{1}{Y}\int_2^Y \mathbf{1}_{\geq 0}(E_{\mathcal{S}}(e^y))dy$$

coïncident. On approche la fonction indicatrice par une fonction continue bornée et lipschitzienne. On écrit $\mathbf{1}_{\geq 0} = g_n + (\mathbf{1}_{\geq 0} - g_n)$ où g_n est la fonction n-lipschitzienne vérifiant

$$g_n(x) = \begin{cases} 0 & \text{si } x \leq -1/2n, \\ 1 & \text{si } x \geq 1/2n, \\ nx + 1/2 & \text{sinon.} \end{cases}$$

Ainsi les fonctions g_n et $|\mathbf{1}_{\geq 0} - g_n|$ sont bornées continues et n-lipschitziennes. On a donc :

$$\lim_{Y\to\infty}\frac{1}{Y}\int_2^Y g_n(G_{\mathcal{S},T}(e^y))dy = \int_{\mathbf{R}} g_n(t)d\mu_{\mathcal{S},T}(t),$$

et il en est de même pour la fonction $|\mathbf{1}_{\geq 0} - g_n|$. Ensuite en prenant T arbitrairement grand on s'approche de la distribution limite $\mu_{\mathcal{S}}$. Plus précisément on a

$$\begin{aligned}\int_{\mathbf{R}} g_n(t)d\mu_{\mathcal{S},T} - \int_{\mathbf{R}} |\mathbf{1}_{\geq 0} - g_n|(t)d\mu_{\mathcal{S},T} + O_{\mathcal{S}}\left(n\frac{\log(T)}{\sqrt{T}}\right) \\ \leq \liminf_{Y\to\infty}\frac{1}{Y}\int_2^Y \mathbf{1}_{\geq 0}(E_{\mathcal{S}}(e^y))dy \leq \limsup_{Y\to\infty}\frac{1}{Y}\int_2^Y \mathbf{1}_{\geq 0}(E_{\mathcal{S}}(e^y))dy \\ \leq \int_{\mathbf{R}} g_n(t)d\mu_{\mathcal{S},T} + \int_{\mathbf{R}} |\mathbf{1}_{\geq 0} - g_n|(t)d\mu_{\mathcal{S},T} + O_{\mathcal{S}}\left(n\frac{\log(T)}{\sqrt{T}}\right). \quad (3.18)\end{aligned}$$

De plus on peut borner les $\mu_{\mathcal{S},T}(|\mathbf{1}_{\geq 0} - g_n|)$. D'après la formule de Parseval (voir par exemple [Kat04, Th. VI.2.2]) on a :

$$\begin{aligned}\int_{\mathbf{R}} |\mathbf{1}_{\geq 0} - g_n|d\mu_{\mathcal{S},T} &= \int_{\mathbf{R}} 2n\frac{1-\cos(\xi/2n)}{\xi^2}\hat{\mu}_{\mathcal{S},T}(\xi)d\xi \\ &\ll \int_{|\xi|\leq\alpha(n)}\frac{1}{2n}|\hat{\mu}_{\mathcal{S},T}(\xi)|d\xi + \int_{|\xi|\geq\alpha(n)}\frac{4n}{\xi^2}|\hat{\mu}_{\mathcal{S},T}(\xi)|d\xi\end{aligned}$$

en choisissant de couper à un $\alpha(n) < 2n$. D'après la majoration (3.17), on a :

$$\begin{aligned}\int_{\mathbf{R}} |\mathbf{1}_{\geq 0} - g_n|d\mu_{\mathcal{S},T} &\ll \frac{2\alpha(n)}{2n} + \int_{|\xi|\geq\alpha(n)}\frac{4n\sqrt{\gamma_T}}{|\xi|^{5/2}}d\xi \\ &\ll \frac{\alpha(n)}{n} + \frac{n\sqrt{\gamma_T}}{\alpha(n)^{3/2}}.\end{aligned}$$

Prenons $n = \sqrt{T^{1-\epsilon}}$ et $\alpha(n) = n^{1-\frac{\epsilon}{3}}$, alors comme $\gamma_T \leq T^{\frac{1}{2}-\epsilon}$, les termes de reste dans l'expression (3.18) tendent vers 0 quand $T \to +\infty$. On en déduit que les densités inférieure et supérieure coïncident, donc on a prouvé le point 1.

Pour 2, on revient à l'expression (3.17) mais cette fois le zéro autonome ne dépend plus de T. On a donc une borne comme en (3.17) indépendante de T pour tout $T \geq \gamma_{T_0}$. En faisant $T \to +\infty$ on obtient la même borne pour $\hat{\mu}_{\mathcal{S}}$. Alors le fait que la distribution $\mu_{\mathcal{S}}$ est continue est une conséquence d'un théorème de Wiener (voir par exemple [Kat04, Th. VI.2.11]). En effet ce théorème de Wiener assure qu'une mesure μ est continue si et seulement si

$$\lim_{Y\to\infty}\frac{1}{2Y}\int_{-Y}^Y |\hat{\mu}(\xi)|^2 d\xi = 0.$$

La borne obtenue dans (3.17) garantit qu'on a cette condition, donc $\mu_{\mathcal{S}}$ est bien continue.

Pour 3 et 4 on peut de nouveau faire le même raisonnement que précédemment. Dans le calcul de la transformée de Fourier de $\mu_{\mathcal{S},T}$ on va trouver autant de facteurs J_0 qu'on a de zéros autonomes. En bornant les facteurs J_0 comme précédemment et le facteur venant de l'intégrale sur les zéros qui ne sont pas autonomes par 1 on obtient ainsi une borne pour la transformée de Fourier de $\mu_{\mathcal{S}}$. Ces bornes permettent de déduire les résultats annoncés. En effet pour 3, on déduit que $\hat{\mu}_{\mathcal{S}} \in L^1 \cap L^2$. Pour 4, de la même façon on obtient une majoration de $\hat{\mu}_{\mathcal{S},T}$ pour tout T qui permet de déduire que $\hat{\mu}_{\mathcal{S}}$ décroît plus vite que toute inverse de polynôme. On montre ainsi que $\mu_{\mathcal{S}}$ admet une densité $\phi \in C^\infty \cap L^1$. La décroissance rapide est une conséquence du lemme 3.27. □

3.5.2 Symétrie

Sous l'hypothèse LI (conjecture 3.10) Rubinstein et Sarnak montrent que la distribution $\mu_{\mathcal{S}}$ est symétrique par rapport à sa moyenne. On va montrer la symétrie sous une hypothèse plus faible, mais qui repose encore sur une certaine propriété d'indépendance linéaire entre les éléments de $\mathcal{Z}_{\mathcal{S}}$.

