Numéro d'ordre : 19-2007

Université Claude Bernard Lyon 1

Habilitation à Diriger des Recherches

spécialité : **mathématiques pures**

Calculs et expérimentations en théorie des nombres

Xavier-François ROBLOT

– RAPPORTEURS –

M. Henri COHEN	Université Bordeaux 1
M. Henri DARMON	McGill University (Montréal)
M. David SOLOMON	King's College (Londres)

– JURY –

M. Karim BELABAS	Université Bordeaux 1
M. Henri COHEN	Université Bordeaux 1
M. Jean-Marc COUVEIGNES	Université Toulouse 2
M. David FORD	Concordia University (Montréal)
M. Laurent HABSIEGER	Université Claude Bernard Lyon 1
M. Jean-Louis NICOLAS	Université Claude Bernard Lyon 1
M. Harold STARK	University of California at San Diego

- Juin 2007 -

Remerciements

Je tiens tout d'abord à exprimer toute ma gratitude à Henri Cohen, David Ford et David Solomon. Ils ont eu chacun une très grande et significative influence sur le développement de mes activités de recherche, et sans aucun doute, sans eux, ma carrière scientifique eut été bien moins passionnante. Ainsi, je suis particulièrement heureux qu'ils aient accepté d'être acteur dans cette habilitation : David Solomon en tant que rapporteur, David Ford en tant que membre du jury, et Henri Cohen en tant que rapporteur et membre du jury.

Je suis aussi très touché du grand honneur que me fait Henri Darmon en ayant accepté de rapporter sur mes travaux. Et je suis extrêmement honoré que Harold Stark, dont les recherches sont à l'origine d'une grande partie de ces travaux, est accepté de faire partie du jury. Je les remercie vivement tous les deux.

Mes remerciements vont également à Karim Belabas et Jean-Marc Couveignes pour leur participation au jury. Je profite de l'occasion pour remercier Karim de son travail constant et de son enthousiasme dans la maintenance et le développement du système PARI/GP, à la suite de Henri Cohen. Sans ce système, bon nombre de mes recherches n'aurait pas pu avoir lieu.

Mes collègues Laurent Habsieger et Jean-Louis Nicolas me font l'amitié de bien vouloir participer à ce jury. Je leur en suis très reconnaissant, et je les remercie aussi pour la très bonne ambiance et l'excellente qualité mathématique qu'ils ont su instaurer au sein du groupe de théorie des nombres et combinatoire de Lyon.

Je n'oublie pas les chercheurs avec qui j'ai eu la chance de collaborer et auprès desquels j'ai beaucoup appris, ainsi que les nombreux mathématiciens qui, au cours de ces années, ont contribué à mes recherches grâce à d'enrichissantes discussions, et tout ceux qui m'ont fait le cadeau de leur amitié.

Dix ans après ma soutenance de thèse, j'ai aussi une pensée pleine de gratitude envers mes directeurs de thèse : Francisco Diaz y Diaz et Michel Olivier qui ont guidé mes premiers pas dans le monde de la recherche.

Enfin, j'adresse toute ma tendresse à Michiko et à Koské.

Sommaire

Liste des travaux présentés

[T1] Henri Cohen et Xavier-François Roblot. Computing the Hilbert class field of real quadratic fields. *Math. Comp.*, 69(231), 1229–1244, 2000.

[T2] Xavier-François Roblot et Brett A. Tangedal. Numerical verification of the Brumer-Stark conjecture. In *Algorithmic number theory (Leiden, 2000)*, volume 1838 de *Lecture Notes in Comput. Sci.*, pages 491–503. Springer, Berlin, 2000.

[T3] Sebastian Pauli et Xavier-François Roblot. On the computation of all extensions of a p-adic field of a given degree. *Math. Comp.*, 70(236), 1641–1659, 2001.

[T4] David Ford, Sebastian Pauli et Xavier-François Roblot. A fast algorithm for polynomial factorization over $\mathbb{Q}_p$. *J. Théor. Nombres Bordeaux*, 14(1), 151–169, 2002.

[T5] Roland Gillard, Franck Leprevost, Alexei Panchishkin et Xavier-François Roblot. Utilisation des modules de Drinfeld en cryptologie. *C. R. Math. Acad. Sci. Paris*, 336(11), 879–882, 2003.

[T6] Arnaud Jehanne, Xavier-François Roblot et Jonathan Sands. Numerical verification of the Stark-Chinburg conjecture for some icosahedral representations. *Experiment. Math.*, 12(4), 419–432, 2003.

[T7] Cornelius Greither, Xavier-François Roblot et Brett A. Tangedal. The Brumer-Stark conjecture in some families of extensions of specified degree. *Math. Comp.*, 73(245), 297–315, 2004.

[T8] Marc Deléglise, Pierre Dusart et Xavier-François Roblot. Counting primes in residue classes. *Math. Comp.*, 73(247), 1565–1575, 2004.

[T9] Xavier-François Roblot et David Solomon. Verifying a p-adic abelian Stark conjecture at $s = 1$. *J. Number Theory*, 107(1), 168–206, 2004.

[T10] Jean-Michel Muller, Jean-Louis Nicolas et Xavier-François Roblot. Nombre de solutions dans une binade de l'équation $A^2 + B^2 = C^2 + C$. *Enseign. Math. (2)*, 50(1-2), 147–182, 2004.

[T11] Laurent Habsieger et Xavier-François Roblot. On integers of the form $p + 2^k$. *Acta Arith.*, 122(1), 45–50, 2006.

Description des travaux présentés

Dans *Mathematics Unlimited*, livre qui offre un panorama des mathématiques à l'aube du XXI$^{\text{ème}}$ siècle et quelques perspectives pour le futur, H. Cohen [2001] écrit au sujet de la théorie des nombres

> "(...) [N]*umber theory* (...) *should be thought of more as a natural science. In particular, it shares in common with the natural sciences the property that it is a strongly* experimental *subject. In this respect, experiments allow the number theorist to* interact *with the nature of numbers, much as natural scientist interacts with Nature.*"

Les travaux présentés dans ce mémoire se placent dans cette perspective et tentent d'étudier la théorie des nombres du point de vue théorique et du point de vue expérimental. Ces travaux se partagent naturellement en trois parties : les aspects explicites des conjectures de Stark, l'algorithmique des nombres p-adiques, et les recherches provenant de collaboration sur d'autres domaines.

Les conjectures de Stark et leurs variations forment un domaine très vaste et fécond qui se prête particulièrement bien aux méthodes explicites, puisque, de fait, la plupart des résultats sont des conjectures qui restent à démontrer. Je décrit dans ce mémoire des recherches effectuées pour vérifier numériquement plusieurs variations : la conjecture de Brumer-Stark sur des corps quadratiques et cubiques,[†] la conjecture de Stark-Chinburg pour les répresentations icosaèdrales, une conjecture de Solomon portant à la fois sur les valeurs des fonctions L complexes et des fonctions L p-adiques. De telles vérifications numériques ont essentiellement deux buts : dans un premier temps, il s'agit de donner plus de poids à ces conjectures ; dans un deuxième temps, elles permettent de mieux cerner l'objet prédit et d'en étudier les propriétés.[‡] Un autre champ d'application des conjectures de Stark est la résolution du 12ème problème de Hilbert. Un travail montrant comment construire (conjecturalement) les corps de classes de Hilbert de corps quadratiques réels est présenté en début de section.

La deuxième partie porte sur l'algorithmique des nombres p-adiques et décrit trois algorithmes de calcul. Le premier algorithme, suivant les travaux initiés par Krasner, permet de construire toutes les extensions de degré donné d'un corps p-adique. Le deuxième factorise les polynômes sur le corps $\mathbb{Q}_p$ des nombres p-adiques rationnels. Ce problème a de nombreuses applications en théorie algorithmique des nombres et ainsi il est important de pouvoir le résoudre de manière efficace. Le troisième calcule la

[†] Plusieurs cas de cette conjecture sont aussi démontrés dans les travaux présentés.

[‡] Ce qui peut amener parfois à des raffinements.

valeur en $s = 1$ de fonctions zêta (tordues) p-adiques de corps quadratiques réels. Ce calcul est notamment utilisé pour vérifier numériquement la conjecture de Solomon, mentionnée ci-dessus.

La dernière partie est le fruit de collaborations initiées par mes collègues de Lyon et de Grenoble. Une de ces collaborations porte sur l'utilisation des modules de Drinfeld en cryptographie, les autres sur des aspects explicites de la théorie analytique des nombres.

1 Aspects explicites des conjectures de Stark

Les conjectures de Stark portent sur les valeurs du terme dominant en $s = 0$ des fonctions L de corps de nombres. Elles ont été développées par Stark dans une série d'articles fondateurs [Stark, 1971, 1975, 1976, 1977a,b, 1980, 1981]. Ces conjectures, leurs généralisations et leurs variations sont de nos jours au coeur d'un vaste domaine de recherche en pleine activité, comme le prouvent par exemple les actes de la conférence sur ce thème qui s'est tenue en 2002 à Baltimore [Burns et al., 2004]. Un excellent ouvrage de référence sur le sujet, bien que datant un peu, est le livre de Tate [1984].

Dès l'origine, les aspects explicites ont joué un rôle primordial dans ce domaine, avec d'ailleurs plusieurs vérifications numériques effectuées par Stark [1976, 1977a,b, 1980] lui-même. L'article [Dummit, 2004] donne un survol récent des différents calculs numériques autour ces conjectures. C'est dans le cadre de cet étude explicite et algorithmique que s'inscrit une partie importante de mes travaux de recherche, à savoir les articles [T1, T2, T6, T7, T9], que je présente dans ce chapitre.

Notations et conventions. Dans ce texte, tous les corps de nombres sont vus comme sous-corps de $\bar{\mathbb{Q}} \subset \mathbb{C}$, donc il existe toujours une place infinie particulière, à savoir l'identité. Pour E un corps de nombres, on note $\mathcal{O}_E$ et d_E l'anneau des entiers et le discriminant de E.

1.1 La conjecture abélienne de rang 1

Soit K/k une extension abélienne de corps de nombres, de degré relatif N et de groupe de Galois G. Soit S un ensemble fini de places de k contenant les places infinies ainsi que les places finies qui se ramifient dans K/k. A chaque caractère $\chi \in \hat{G}$, le groupe des caractères de G, est associé une fonction L de Hecke définie pour tout nombre complexe s avec $\Re(s) > 1$ par le produit eulérien

$$L_S(s, \chi) = \prod_{\mathfrak{p} \notin S} (1 - \chi(\mathfrak{p}) \mathcal{N}\mathfrak{p}^{-s})^{-1}$$

où $\mathfrak{p}$ parcourt les idéaux premiers de k n'appartenant pas à S et $\chi(\mathfrak{p}) = \chi(\sigma_\mathfrak{p})$ avec $\sigma_\mathfrak{p}$ l'automorphisme de Frobenius de $\mathfrak{p}$ dans G. Ces fonctions admettent un prolongement holomorphe au plan complexe si χ n'est pas le caractère trivial de G, et un prolongement méromorphe avec un pôle simple en $s = 1$ sinon.

Soit $\sigma \in G$, on définit la fonction zêta partielle associée à σ par

$$\zeta_S(s,\sigma) = \frac{1}{N}\sum_{\chi\in\widehat{G}} L_S(s,\chi)\overline{\chi}(\sigma) = \sum_{\substack{(\mathfrak{a},S)=1\\ \sigma_{\mathfrak{a}}=\sigma}} \mathcal{N}\mathfrak{a}^{-s} \tag{1.1}$$

où la dernière somme, convergeante pour $\Re(s) > 1$, porte sur tous les idéaux entiers $\mathfrak{a}$ de k premiers avec les idéaux premiers de S et dont le symbole d'Artin $\sigma_{\mathfrak{a}}$ est égal à σ.

