Université Paris Sud – Centre d'Orsay

HABILITATION À DIRIGER DES RECHERCHES

spécialité : **Mathématiques**

Contributions à l'algorithmique des corps de nombres

Karim BELABAS

– Jury –

M. Henri COHEN	Université Bordeaux I
M. Étienne FOUVRY	Université Paris XI
M. Hendrik LENSTRA	Universiteit Leiden
M. Jean-François MESTRE	Université Paris VII
Mme. Bernadette PERRIN-RIOU	Université Paris XI
M. Don ZAGIER	Collège de France

– décembre 2003 –

à Layla

Je voudrais tout d'abord remercier Étienne Fouvry qui m'a suggéré, il y a près de douze ans, de travailler sur un article oublié de Davenport et Heilbronn, et n'a cessé de me soutenir depuis ces premiers pas, pour finalement présenter aujourd'hui mes travaux.

Je voudrais ensuite chaleureusement remercier mes rapporteurs Hendrik Lenstra et Jean-François Mestre, ainsi qu'Henri Cohen, Bernadette Perrin-Riou et Don Zagier qui me font l'honneur d'être membres de mon jury.

Ces recherches ont été menées d'abord au Max-Planck-Institut für Mathematik (Bonn) jusqu'en avril 1998, puis dans l'équipe « Arithmétique et Géométrie Algébrique » du département de mathématiques de l'Université Paris XI (Orsay). Je voudrais remercier tous ceux que j'y ai côtoyé quotidiennement, pour de multiples, amicales, et fructueuses discussions.

L'essentiel des calculs décrits ont été menés sur les ordinateurs du centre de calcul formel MEDICIS (École Polytechnique) et du laboratoire A2X (Bordeaux I), et je voudrais finalement remercier ceux qui ont créé ces centres, en particulier Marc Giusti et Jacques Martinet, ainsi que les ingénieurs qui en assurent la maintenance.

Ces travaux ont bénéficié de l'existence d'une foule de logiciels libres de grande qualité, notamment initiés par Donald Knuth (TEX), Bram Moolenaar (Vim), Richard Stallman (le projet GNU), Chet Ramey (Bash et readline), Linus Torvalds (le noyau Linux), Larry Wall (Perl), et bien d'autres enthousiastes.

Table des matières

1. Introduction

L'algorithmique des corps de nombres est née au cours des années 1970 comme sujet autonome. Elle a pour objet l'analyse et la réalisation de calculs portant sur les extensions finies de $\mathbb{Q}$. Parmi les grandes familles d'applications, j'en mentionnerai cinq, parmi les plus significatives. En premier lieu se trouve le calcul brut d'invariants, dont on désire par exemple étudier expérimentalement la statistique sur des familles de corps. Ce point est parfois accessible aux méthodes de la théorie analytique des nombres, qui permet alors des estimations asymptotiques rigoureuses. En second et troisième lieu, la théorie de Galois et la théorie du corps de classes effectives décrivent et explicitent des extensions. En quatrième lieu, le zoo des séries L et de leurs valeurs spéciales fournit conjectures et formules qu'il est intéressant de tester, ou d'utiliser pour mettre en œuvre le premier point. Et finalement, les motivations diophantiennes aux origines de la théorie algébrique des nombres sont toujours présentes, souvent sous l'angle de la recherche et l'étude des points rationnels de variétés algébriques.

Mes contributions[1] s'inscrivent dans ces différents thèmes à l'exception du dernier : estimations et calculs liés aux corps quadratiques ou cubiques (§2), dans leur versant analytique [T2, T5, T6, T8] et algorithmique [T1, T3, T4, T9], factorisation des polynômes (§3,[T10, T13]), théorie du corps de classes (§4, [T12]) et K_2-théorie effectives (§5, [T7, T11]). Ces recherches ont été en grande partie motivées par, et ont accompagné, le développement du système de calcul formel Pari/Gp (§6, [T14]).

Dans la suite du texte, la lettre F désigne un corps de nombres, $\mathcal{O}_F$ son ordre maximal et $\mathrm{Cl}(F)$ son groupe des classes ; p est toujours un nombre premier.