Théorème 3.37. *Supposons la conjecture 3.14 vérifiée : pour tout $(k_\gamma)_\gamma \in \mathbf{Z}^{(\mathcal{Z}_{\mathcal{S}})}$ tel que $\sum_{\gamma \in \mathcal{Z}_{\mathcal{S}}} k_\gamma \gamma = 0$ on a $\sum_{\gamma \in \mathcal{Z}_{\mathcal{S}}} k_\gamma \equiv 0 \,[\bmod\ 2]$. Alors la distribution limite $\mu_{\mathcal{S}}$ est symétrique par rapport à sa moyenne $m_{\mathcal{S}}$.*

On va montrer ce résultat en montrant que pour tout T la distribution $\mu_{\mathcal{S},T}$ est symétrique. Pour cela on va donner plus de précisions sur la mesure de Haar normalisée venant du théorème de Kronecker–Weyl tel qu'on l'a utilisé dans la preuve du lemme 3.26. Commençons par reformuler la conjecture 3.14.

Lemme 3.38. *Les assertions suivantes sont équivalentes :*

- *pour toute combinaison linéaire entière $\sum_{\gamma \in \mathcal{Z}_{\mathcal{S}}} k_\gamma \gamma = 0$, $k_\gamma \in \mathbf{Z}$, on a $\sum_{\gamma \in \mathcal{Z}} k_\gamma \equiv 0$ [mod 2],*
- *pour tout sous-ensemble fini $\{\gamma_1, \dots \gamma_N\} \subset \mathcal{Z}_{\mathcal{S}}$, l'élément $\left(\frac{1}{2}, \dots, \frac{1}{2}\right)$ est dans l'adhérence du groupe à un paramètre*

$$\{(\frac{\gamma_1}{2\pi} y, \dots, \frac{\gamma_N}{2\pi} y), y \in \mathbf{R}\}/\mathbf{Z}^N$$

dans $\mathbf{T}^N$.

Remarque 54. La conjecture 3.10 est elle équivalente au fait que l'adhérence de chacun de ces groupes à un paramètre est le tore $\mathbf{T}^N$ tout entier. Cependant pour montrer la symétrie il suffit de savoir que ces adhérences contiennent le point central.

Démonstration. Prenons le sous-espace $\mathbf{Q}$-orthogonal à l'ensemble

$$\Gamma := \{(\frac{\gamma_1}{2\pi} y, \dots, \frac{\gamma_N}{2\pi} y), y \in \mathbf{R}\}/\mathbf{Z}^{N(T)}.$$

On a

$$\Gamma^\perp = \{(r_1, \dots, r_N) \in \mathbf{Q}^N : \sum_{i=1}^N r_i \frac{\gamma_i}{2\pi} = 0\}.$$

Quitte à multiplier par les dénominateurs, on ne perd pas d'information en ne considérant que les éléments dans $\mathbf{Z}^N$ de cet ensemble. Alors l'adhérence de Γ est l'orthogonal de son orthogonal :

$$A = (\Gamma^\perp)_\perp = \{(\theta_1, \dots, \theta_N) \in \mathbf{T}^N : \forall k \in \Gamma^\perp, \sum_{i=1}^N k_i \theta_i = 0 \ [\bmod\ 1]\}.$$

Ainsi $\left(\frac{1}{2}, \dots, \frac{1}{2}\right) \in A$ si et seulement si pour tout $k \in \Gamma^\perp$ on a $\sum_{i=1}^N k_i = 0$ [mod 2] □

On peut maintenant montrer le théorème 3.37.

Démonstration du théorème 3.37. On montre que pour tout $T > 2$, la distribution $\mu_{\mathcal{S},T}$ est symétrique par rapport à sa moyenne. D'après la preuve du lemme 3.26, la distribution $\mu_{\mathcal{S},T}$ est la tirée en arrière de la mesure de Haar normalisée ω_{A_T} sur l'adhérence du groupe à un paramètre $\{(\frac{\gamma_1}{2\pi}y, \dots, \frac{\gamma_{N(T)}}{2\pi}y), y \in \mathbf{R}\}/\mathbf{Z}^{N(T)}$ dans $\mathbf{T}^{N(T)}$.

D'après le lemme 3.38, le point $\left(\frac{1}{2}, \dots, \frac{1}{2}\right)$ est dans le sous-tore A_T, donc $A = A + \left(\frac{1}{2}, \dots, \frac{1}{2}\right)$. On fait le changement de variable $a \to a + (\frac{1}{2}, \dots, \frac{1}{2})$ dans l'intégrale qui définit $\mu_{\mathcal{S},T}$. Pour tout $T > 2$ et pour toute fonction g continue bornée lipschitzienne, on a

$$\begin{aligned}\int_{\mathbf{R}} g(t)d\mu_{\mathcal{S},T} &= \int_{A_T} \tilde{g}(a)d\omega_{A_T} \\ &= \int_{A_T} \tilde{g}\left(a + \left(\frac{1}{2}, \dots, \frac{1}{2}\right)\right) d\omega_{A_T} = \int_{\mathbf{R}} g(2m_f - t)d\mu_{\mathcal{S},T}\end{aligned}$$

où on utilise la notation $\tilde{g}$ définie en (3.12). On a $\tilde{g}((a + (\frac{1}{2}, \dots, \frac{1}{2}))) = \tilde{h}(a)$ où h est la fonction donnée par $h(x) = g(2m_f - x)$.

En prenant T arbitrairement grand dans (3.14), on en déduit que la distribution $\mu_{\mathcal{S}}$ est aussi symétrique. □

Revenons sur la valeur de l'espérance,

$$m_{\mathcal{S}} = \sum_{f \in \mathcal{S}} a_f \left(-\frac{m(L(f), \beta_{\mathcal{S},0})}{\beta_{\mathcal{S},0}} + m(L(f^{(2)}), 1)\delta_{\frac{1}{2}, \beta_{\mathcal{S},0}} \right).$$

Cette valeur est non-nulle seulement si il existe un f tel que $L(f, \beta_{\mathcal{S},0}) = 0$ ou si l'hypothèse de Riemann est vérifiée pour chacune des fonctions L de l'ensemble $\mathcal{S}$.

En supposant la conjecture 3.14, la distribution $\mu_{\mathcal{S}}$ est symétrique par rapport à son espérance. Dans le cas où cette espérance est nulle on a $\mu(\infty, 0] - \mu[0, \infty) = 0$ donc pas de biais a priori. Par contre si l'espérance n'est pas nulle, on a tendance à penser que le biais sera différent de $\frac{1}{2}$. Si la distribution $\mu_{\mathcal{S}}$ admet une densité lisse (voir le théorème 3.36.4), on peut effectivement en déduire que le biais est en direction du signe de la moyenne.

Prenons le problème dans l'autre sens, comme dans [Fio14a, Th. 1.7]. Les remarques précédentes permettent de déduire le résultat suivant.

Proposition 3.39. *Soit $\mathcal{S}$ un ensemble fini de fonctions L analytiques stable par conjugaison. On suppose vérifiée la conjecture 3.14. Alors si $\mu_{\mathcal{S}}[0, \infty) - \mu_{\mathcal{S}}(-\infty, 0] \neq 0$, soit l'hypothèse de Riemann est satisfaite pour toutes les fonctions L de $\mathcal{S}$, soit il existe f telle que $L(f, \beta_{\mathcal{S},0}) = 0$.*

3.5.3 Support

Dans [RS94, Th. 1.2], Rubinstein et Sarnak montrent conditionnellement à l'hypothèse de Riemann généralisée pour les fonctions L de Dirichlet que la distribution $\mu_{R,N,q}$ associée à la course entre les carrés et non carrés modulo q est supportée dans tout $\mathbf{R}$. En particulier il ne peut pas y avoir de biais extrême (égal à 0 ou à 1). Dit autrement, la fonction $E_{R,N,q}$ associée change infiniment souvent de signe : chaque concurrent prend la tête de la course une infinité de fois.