On suppose à présent que S contient au moins trois éléments et une place v qui se décompose totalement dans K (pour une place infinie, cela signifie qu'il s'agit ou bien d'une place complexe, ou bien d'une place réelle qui reste réelle dans K). Sous ces conditions, l'ordre d'annulation en $s = 0$ des fonctions $L_S(s,\chi)$ est au moins de 1[†] (voir [Tate, 1984, Proposition I.3.4]), et on a la conjecture suivante (une version incluant aussi le cas $|S| = 2$ qui est exclu ici pour simplifier l'énoncé est donnée dans [Tate, 1984, Chapitre IV, §2]).

Conjecture 1.1 (Stark)**.** *Soit m le nombre de racines de l'unité contenues dans K et soit w une place fixée de K au-dessus de v. Il existe une v-unité ε de K telle que, pour tout $\sigma \in G$, on a*

$$\log|\sigma(\varepsilon)|_w = -m\zeta_S'(0,\sigma). \tag{1.2}$$

De plus, pour tout $\lambda \in \bar{\mathbb{Q}}$ tel que $\lambda^m = \varepsilon$, l'extension $K(\lambda)/k$ est une extension abélienne.

Remarque 1.2. L'élément ε, quand il existe, est appelé l'unité de Stark associée à l'extension K/k, à l'ensemble de places S et à la place w de K, ou plus simplement une unité de Stark.

Remarque 1.3. Une v-unité ε de K est un entier algébrique de K tel que $|\varepsilon|_{w'} = 1$ pour toute place w' de K ne divisant pas v. En particulier, si v est une place infinie, alors une v-unité est aussi une unité.

Remarque 1.4. Pour $l \geq 2$ tel que K contienne les racines l-ièmes de l'unité, un élément $\alpha \in K^\times$ est dit l-abélien pour K/k si pour tout $\lambda \in \bar{\mathbb{Q}}$ tel que $\lambda^l = \alpha$, l'extension $K(\lambda)/k$ est abélienne.[‡] Ainsi, la dernière propriété peut se reformuler en disant que ε est m-abélien pour K/k.

Corps de classes de Hilbert des corps quadratiques réels

Le 12ème problème de Hilbert [2000] pose la question de construire les corps de classes de rayon d'un corps de nombres k à l'aide de valeurs spéciales de fonctions analytiques attachées à ce corps. De telles constructions sont connues quand k est le corps des rationnels (en utilisant le théorème de Kronecker-Weber [Lang, 1994, Chapitre X, §3]) ou un corps quadratique imaginaire (en utilisant la théorie de la

[†] Et donc par (1.1) il en est de même pour les fonctions zêta partielles $\zeta_S(s,\sigma)$.

[‡] Puisque K contient les racines de l'unité d'ordre l, le corps $K(\lambda)$ ne dépend pas du choix de λ.

multiplication complexe, voir [Cohen, 2000, Section 6.3]). Une des motivations des conjectures de Stark était de fournir une réponse à ce problème.

De fait, dans le cas où le corps k est totalement réel, on obtient une réponse partielle grâce à la conjecture 1.1, notamment en utilisant le résultat suivant, démontré dans [Roblot, 2000], et qui est extrait de mon travail de thèse.

Théorème 1.5. *Soit k un corps totalement réel distinct de $\mathbb{Q}$. Soit v la place infinie de k correspondant à l'identité. On suppose que la conjecture 1.1 est vérifiée pour toutes les extensions abéliennes finies de k dans lesquelles v est totalement décomposée.*

Alors, pour toute extension abélienne finie L/k avec L totalement réelle, il existe des unités de Stark $\varepsilon_1, \dots, \varepsilon_l$ telles que

$$L = \mathbb{Q}(\varepsilon_1 + \varepsilon_1^{-1} + \cdots + \varepsilon_l + \varepsilon_l^{-1}) .$$

Dans l'article [T1], écrit en collaboration avec H. Cohen, nous nous sommes intéressés à un cas particulier, à savoir celui où k est un corps quadratique réel et le corps L, que l'on cherche à construire, le corps de classes de Hilbert de k. En effet, certains résultats et calculs se simplifient ce qui permet d'obtenir une méthode de construction efficace du corps de classes de Hilbert. Bien sûr, cette construction est conjecturale, mais il est possible a posteriori de vérifier, indépendamment de toute conjecture, que le corps construit est bien celui recherché.

Soit k un corps quadratique réel. On note $v = \mathrm{Id}$ et $\bar{v}$ les deux places infinies de k et H_k le corps de classes de Hilbert de k. Soit $K \subset \mathbb{R}$ une extension quadratique de H_k telle que K/k est une extension abélienne dans laquelle la place $\bar{v}$ devient complexe. Soit w la place infinie de K correspondant à l'identité (et donc divisant v). Le théorème suivant se déduit du théorème 1.5.

Proposition 1.6. *On suppose que la conjecture 1.1 est vraie pour l'extension K/k, l'ensemble de places S constitué des places infinies v et $\bar{v}$ et des places finies de k ramifiées dans K, et la place w.*

Alors, il existe une unité $\varepsilon \in \mathcal{O}_K$ telle que, pour tout $\sigma \in \mathrm{Gal}(K/k)$, on a

$$\sigma(\varepsilon) = \exp\left(-2\zeta_S'(0,\sigma)\right) . \tag{1.3}$$

De plus, si on pose $\alpha = \varepsilon + \varepsilon^{-1}$, alors $H_k = \mathbb{Q}(\alpha)$ et on a $|\alpha|_{w'} \leq 2$ pour toute place infinie w' de H_k qui ne divise pas v.

Il faut maintenant déterminer explicitement l'élément α.[†] La stratégie est de calculer des valeurs approchées de $\zeta_S'(0,\sigma)$ pour tout $\sigma \in G$. Par (1.1), cela revient à calculer des valeurs approchées de $L_S'(0,\chi)$ pour tout $\chi \in \hat{G}$. Notons $\tau \in G$ la conjugaison complexe associée à $\bar{v}$. Soit $\chi \in \hat{G}$, on montre par [Tate, 1984, Proposition I.3.4] que $L_S'(0,\chi) = 0$ si $\chi(\tau) = 1$, et sinon, $\chi(\tau) = -1$, χ est un caractère primitif et $L_S'(0,\chi) \neq 0$. Une méthode générale pour calculer des valeurs approchées des fonctions L de Hecke est donnée dans [Dummit et Tangedal, 1998] (voir aussi [Cohen, 2000, Section 10.3]). J'ai implanté cette méthode pour le calcul des fonctions L en $s = 1$ (et par l'équation fonctionnelle du premier coefficient de Taylor non nul en $s = 0$) dans PARI/GP (fonction : `bnrL1`). Dans le cas présent, ce calcul se simplifie beaucoup.

[†] Notons que α est un entier algébrique puisque ε est une unité.

Proposition 1.7. *Soit χ un caractère de G tel que $\chi(\tau) = -1$. On note $W(\chi)$ la constante d'Artin[†] de χ et on pose*

$$C = \frac{\sqrt{d_k \mathcal{N}\mathfrak{f}}}{\pi}$$

où $\mathfrak{f}$ est la partie finie du conducteur de K/k.

Pour tout $n \geq 1$, on pose

$$a_n(\chi) = \sum_{\substack{(\mathfrak{a},S)=1 \\ \mathcal{N}\mathfrak{a}=n}} \chi(\sigma_{\mathfrak{a}})$$

où la somme porte sur tous les idéaux entiers de k premiers avec les idéaux premiers de S et de norme n.

Soit $0 < \varkappa < 1$ un nombre réel. On pose $N = \left\lceil \frac{-C \log \varkappa}{2} \right\rceil$ et on définit les deux quantités suivantes

$$T(\chi) = \sum_{n=1}^{N} \overline{a_n(\chi)} \frac{C}{2n} e^{-2n/C} \quad \text{et} \quad S(\chi) = \sum_{n=1}^{N} a_n(\chi) \operatorname{Ei}(2n/C)$$

où $\operatorname{Ei}(x) = \int_x^{+\infty} e^{-t} dt/t$ est la fonction exponentielle intégrale. Alors, on a

$$\left| L'_S(0,\chi) - \big(S(\chi) + W(\chi) T(\chi)\big) \right| \leq \varkappa .$$

L'évaluation des sommes T et S peut se faire de manière très efficace comme ceci est expliqué dans l'article. Une fois déterminées des valeurs approchées de $\zeta'_S(0,\sigma)$, on peut à l'aide de (1.3) former un polynôme à coefficients dans $\mathbb{R}$ qui est une approximation du polynôme minimal de α sur k. En utilisant les bornes données dans la proposition 1.6, on peut alors reconnaître ces coefficients comme éléments de $\mathcal{O}_k$ et obtenir ainsi un polynôme $P(X) \in \mathcal{O}_k[X]$. Sous l'hypothèse que la conjecture 1.1 est vérifiée pour ces données, le polynôme P est le polynôme minimal sur k d'un générateur du corps de classes de Hilbert de k.

Pour conclure, et pour avoir un résultat qui ne dépende pas d'une conjecture et de calculs approchés, il reste à vérifier que le corps $\tilde{H}$ engendré par le polynôme P est bien le corps de classes de Hilbert de k. Pour cela, il faut vérifier les trois propriétés suivantes.

1. Le degré de l'extension $\tilde{H}/k$ est le nombre de classes de k ;
2. L'extension $\tilde{H}/k$ est non ramifiée (aux places finies et infinies) ;
3. L'extension $\tilde{H}/k$ est abélienne.

La propriété 1 est satisfaite si le polynôme P est irréductible sur k, ce qui être vérifié par exemple en utilisant l'algorithme de factorisation des polynômes sur un corps de nombres développé durant ma thèse et publié dans [Roblot, 2004]. Pour la propriété 2,

[†] Il s'agit de la constante intervenant dans l'équation fonctionnelle de la fonction L associée à χ, voir [Dummit et Tangedal, 1998] pour son calcul.

on vérifie que les places infinies sont non ramifiées en utilisant l'algorithme de Sturm (voir [Cohen, 1993, Section 4.1.2]) et pour les places finies, on utilise l'algorithme de calcul de discriminant relatif d'une extension de corps de nombres donné dans [Cohen, 2000, Section 2.4]. Finalement, pour la propriété 3, on calcule les k-automorphismes de $\tilde{H}$ en factorisant P dans $\tilde{H}[X]$ ou par la méthode développée dans [Allombert, 2004], puis on vérifie s'il y en a le bon nombre et s'ils commutent. Une autre méthode pour vérifier la propriété 3 est de calculer le groupe des normes de $\tilde{H}/k$ en regardant la factorisation de P modulo les idéaux premiers de k. Cette méthode a été développée dans ma thèse [Roblot, 1997] et, pour pouvoir être utilisée dans la pratique, nécessite de supposer l'hypothèse de Riemann généralisée.

Par la procédure de construction décrite ci-dessus, nous avons déterminé dans [T1] le corps de classes de Hilbert de tous les corps quadratiques réels de discriminant $\leq 2\,000$. De plus, cette procédure est à présent implantée dans PARI/GP (fonction : `quadhilbert`).

Conjecture de Brumer-Stark

Supposons que K/k est une extension abélienne de corps de nombres avec k totalement réel et K totalement complexe. On note toujours G le groupe de Galois de cette extension, et on pose S_0 l'ensemble de places infinies de k et des places finies de k ramifiées dans K. Pour tout idéal premier $\mathfrak{p}$ de k totalement décomposé dans K/k, on peut appliquer la conjecture 1.1 à l'extension K/k, l'ensemble de places $S = S_0 \cup \{\mathfrak{p}\}$, et pour w la place associée à un idéal premier de K au-dessus $\mathfrak{p}$ fixé. En collectant les prédictions de ces conjectures pour tous les idéaux premiers de k totalement décomposés dans K, Tate [1981] obtient la conjecture suivante (voir aussi [Tate, 1984, Chapitre IV, §6]).