2. Corps cubiques : tables, estimations asymptotiques

2.1. **Corps, anneaux et formes cubiques.** On appelle *anneau de degré n* un anneau commutatif, libre de rang n comme $\mathbb{Z}$-module. Un anneau intègre de degré n est appelé *ordre* ; son corps des fractions est un corps de nombres de degré n. Soit $\mathcal{O}_n$ l'ensemble des classes d'isomorphismes d'ordres de degré n. Pour un anneau commutatif A, on identifie $\mathrm{Sym}^n(A^k)$ à l'ensemble des polynômes homogènes

[1] [T1, T2, T3, T4] et une partie de [T5] correspondent à ma thèse de doctorat, et ne sont pas développées. [T8], quoique lié au §2, ne s'y inscrivait pas naturellement et ne sera plus mentionné : cet article, en collaboration avec Hersonsky et Paulin, explore des conséquences de leur théorie de l'approximation des géodésiques rationnelles sur une variété riemannienne M de courbure négative [36], et majore asymptotiquement le nombre $\mathcal{N}_e(X)$ de géodésiques rationnelles pour la pointe e, de profondeur bornée par X, en fonction de l'exposant de Poincaré du groupe fondamental de M. Dans les cas particuliers de $\mathcal{H}^2/\mathrm{PSL}(2,\mathbb{Z})$ et des orbifolds de Bianchi $\mathcal{H}^3/\mathrm{PSL}(2,\mathcal{O}_F)$, où F est quadratique imaginaire, on obtient un équivalent.

sur A, de degré n en k variables, à coefficients pondérés par les coefficients multinomiaux :

$$\mathrm{Sym}^n(A^k) := \left\{ \sum_{\substack{0\leqslant i_1\leqslant\cdots\leqslant i_k\\ i_1+\cdots+i_k=n}} \binom{n}{i_1,\ldots,i_k} a_{\underline{i}} x_1^{i_1}\ldots x_k^{i_k} : a_{\underline{i}} \in A \right\};$$

on définit aussi l'analogue plus naturel

$$\mathrm{Sym}^n(A^k)^* := \left\{ \sum_{\substack{0\leqslant i_1\leqslant\cdots\leqslant i_k\\ i_1+\cdots+i_k=n}} a_{\underline{i}} x_1^{i_1}\ldots x_k^{i_k} : a_{\underline{i}} \in A \right\}.$$

On note respectivement $\mathrm{Sym}^n_{irr}(A^k)$ et $\mathrm{Sym}^n_{irr}(A^k)^*$ les sous-ensembles constitués de polynômes irréductibles sur A. Le groupe $\mathrm{GL}(k,A)$ agit sur ces modules par changement de variable. On définit deux applications naturelles données par :

• le polynôme indice : $\mathcal{O}_n \to \mathrm{Sym}^{n(n-1)/2}(\mathbb{Q}^{n-1})^*/\mathrm{GL}(n-1,\mathbb{Z})$ qui associe à un ordre $\mathcal{O}$ de base $(1,\alpha_1,\ldots,\alpha_{n-1})$ le polynôme homogène

$$I_{\mathcal{O}}(x_1,\ldots,x_{n-1}) := \frac{i^{r_2}\det(\sigma(1),\sigma(X),\ldots,\sigma(X^{n-1}))}{\sqrt{|\mathrm{disc}\,\mathcal{O}|}},$$

où σ désigne le vecteur des plongements complexes de $K = \mathrm{Frac}(\mathcal{O})$ dans $\mathbb{C}^n$ étendu à $K[x_1,\ldots,x_{n-1}]$, r_2 est le nombre de places complexes, et X désigne la forme linéaire $\sum_{i=1}^{n-1}\alpha_i x_i$. La classe de $I_{\mathcal{O}}$ modulo $\mathrm{GL}(n-1,\mathbb{Z})$ ne dépend pas de la base choisie, pourvue que son premier élément soit 1 comme ci-dessus. Ses coefficients sont a priori rationnels, mais ses valeurs aux points entiers sont entières. De façon plus invariante (Zagier), $I_{\mathcal{O}}$ s'identifie à l'application de $\mathcal{O}/\mathbb{Z}$ dans $\Lambda^n\mathbb{C}^n = \mathbb{C}$ donnée par $X \mapsto \sigma(1)\wedge\sigma(X)\wedge\cdots\wedge\sigma(X^{n-1})$.