La preuve de Rubinstein et Sarnak s'adapte bien dans notre cadre plus général toujours conditionnellement à l'hypothèse de Riemann généralisée. Si l'hypothèse de Riemann n'est pas satisfaite, on suppose que la conjecture 3.8 s'applique. On peut alors montrer dans ce cas que la distribution associée a un support borné. Précisément on a la dichotomie suivante.

Théorème 3.40. *Soit $\mathcal{S}$ un ensemble fini de fonctions L analytiques vérifiant $\overline{\mathcal{S}} = \mathcal{S}$, et soit $(a_f)_{f\in\mathcal{S}}$ un ensemble de nombres complexes vérifiant $a_{\overline{f}} = \overline{a_f}$.*

1. *Supposons que l'hypothèse de Riemann généralisée est satisfaite pour toutes les fonctions L de $\mathcal{S}$ (conjecture 3.6). Supposons de plus que $\mathrm{Re}(a_f) \geq 0$ pour tout $f \in \mathcal{S}$, et qu'il existe $f \in \mathcal{S}$ tel que $\mathrm{Re}(a_f) > 0$, alors $\operatorname{supp}\mu_{\mathcal{S}} = \mathbf{R}$. En particulier*

$$0 < \underline{\delta}(\mathcal{S}) \leq \overline{\delta}(\mathcal{S}) < 1.$$

2. *Supposons que $\beta_{\mathcal{S},0} > \frac{1}{2}$ et que la conjecture 3.8 est satisfaite pour toutes les fonctions L de $\mathcal{S}$. Alors*

$$\operatorname{supp}\mu_{\mathcal{S}} \subset \left[m_{\mathcal{S}} - \sum_{\gamma\in\mathcal{Z}_{\mathcal{S}}^*} \frac{|M_{\mathcal{S}}(\gamma)|}{|\beta_{\mathcal{S},0}+i\gamma|}, m_{\mathcal{S}} + \sum_{\gamma\in\mathcal{Z}_{\mathcal{S}}} \frac{|M_{\mathcal{S}}(\gamma)|}{|\beta_{\mathcal{S},0}+i\gamma|} \right].$$

Remarque 55.
1. En particulier l'hypothèse supplémentaire de 1 est vérifiée si l'ensemble $\mathcal{S}$ est un singleton. Elle est aussi vérifiée dans le cas où on fait la course des nombres premiers dans les classes de congruences modulo un entier q entre la classe 1 [mod q] et une autre classe inversible selon la situation exposée dans la sous-section 3.4.1.
2. D'après le théorème de Kaczorowski–Perelli (théorème 3.9), si les fonctions L de l'ensemble $\mathcal{S}$ sont toutes de degré au plus d et si on a $\beta_{\mathcal{S},0} \geq 1 - \frac{1}{4(d+3)}$ alors 2 s'applique, donc la mesure $\mu_{\mathcal{S}}$ a support borné.

Démonstration du théorème 3.40. Commençons par le point 2 ; plus facile.

D'après la conjecture 3.8, la somme sur les zéros $\sum_{\gamma\in\mathcal{Z}_{\mathcal{S}}^*} \frac{|M_{\mathcal{S}}(\gamma)|}{|\beta_{\mathcal{S},0}+i\gamma|}$ est convergente. Donc pour tout $T > 2$, la distribution logarithmique limite $\mu_{\mathcal{S},T}$ a un support inclus dans l'intervalle

$$\left[m_{\mathcal{S}} - \sum_{\gamma\in\mathcal{Z}_{\mathcal{S}}^*} \frac{|M_{\mathcal{S}}(\gamma)|}{|\beta_{\mathcal{S},0}+i\gamma|}, m_{\mathcal{S}} + \sum_{\gamma\in\mathcal{Z}_{\mathcal{S}}^*} \frac{|M_{\mathcal{S}}(\gamma)|}{|\beta_{\mathcal{S},0}+i\gamma|} \right].$$

Cet intervalle ne dépend pas de T, donc on peut passer à la limite quand $T \to \infty$ dans l'expression (3.14).

Prouvons maintenant le point 1. On suit pour cela la preuve de [RS94, Th. 1.2]. L'idée est de montrer que $\mu_{\mathcal{S}}([A,\infty)) \geq \phi(A) > 0$ pour une certaine fonction strictement positive ϕ de A. Pour cela on va minorer la mesure d'ensembles du type $\{y \leq M, E_{\mathcal{S}}(e^y) > A\}$ en minorant des intégrales de $E_{\mathcal{S}}(e^y)$ sur des intervalles assez petits pour que $E_{\mathcal{S}}(e^y)$ ne varie pas trop.

Précisément, pour $\epsilon > 0$ petit et $t \geq 1$ on définit

$$F_\epsilon(t) = \frac{1}{2\epsilon}\int_{t-\epsilon}^{t+\epsilon} E_{\mathcal{S}}(e^y)dy.$$

D'après l'expression (3.11) en supposant l'hypothèse de Riemann, on a

$$E_{\mathcal{S}}(e^y) = m_{\mathcal{S}} - \sum_{\gamma\in\mathcal{Z}_{\mathcal{S}}^*(T)} 2\,\mathrm{Re}\left(M_{\mathcal{S}}(\gamma)\frac{e^{i\gamma y}}{\frac{1}{2}+i\gamma}\right) - \epsilon_{\mathcal{S}}(e^y,T) + o(1).$$

D'après l'expression (3.8), on a

$$|\epsilon_{\mathcal{S}}(e^y,T)| \ll_{\mathcal{S}} ye^{-\frac{y}{2}} + \frac{y^2e^{\frac{y}{2}}}{T} + \frac{e^{\frac{y}{2}}\log(T)}{T}.$$

Comme la somme $\sum \frac{1}{\gamma^2}$ est convergente, on en déduit en intégrant autour de t que

$$F_\epsilon(t) = \frac{2}{\epsilon} \sum_{\gamma \in \mathcal{Z}_{\mathcal{S}}^*(T)} \mathrm{Re}(M_{\mathcal{S}}(\gamma)) \frac{\sin(\gamma t)\sin(\gamma\epsilon)}{\gamma^2} + O_{\mathcal{S}}\left(e^{t/2}\left(\frac{t^2}{T} + \frac{\log(T)}{T}\right) + 1\right).$$

On prend la limite quand $T \to \infty$, alors

$$F_\epsilon(t) = \frac{2}{\epsilon} \sum_{\gamma \in \mathcal{Z}_{\mathcal{S}}^*} \frac{\sin(\gamma t)\sin(\gamma\epsilon)}{\gamma^2} + O_{\mathcal{S}}(1) \tag{3.19}$$

pour $t \geq 1$.