Conjecture 1.8 (Brumer-Stark)**.** *On définit l'élément de Brumer par*

$$\Theta_{K/k} = m \sum_{\chi \in \widehat{G}} L_{S_0}(0, \chi)\, e_{\bar{\chi}} \in \mathbb{Z}[G] \tag{1.4}$$

où m est le nombre de racines de l'unité contenues dans K et $e_\chi \in \mathbb{C}[G]$ est l'idempotent associé à χ.

Alors, pour tout idéal $\mathfrak{A}$ de K, on a les propriétés suivantes

1. *L'idéal $\mathfrak{A}^{\Theta_{K/k}}$ est un idéal principal ;*

Il existe un générateur $\alpha_{\mathfrak{A}}$ de $\mathfrak{A}^{\Theta_{K/k}}$ tel que

2. *L'élément $\alpha_{\mathfrak{A}}$ est une anti-unité de K ;*
3. *L'élément $\alpha_{\mathfrak{A}}$ est m-abélien pour K/k (cf. remarque 1.4).*

Remarque 1.9. Une anti-unité de K est un élément $\alpha \in K^\times$ tel que $|\alpha|_w = 1$ pour toute place infinie w de K. En particulier, une anti-unité qui est aussi un entier algébrique est nécessairement une racine de l'unité.

Remarque 1.10. Par la suite, pour un idéal fractionnaire $\mathfrak{A}$ de K, on dit que BS($\mathfrak{A}$) est vérifié si l'idéal $\mathfrak{A}$ vérifie les propriétés 1, 2 et 3 de la conjecture.

Remarque 1.11. La conjecture implique que l'élément $\Theta_{K/k}$ est un annulateur dans $\mathbb{Z}[G]$ du groupe de classes Cl_K. Cette affirmation est une partie de la conjecture de Brumer, ce qui explique l'appellation "élément de Brumer" suggérée par Hayes [1990]. La conjecture de Brumer affirme que, pour tout $\alpha \in \mathcal{A}(K/k)$, l'annulateur dans $\mathbb{Z}[G]$ du groupe des racines de l'unité de K, l'élément

$$\alpha \sum_{\chi \in \widehat{G}} L_{S_0}(0, \chi)\, e_{\bar{\chi}} \in \mathbb{Z}[G]$$

annule le groupe de classes de K.[†]

Dans deux travaux [T2], en collaboration avec B. Tangedal, et [T7], en collaboration avec C. Greither et B. Tangedal, nous avons procédé à une étude théorique et algorithmique de plusieurs cas de cette conjecture. Pour un nombre premier l, on commence par définir une version locale de la conjecture.

Conjecture 1.12 (Brumer-Stark, version locale en l)**.** *Soit l un nombre premier. Pour tout idéal fractionnaire $\mathfrak{A}$ de K dont la classe est dans la l-partie du groupe de classes de K, on a les propriétés suivantes*

1. *L'idéal $\mathfrak{A}^{\Theta_{K/k}}$ est un idéal principal ;*

Il existe un générateur $\alpha_{\mathfrak{A}}$ de $\mathfrak{A}^{\Theta_{K/k}}$ tel que

2. *L'élément $\alpha_{\mathfrak{A}}$ est une anti-unité de K ;*
3. *L'élément $\alpha_{\mathfrak{A}}$ est m_l-abélien pour K/k où m_l est le cardinal de la l-partie du groupe des racines de l'unité contenues dans K.*

Remarque 1.13. Si l est impair, il n'est pas nécessaire de supposer que $\alpha_{\mathfrak{A}}$ est une anti-unité comme ceci est expliqué dans la remarque au bas de la page 299 de [T7].

Il est clair que la conjecture 1.8 implique les versions locales 1.12 pour tous les nombres premiers l. Le résultat suivant donne la réciproque.

Proposition 1.14. *Supposons que les conjectures locales 1.12 sont vérifiées pour l'extension K/k et tous les nombres premiers l. Alors, la conjecture 1.8 est vérifiée pour l'extension K/k.*

En utilisant des résultats récents sur la conjecture de Brumer [Greither, 2000; Wiles, 1990], qui admet aussi une version locale, et le fait que, pour l impair tel que la l-partie du groupe des unités de K est cohomologiquement triviale (comme G-module) alors les versions locales en l de la conjecture de Brumer-Stark et de la conjecture de Brumer sont équivalentes, on en déduit des résultats concernant la validité de la version locale de la conjecture de Brumer-Stark. Je réunis dans un seul théorème l'ensemble de ces résultats.

[†] On sait que cet élément est dans $\mathbb{Z}[G]$ par [Cassou-Noguès, 1979] ou [Deligne et Ribet, 1980].

Théorème 1.15. *Soit l un nombre premier. On suppose que le corps K est un corps CM.*[†] *Alors, la conjecture 1.12 est vérifiée pour l'extension K/k et le nombre premier l dans les cas suivants.*

- *Le premier l est impair, le degré de K/k n'est pas divisible par l, l'extension $k/\mathbb{Q}$ est abélienne et la l-partie de $\mathrm{Gal}(k/\mathbb{Q})$ est cyclique ;*
- *Le premier l est impair, le degré de K/k n'est pas divisible par l et k est une extension cubique de $\mathbb{Q}$ dont le discriminant n'est pas divisible par l^2 ;*
- *Le premier l est impair, le groupe G est d'ordre $2l$ et l'extension K/k n'est pas de type $\flat$ ou $\sharp$ (voir la remarque ci-dessous) ;*
- *Le premier l est 2, k est un corps quadratique réel et K/k est cyclique d'ordre 6.*

Remarque 1.16. L'extension K/k de degré $2l$ (l impair) est de type $\flat$ si K ne contient pas les racines p-ièmes de l'unité, si les idéaux premiers décomposés dans E/k ne sont pas ramifiés dans K/E (où E/k est l'unique extension quadratique contenue dans K/k) et si la clôture galoisienne (sur $\mathbb{Q}$) de K est contenue dans la clôture galoisienne de son sous-corps réel maximal K^+ auquel on a rajouté les racines primitives l-ièmes de l'unité.

L'extension K/k de degré $2l$ (l impair) est de type $\sharp$ si K contient les racines primitives l-ièmes de l'unité et si elle est non ramifiée en dehors des idéaux premiers divisant l.

Passons à présent aux résultats numériques. Contrairement aux vérifications décrites dans la section précédente (et qui reposent sur des calculs approchés), une des particularités de la conjecture 1.8 est qu'elle peut être établie par des calculs exacts et ainsi complètement démontrée sur des exemples. Une première réduction consiste à montrer que l'ensemble des idéaux fractionnaires $\mathfrak{A}$ de K tel que $\mathrm{BS}(\mathfrak{A})$ est vérifié est un sous-groupe du groupe des idéaux de K, contenant les idéaux principaux, et stable sous l'action du groupe de Galois G. Ce résultat permet de réduire la vérification de la conjecture 1.8 à une vérification portant sur un nombre fini d'idéaux.

Proposition 1.17. *Soient $\mathfrak{A}_1, \ldots, \mathfrak{A}_t$ des idéaux de K tels que les classes des idéaux $\mathfrak{A}_i^\sigma$, avec $i = 1, \ldots, t$ et $\sigma \in G$, engendrent le groupe des classes Cl_K de K. Alors, la conjecture 1.8 est vérifiée si et seulement si $\mathrm{BS}(\mathfrak{A}_i)$ est vérifié pour $i = 1, \ldots, t$.*

Remarque 1.18. Ainsi la conjecture 1.8 est vérifiée si le corps K est principal. De même, pour l premier, la conjecture locale 1.12 en l est vérifiée si le nombre de classes de K n'est pas divisible par l.

Pour procéder à la vérification, on commence par calculer les valeurs de $L_{S_0}(0, \chi)$ pour tous les caractères de G par la méthode de Dummit et Tangedal [1998] mentionnée ci-dessus. On remplace dans l'équation (1.4) et on arrondit les coefficients aux entiers les plus proches. Puisque le nombre de racines de l'unité dans K est généralement petit, une faible précision suffit pour ce calcul. Une fois, $\Theta_{K/k}$ déterminé, on trouve une famille d'idéaux de K vérifiant les hypothèses de la proposition ci-dessus. Pour

[†] *i.e* K, totalement complexe, est une extensions quadratique d'un corps totalement réel.

chaque idéal $\mathfrak{A}$ de cette famille, on calcule l'action de $\Theta_{K/k}$ sur $\mathfrak{A}$ et on vérifie que l'idéal obtenu est bien principal. Si ce n'est pas le cas, alors la conjecture n'est pas vérifiée pour cette extension.[†] Puis, il faut trouver un générateur $\alpha_{\mathfrak{A}}$ qui soit une anti-unité, et vérifier que cet élément est aussi m-abélien. En effet, tous les générateurs de cet idéal principal qui sont aussi des anti-unités différent par une racine de l'unité de K et donc sont simultanément ou non m-abéliens. Trouver un tel générateur n'est pas difficile en général. De fait, le générateur rendu par la fonction `bnfisprincipal` de PARI/GP est par construction particulièrement simple et ainsi, dans notre cas, est très souvent déjà une anti-unité. Le résultat suivant permet de le démontrer.

Proposition 1.19. *Soient $c_1, \dots, c_s \in G$ les conjugaisons complexes de K. L'élément $\alpha \in K^\times$ est une anti-unité si et seulement si $\alpha^{1+c_j} = 1$ pour $j = 1, \dots, s$.*

Finalement, pour vérifier si ce générateur est m-abélien, on peut utiliser la proposition suivante qui est une reformulation de [Tate, 1984, Proposition IV.1.2].

Proposition 1.20. *Notons $\sigma_1, \dots, \sigma_r$ un système de générateurs de G. On note N_i, pour $i = 1, \dots, r$, un entier tel que $\sigma_i(\zeta) = \zeta^{N_i}$ pour toute racine de l'unité ζ dans K. Alors, l'élément $\alpha \in K^\times$ est m-abélien si et seulement si il existe $\beta_1, \dots, \beta_r \in K^\times$ tels que*

$$\alpha^{\sigma_i - N_i} = \beta_i^m, \ 1 \le i \le r, \quad \text{et} \quad \beta_i^{\sigma_j - N_j} = \beta_j^{\sigma_i - N_i}, \ 1 \le i, j \le r\,.$$

A l'aide de cette méthode, nous avons vérifié la conjecture de Brumer-Stark dans un grand nombre d'exemples où elle n'était pas démontrée. Dans [T2], nous avons démontré la validité de la conjecture pour 379 extensions du premier type non démontré à cette époque, à savoir : k corps quadratique réel et K/k extension cyclique d'ordre 4. Par le théorème 1.15, seule à présent la conjecture locale en $l = 2$ reste non établie. Dans ce travail, nous avons aussi observé un comportement particulièrement intéressant. En effet, dans tous les exemples, l'élément $\Theta_{K/k}$ possède une 2-partie non triviale, c'est-à-dire qu'il existe un entier $e \ge 1$ tel que $2^{-e}\,\Theta_{K/k} \in \mathbb{Z}[G]$. Nos expérimentations ont montré que, dans tous ces exemples la totalité de cette 2-partie n'est pas nécessaire pour que le conjecture soit vérifiée, *i.e.* on peut remplacer l'élément $\Theta_{K/k}$ par $2^{-f}\,\Theta_{K/k} \in \mathbb{Z}[G]$ avec $1 \le f \le e$ dans l'énoncé de la conjecture (avec f variant suivant les exemples). Cela suggère qu'une conjecture plus précise doit exister dans ce cas.