• l'ordre de Dedekind : $\mathrm{Sym}^n_{irr}(\mathbb{Z}^2)^* \to \mathcal{O}_n$ qui, au polynôme $F(x) = \sum_{i=0}^n a_i x^{n-i}y^i$ associe l'ordre

$$\mathcal{O}(F) := \left\langle 1, a_0x, a_0x^2+a_1x, \ldots, a_0x^{n-1}+\cdots+a_{n-2}x \right\rangle \subset K := \mathbb{Q}[x]/(f(x)),$$

où $f(x) := F(x,1)$. Là aussi de façon plus invariante, en notant M le sous $\mathbb{Z}$-module de K de rang n engendré par les classes de $\{1,x,\ldots,x^{n-1}\}$, on a

$$\mathcal{O}(F) = (M:M) := \{\alpha\in K : \alpha M\subset M\},$$

si F est de contenu 1, et $\mathcal{O}(\lambda F)/\mathbb{Z} = \lambda\cdot\mathcal{O}(F)/\mathbb{Z}$ pour tout $\lambda\in\mathbb{N}_{>0}$. La construction de l'ordre $(M:M)$ pour un $\mathbb{Z}$-module libre M est due à Dedekind et est à l'origine de sa définition des modules et des ordres. La classe d'isomorphisme de l'ordre $\mathcal{O}(F)$ dans $\mathcal{O}_n$ ne dépend que de l'orbite de F modulo $\mathrm{GL}(2,\mathbb{Z})$.

Ces deux applications sont compatibles si et seulement si $n=3$, auquel cas le miracle escompté se produit :

Théorème 2.1 (Delone-Faddeev [23])**.** *L'application de Dedekind induit une bijection*

$$\mathrm{Sym}^3_{irr}(\mathbb{Z}^2)^*/\mathrm{GL}(2,\mathbb{Z}) \simeq \mathcal{O}_3$$

dont l'inverse est induit par la forme indice. Ces applications conservent le discriminant.

La bijection s'étend aux orbites de $\mathrm{Sym}^3(\mathbb{Z}^2)^*$, sur les anneaux de degré 3, incluant les anneaux non intègres, voire non réduits comme $\mathbb{Z}[X]/(X^3)$. Un ordre est maximal[2] s'il est maximal en tout p. Localement, la caractérisation est immédiate :

Théorème 2.2 ([T9])**.** *Un ordre cubique $\mathcal{O}$ n'est pas maximal en p si et seulement si la forme associée f est divisible par p ou est équivalente à une forme (a, b, pc, p^2d).*

Preuve. Si p ne divise pas le discriminant, $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ est maximal. Si $p \mid f$, l'ordre n'est pas maximal puisqu'il est contenu dans l'ordre associé à f/p. Sinon, modulo $\mathrm{GL}(2, \mathbb{Z})$, on peut supposer que f modulo p n'a pas de racine à l'infini, une racine multiple en 0, et appliquer le critère de Dedekind [15, §6.1.2]. □

Ce résultat est en substance dû à Davenport et Heilbronn. J'ai suivi la formulation et la présentation de [T9], qui simplifie notablement la preuve originale[3]. Indépendamment, Bhargava a donné une preuve plus directe de ce résultat, qui reste valable pour les anneaux cubiques. Il a aussi généralisé ces constructions aux anneaux quartiques dans sa thèse [7], et aux anneaux quintiques plus récemment.

Soit U_p l'ensemble des formes cubiques dont l'ordre associé est maximal en p. La condition $f \in U_p$ se traduit par une congruence modulo p^2 (resp. 2^4) sur les coefficients de f pour p impair (resp. $p = 2$), bien sûr compatible à l'action de $\mathrm{GL}(2, \mathbb{Z})$. Par ailleurs, la réduction des formes cubiques binaires donne un domaine fondamental semi-algébrique explicite contenant une forme canonique (ou *réduite*) pour chaque orbite sous $\mathrm{GL}(2, \mathbb{Z})$.