On va montrer que $F_\epsilon(t)$ est assez grande pour « suffisamment » de $t \geq 1$. On commence par étudier les fonctions auxiliaires

$$\tilde{F}_{\epsilon,T}(t) := \frac{2}{\epsilon} \sum_{\gamma \in \mathcal{Z}_{\mathcal{S}}^*(T)} \mathrm{Re}(M_{\mathcal{S}}(\gamma)) \frac{\sin(\gamma t)\sin(\gamma\epsilon)}{\gamma^2}.$$

On a

$$\begin{aligned}\tilde{F}_{\epsilon,T}(\epsilon) &= 2\epsilon \sum_{\gamma \in \mathcal{Z}_{\mathcal{S}}^*(T)} \mathrm{Re}(M_{\mathcal{S}}(\gamma)) \left(\frac{\sin(\gamma\epsilon)}{\gamma\epsilon}\right)^2 \\ &\geq c_0\epsilon \sum_{\gamma \in \mathcal{Z}_{\mathcal{S}}^*(1/\epsilon)} \mathrm{Re}(M_{\mathcal{S}}(\gamma)) = c_0\epsilon N(1/\epsilon),\end{aligned}$$

pour un certain $c_0 > 0$, si $T \geq 1/\epsilon$. Ici on a utilisé l'hypothèse $\mathrm{Re}(M_{\mathcal{S}}(\gamma)) \geq 0$ (avec l'inégalité stricte pour certains γ). La fonction N est définie par $N(T) := \sum_{\mathrm{Re}(a_f)>0} |\mathcal{Z}_f(T)|$. Sous l'hypothèse de Riemann d'après la proposition 3.4 on a $N(T) \asymp T\log(T)$.

Remarque 56. Si on ne suppose pas l'hypothèse de Riemann, on n'a pas de minorant pour la valeur de $N(T)$. De plus si on suppose la conjecture 3.8, on en déduit que $\epsilon N(1/\epsilon) \to 0$ quand $\epsilon \to 0$. En particulier, il est difficile de montrer que $\tilde{F}_{\epsilon,T}(\epsilon)$ est grand.

On cherche d'autres valeurs où $\tilde{F}_{\epsilon,T}$ est grande. Pour tout entier m on a :

$$\begin{aligned}|\tilde{F}_{\epsilon,T}(\epsilon) - \tilde{F}_{\epsilon,T}((m+1)\epsilon)| &\leq 2 \sum_{\gamma \in \mathcal{Z}_{\mathcal{S}}^*(T)} \mathrm{Re}(M_{\mathcal{S}}(\gamma)) |\sin(\gamma\epsilon) - \sin(\gamma(m+1)\epsilon)| \frac{|\sin(\gamma\epsilon)|}{\gamma^2\epsilon} \\ &\leq 2 \max_{\gamma \in \mathcal{Z}_{\mathcal{S}}^*(T)} (\|\gamma m\epsilon\|) \sum_{\gamma \in \mathcal{Z}_{\mathcal{S}}^*(T)} \frac{\mathrm{Re}(M_{\mathcal{S}}(\gamma))}{\gamma}\end{aligned}$$

où $\|\cdot\|$ est la distance au multiple entier de 2π le plus proche. On veut que le terme de droite soit suffisamment petit pour assurer que $\tilde{F}_{\epsilon,T}((m+1)\epsilon)$ est assez grand. Il suffit que m vérifie

$$\max_{\gamma \in \mathcal{Z}_{\mathcal{S}}^*(T)} (\|\gamma m\epsilon\|) \leq \frac{c_0\epsilon N(1/\epsilon)}{4\sum_{\gamma \in \mathcal{Z}_{\mathcal{S}}^*(T)} \frac{\mathrm{Re}(M_{\mathcal{S}}(\gamma))}{\gamma}}, \tag{3.20}$$

alors $\tilde{F}_{\epsilon,T}((m+1)\epsilon) \geq \frac{c_0}{2}\epsilon N(1/\epsilon)$.

Remarque 57. Si on ne suppose pas l'hypothèse de Riemann, la condition que l'on obtient ici est

$$\max_{\gamma \in \mathcal{Z}_{\mathcal{S}}^*(T)} \left(\|\gamma m\epsilon\| + \frac{1}{2}|1 - e^{(1-2\beta_{\mathcal{S},0})(m+1)\epsilon}| \|2\gamma(m+1)\epsilon\|\right) \leq \frac{\tilde{F}_{\epsilon,T}(\epsilon)}{4S(T)} \tag{3.21}$$

où $S(T) = \sum_{\gamma \in \mathcal{Z}_{\mathcal{S}}^*(T)} \frac{\mathrm{Re}(M_{\mathcal{S}}(\gamma))}{\gamma}$. Cette somme est bornée si on suppose la conjecture 3.8 vérifiée. On a pour tout γ,

$$\|\gamma m\epsilon\| + \frac{1}{2}|1 - e^{(1-2\beta_{\mathcal{S},0})(m+1)\epsilon}|\|2\gamma(m+1)\epsilon\| \geq \frac{1}{2}|1 - e^{(1-2\beta_{\mathcal{S},0})(m+1)\epsilon}|\|2\gamma\epsilon\|.$$

Pour avoir l'inégalité (3.21) il nous faut donc au moins

$$\|2\gamma\epsilon\| \ll \tilde{F}_{\epsilon,T}(\epsilon),$$

pour tout $\gamma \leq T$. On a la condition $T \geq 1/\epsilon$, et on a seulement une borne inférieure sur la valeur $\tilde{F}_{\epsilon,T}(\epsilon) \gg \epsilon$ en supposant l'ensemble $\mathcal{Z}_{\mathcal{S}}^*$ non vide. La condition (3.21) semble donc vraiment trop forte pour pouvoir être réalisée en général.

Montrons que si la condition (3.20) est vérifiée pour un entier m, alors la valeur $F_\epsilon((m+1)\epsilon)$ est aussi assez grande. Soit M un entier fixé, on pose G_M l'ensemble des m tels que $1/\epsilon \leq m \leq M/\epsilon$ vérifiant la condition (3.20). Alors pour $m \in G_M$, on a

$$\begin{aligned}|F_\epsilon((m+1)\epsilon) - \tilde{F}_{\epsilon,T}((m+1)\epsilon)| &\leq \frac{2}{\epsilon}\sum_{T<\gamma} \frac{|\sin(\gamma(m+1)\epsilon)\sin(\gamma\epsilon)|}{\gamma^2} + O(1)\\ &\ll \frac{2}{\epsilon}\frac{\log(T)}{T} + 1 \ll \frac{c_0}{4}\epsilon N(1/\epsilon).\end{aligned}$$