Par le théorème 1.15, quand le corps de base est quadratique ou cubique et le degré d'ordre $2l$ (l premier impair), la version locale 1.12 de la conjecture de Brumer-Stark est démontrée pour les premiers impairs sauf quand l'extension K/k est de type $\flat$ ou $\sharp$. Dans [T7], nous avons donc procédé à la vérification pour de telles extensions avec $l = 3$ dans un grand nombre de cas. Plus précisement, la conjecture locale en 3 a été démontrée pour 534 extensions de type $\sharp$ avec un corps de base quadratique réel. Pour un corps de base cubique réel, la version locale a été démontrée pour 114 extensions de type $\sharp$ et 145 extensions de type $\flat$. Dans ces derniers cas, il est à noter que nous avons en fait vérifié la version locale de la conjecture de Brumer (qui est alors plus

[†] Bien sûr, ce cas ne s'est jamais présenté !

simple à vérifier algorithmiquement) et qui est pour cette construction équivalente à la version locale de la conjecture de Brumer-Stark.

1.2 Le cas non abélien

Soit $K/\mathbb{Q}$ une extension galoisienne de groupe de Galois G avec K un corps totalement complexe. On note $\tau \in G$ la restriction de la conjugaison complexe à K.

Soit ρ une représentation impaire, irréductible de dimension 2 de G. On note ψ le caractère associé et $L(s,\rho) = L(s,\psi)$ la fonction L d'Artin associée (voir [Martinet, 1977] pour une introduction aux fonctions L d'Artin). On pose $E = \mathbb{Q}(\psi)$ le corps des valeurs de ψ et Γ le groupe de Galois de $E/\mathbb{Q}$. Pour tout $d \in E$, on définit

$$f_d(s) = \sum_{\gamma\in\Gamma} d^\gamma\, L(s,\psi^\gamma). \tag{1.5}$$

Pour tout $s \in \mathbb{C}$ avec $\Re(s) > 1$, on peut développer f_d en une série de Dirichlet

$$f_d(s) = \sum_{n\geq 1} A_n(d)\, n^{-s} \tag{1.6}$$

où les coefficients $A_n(d)$ sont dans $\mathbb{Q}$.

Conjecture 1.21 (Stark-Chinburg)**.** *Soit $d \in E$ tel que les coefficients $A_n(d)$ sont tous des entiers. Alors il existe une unité $\varepsilon(d) \in K^+$, avec $K^+ = K \cap \mathbb{R}$, telle que, pour tout $\sigma \in G$, on a*

$$\log|\varepsilon(d)^\sigma| = \frac{1}{2} f'_{d(\psi(\sigma^{-1})+\psi(\sigma^{-1}\tau))}(0).$$

De plus, les conjugués réels de ε sont tous positifs.

Remarque 1.22. L'élément $\varepsilon(d)$ est unique s'il existe et est appelé, comme ci-dessus, une unité de Stark.

Remarque 1.23. Dans la formulation de la conjecture donnée dans [T6], c'est la valeur absolue normalisée $||\cdot||$ qui apparaît. Comme K est complexe, cette valeur absolue est le carré de la valeur absolue usuelle, ce qui explique le facteur 1/2. Ce facteur a été oublié dans les calculs de [T6], ce qui explique que toutes les unités de Stark calculées dans l'article sont des carrés.

Remarque 1.24. La conjecture formulée par Chinburg [1983] est beaucoup plus générale que l'énoncé donné ci-dessus.

Les représentations irréductibles de dimension 2 sont classifiées suivant la classe d'isomorphisme de leurs images dans $\mathrm{PGL}_2(\mathbb{C})$. Les quatre types posssibles sont : diédral, tétraédral, octaédral et icosaédral. La conjecture pour le type diédral a été démontrée par Stark [1981] sous certaines conditions, Chinburg [1983] a vérifié numériquement plusieurs exemples de type tétraédral, et Fogel [1998] de type octaédral. Le

type icosaédral a été étudié dans un travail [T6] en collaboration avec A. Jehanne et J. Sands.

Le extensions $K/\mathbb{Q}$ considérées dans cet article sont de degré 240 avec un groupe de Galois isomorphe au groupe $\hat{A}_5$, extension centrale de A_5 par C_4. Le groupe $\hat{A}_5$ peut aussi être vu comme le groupe des matrices 2×2 à coefficients dans $\mathbb{F}_5$ et de déterminant ± 1. C'est le plus petit groupe pour lequel une représentation du type recherché existe. De telles extensions sont construites en partant d'extensions totalement complexes $N/\mathbb{Q}$ de degré 5 dont la clôture galoisienne a pour groupe A_5. Le corps E des valeurs de ψ est le corps $\mathbb{Q}(i, \sqrt{5})$ et on a le résultat suivant.

Lemme 1.25. *Pour ces données, la conjecture 1.21 est vérifiée si et seulement si elle est vérifiée pour*

$$d = \frac{1}{2} \quad et \quad d = \frac{5+\sqrt{5}}{20}.$$

L'unité (conjecturale) $\varepsilon(d)$ est construite en calculant ses quatre conjuguées sur $M \subset K^+$, le sous-corps de K fixé par le centre de G. La conjecture implique que ces conjugués sont réels et positifs, et ainsi peuvent être calculées (à une précision donnée) à partir de valeurs approchées des dérivées des fonctions f_d. Ces valeurs sont obtenues par (1.5) en utilisant la méthode pour le calcul des dérivées des fonctions L utilisée dans Stark [1977a]. Il est à noter que les coefficients du développement en série de Dirichlet de ces fonctions L sont déterminés en considérant la décomposition des nombres premiers dans diverses sous-extensions de $K/\mathbb{Q}$ de petits degrés, voir [Jehanne, 2001].

A l'aide de ces conjugués, on construit une approximation du polynôme minimal de $\varepsilon(d)$ sur M. Il faut à présent reconnaître les cofficients (réels) de ce polynôme comme des entiers algébriques de M. Cette étape se fait par une généralisation d'une méthode de Cohen [2000, Section 6.2.4] en trouvant les vecteurs de petite norme pour une forme quadratique (en 31 variables) bien choisie. Une fois les coefficients de ce polynôme minimal reconnus, des tests sont effectués pour vérifier que les racines de ce polynôme possèdent bien les propriétés attendues.

Théorème 1.26. *La conjecture 1.21 est vérifiée à la précision des calculs pour les* 14 *représentations icosaédrales impaires données dans la Table 1 de* [T6].

Dans presque tous les exemples, nous avons remarqué que les unités de Stark $\varepsilon(d)$ trouvées étaient des carrés dans K^+ (incorrectement données comme des puissances quatrième dans l'article, voir la remarque 1.23). Comme il nous a été suggéré par H. Stark, ce fait peut s'expliquer par la "propriété d'abélianité" souvent présente dans les conjectures de Stark, voir les conjectures 1.1 et 1.8 citées précédemment, et qui manque dans la formulation de la conjecture 1.21. Cette remarque inspire le renforcement suivant de la conjecture.

Conjecture 1.27 (Condition d'abélianité pour Stark-Chinburg)**.** *Dans cette construction, l'unité de Stark $\varepsilon(d)$ de la conjecture 1.21 est 2-abélienne pour K^+/M.*

Nous avons vérifié que cette condition supplémentaire est bien satisfaite dans tous les exemples où $\varepsilon(d)$ n'est pas un carré dans K^+.

1.3 Une conjecture de Solomon

Plusieurs conjectures généralisent la conjecture abélienne de Stark de rang 1 (conjecture 1.1) au rang supérieur, voir [Popescu, 2004] pour un survol. Une autre approche a été développée par Solomon [2002] qui formule plusieurs conjectures combinant à la fois une partie complexe et une partie p-adique, et qui s'expriment en termes de valeurs de fonctions L en $s = 1$, et non en $s = 0$.[†] Dans [T9], travail en collaboration avec D. Solomon, nous avons vérifié numériquement une de ses conjectures. Il est difficile de donner succinctement les définitions complètes des objets intervenant dans cette conjecture, ainsi je donne ci-dessous une idée de ces objets et je réfère à l'article pour des énoncés plus précis.

Soit k un corps totalement réel de degré d et $\mathfrak{f}$ un idéal entier de k, distinct de $\mathcal{O}_k$. On pose K le corps de classes de rayon modulo $\mathfrak{f}$, le corps K est une extension abélienne totalement réelle de k. On prend pour S l'union des places infinies de k et des places finies de k ramifiées dans K/k. On définit $\Phi_{\mathfrak{f}}(s)$, une fonction méromorphe à valeurs dans $\mathbb{C}[G]$, où G est le groupe de Galois de K/k, en termes de fonctions zêta tordues de k, voir [T9, §2.1]. Pour tout nombre premier p, premier avec $\mathfrak{f}$, on définit aussi une version p-adique $\Phi_{\mathfrak{f},p}(s)$, voir [T9, §2.2]. On note $\mathbb{Q}U_S$, le tensorisé par $\mathbb{Q}$ du groupe de $S(K)$-unités de K avec $S(K)$ l'ensemble des places de K au-dessus des places de S. Pour tout élément $\eta \in \bigwedge^d_{\mathbb{Q}[G]} \mathbb{Q}U_S$, le d-ième produit extérieur du $\mathbb{Q}[G]$-module $\mathbb{Q}U_S$, on définit un régulateur complexe R (resp. p-adique R_p) à valeurs dans $\mathbb{R}[G]$ (resp. $\mathbb{C}_p[G]$), voir [T9, §2.3]. Finalement, on note $\mathcal{A}_{S,d}$ le noyau de l'action d'un certain idempotent $\tilde{e}_{S,d} \in \mathbb{Q}[G]$ sur $\bigwedge^d_{\mathbb{Q}[G]} \mathbb{Q}U_S$. En simplifiant, cet idempotent tue la "χ-partie" de $\bigwedge^d_{\mathbb{Q}[G]} \mathbb{Q}U_S$ pour tous les caractères χ pour lesquels l'ordre d'annulation en $s = 0$ de la fonction $L_S(s, \chi)$ est strictement plus grand que d.

Conjecture 1.28 (Solomon). *Il existe un unique élément $\eta_{\mathfrak{f}} \in \mathcal{A}_{S,d}$ possédant les propriétés suivantes*

1. $$\frac{2^d}{\sqrt{d_k}} R(\eta_{\mathfrak{f}}) = \Phi_{\mathfrak{f}}(1)\,.$$

2. *Pour tout nombre premier p, premier avec $\mathfrak{f}$, on a*

$$\prod_{\mathfrak{p}|p} (1 - \mathcal{N}\mathfrak{p}^{-1}\sigma_{\mathfrak{p}}) \frac{2^d}{\sqrt{d_k}} R_p(\eta_{\mathfrak{f}}) = \Phi_{\mathfrak{f},p}(1)\,,$$

   où le produit porte sur les idéaux premiers de k divisant p.

3. *L'élément $\eta_{\mathfrak{f}}$ vit dans un sous-réseau explicite $\Lambda_{S,d} \subset \mathcal{A}_{S,d}$.*

Remarque 1.29. La conjecture donnée dans l'article [T9, Conjecture 2.2] contient une définition explicite du réseau $\Lambda_{S,d}$.

[†] Ce qui est important dans le cas p-adique vue l'absence d'équation fonctionnelle.