Corollaire 2.3 (Davenport-Heilbronn [22])**.** *Les corps cubiques F de discriminant fixé, à isomorphisme près, sont en bijection avec les formes réduites de même discriminant, vérifiant la congruence adélique $f \in \cap_p U_p$.*

(Une forme réduite appartenant à $\cap U_p$ est irréductible.) La ramification de p dans le corps F se lit sur la décomposition de f modulo p. En particulier, le résultat suivant est fondamental pour le reste du chapitre :

Lemme 2.4 (Hasse [35])**.** *On note $\Delta = \mathrm{disc}(f) = \mathrm{disc}(F)$. Les conditions suivantes sont équivalentes :*

(1) *Δ est fondamental (i.e. $\mathrm{disc}(\mathbb{Q}(\sqrt{\Delta})) = \Delta$).*
(2) *Aucun nombre premier n'est totalement ramifié dans F.*
(3) *$F(\sqrt{\Delta})$ est une extension (cubique cyclique) non ramifiée de $\mathbb{Q}(\sqrt{\Delta})$.*

[2] On peut définir la maximalité intrinsèquement pour la relation d'inclusion, ou comme clôture intégrale, en liaison avec l'arithmétique du corps des fractions.

[3] Qui utilise la théorie du corps de classes (structure des conducteurs), la théorie des diviseurs inessentiels (du discriminant), et traite des cas particuliers désagréables en $p = 2$ ou 3 par des calculs explicites. Sa simplification dans [16, Chapitre 8] couvre encore une dizaine de pages.

Soit $k = \mathbb{Q}(\sqrt{\Delta})$, on note $r_p(\Delta)$ la dimension de $\mathrm{Cl}(k) \otimes_{\mathbb{Z}} \mathbb{F}_p$. Les extensions cubiques cycliques non ramifiées de k correspondent aux sous-groupes d'indice 3 de son groupe des classes. On en déduit :

Corollaire 2.5 (Davenport-Heilbronn [22]). *Pour chaque Δ discriminant fondamental, il existe exactement $(3^{r_3(\Delta)} - 1)/2$ formes cubiques réduites de discriminant Δ.*

Cette description très explicite peut maintenant fournir des tables (une approche initiée par Ennola et Turunen [26]), ou des estimations asymptotiques, comme dans l'article original de Davenport et Heilbronn, aussi bien pour les corps cubiques, que pour le 3-rang des corps quadratiques. C'était le cœur de mon travail de thèse. Je présente ici les résultats obtenus par la suite.

2.2. **Énumération exacte, tables.** Dans cette section, on désire produire les corps cubiques F, de discriminant inférieur à X en valeur absolue[4]. C'était le sujet de [T3, T4] ; j'ai amélioré ces algorithmes pour obtenir

Théorème 2.6 ([T9]). *Les équations canoniques des corps cubiques F vérifiant $|\mathrm{disc}(F)| \leqslant X$, peuvent être produites en temps $O(X)$, et espace $O(X^{3/4})$. Plus généralement en temps $O(X + X^{7/4}M^{-1})$ et espace $O(M + X^{1/2})$, où $M \geqslant 1$ est un paramètre libre.*

Les extensions cubiques cycliques non ramifiées des corps quadratiques de discriminant Δ, $|\Delta| \leqslant X$ sont obtenues avec la même complexité temporelle, mais une complexité spatiale réduite à $M + O(1)$.

Le cardinal des extensions produites est dans les deux cas de l'ordre de X, donc le problème est en $\Omega(X)$. L'algorithme de [T3] était de complexité $O(X^2/M)$ pour une complexité spatiale $O(M)$. Pour $X \approx 10^{12}$, le gain d'un facteur $X^{1/4} \approx 1000$ est appréciable. Le nouvel algorithme calcule les corps de discriminant appartenant à un intervalle de la forme $I_k = [kM, (k+1)M[$ fixé. Pour chaque forme réduite f, de discriminant dans I_k, on teste si $f \in \cap U_p$. Ce test s'effectue en calculant un conducteur potentiel (voir plus loin), puis en vérifiant si $f \in \cap_{p \geqslant 5} U_p$, les cas $p = 2, 3$ se traitant à part.