On choisit $T = \epsilon^{-2}$, alors le membre de gauche est borné. Ainsi, pour m dans G_M,

$$F_\epsilon((m+1)\epsilon) \geq \frac{c_0}{4}\epsilon N(1/\epsilon).$$

On veut maintenant minorer la taille de l'ensemble G_M. On utilise le principe des tiroirs. On coupe le cube $N(1/\epsilon)$-dimensionnel en petits cubes de taille $\frac{c_0\epsilon N(1/\epsilon)}{8S(\epsilon^{-2})}$, on obtient ainsi de l'ordre de $\left(\frac{c_0\epsilon N(1/\epsilon)}{8S(\epsilon^{-2})}\right)^{-N(1/\epsilon)}$ petits cubes. Alors il existe un petit cube qui contient au moins

$$\nu = \left[(M-1)\left(\frac{c_0\epsilon N(1/\epsilon)}{8S(\epsilon^{-2})}\right)^{N(1/\epsilon)}\right]$$

vecteurs de la forme $m(\gamma_1\epsilon/2\pi, \ldots, \gamma_{N(1/\epsilon)}\epsilon/2\pi)$ pour $\frac{1}{\epsilon} < m < \frac{M}{\epsilon}$ de la forme $m = k\,([1/\epsilon]+1)$. On a donc ν entiers $m_1 < m_2 < \ldots < m_\nu$, pour chaque $2 \leq i \leq \nu$ on forme l'entier $n_i = m_i - m_1$, c'est un élément de G_M. Ainsi

$$|G_M| \geq \nu - 1 \gg M\left(\frac{c_0\log(1/\epsilon)}{8\log(\epsilon^{-2})}\right)^{\epsilon\log(1/\epsilon)}. \tag{3.22}$$

Soit $m \in G_M$, on va montrer qu'il y a un ensemble de y de mesure positive autour de $(m+1)\epsilon$ pour lesquels $E_{\mathcal{S}}(e^y)$ est grand. On note λ la mesure de Lebesgue sur $\mathbf{R}$. On veut minorer

$$\lambda(m,\epsilon) = \lambda\left(\{y \in [m\epsilon,(m+2)\epsilon], E_{\mathcal{S}}(e^y) > \frac{c_0}{8}\epsilon N(1/\epsilon)\}\right).$$

On a

$$\frac{1}{2\epsilon}\int_{m\epsilon}^{(m+2)\epsilon} E_{\mathcal{S}}(e^y)\mathbf{1}_{E_{\mathcal{S}}(e^y)<\frac{c_0}{8}\epsilon N(1/\epsilon)}dy < \frac{c_0}{8}\epsilon N(1/\epsilon).$$

Donc

$$\begin{aligned}\frac{1}{2\epsilon}\int_{m\epsilon}^{(m+2)\epsilon} E_{\mathcal{S}}(e^y)\mathbf{1}_{E_{\mathcal{S}}(e^y)\geq\frac{c_0}{8}\epsilon N(1/\epsilon)}dy &\geq F_\epsilon((m+1)\epsilon) - \frac{c_0}{8}\epsilon N(1/\epsilon)\\ &\geq \frac{c_0}{8}\epsilon N(1/\epsilon).\end{aligned}$$

D'autre part, en utilisant l'inégalité de Cauchy-Schwarz, on a

$$\frac{1}{2\epsilon}\int_{m\epsilon}^{(m+2)\epsilon} E_{\mathcal{S}}(e^y)\mathbf{1}_{E_{\mathcal{S}}(e^y)\geq \frac{c_0}{8}\epsilon N(1/\epsilon)}dy \leq \frac{1}{2\epsilon}\left(\int_{m\epsilon}^{(m+2)\epsilon} E_{\mathcal{S}}(e^y)^2 dy\right)^{1/2}\lambda(m,\epsilon)^{1/2},$$

d'où

$$\lambda(m,\epsilon) \geq 4\epsilon^2\left(\int_{m\epsilon}^{(m+2)\epsilon} E_{\mathcal{S}}(e^y)^2 dy\right)^{-1}\left(\frac{c_0}{8}\epsilon N(1/\epsilon)\right)^2.$$

On peut maintenant minorer la mesure de Lebesgue de la réunion de tels ensembles. On a

$$\begin{aligned}\lambda\left(\{y\in[1,M+2\epsilon], E_{\mathcal{S}}(e^y) > \frac{c_0}{8}\epsilon N(1/\epsilon)\}\right) &\geq \frac{1}{2}\sum_{m\in G_M}\lambda(m,\epsilon)\\ &\geq \frac{1}{2}\sum_{m\in G_M}\left(\int_{m\epsilon}^{(m+2)\epsilon} E_{\mathcal{S}}(e^y)^2 dy\right)^{-1}\left(\frac{c_0}{4}\epsilon^2 N(1/\epsilon)\right)^2.\end{aligned}$$

Grâce à l'inégalité de Cauchy-Schwarz, on a

$$\sum_{m\in G_M}\left(\int_{m\epsilon}^{(m+2)\epsilon} E_{\mathcal{S}}(e^y)^2 dy\right)^{-1} \geq |G_M|^2\left(2\int_{\log(2)}^{M+2} E_{\mathcal{S}}(e^y)^2 dy\right)^{-1}.$$

On utilise l'expression (3.11), et le lemme 3.23 pour T fixé. Il existe une constante c telle que

$$\int_{\log(2)}^{M+2} E_{\mathcal{S}}(e^y)^2 dy \leq cM.$$

Finalement en utilisant (3.22), on obtient

$$\lambda\left(\{y\in[1,M+2\epsilon], E_{\mathcal{S}}(e^y) > \frac{c_0}{8}\epsilon N(1/\epsilon)\}\right) \gg M\left(\frac{\log(1/\epsilon)}{\log(\epsilon^{-2})}\right)^{2\epsilon\log(1/\epsilon)}(\epsilon\log(1/\epsilon))^2.$$

On divise par M et on fait tendre M vers l'infini, le terme de gauche donne la densité logarithmique $\mu((\frac{c_0}{8}\epsilon N(1/\epsilon),\infty))$. Ainsi prenons $A = \frac{c_0}{8}\epsilon N(1/\epsilon)$, en inversant la fonction (décroissante) $\epsilon \mapsto A = \frac{c_0}{8}\epsilon N(1/\epsilon)$ pour ϵ assez petit on trouve une minoration de la forme

$$\mu((A,\infty)) \geq \phi(A) > 0,$$

pour A assez grand. Ce qui conclut.

On peut suivre le même argument pour $-\epsilon$ au lieu de ϵ. On a

$$\tilde{F}_{\epsilon,T}(-\epsilon) \leq -c_0\epsilon N(1/\epsilon).$$

Donc en suivant le raisonnement, on obtient

$$\mu((-\infty,-A)) \geq \phi(A) > 0$$

pour A assez grand.

□

Bibliographie

[ABBVA14] A. Auel, M. Bernardara, M. Bolognesi, and A. Várilly-Alvarado. Cubic fourfolds containing a plane and a quintic del Pezzo surface. *Algebr. Geom.*, 1(2) :181–193, 2014.

[ANS14] A. Akbary, N. Ng, and M. Shahabi. Limiting distributions of the classical error terms of prime number theory. *Q. J. Math.*, 65(3) :743–780, 2014.