Nous avons procédé à une vérification numérique de cette conjecture sur plusieurs exemples avec k un corps quadratique réel, *i.e* $d = 2$. Pour cela, il est nécessaire de résoudre plusieurs problèmes. Il faut tout d'abord construire le $\mathbb{Q}[G]$-module $\mathcal{A}_{S,2}$. On commence par expliciter la structure de $\mathbb{Q}U_S$ comme $\mathbb{Q}[G]$-module, voir [Tate, 1984, Chapitre I, §4], et on en déduit une base de $\bigwedge^2_{\mathbb{Q}[G]} \mathbb{Q}U_S$ comme $\mathbb{Q}$-espace vectoriel et l'action de G sur cette base. Ainsi, on obtient l'action de l'idempotent $\tilde{e}_{S,2}$ comme application linéaire et donc son noyau $\mathcal{A}_{S,2}$. Pour déterminer l'élément $\eta_{\mathfrak{f}}$, on utilise la propriété *1*. On calcule le terme de droite à l'aide de l'expression de $\Phi_{\mathfrak{f}}$ en termes de fonctions L par les méthodes de Dummit et Tangedal [1998]. Puis, on trouve un générateur γ de $\mathcal{A}_{S,2}$ comme $\mathbb{Q}[G]$-module. Si la conjecture est vérifiée, alors il existe un élément $M \in \mathbb{Q}[G]$ tel que

$$M \frac{4}{\sqrt{d_k}} R(\gamma) = \Phi_{\mathfrak{f}}(1) .$$

Dans un premier temps, on résout cette équation avec $M \in \mathbb{R}[G]$ (il existe toujours une solution), puis on "reconnaît" les coefficients de A comme des nombres rationnels. Ceci est bien sûr toujours possible (à une précision fixée), mais le fait significatif est que, dans tous nos exemples, les nombres rationnels trouvées sont toujours de très petites hauteurs. Une fois M reconnut comme élément de $\mathbb{Q}[G]$, on pose $\eta_{\mathfrak{f}} = M \cdot \gamma$ et on vérifie la propriété *2* pour des nombres premiers p. La détermination du terme de droite nécessite de calculer les valeurs en $s = 1$ de fonctions zêta tordues p-adiques. Je parlerai de ce calcul dans la section 2.3. Finalement, il faut vérifier que $\eta_{\mathfrak{f}}$ est bien dans le réseau Λ_S. Pour cela, on utilise à nouveau l'expression trouvée de $\bigwedge^2_{\mathbb{Q}[G]} \mathbb{Q}U_S$ comme $\mathbb{Q}$-espace vectoriel.

Théorème 1.30. *La conjecture 1.28 est vérifiée à la précision des calculs, et pour la partie 2 pour certains nombres premiers p, pour les* 15 *exemples données dans la Table 1 de* [T9].

2 Algorithmique des nombres p-adiques

Les nombres p-adiques ont été découverts il y a maintenant un peu plus d'un siècle. Ils forment un outil théorique et algorithmique fondamental en théorie des nombres, et offrent aussi un intérêt intrinsèque dans leur étude explicite. De mon point de vue, les calculs sur les nombres p-adiques possèdent une bivalence séduisante : d'un côté, il y a un aspect calculs approchés puisque les nombres p-adiques ne peuvent être représentés, en général, que par des approximations, et d'un autre côté, il y aussi un aspect calcul exact car dans bien des applications une bonne approximation est suffisante pour obtenir un résultat exact, et il n'y a pas de phénomènes de perte de précision similaires à ce qui peut se passer avec les nombres réels. Dans ce chapitre, je donne une rapide description de mes articles [T3, T4, T9] dans ce domaine.

Notations et conventions. Soit p un nombre premier. On note $\mathbb{Q}_p$ le corps des nombres p-adiques rationnels et on fixe $\overline{\mathbb{Q}}_p$ une clôture algébrique de $\mathbb{Q}_p$. Toutes les extensions algébriques de $\mathbb{Q}_p$ considérées par la suite sont vues comme des sous-corps de $\overline{\mathbb{Q}}_p$.

2.1 Extensions d'un corps p-adique

Un résultat classique de la théorie des corps p-adiques (voir par exemple [Lang, 1994, Proposition 14, Chapitre II, §5]) affirme que tout corps p-adique possède un nombre fini d'extensions d'un degré donné. On peut donner une démonstration succincte de la manière suivante. Soit k un corps p-adique, on note $\mathfrak{p}$ son idéal maximal. Toute extension finie de k se décompose de manière unique en une sous-extension non ramifiée suivie d'une sous-extension totalement ramifiée, et il n'existe qu'une extension non ramifiée de k pour chaque degré, donc il suffit de démontrer qu'il n'existe qu'un nombre fini d'extensions totalement ramifiées de k d'un degré donné, disons N. Une telle extension K est engendrée sur k par la racine d'un polynôme d'Eisenstein de degré N. L'ensemble de tous ces polynômes s'identifie naturellement avec l'espace topologique

$$\mathbb{E}_N = \underbrace{\mathfrak{p} \times \cdots \times \mathfrak{p}}_{N-1 \text{ fois}} \times (\mathfrak{p} \setminus \mathfrak{p}^2). \tag{2.1}$$

Par le lemme de Krasner (voir [Lang, 1994, Chapitre II, §2, Proposition 3]), il existe dans $\mathbb{E}_N$ autour de chaque polynôme d'Eisenstein de degré N un disque ouvert tel que tous les polynômes contenus dans ce disque engendrent exactement les mêmes extensions de k que ce polynôme. Puisque $\mathbb{E}_N$ est compact, il suffit donc d'un nombre fini de polynômes d'Eisenstein pour obtenir toutes les extensions totalement ramifiées de k de degré N et le résultat s'ensuit.

Dans une série de notes au Comptes-Rendus de l'Académie des Sciences, Krasner [1962] (voir aussi l'article [Krasner, 1966] qui reprend l'ensemble des notes) donne des formules pour calculer le nombre d'extensions de k de degré fixé.[†] Dans l'article [T3] avec S. Pauli, nous montrons comment les méthodes utilisées par Krasner peuvent être rendues explicites afin d'obtenir, pour un degré donné, un ensemble de polynômes à coefficients dans k tel que les racines de ces polynômes engendrent toutes les extensions de k de degré N, et qui est minimal dans le sens que deux polynômes distincts de cet ensemble donnent des extensions non isomorphes. Comme décrit ci-dessus, le problème revient essentiellement à construire toutes les extensions totalement ramifiées. J'explique brièvement comment résoudre ce problème.

Soit $N \geq 2$. On cherche à construire toutes les extensions totalement ramifiées de degré N de k. Un premier résultat de Ore [1926] permet de donner les valeurs possibles pour le discriminant de ces extensions.

Lemme 2.1 (Ore)**.** *Soit j un entier relatif. On pose $j = aN + b$ la division euclidienne de j par N. Il existe une extension totalement ramifiée de k de degré N et de discriminant $\mathfrak{p}^{N+j-1}$ si et seulement si*

$$\min\{v_{\mathfrak{p}}(b), v_{\mathfrak{p}}(N)\} \leq \frac{j}{N} \leq v_{\mathfrak{p}}(N)$$

où $v_{\mathfrak{p}}$ est la valuation en $\mathfrak{p}$.

[†] En fait, les travaux de Krasner portent sur la situation plus générale du nombre d'extensions de degré et de discriminant fixés d'un corps localement compact.

On fixe à présent une valeur de j vérifiant les propriétés du lemme précédent. On note $\mathcal{K}_{N,j}$ l'ensemble des extensions totalement ramifiées de k de degré N et de discriminant $\mathfrak{p}^{N+j-1}$. On cherche à construire un ensemble minimal de polynômes d'Eisenstein donnant tous les éléments de $\mathcal{K}_{N,j}$. Une étude précise de la valuation p-adique des racines d'un polynôme d'Eisenstein suivant la valuation de ses coefficients permet de trouver la forme générale d'un polynôme d'Eisenstein de degré N et de discriminant $\mathfrak{p}^{N+j-1}$.[†] Puis en utilisant une version explicite du lemme de Krasner transposée sur les polynômes d'Eisenstein, on détermine une condition suffisante pour que deux tels polynômes engendrent des corps isomorphes. On obtient ainsi le résultat suivant (en conservant les notations du lemme 2.1).

Proposition 2.2. *Pour deux entiers m et l tels que $m \geq l \geq 1$, on fixe $\mathcal{R}_{l,m}$ un système de représentants dans $\mathcal{O}_k$ du quotient $\mathfrak{p}^l/\mathfrak{p}^m$. On note $\mathcal{R}^*_{l,m}$ le sous-ensemble des éléments de $\mathcal{R}_{l,m}$ dont la valuation en $\mathfrak{p}$ est exactement l.*

On définit pour $0 \leq i \leq N-1$

$$l(i) = \begin{cases} \max\{2 + a - v_{\mathfrak{p}}(i), 1\} & si \;\; i < b \\ \max\{1 + a - v_{\mathfrak{p}}(i), 1\} & si \;\; i \geq b. \end{cases}$$

et on pose c un entier tel que $c > 1 + 2j/N$.

On note Ω l'ensemble des vecteurs $(\omega_0, \ldots, \omega_{N-1}) \in \mathcal{O}_k^N$ tels que

$$\omega_i \in \begin{cases} \mathcal{R}^*_{1,c} & si \;\; i = 0, \\ \mathcal{R}_{l(i),c} & si \;\; 1 \leq i \leq N-1 \text{ et } i \neq b, \\ \mathcal{R}^*_{l(i),c} & si \;\; i = b \neq 0. \end{cases}$$

Alors, pour tout $(\omega_0, \ldots, \omega_{N-1}) \in \Omega$, les racines du polynôme d'Eisenstein

$$X^N + \omega_{N-1}X^{N-1} + \cdots + \omega_1 X + \omega_0$$

engendrent des éléments de $\mathcal{K}_{N,j}$ et, de plus, tous les éléments de $\mathcal{K}_{N,j}$ sont obtenus de cette manière.

L'ensemble Ω étant fini, il suffirait a priori pour répondre au problème de parcourir cet ensemble et de supprimer les polynômes superflus. Cependant, du point algorithmique, cette méthode n'est pas satisfaisante car le nombre d'éléments de Ω est bien trop grand par rapport au nombre minimal de polynômes requis pour engendrer tous les éléments de $\mathcal{K}_{N,j}$. Dans un premier temps, suivant la méthode mise au point par Krasner, on détermine le cardinal de cet ensemble.

Proposition 2.3 (Krasner)**.** *Avec les notations du lemme 2.1, on a*

$$\#\mathcal{K}_{N,j} = \begin{cases} N\, q^{s_0} & si \; b = 0, \\ N\,(q-1)\, q^{s_0+s_1} & sinon, \end{cases}$$

[†] Dans le cas d'un polynôme d'Eisenstein, le discriminant du corps engendré par une de ses racines est toujours égal au discriminant du polynôme.

où

$$s_0 = \sum_{i=1}^{\lfloor a/e \rfloor} \frac{eN}{p^i}\,, \qquad s_1 = \Big\lfloor \frac{j - \lfloor a/e \rfloor eN - 1}{p^{\lfloor a/e \rfloor + 1}} \Big\rfloor$$

et e l'indice de ramification de $k/\mathbb{Q}_p$.

La procédure pour trouver un ensemble minimal $\mathcal{E}$ de polynômes engendrant tous les éléments de $\mathcal{K}_{N,j}$ est la suivante. On commence avec $\mathcal{E} = \emptyset$ et un compteur c initialisé à 0. On énumère les éléments de Ω et à chaque nouveau polynôme, on teste si ce polynôme définit un corps déjà défini par un élément de $\mathcal{E}$. Si ce n'est pas le cas, on ajoute le polynôme à $\mathcal{E}$ et on incrémente c du nombre d'extensions distinctes engendrées par ce polynôme. Quand on arrive à $c = \#\mathcal{K}_{N,j}$, on sait que l'ensemble $\mathcal{E}$ est l'ensemble recherché.

2.2 Factorisation des polynômes dans $\mathbb{Q}_p[X]$

Soit Φ un polynôme irréductible, unitaire et à coefficients entiers. Alors Φ définit (à isomorphisme près) un corps de nombres K et le problème du calcul d'une base de l'anneau des entiers $\mathcal{O}_K$ de K, ou de manière équivalente du discriminant de K, est un problème fondamental de la théorie algorithmique des nombres. Plusieurs algorithmes ont été mis au point pour résoudre ces problèmes, notamment les algorithmes Round 2 [Cohen, 1993, Section 6.1] et Round 4 [Pohst et Zassenhaus, 1989, Chapitre 4]. L'algorithme Round 4, qui trouve ses bases dans [Zassenhaus, 1975], est un algorithme très complexe mais en général plus efficace que l'algorithme Round 2. Une première implantation est décrite dans [Ford, 1987] et une implantation plus complète est donnée dans [Ford et Letard, 1994]. En plus de cette complexité inhérente, l'algorithme Round 4 est très inefficace dans certains cas extrêmes.