Mis à part la segmentation $[-X, X] \subset \cup I_k$, il s'agit encore de l'algorithme générique de [T3]. Le nouvel ingrédient est un test d'appartenance $f \in \cap U_p$ pour une forme f de discriminant D, essentiellement équivalent au calcul de $\mathrm{cond}(D)$, qui est par définition le conducteur de l'ordre quadratique de discriminant D. Plus précisément, on dit que D est *admissible* si D est sans facteur cubique, à des puissance de 2 et de 3 près.

Lemme 2.7 (Hasse [35]). *Soit F est un corps cubique et $D := \mathrm{disc}\, F$. Alors D est admissible. De plus, $p \mid \mathrm{cond}(D)$ si et seulement si p est totalement ramifié.*

[4]Pour éviter les détails liés à l'arithmétique multiprécision, les estimations de complexité comptent les opérations arithmétiques sur des entiers en $O(X^{3/2})$; donc, *en temps $O(f(X))$* se lit : avec une complexité binaire $O(f(X)(\log X)^2)$ dans le modèle RAM, pour une arithmétique classique. Le coût en espace indique le nombre d'entiers en $O(X)$ stockés simultanément.

Ceci résulte du fait que l'idéal engendré par $\mathrm{cond}(D)$ est le conducteur de l'extension cubique cyclique $F(\sqrt{D})/\mathbb{Q}(\sqrt{D})$, principe déjà mis en œuvre au Corollaire 2.5.

Lemme 2.8 ([T3]). *Si $f = ax^3 + bx^2 + cx + d \in U_2 \cap U_3$, de discriminant D. Alors $f \in \cap U_p$ si et seulement si D est admissible et* $\mathrm{cond}(D)$ *divise*

$$\mathrm{pgcd}(b^2 - 3ac, bc - 9ad, c^2 - 3bd). \tag{1}$$

La dernière condition est surprenante, mais essentiellement équivalente à ce que f soit un cube modulo p pour tout $p \mid \mathrm{cond}(D)$, et nous avons déjà vu que la factorisation de p dans $\mathcal{O}(F)$ se lit sur celle de f modulo p.

Pour tout $D \in I_k$, on précalcule $\mathrm{cond}(D)$ si D est admissible et on marque D sinon : un premier crible par les $p^3 \leqslant X$ ($p > 3$) élimine les $D \in I_k$ qui ne peuvent être admissibles, un deuxième par les $p^2 \leqslant X$ ($p \neq 2$) calcule leur conducteur, sous l'hypothèse que $p^3 \mid D$ implique $p = 2$ ou 3. À condition de disposer d'une table des nombres premiers inférieurs à $X^{1/2}$, on calcule tous les $\mathrm{cond}(D)$, $D \in I_k$, en temps linéaire $O(M)$, travail qui semblait nécessiter la factorisation des M éléments de l'intervalle. On peut maintenant tester $f \in \cap U_p$ pour $\mathrm{disc}\, f \in I_k$ en temps $O(1)$: il suffit de calculer $\mathrm{disc}\, f$, vérifier qu'il est admissible et obtenir son conducteur grâce à la table, et éventuellement tester la propriété de divisibilité (1). La segmentation $[-X, X] \subset \cup I_k$ maintient l'occupation mémoire dans des limites fixées à l'avance. La construction est parallélisable et cet algorithme est nettement plus efficace que [T3] pour $X > 10^{10}$. On obtient par exemple

Théorème 2.9 ([T9]). *Soit $\Delta_0 := -5393946914743 \approx -5.10^{12}$. Le corps $\mathbb{Q}(\sqrt{\Delta_0})$ est le corps quadratique de plus petit discriminant en valeur absolue, tel que $r_3(\Delta_0) = 5$.*

Le calcul était distribué sur une grappe du centre de calcul Medicis [50] ; rapporté à une unique machine à 1GHz, le temps de calcul serait de 65 jours[5].