[BCDT01] C. Breuil, B. Conrad, F. Diamond, and R. Taylor. On the modularity of elliptic curves over **Q** : wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4) :843–939, 2001.

[Bel16] J. Bellaïche. Théorème de Chebotarev et complexité de Littlewood. *Annales scientifiques de l'ENS*, 49(fascicule 3) :579–632, 2016.

[BG92] D. Bump and D. Ginzburg. Symmetric square L-functions on $\mathrm{GL}(r)$. *Ann. of Math. (2)*, 136(1) :137–205, 1992.

[BO78] P. Berthelot and A. Ogus. *Notes on crystalline cohomology*. Princeton University Press, Princeton, N.J. ; University of Tokyo Press, Tokyo, 1978.

[BPVdV84] W. Barth, C. Peters, and A. Van de Ven. *Compact complex surfaces*, volume 4 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1984.

[Bru95] A. Brumer. The rank of $J_0(N)$. *Astérisque*, (228) :3, 41–68, 1995. Columbia University Number Theory Seminar (New York, 1992).

[Cha97] N. Chavdarov. The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy. *Duke Math. J.*, 87(1) :151–180, 1997.

[Che99] P.L. Chebyshev. *Oeuvres de P.L. Tchebychef*, volume I, chapter Lettre de M. le professeur Tchebychev à M. Fuss, sur le nouveau théorème relatif aux nombres premiers contenus dans les formes $4n+1$ et $4n+3$., pages 697–698. St. Petersbourg, Commissionaires de l'Academie imperiale des sciences, 1899.

[CHT08] L. Clozel, M. Harris, and R. Taylor. Automorphy for some l-adic lifts of automorphic mod l Galois representations. *Publ. Math. Inst. Hautes Études Sci.*, (108) :1–181, 2008. With Appendix A, summarizing unpublished work of Russ Mann, and Appendix B by Marie-France Vignéras.

[Cog04] J. W. Cogdell. Lectures on L-functions, converse theorems, and functoriality for GL_n. In *Lectures on automorphic L-functions*, volume 20 of *Fields Inst. Monogr.*, pages 1–96. Amer. Math. Soc., Providence, RI, 2004.

[CR12] S. Cynk and S. Rams. Invariants of hypersurfaces and logarithmic differential forms. In *Contributions to algebraic geometry*, EMS Ser. Congr. Rep., pages 189–213. Eur. Math. Soc., Zürich, 2012.

[Del74] P. Deligne. La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.*, (43) :273–307, 1974.

[Del77] P. Deligne. *Cohomologie étale.* Lecture Notes in Mathematics, Vol. 569. Springer-Verlag, Berlin-New York, 1977. Séminaire de Géométrie Algébrique du Bois-Marie SGA $4\frac{1}{2}$, Avec la collaboration de J. F. Boutot, A. Grothendieck, L. Illusie et J. L. Verdier.

[Del80] P. Deligne. La conjecture de Weil. II. *Inst. Hautes Études Sci. Publ. Math.*, (52) :137–252, 1980.

[Dev17] L. Devin. On the congruence class modulo prime numbers of the number of rational points of a variety. *Int. Math. Res. Notices*, 2017.

[Dim92] A. Dimca. *Singularities and topology of hypersurfaces.* Universitext. Springer-Verlag, New York, 1992.

[DS74] P. Deligne and J.-P. Serre. Formes modulaires de poids 1. *Ann. Sci. École Norm. Sup. (4)*, 7 :507–530 (1975), 1974.

[EEHK09] J. S. Ellenberg, C. Elsholtz, C. Hall, and E. Kowalski. Non-simple abelian varieties in a family : geometric and analytic approaches. *J. Lond. Math. Soc. (2)*, 80(1) :135–154, 2009.

[Elk87] N. D. Elkies. The existence of infinitely many supersingular primes for every elliptic curve over $\mathbf{Q}$. *Invent. Math.*, 89(3) :561–567, 1987.

[Esn03] H. Esnault. Varieties over a finite field with trivial Chow group of 0-cycles have a rational point. *Invent. Math.*, 151(1) :187–191, 2003.

[Fio14a] D. Fiorilli. Elliptic curves of unbounded rank and Chebyshev's bias. *Int. Math. Res. Not. IMRN*, (18) :4997–5024, 2014.

[Fio14b] D. Fiorilli. Highly biased prime number races. *Algebra Number Theory*, 8(7) :1733–1767, 2014.

[FK01] E. Fouvry and N. Katz. A general stratification theorem for exponential sums, and applications. *J. Reine Angew. Math.*, 540 :115–166, 2001.

[FK02] K. Ford and S. Konyagin. The prime number race and zeros of L-functions off the critical line. *Duke Math. J.*, 113(2) :313–330, 2002.

[FKRS12] F. Fité, K. S. Kedlaya, V. Rotger, and A. V. Sutherland. Sato–Tate distributions and Galois endomorphism modules in genus 2. *Compositio Mathematica*, 148(5) :1390–1442, Sep 2012.

[FL96] A. Fuchs and G. Letta. Le problème du premier chiffre décimal pour les nombres premiers. *Electron. J. Combin.*, 3(2) :Research Paper 25, approx. 7 pp. 1996. The Foata Festschrift.

[FM13] D. Fiorilli and G. Martin. Inequities in the Shanks-Rényi prime number race : an asymptotic formula for the densities. *J. Reine Angew. Math.*, 676 :121–212, 2013.

[Gal73] P. X. Gallagher. The large sieve and probabilistic Galois theory. pages 91–101, 1973.

[GJ72] R. Godement and H. Jacquet. *Zeta functions of simple algebras.* Lecture Notes in Mathematics, Vol. 260. Springer-Verlag, Berlin-New York, 1972.

[GM06] A. Granville and G. Martin. Prime number races. *Amer. Math. Monthly*, 113(1) :1–33, 2006.

[Gro68] A. Grothendieck. Le groupe de Brauer. I. Algèbres d'Azumaya et interprétations diverses. In *Dix Exposés sur la Cohomologie des Schémas*, pages 46–66. North-Holland, Amsterdam ; Masson, Paris, 1968.

[Hal08] C. Hall. Big symplectic or orthogonal monodromy modulo l. *Duke Math. J.*, 141(1) :179–203, 2008.

[Har77] R. Hartshorne. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

[Har09] M. Harris. Potential automorphy of odd-dimensional symmetric powers of elliptic curves and applications. In *Algebra, arithmetic, and geometry : in honor of Yu. I. Manin. Vol. II*, volume 270 of *Progr. Math.*, pages 1–21. Birkhäuser Boston, Inc., Boston, MA, 2009.

[HNR09] E. W. Howe, E. Nart, and C. Ritzenthaler. Jacobians in isogeny classes of abelian surfaces over finite fields. *Ann. Inst. Fourier (Grenoble)*, 59(1) :239–289, 2009.

[HSBT10] M. Harris, N. Shepherd-Barron, and R. Taylor. A family of Calabi-Yau varieties and potential automorphy. *Ann. of Math. (2)*, 171(2) :779–813, 2010.