Dans un travail [T4], en collaboration avec D. Ford et S. Pauli, en prenant pour base cet algorithme Round 4 nous avons développé une nouvelle méthode de factorisation des polynômes dans $\mathbb{Q}_p[X]$,[†] significativement plus simple et plus efficace en pratique que l'algorithme Round 4.

Soit $\Phi \in \mathbb{Q}_p[X]$ est un polynôme de degré d. On peut supposer sans perte de généralités que Φ est un polynôme unitaire, séparable et à coefficients dans $\mathbb{Z}_p$. Pour factoriser $\Phi(X)$, il suffit de résoudre l'alternative suivante

1. Montrer que Φ est irréductible ;
2. Trouver $\Phi_1, \Phi_2 \in \mathbb{Z}_p[X]$, non constants, tels que $\Phi(X) = \Phi_1(X)\,\Phi_2(X)$.

Soient $\phi_1, \ldots, \phi_d$ les racines (distinctes) de Φ dans $\overline{\mathbb{Q}}_p$. Pour tout $\alpha(T) \in \mathbb{Q}_p[T]$, on pose

$$\Phi_\alpha(X) = \prod_{i=1}^{d} (X - \alpha(\phi_i)) \in \mathbb{Q}_p[X]\,.$$

[†] Les trois problèmes algorithmiques de factorisation du polynôme F dans $\mathbb{Q}_p[X]$, de décomposition de p en idéaux premiers de K, et du calcul d'un sous-ordre p-maximal de $\mathcal{O}_K$ sont équivalents, voir [T4, §6].

Puis, on définit

$$\mathcal{O}_\Phi = \{\alpha(T) \in \mathbb{Q}_p[T] \text{ tel que } \Phi_\alpha(X) \in \mathbb{Z}_p[X]\}\,.$$

Les deux résultats suivants correspondent aux deux termes de l'alternative ci-dessus.

Proposition 2.4. *Le polynôme Φ est irréductible sur $\mathbb{Q}_p[X]$ si et seulement si il existe $\alpha(T) \in \mathcal{O}_\Phi$, un entier $k \geq 1$ et des polynômes B, C et D de $\mathbb{Z}_p[X]$ tels que*

$$\Phi_\alpha(X) = B(X)^k + p\big(B(X)\,C(X) + D(X)\big)$$

avec $\deg D < \deg B$ *et* $D \not\equiv 0 \pmod p$.

Remarque 2.5. Dans ce cas, on dit que α certifie Φ et, pour $i = 1, \ldots, d$, $\mathbb{Z}_p[\alpha(\phi_i)]$ est l'anneau des entiers du corps $\mathbb{Q}_p(\phi_i)$.

Proposition 2.6. *Le polynôme Φ est réductible sur $\mathbb{Q}_p[X]$ si et seulement si il existe $\alpha(T) \in \mathcal{O}_\Phi$ et deux polynômes B et C non constants et unitaires de $\mathbb{Z}_p[X]$ tels que*

$$\Phi_\alpha(X) \equiv B(X)\,C(X) \pmod p$$

avec B et C premiers entre eux modulo p.

Remarque 2.7. On sait calculer la factorisation de Φ_α modulo p en temps probabiliste polynômial, voir [Cohen, 1993, Section 3.4].

Remarque 2.8. Cette proposition peut être rendue explicite dans le sens où on peut déduire de la factorisation de Φ_α modulo p, une factorisation de Φ dans $\mathbb{Q}_p[X]$.

L'algorithme consiste à essayer d'écrire le développement d'un élément $\beta \in \mathcal{O}_\Phi$

$$\begin{aligned}\beta = M_{0,0}(\xi) + M_{0,1}(\xi)\pi + \cdots + M_{0,E-1}(\xi)\pi^{E-1} \\ + p \cdot (M_{1,0}(\xi) + M_{1,1}(\xi)\pi + \cdots + M_{1,E-1}(\xi)\pi^{E-1}) \\ + p^2 \cdot (M_{2,0}(\xi) + M_{2,1}(\xi)\pi + \cdots + M_{2,E-1}(\xi)\pi^{E-1}) + \cdots\end{aligned}$$

où $M_{i,j} \in \mathbb{Z}_p[X]$, $\pi \in \mathcal{O}_\Phi$ est tel que $v(\pi) = 1/E > 0$ et $\xi \in \mathcal{O}_\Phi$ engendre un corps résiduel $\mathbb{F}_p(\xi)$ de degré F sur $\mathbb{F}_p$.[†] Notons qu'on a toujours $EF \leq \deg(\Phi)$ avec égalité si et seulement si Φ est irréductible.

On calcule les polynômes $M_{i,j}$ les uns après les autres. Si, au cours de cette construction, on découvre un élément $\pi' \in \mathcal{O}_\Phi$ tel que $v(\pi') = 1/E' < v(\pi)$, on remplace π par π'. De même, si on trouve $\xi' \in \mathcal{O}_\Phi$ tel que $\mathbb{F}_p(\xi') \supsetneq \mathbb{F}_p(\xi)$, on remplace ξ par ξ'. On montre que si Φ est irréductible, alors, après un certain nombre d'étapes, on obtient π et ξ tels $EF = \deg(\Phi)$. Sinon, Φ est réductible, et on montre qu'après un certain nombre d'étapes, il y a plus d'un choix possible pour le polynôme $M_{i,j}$ ce qui mène

[†] Un tel développement est possible si Φ est irréductible, π une uniformisante de $\mathcal{O}_\Phi$ (qui est isomorphe à l'anneau des entiers d'un corps p-adique dans ce cas), et ξ un élément primitif du corps résiduel $\mathcal{O}_\Phi/(\pi)$.

à une factorisation de F. De plus, à chaque étape, on teste également si les éléments trouvés durant la construction vérifient une des deux propositions 2.4 ou 2.6 ce qui donne directement l'irréductibilité ou une factorisation de Φ.

Cette méthode a été implantée dans le système PARI/GP (et est utilisée par les fonctions : `factorpadic`, `nfdisc`, `nfinit`, etc). Elle est expérimentalement beaucoup plus efficace que les autres méthodes connues de factorisation des polynômes dans $\mathbb{Q}_p[X]$.

2.3 Fonctions zêta p-adiques de corps quadratiques réels

La vérification numérique effectuée dans [T9] de la conjecture 1.28 nécessite de calculer les valeurs en $s = 1$ de fonctions zêta tordues p-adiques d'un corps quadratique réel k. La méthode que nous avons utilisée dans ce travail généralise la méthode de calcul de $L_p(1, \chi)$ donnée dans [Lang, 1990, Chapitre 4]. Afin de simplifier la présentation, on suppose dans cette section que p est un nombre premier impair.

Soient τ_1, τ_2 deux éléments totalement positifs et non proportionnels du corps quadratique réel k. On considère le cône défini par ces deux éléments

$$C(\tau_1, \tau_2) = \left\{ r_1\tau_1 + r_2\tau_2 \text{ pour } r_1, r_2 \in \mathbb{Q} \text{ avec } 0 < r_1,\ 0 \leq r_2 \right\},$$

et le parallélogramme fondamental associé

$$P(\tau_1, \tau_2) = \left\{ r_1\tau_1 + r_2\tau_2 \text{ pour } r_1, r_2 \in \mathbb{Q} \text{ avec } 0 < r_1 \leq 1,\ 0 \leq r_2 < 1 \right\} \subset C(\tau_1, \tau_2).$$

Il est facile de voir que le cône $C(\tau_1, \tau_2)$ est l'union disjointe des translatés

$$P(\tau_1, \tau_2) + m_1\tau_1 + m_2\tau_2$$

pour m_1 et m_2 parcourant $\mathbb{N}$.

Soit I un idéal fractionnaire de $\mathcal{O}_k$ et soit $\xi : I \to \mathbb{C}^\times$ un caractère additif. On suppose que $\tau_1, \tau_2 \in I$ et que $\xi(\tau_1), \xi(\tau_2) \neq 1$. La fonction zêta tordue associée à ces données est définie, pour $s \in \mathbb{C}$ avec $\Re(s) > 1$, par

$$Z(s; \xi, \tau_1, \tau_2) = \sum_{a \in I \cap C(\tau_1, \tau_2)} \xi(a)\, \mathcal{N}a^{-s}. \tag{2.2}$$

Cette fonction admet une prolongement méromorphe à $\mathbb{C}$. La base de l'interpolation p-adique est le résultat suivant.

Théorème 2.9. *Il existe une série formelle $F(X_1, X_2; \xi, \tau_1, \tau_2) \in \bar{\mathbb{Q}}[X_1, X_2]$ telle que*

$$Z(m; \xi, \tau_1, \tau_2) = \left(\Delta^{-m} F(X_1, X_2; \xi, \tau_1, \tau_2)\right)_{|X_1 = X_2 = 0}$$

pour tout entier $m \leq 0$, où Δ est l'opérateur

$$(1 + X_1)(1 + X_2)\, \frac{\partial^2}{\partial X_1\, \partial X_2}.$$

Remarque 2.10. La série $F(X_1, X_2; \xi, \tau_1, \tau_2)$ est définie de manière explicite par une somme finie portant sur les éléments de $I \cap P(\tau_1, \tau_2)$.

Pour que l'interpolation soit possible, on doit enlever "les facteurs eulériens en p", c'est-à-dire dans la définition (2.2), on restreint la somme aux éléments a tels que l'indice $(I : (a))$ n'est pas divisible par p. On note $Z_{(p)}(s; \xi, \tau_1, \tau_2)$ la fonction ainsi obtenue et $F_{(p)}(X_1, X_2; \xi, \tau_1, \tau_2)$ la série formelle modifiée de manière à ce que le théorème 2.9 reste valide. La méthode d'interpolation utilisée dans [T9] nécessite les hypothèses suivantes[†]

(H1) p est premier avec le noyau de ξ ;

(H2) p est décomposé dans k ;

(H3) l'idéal I est premier avec p.

Sous ces hypothèses, on interprète la série $F_{(p)}(X_1, X_2; \xi, \tau_1, \tau_2)$ comme une mesure μ_{ξ,τ_1,τ_2} sur $\mathbb{Z}_p^2$ à support dans $(\mathbb{Z}_p^\times)^2$, et le théorème 2.9, ou plutôt sa version modifiée, se reformule en l'équation suivante

$$Z_{(p)}(m; \xi, \tau_1, \tau_2) = \int_{(\mathbb{Z}_p^\times)^2} \psi_m(x_1, x_2)\, d\mu_{\xi,\tau_1,\tau_2}(x_1, x_2) \tag{2.3}$$

pour tout $m \in \mathbb{Z}_{\leq 0}$ pour certaines fonctions p-adiques ψ_m. la méthode consiste alors à trouver une fonction p-adique continue $s \mapsto \psi_s$ qui "interpole" les fonctions ψ_m. On obtient le résultat suivant.

Théorème 2.11. *Il existe une unique fonction $Z_p(s; \xi, \tau_1, \tau_2)$, définie et continue sur $\mathbb{Z}_p$ telle que*

$$Z_p(m; \xi, \tau_1, \tau_2) = Z_{(p)}(m; \xi, \tau_1, \tau_2)$$

pour tout entier $m \leq 0$ avec $m \equiv 1 \pmod{p-1}$.

De plus, si on écrit

$$\frac{F_{(p)}(X_1, X_2; \xi, \tau_1, \tau_2)}{(1+X_1)(1+X_2)} = \sum_{n_1, n_2 \geq 0} a_{n_1,n_2} X_1^{n_1} X_2^{n_2}$$

où les coefficients a_{n_1,n_2} sont vus comme des éléments de $\overline{\mathbb{Q}}_p$, alors on a

$$Z_p(1; \xi, \tau_1, \tau_2) = \frac{1}{p^2} \sum_{n_1, n_2 \geq 0} \frac{c_{n_1+1}\, c_{n_2+1}\, a_{n_1,n_2}}{(n_1+1)(n_2+1)} \tag{2.4}$$

avec $c_n = \sum_{\zeta^p = 1} (\zeta - 1)^n \in \mathbb{Z}_p$ où ζ parcourt les racines p-ièmes de l'unité dans $\overline{\mathbb{Q}}_p$.

L'équation (2.4) nécessite le calcul explicite des coefficients de la série entière $F_{(p)}(X_1, X_2; \xi, \tau_1, \tau_2)$, ce qui exige, par la remarque 2.10, d'énumérer les points de

[†] L'hypothèse (H1) est essentielle pour cette méthode d'interpolation, l'hypothèse (H2) simplifie l'exposition et les calculs, l'hypothèse (H3) ne pose pas de problèmes dans la pratique.

$P(\tau_1, \tau_2)$. Dans nos applications, on a $\tau_2 = \epsilon\tau_1$ avec ϵ une puissance de l'unité fondamentale de k et donc le nombre de points dans ce parallèlogramme est en général beaucoup trop grand pour permettre le calcul. Nous utilisons donc une méthode de Zagier [1977], voir aussi [Hayes, 1990], pour partitionner le cône $C(\tau_1, \tau_2)$ en un ensemble fini de sous-cônes[†] grâce à l'écriture en fraction continue de ϵ, chaque sous-cône contenant un nombre très faible d'éléments. Cette méthode nous a permis dans [T9] de calculer efficacement les valeurs en $s = 1$ de fonctions zêta tordues p-adiques de corps quadratiques réels pour des nombres premiers jusqu'à $p = 41$.

3 Autres travaux

Depuis mon arrivée à l'université Claude Bernard Lyon 1, plusieurs collaborations sont nées de discussions avec mes collègues sur des aspects explicites de la théorie analytique des nombres. J'ai aussi collaboré en cryptographie avec des collègues de Grenoble dans le cadre d'un projet commun. Dans ce chapitre, je décris brièvement les articles [T5, T8, T10, T11], fruits de ces collaborations.

3.1 Cryptographie sur les modules de Drinfeld

Soit $q = p^d$ où p est un nombre premier et $d \geq 1$. On cherche à construire des polynômes $P(X) \in \mathbb{F}_q[X]$ possédant les propriétes suivantes

1. La fonction $x \mapsto P(x)$ est injective (et donc bijective) ;
2. La construction de P donne aussi la construction de l'application réciproque ;
3. La construction de l'application réciproque est très difficile à partir uniquement du polynôme P ;
4. Le polynôme P est facile à évaluer.

Un tel polynôme définit une fonction à *sens unique à trappe*, fonctions qui jouent un rôle capital en cryptographie, voir [Menezes et al., 1997, Section 1.3.1].

Dans le travail [T5] en collaboration avec R. Gillard, F. Leprevost et A. Panchishkin, nous utilisons les modules de Drinfeld pour construire de tels polynômes. Les modules de Drinfeld, qui peuvent être vus comme des analogues des courbes elliptiques, ont été déjà étudiés en cryptographie et n'ont pas été jugés sûrs, voir [Scanlon, 2001]. Cependant, notre point de vue dans [T5] est différent car il ne s'agit pas de transposer aux modules de Drinfeld les protocoles existants pour les courbes elliptiques, mais d'utiliser des propriétés qui leurs sont spécifiques. Sans donner trop de détails sur la théorie des modules de Drinfeld, voir [Drinfeld, 1974, 1977] pour plus de renseignements, cette théorie permet de munir le corps $\mathbb{F}_q$ d'une structure de $\mathbb{F}_p[T]$-module. Cette structure n'est pas la structure naturelle provenant de l'isomorphisme entre $\mathbb{F}_q$ et $\mathbb{F}_p[T]/(f)$ pour f polynôme irréductible de $\mathbb{F}_p[T]$. L'idée est alors de combiner cette nouvelle structure avec la structure naturelle pour construire un polynôme

[†] Ce qui revient à écrire la série $F_{(p)}(X_1, X_2; \xi, \tau_1, \tau_2)$ comme somme de séries similaires, chacune associée à un sous-cône.

à coefficients dans $\mathbb{F}_q$ satisfaisant aux propriétés 1 et 2. La propriété 3 est assurée par le fait que pour construire l'application réciproque, il est nécessaire de connaître les paramètres qui ont permis la construction du polynôme. Cependant, pour avoir la propriété 4, il faut construire un polynôme avec beaucoup de coefficients nuls. Cela impose un grand nombre de restrictions sur les paramètres qui interviennent dans la construction et aussi, par conséquence, sur la forme du polynôme construit. En prenant avantage de ces restrictions, une attaque a été mise au point dans [Blackburn et al., 2006] en utilisant la méthode de relinéarisation de Kipnis et Shamir [1999]. A l'heure actuelle, pour tous les choix des paramètres pouvant permettre une utilisation réelle de ce protocole, celui-ci n'offre que peu de sécurité.

3.2 Compter les nombres premiers dans les classes de congruences

Deléglise et Rivat [1996] ont élaboré un algorithme pour calculer $\pi(x)$, le nombre de nombres premiers $\leq x$, en temps $O(x^{2/3}/(\log x)^2)$ en améliorant un algorithme de Lagarias et al. [1985] basé sur une idée de l'astronome allemand Meissel. Dans ce travail [T8] en collaboration avec M. Deléglise et P. Dusart, nous montrons comment modifier cet algorithme pour calculer $\pi(x;k,l)$, le nombre de nombres premiers $\leq x$ congrus à l modulo k. La méthode consiste à traiter en parallèle les différentes classes de congruence et a aussi une complexité de $O(x^{2/3}/(\log x)^2)$.

L'algorithme repose sur l'idée suivante. Pour y tel que $x^{1/3} \leq y \leq x^{1/2}$, on pose $T(x,y;k,l)$ l'ensemble des entiers $\leq x$, congrus à l modulo k et dont tous les facteurs premiers sont $> y$. Tout élément de cet ensemble a au plus deux facteurs premiers (non nécessairement distincts) et on peut le partionner en trois sous-ensembles T_0, T_1 et T_2 suivant ce nombre de facteurs premiers. L'ensemble $T_0(x,y;k,l)$ contient au plus 1 et son cardinal est $\delta_{l,1}$. L'ensemble $T_1(x,y;k,l)$ est formé de tous les nombres premiers p avec $p \equiv l \pmod{k}$ et $y < p \leq x$, et donc son cardinal est $\pi(x;k,l) - \pi(y;k,l)$. On a donc

$$\pi(x;k,l) = |T(x,y;k,l)| + \pi(y;k,l) - \delta_{l,1} - |T_2(x,y;k,l)|.$$

Le calcul du cardinal de $T_2(x,y;k,l)$ se fait en temps $O(x^{1/2+\epsilon})$ par un crible parallèle sur les différentes classes de congruence modulo k. Le calcul de $\pi(y;k,l)$ se fait par une version modifiée du crible d'Erathosthène. Le coût est de $O(y \log y) = O(x^{1/2} \log x)$. Le coût le plus important est pour le calcul du cardinal de $T(x,y;k,l)$. Ce calcul est assez technique et nécessite de combiner plusieurs approches. La complexité de cette partie est $O(x^{2/3}/(\log x)^2)$ et donc domine largement le reste des calculs.

Comme application de cette méthode, nous avons considéré le problème des nombres premiers modulo 4. Asymptotiquement, le nombre de nombres premiers congrus à 1 modulo 4 et le nombre de nombre premiers congrus à 3 modulo 4 sont les mêmes. Cependant, pour des valeurs de x prises au hasard, on remarque qu'on a très majori-

tairement

$$\pi(x;4,1) < \pi(x;4,3).^{\dagger}$$

Cependant, Littlewood [1914] a démontré que la quantité $\pi(x;4,1) - \pi(x;4,3)$ change de signe un nombre infini de fois et prend des valeurs arbitrairement grandes et petites. Ainsi, il existe un nombre infini de plages sur lesquelles $\pi(x;4,1) > \pi(x;4,3)$. Jusqu'à présent, les huit premières plages étaient connues, la plus grande se trouvant juste avant 10^{13}. Grâce à notre méthode, nous avons réussi à déterminer une neuvième plage aux alentours de 10^{18}.

3.3 Nombre de solutions de $A^2 + B^2 = C^2 + C$

Dans l'article [T10] en collaboration avec J.-L. Nicolas et J.-M. Muller, nous étudions le nombre de solutions entières de l'équation

$$A^2 + B^2 = C^2 + C \tag{3.1}$$

satisfaisant des conditions de taille. Plus précisément, le résultat principal de l'article est le suivant

Théorème 3.1. *Pour $\lambda > \sqrt{2}$, on note $Q(N,\lambda)$ le nombre de triplets (A,B,C) d'entiers vérifiant* (3.1) *et tels que*

$$N \le A \le B \le C \le \lambda N - \frac{1}{2}.$$

Alors, on a

$$Q(N,\lambda) = \alpha(\lambda)N + O(N^{7/8}\log N)$$

où

$$\alpha(\lambda) = \frac{\lambda}{4} - \frac{\lambda}{\pi}\arcsin(1/\lambda) + \frac{\log(1+\sqrt{2})}{\pi} - \frac{\log(\lambda+\sqrt{\lambda^2-1})}{\pi}.$$

La démonstration de ce résultat consiste à transformer l'équation sous la forme

$$X^2 + Y^2 = Z^2 - 1$$

puis utilise différentes techniques provenant des travaux de Hooley [1976] et des estimations précises de sommes de Kloosterman. L'article présente aussi des résultats numériques plus explicites dans le cas $\lambda = 2$.

3.4 Densité des entiers de la forme $p + 2^k$

Romanoff [1934] a démontré que l'ensemble des entiers impairs qui peuvent s'écrire comme somme d'une puissance de 2 et d'un nombre premier possède une densité positive. Erdös [1950] a remarqué qu'aucun terme de la progression arithmétique 7 629 217 modulo 11 184 810 [‡] ne peut s'écrire sous la forme $p + 2^k$ et ainsi cette densité est strictement plus petite que 1. Dans l'article [T11], en collaboration avec L. Habsieger, nous avons donné de nouvelles bornes inférieure et supérieure sur cette densité.

[†] Une explication heuristique de ce phénomène est que tous les carrés sont congrus à 1 modulo 4.

[‡] Les valeurs données dans l'article sont incorrectes.

Théorème 3.2. *On note*

$$\underline{d} = \liminf_{x\to\infty} \frac{\#\{p + 2^k \leq x\}}{x/2} \quad \textit{et} \quad \bar{d} = \limsup_{x\to\infty} \frac{\#\{p + 2^k \leq x\}}{x/2}.$$

Alors, on a

$$0,1866 \leq \underline{d} \leq \bar{d} \leq 0,9819.^{\dagger}$$

La borne inférieur est obtenue en utilisant en raffinant un résultat récent de Pintz et Ruzsa [2003]. La borne supérieure est obtenue par des méthodes algorithmiques, généralisant la remarque d'Erdös par le lemme suivant.