[Hua82] L. K. Hua. *Introduction to number theory*. Springer-Verlag, Berlin-New York, 1982. Translated from the Chinese by Peter Shiu.

[Hum] P. Humphries. Reference for kronecker-weyl theorem in full generality. MathOverflow. URL :http ://mathoverflow.net/q/162929 (version : 2014-04-09).

[IK04] H. Iwaniec and E. Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[Ill94] L. Illusie. Crystalline cohomology. In *Motives (Seattle, WA, 1991)*, volume 55 of *Proc. Sympos. Pure Math.*, pages 43–70. Amer. Math. Soc., Providence, RI, 1994.

[Ino76] H. Inose. On certain Kummer surfaces which can be realized as non-singular quartic surfaces in P^3. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 23(3) :545–560, 1976.

[Jou07] F. Jouve. *Sommes exponentielles cribles et variétés sur les corps finis*. PhD thesis, Université Bordeaux I, 2007.

[Kac95] J. Kaczorowski. On the distribution of primes (mod 4). *Analysis*, 15(2) :159–171, 1995.

[Kat71] N. M. Katz. On a theorem of Ax. *Amer. J. Math.*, 93 :485–499, 1971.

[Kat80] N. M. Katz. *Sommes exponentielles*, volume 79 of *Astérisque*. Société Mathématique de France, Paris, 1980.

[Kat89] N. M. Katz. Perversity and exponential sums. In *Algebraic number theory*, volume 17 of *Adv. Stud. Pure Math.*, pages 209–259. Academic Press, Boston, MA, 1989.

[Kat90] N. M. Katz. Factoring polynomials in finite fields : an application of Lang-Weil to a problem in graph theory. *Math. Ann.*, 286(4) :625–637, 1990.

[Kat94a] N. M. Katz. Perversity and exponential sums. II. Estimates for and inequalities among A-numbers. In *Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991)*, volume 15 of *Perspect. Math.*, pages 205–252. Academic Press, San Diego, CA, 1994.

[Kat94b] N. M. Katz. Review of l-adic cohomology. In *Motives (Seattle, WA, 1991)*, volume 55 of *Proc. Sympos. Pure Math.*, pages 21–30. Amer. Math. Soc., Providence, RI, 1994.

[Kat04] Y. Katznelson. *An introduction to harmonic analysis*. Cambridge Mathematical Library. Cambridge University Press, Cambridge, third edition, 2004.

[Kat09] N. M. Katz. Lang-Trotter revisited. *Bull. Amer. Math. Soc. (N.S.)*, 46(3) :413–457, 2009.

[KL85] N. M. Katz and G. Laumon. Transformation de Fourier et majoration de sommes exponentielles. *Inst. Hautes Études Sci. Publ. Math.*, (62) :361–418, 1985.

[Kli] B. Klingler. Etale cohomology and the Weil conjectures. notes de cours, disponibles à https ://webusers.imj-prg.fr/ bruno.klingler/cours/Weil.pdf.

[KM00a] E. Kowalski and P. Michel. Explicit upper bound for the (analytic) rank of $J_0(q)$. *Israel J. Math.*, 120(part A) :179–204, 2000.

[KM00b] E. Kowalski and P. Michel. A lower bound for the rank of $J_0(q)$. *Acta Arith.*, 94(4) :303–343, 2000.

[Kol07] J. Kollár. *Lectures on resolution of singularities*, volume 166 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2007.

[Kow06a] E. Kowalski. The large sieve, monodromy and zeta functions of curves. *J. Reine Angew. Math.*, 601 :29–69, 2006.

[Kow06b] E. Kowalski. On the rank of quadratic twists of elliptic curves over function fields. *Int. J. Number Theory*, 2(2) :267–288, 2006.

[Kow08a] E. Kowalski. *The large sieve and its applications*, volume 175 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2008. Arithmetic geometry, random walks and discrete groups.

[Kow08b] E. Kowalski. The large sieve, monodromy, and zeta functions of algebraic curves. II. Independence of the zeros. *Int. Math. Res. Not. IMRN*, pages Art. ID rnn 091, 57, 2008.

[KP99] J. Kaczorowski and A. Perelli. The Selberg class : a survey. In *Number theory in progress, Vol. 2 (Zakopane-Kościelisko, 1997)*, pages 953–992. de Gruyter, Berlin, 1999.

[KP03] J. Kaczorowski and A. Perelli. On the prime number theorem for the Selberg class. *Archiv der Mathematik*, 80(3) :255–263, 2003.

[LO77] J. C. Lagarias and A. M. Odlyzko. Effective versions of the Chebotarev density theorem. pages 409–464, 1977.

[Lub99] A. Lubotzky. One for almost all : generation of $\mathrm{SL}(n, p)$ by subsets of $\mathrm{SL}(n, \mathbf{Z})$. In *Algebra, K-theory, groups, and education (New York, 1997)*, volume 243 of *Contemp. Math.*, pages 125–128. Amer. Math. Soc., Providence, RI, 1999.

[LW02] Y. K. Lau and J. Wu. Sums of some multiplicative functions over a special set of integers. *Acta Arith.*, 101(4) :365–394, 2002.

[Man74] Yu. I. Manin. *Cubic forms : algebra, geometry, arithmetic*. North-Holland Publishing Co., Amsterdam-London ; American Elsevier Publishing Co., New York, 1974. Translated from the Russian by M. Hazewinkel, North-Holland Mathematical Library, Vol. 4.

[Maz72] B. Mazur. Frobenius and the Hodge filtration. *Bull. Amer. Math. Soc.*, 78 :653–667, 1972.

[Maz08] B. Mazur. Finding meaning in error terms. *Bull. Amer. Math. Soc. (N.S.)*, 45(2) :185–228, 2008.

[Mil80] J. S. Milne. *Étale cohomology*, volume 33 of *Princeton Mathematical Series*. Princeton University Press, Princeton, N.J., 1980.

[MN] G. Martin and N. Ng. Inclusive prime number races. in preparation.

[Mur82] V. K. Murty. On the Sato-Tate conjecture. In *Number theory related to Fermat's last theorem (Cambridge, Mass., 1981)*, volume 26 of *Progr. Math.*, pages 195–205. Birkhäuser, Boston, Mass., 1982.

[MV07] H. L. Montgomery and R. C. Vaughan. *Multiplicative number theory. I. Classical theory*, volume 97 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2007.

[MW89] C. Mœglin and J.-L. Waldspurger. Le spectre résiduel de GL(n). *Ann. Sci. École Norm. Sup. (4)*, 22(4) :605–674, 1989.

[Ogu81] A. Ogus. Hodge cycles and crystalline cohomology. In *Hodge cycles, motives, and shimura varieties*, pages 357–414. Springer, 1981.

[PTvdV92] C. Peters, J. Top, and M. van der Vlugt. The Hasse zeta function of a $K3$ surface related to the number of words of weight 5 in the Melas codes. *J. Reine Angew. Math.*, 432 :151–176, 1992.

[Ram00] D. Ramakrishnan. Modularity of the Rankin-Selberg L-series, and multiplicity one for SL(2). *Ann. of Math. (2)*, 152(1) :45–111, 2000.

[RS94] M. Rubinstein and P. Sarnak. Chebyshev's bias. *Experiment. Math.*, 3(3) :173–197, 1994.

[Rud80] W. Rudin. *Analyse réelle et complexe*. Masson, Paris, 1980. Translated from the first English edition by N. Dhombres and F. Hoffman, Third printing.

[Sar07] P. Sarnak. Letter to : Barry Mazur on "Chebychev's bias" for $\tau(p)$. Publications.ias, 2007. URL : https ://publications.ias.edu/sites/default/files/MazurLtrMay08.PDF (version : 2008-05).

[Saw16] W. F. Sawin. Ordinary primes for Abelian surfaces. *C. R. Math. Acad. Sci. Paris*, 354(6) :566–568, 2016.

[SB85] J. Stienstra and F. Beukers. On the Picard-Fuchs equation and the formal Brauer group of certain elliptic $K3$-surfaces. *Math. Ann.*, 271(2) :269–304, 1985.

[Sch53] B. Schoeneberg. über den Zusammenhang der Eisensteinschen Reihen und Thetareihen mit der Diskriminante der elliptischen Funktionen. *Math. Ann.*, 126 :177–184, 1953.

[SD16] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 7.3)*, 2016. `http://www.sagemath.org`.

[Ser70] J.-P. Serre. *Cours d'arithmétique*, volume 2 of *Collection SUP : "Le Mathématicien"*. Presses Universitaires de France, Paris, 1970.

[Ser81] J.-P. Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, (54) :323–401, 1981.

[Ser12] J.-P. Serre. *Lectures on $N_X(p)$*, volume 11 of *Chapman & Hall/CRC Research Notes in Mathematics*. CRC Press, Boca Raton, FL, 2012.

[SGA03] *Revêtements étales et groupe fondamental (SGA 1)*, volume 3 of *Documents Mathématiques (Paris) [Mathematical Documents (Paris)]*. Société Mathématique de France, Paris, 2003. Séminaire de géométrie algébrique du Bois Marie 1960–61. [Algebraic Geometry Seminar of Bois Marie 1960-61], Directed by A. Grothendieck, With two papers by M. Raynaud, Updated and annotated reprint of the 1971 original [Lecture Notes in Math., 224, Springer, Berlin ; MR0354651 (50 #7129)].

[Sha97] F. Shahidi. On non-vanishing of twisted symmetric and exterior square L-functions for GL(n). *Pacific J. Math.*, (Special Issue) :311–322, 1997. Olga Taussky-Todd : in memoriam.

[Shi94] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publications of the Mathematical Society of Japan*. Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kanô Memorial Lectures, 1.

[Ten15] G. Tenenbaum. *Introduction to analytic and probabilistic number theory*, volume 163 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, third edition, 2015. Translated from the 2008 French edition by Patrick D. F. Ion.

[TW95] R. Taylor and A. Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3) :553–572, 1995.

[Voi02] C. Voisin. *Théorie de Hodge et géométrie algébrique complexe*, volume 10 of *Cours Spécialisés [Specialized Courses]*. Société Mathématique de France, Paris, 2002.

[Wat95] G. N. Watson. *A treatise on the theory of Bessel functions*. Cambridge Mathematical Library. Cambridge University Press, Cambridge, 1995. Reprint of the second (1944) edition.

[Wen06] K. Wendland. A family of SCFTs hosting all "very attractive" relatives of the $(2)^4$ Gepner model. *J. High Energy Phys.*, (3) :102, 51 pp. (electronic), 2006.

[Wil95] A. Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3) :443–551, 1995.

[Win35] A. Wintner. On the Asymptotic Distribution of the Remainder Term of the Prime-Number Theorem. *Amer. J. Math.*, 57(3) :534–538, 1935.

[Win41] A. Wintner. On the distribution function of the remainder term of the prime number theorem. *Amer. J. Math.*, 63 :233–248, 1941.

[Zyw10] D. Zywina. Hilbert's irreducibility theorem and the larger sieve. arXiv : 1011.6465, November 2010.

université PARIS-SACLAY | École doctorale de mathématiques Hadamard (EDMH)

Titre : Propriétés algébriques et analytiques de certaines suites indexées par les nombres premiers

Mots Clefs : Théorème de Chebotarev, Variétés algébriques sur les corps finis, Grand crible, Biais de Chebyshev

Résumé : Dans la première partie de cette thèse, on s'intéresse à la suite $N_X(p) \pmod p$ où X est un schéma séparé réduit de type fini sur $\mathbf{Z}$, et pour tout p premier, $N_X(p)$ est le nombre de $\mathbf{F}_p$-points de la réduction modulo p de X. Sous certaines hypothèses sur la géométrie de X, on donne une condition simple pour garantir que cette suite diffère en une densité positive de coordonnées de la suite identiquement nulle, ou plus généralement de suites dont les coordonnées sont obtenues par réduction modulo p d'un nombre fini d'entiers. Dans le cas où X parcourt une famille de courbes hyperelliptiques, on donne une borne en moyenne sur le plus petit premier p pour lequel $N_X(p) \pmod p$ n'est pas dans un certain ensemble de valeurs fixées.
La seconde partie est dédiée à des généralisations de la notion de biais de Chebyshev. On se donne une fonction L vérifiant certaines propriétés analytiques généralisant celles vérifiées par les fonctions L de Dirichlet. On s'intéresse à la suite des coefficients de Fourier a_p pour p premier. Plus précisément on étudie le signe de la fonction sommatoire des coefficients de Fourier de la fonction L. On montre sous des conditions classiques que cette fonction admet une distribution logarithmique limite. Sous des hypothèses supplémentaires on obtient de bonnes propriétés telles que la régularité, la symétrie et des informations sur le support de cette distribution.

Title : Algebraic and analytic properties of some sequences indexed by prime numbers

Keywords : Chebotarev Density Theorem, Algebraic varieties over finite fields, Large and larger sieve, Chebyshev's bias

Abstract : In the first part of this Thesis, we study the sequence $N_X(p) \pmod p$ where X is a reduced separated scheme of finite type over $\mathbf{Z}$, and $N_X(p)$ is the number of $\mathbf{F}_p$-points of the reduction modulo p of X, for every prime p. Under some hypotheses on the geometry of X, we give a simple condition to ensure that this sequence is distinct at a positive proportion of indices from the zero sequence, or generalizations obtained by reduction modulo p of finitely many integers. We give a bound on average over a family of hyperelliptic curves for the least prime p such that $N_X(p) \pmod p$ avoids the reduction modulo p of finitely many fixed integers.
The second part deals with generalizations of Chebyshev's bias. We consider an L-function satisfying some analytic properties that generalize those satisfied by Dirichlet L-functions. We study the sequence of coefficients a_p as p runs through the set of prime numbers. Precisely, we study the sign of the summatory function of the Fourier coefficients of the L-function. Under some classical conditions, we show that this function admits a limiting logarithmic distribution. Under stronger hypotheses, we prove regularity, symmetry and get information about the support of this distribution.