Lemme 3.3. *Soit $M \geq 3$ un entier impair. On note ω l'ordre de 2 modulo M. Pour $\bar{m} \in \mathbb{Z}/M\mathbb{Z}$ et $\nu \geq 0$, on pose*

$$\begin{aligned} f_M(\bar{m}) &= \{\bar{k} \in \mathbb{Z}/\omega\mathbb{Z} \textit{ tel que } \bar{m} - 2^{\bar{k}} \in (\mathbb{Z}/M\mathbb{Z})^*\} \\ \delta_M(\nu) &= \left|\{\bar{m} \in \mathbb{Z}/M\mathbb{Z} \textit{ tel que } |f_M(\bar{m})| = \nu\}\right|. \end{aligned}$$

Alors, on a

$$\bar{d} \leq \sum_{\nu=0}^{\omega} \delta_M(\nu) \min\left\{\frac{1}{M}, \frac{2\nu}{\omega\varphi(M)\log 2}\right\}.$$

Il faut donc trouver des valeurs de M telles que la borne donnée dans ce lemme soit la plus petite possible. Ces valeurs de M sont construites par un procédé de type "backtracking" en rajoutant un par un des facteurs premiers à M et en regardant si cela améliore la borne. La valeur obtenue dans l'article pour la borne supérieur est pour

$$M = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 31 \cdot 41 \cdot 73 \cdot 241 \cdot 257.$$

[†] La valeur conjecturée est 0,868.

Bibliographie

[Allombert, 2004] B. Allombert. An efficient algorithm for the computation of Galois automorphisms. *Math. Comp.*, 73(245), 359–375, 2004.

[Blackburn et al., 2006] S. Blackburn, C. Cid, et S. Galbraith. Cryptanalysis of a cryptosystem based on Drinfeld modules. *IEE Proceedings Information Security*, 153(1), 12–14, 2006.

[Burns et al., 2004] D. Burns, J. Sands, et D. Solomon (éditeurs). *Stark's conjectures : recent work and new directions*, volume 358 de *Contemporary Mathematics*. Amer. Math. Soc., Providence, RI, 2004. Actes de la conférence internationale "Stark's Conjectures and Related Topics" à Johns Hopkins University, Baltimore, MD, 5–9 août 2002.

[Cassou-Noguès, 1979] Pi. Cassou-Noguès. Valeurs aux entiers négatifs des fonctions zêta et fonctions zêta p-adiques. *Invent. Math.*, 51(1), 29–59, 1979.

[Chinburg, 1983] T. Chinburg. Stark's conjecture for L-functions with first-order zeroes at $s = 0$. *Adv. in Math.*, 48(1), 82–113, 1983.

[Cohen, 1993] H. Cohen. *A course in computational algebraic number theory*, volume 138 de *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[Cohen, 2000] H. Cohen. *Advanced topics in computational number theory*, volume 193 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[Cohen, 2001] H. Cohen. Computational aspects of number theory. In *Mathematics unlimited—2001 and beyond*, pages 301–330. Springer, Berlin, 2001.

[Deléglise et Rivat, 1996] M. Deléglise et J. Rivat. Computing $\pi(x)$: the Meissel, Lehmer, Lagarias, Miller, Odlyzko method. *Math. Comp.*, 65(213), 235–245, 1996.

[Deligne et Ribet, 1980] P. Deligne et K. Ribet. Values of abelian L-functions at negative integers over totally real fields. *Invent. Math.*, 59(3), 227–286, 1980.

[Drinfeld, 1974] V. Drinfeld. Elliptic modules. *Mat. Sb. (N.S.)*, 94(136), 594–627, 1974.

[Drinfeld, 1977] V. Drinfeld. Elliptic modules. II. *Mat. Sb. (N.S.)*, 102(144), 182–194, 1977.

[Dummit et Tangedal, 1998] D. Dummit et B. Tangedal. Computing the lead term of an abelian L-function. In *Algorithmic number theory (Portland, OR, 1998)*, volume 1423 de *Lecture Notes in Comput. Sci.*, pages 400–411. Springer, Berlin, 1998.

[Dummit, 2004] D. Dummit. Computations related to Stark's conjecture. In *Stark's conjectures : recent work and new directions*, volume 358 de *Contemp. Math.*, pages 37–54. Amer. Math. Soc., Providence, RI, 2004.

[Erdös, 1950] P. Erdös. On integers of the form $2^k + p$ and some related problems. *Summa Brasil. Math.*, 2, 113–123, 1950.

[Fogel, 1998] K. Fogel. *Stark's conjecture for octahedral extensions.* PhD Diss., University of Texas at Austin, 1998.

[Ford et Letard, 1994] D. Ford et P. Letard. Implementing the Round Four maximal order algorithm. *J. Théor. Nombres Bordeaux*, 6(1), 39–80, 1994.

[Ford, 1987] D. Ford. The construction of maximal orders over a Dedekind domain. *J. Symbolic Comput.*, 4(1), 69–75, 1987.

[Greither, 2000] C. Greither. Some cases of Brumer's conjecture for abelian CM extensions of totally real fields. *Math. Z.*, 233(3), 515–534, 2000.

[Hayes, 1990] D. Hayes. Brumer elements over a real quadratic base field. *Exposition. Math.*, 8(2), 137–184, 1990.

[Hilbert, 2000] D. Hilbert. Mathematical problems. *Bull. Amer. Math. Soc. (N.S.)*, 37(4), 407–436, 2000. Réédition de Bull. Amer. Math. Soc. **8** (1902), 437–479.

[Hooley, 1976] C. Hooley. *Applications of sieve methods to the theory of numbers.* Cambridge University Press, Cambridge, 1976. Cambridge Tracts in Mathematics, No. 70.

[Jehanne, 2001] A. Jehanne. Realization over $\mathbb{Q}$ of the groups $\tilde{A}_5$ and $\hat{A}_5$. *J. Number Theory*, 89(2), 340–368, 2001.

[Kipnis et Shamir, 1999] A. Kipnis et A. Shamir. Cryptanalysis of the HFE public key cryptosystem by relinearization. In *Advances in cryptology—CRYPTO '99 (Santa Barbara, CA)*, volume 1666 de *Lecture Notes in Comput. Sci.*, pages 19–30. Springer, Berlin, 1999.

[Krasner, 1962] M. Krasner. Nombre des extensions d'un degré donné d'un corps $\wp$-adique : énoncé des résultats et préliminaires de la démonstration (espace des polynomes, transformation T) ; suite de la démonstration ; les conditions d'Ore et la caractérisation de $E_{k,j}^{(n)}$, préliminaires du calcul de $N_{k,j,s}^{(n)}$; compléments au théorème 1 dans le cas non $\mathfrak{p}$-adique, démonstration du théorème 2 ; calcul de $N_{k,j,s}^{(n)}$, démonstration du théorème 1. *C. R. Acad. Sci. Paris*, 254 :3470–3472 ; 255 :224–226 ; 255 :1682–1684 ; 255 :3095–3097 ; 255 :2342–2344, 1962.

[Krasner, 1966] M. Krasner. Nombre des extensions d'un degré donné d'un corps $\mathfrak{p}$-adique. In *Les Tendances Géom. en Algèbre et Théorie des Nombres*, pages 143–169. Editions du Centre National de la Recherche Scientifique, Paris, 1966.

[Lagarias et al., 1985] J. Lagarias, V. Miller, et A. Odlyzko. Computing $\pi(x)$: the Meissel-Lehmer method. *Math. Comp.*, 44(170), 537–560, 1985.

[Lang, 1990] S. Lang. *Cyclotomic fields I and II*, volume 121 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, seconde édition, 1990.

[Lang, 1994] S. Lang. *Algebraic number theory*, volume 110 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, seconde édition, 1994.

[Littlewood, 1914] J. Littlewood. Sur la distribution des nombres premiers. *C. R. Acad. Sci. Paris*, 158, 1869–1872, 1914.

[Martinet, 1977] J. Martinet. Character theory and Artin L-functions. In *Algebraic number fields : L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 1–87. Academic Press, London, 1977.

[Menezes et al., 1997] A. Menezes, P. van Oorschot, et S. Vanstone. *Handbook of applied cryptography*. CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1997. With a foreword by Ronald L. Rivest.

[Ore, 1926] O. Ore. Bemerkungen zur Theorie der Differente. *Math. Z.*, 25(1), 1–8, 1926.

[Pintz et Ruzsa, 2003] J. Pintz et I. Ruzsa. On Linnik's approximation to Goldbach's problem. I. *Acta Arith.*, 109(2), 169–194, 2003.

[Pohst et Zassenhaus, 1989] M. Pohst et H. Zassenhaus. *Algorithmic algebraic number theory*, volume 30 de *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1989.

[Popescu, 2004] C. Popescu. Rubin's integral refinement of the abelian Stark conjecture. In *Stark's conjectures : recent work and new directions*, volume 358 de *Contemp. Math.*, pages 1–35. Amer. Math. Soc., Providence, RI, 2004.

[Roblot, 1997] X.-F. Roblot. *Algorithmes de factorisation dans les extensions relatives et applications de la conjecture de Stark à la construction des corps de classes de rayon*. Thèse de troisième cycle, Laboratoire A2X, Université Bordeaux 1, 1997.

[Roblot, 2000] X.-F. Roblot. Stark's conjectures and Hilbert's twelfth problem. *Experiment. Math.*, 9(2), 251–260, 2000.

[Roblot, 2004] X.-F. Roblot. Polynomial factorization algorithms over number fields. *J. Symbolic Comput.*, 38(5), 1429–1443, 2004.

[Romanoff, 1934] N. Romanoff. Über einige Sätze der additiven Zahlentheorie. *Math. Ann.*, 109, 668–678, 1934.

[Scanlon, 2001] T. Scanlon. Public key cryptosystems based on Drinfeld modules are insecure. *J. Cryptology*, 14(4), 225–230, 2001.

[Solomon, 2002] D. Solomon. On p-adic abelian Stark conjectures at $s = 1$. *Ann. Inst. Fourier (Grenoble)*, 52(2), 379–417, 2002.

[Stark, 1971] H. Stark. Values of L-functions at $s = 1$. I. L-functions for quadratic forms. *Advances in Math.*, 7, 301–343 (1971), 1971.

[Stark, 1975] H. Stark. L-functions at $s = 1$. II. Artin L-functions with rational characters. *Advances in Math.*, 17(1), 60–92, 1975.

[Stark, 1976] H. Stark. L-functions at $s = 1$. III. Totally real fields and Hilbert's twelfth problem. *Advances in Math.*, 22(1), 64–84, 1976.

[Stark, 1977] H. Stark. Class fields for real quadratic fields and L-series at 1. In *Algebraic number fields : L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 355–375. Academic Press, London, 1977.

[Stark, 1977] H. Stark. Hilbert's twelfth problem and L-series. *Bull. Amer. Math. Soc.*, 83(5), 1072–1074, 1977.

[Stark, 1980] H. Stark. L-functions at $s = 1$. IV. First derivatives at $s = 0$. *Adv. in Math.*, 35(3), 197–235, 1980.

[Stark, 1981] H. Stark. Derivatives of L-series at $s = 0$. In *Automorphic forms, representation theory and arithmetic (Bombay, 1979)*, volume 10 de *Tata Inst. Fund. Res. Studies in Math.*, pages 261–273. Tata Inst. Fund. Res., Bombay, 1981.

[Tate, 1981] J. Tate. Brumer-Stark-Stickelberger. In *Seminar on Number Theory, 1980–1981 (Talence, 1980–1981)*, pages Exp. No. 24, 16. Univ. Bordeaux I, Talence, 1981.

[Tate, 1984] J. Tate. *Les conjectures de Stark sur les fonctions L d'Artin en s = 0*, volume 47 de *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA, 1984. Notes par Dominique Bernardi et Norbert Schappacher.

[Wiles, 1990] A. Wiles. On a conjecture of Brumer. *Ann. of Math. (2)*, 131(3), 555–565, 1990.

[Zagier, 1977] D. Zagier. Valeurs des fonctions zêta des corps quadratiques réels aux entiers négatifs. In *Journées Arithmétiques de Caen (Univ. Caen, Caen, 1976)*, pages 135–151. Astérisque No. 41–42. Soc. Math. France, Paris, 1977.

[Zassenhaus, 1975] H. Zassenhaus. On Hensel factorization. II. In *Symposia Mathematica, Vol. XV (Convegno di Strutture in Corpi Algebrici, INDAM, Rome, 1973)*, pages 499–513. Academic Press, London, 1975.