2.3. **Compatibilité Davenport-Heilbronn / Scholz / Cohen-Lenstra.** En utilisant les bijections du §2.1, Davenport et Heilbronn [22] calculent la valeur moyenne du nombre de corps cubiques de discriminant donné, ainsi que celle de $3^{r_3(F)}$ quand F parcourt les corps quadratiques. Bhargava [7] a fait de même pour les corps quartiques, ainsi que pour $2^{r_3(F)}$ quand F parcourt les corps cubiques.

Ce type de résultats rentre respectivement dans le cadre de la conjecture de Malle [47], pour ce qui concerne les corps de degré n de type de clôture Galoisienne fixée, et des heuristiques de Cohen, Lenstra, Martinet [18, 19] pour ce qui concerne la structure des groupes de classes. Bien qu'étant l'une et l'autre totalement inaccessibles (la première implique par exemple une solution du problème de Galois inverse), elles fournissent des prédictions précises, pour l'instant compatibles avec tous les résultats connus ou conjecturés dans le domaine.

[5]Sous GRH, on calcule expérimentalement le groupe des classes de $\mathbb{Q}(\sqrt{D})$, pour $|D| \approx 5.10^{12}$ en environ 0.1s sur une machine à 1GHz. On peut donc estimer à plus de 10^6 jours la durée d'une vérification (conditionnelle) par le calcul direct des groupes de classes considérés.

Par exemple, au modèle de Cohen-Lenstra, on peut rajouter des heuristiques supplémentaires sur la répartition des éléments p-primaires [25, 42] et étudier la compatibilité de l'ensemble avec les théorèmes de réflexion. Ainsi, soit $\Delta > 0$ un discriminant fondamental, le théorème de Scholz [58] énonce que

$$\delta(\Delta) := r_3(\Delta) + 1 - r_3(-3\Delta) \in \{0, 1\}.$$

Dutarte [25] conjecture, pour $r \geqslant 0$, que

$$P(\delta(\Delta) = 0 \mid r_3(\Delta) = r) = 3^{-r-1},$$

où P est une « probabilité » de Cohen-Lenstra, définie par

$$P(A) := \lim_{X\to\infty} \frac{\sum_{0<\Delta<X} \mathbf{1}_A(\Delta)}{\sum_{0<\Delta<X} 1}$$

en supposant que la limite existe. Soit $q := 1/p$, l'une des conjectures de Cohen-Lenstra énonce

$$P(r_p(\Delta) = r) = \frac{q^{r(r+1)}(q)_\infty}{(q)_r(q)_{r+1}}, \quad \text{où} \quad (q)_n := \prod_{i=1}^{n}(1-q^i).$$

En utilisant la conjecture de Dutarte, et en oubliant que P n'est a priori que finiment additive, on en « déduit »

$$\begin{aligned}\sum_{\substack{\Delta<X\\ \delta(\Delta)=0}} 3^{r_3(\Delta)} \Big/ \sum_{\Delta<X} 1 \quad &\overset{?}{\longrightarrow} \quad \sum_{r\geqslant 0} q^{-r} P(\delta = 0 \mid r_3 = r) P(r_3 = r)\\ &\overset{?}{=} \quad \sum_{r\geqslant 0} q^{-r} \times q^{r+1} \times \frac{q^{r(r+1)}(q)_\infty}{(q)_r(q)_{r+1}}\\ &= \quad q\end{aligned}$$

En utilisant un des théorèmes de Davenport-Heilbronn

$$\sum_{\Delta<X} 3^{r_3(\Delta)} \Big/ \sum_{\Delta<X} 1 \to 4/3,$$

on en tire la conjecture que, pour la mesure pondérée par $3^{r_3(\Delta)}$, la probabilité d'avoir $\delta = 0$ serait de $3q/4 = 1/4$. Je démontre cette conjecture dans [T5][6].

2.4. **3-rang de $\mathbb{Q}(\sqrt{p})$.** Le résultat principal de [T6], obtenu en collaboration avec Fouvry, est une autre application des estimations asymptotiques issues de la théorie de Davenport-Heilbronn, couplées avec des estimations de crible :

Théorème 2.10 ([T6]). *Il existe une infinité de nombres premiers $p \equiv 1 \pmod 4$ tels que le groupe de classes de $\mathbb{Q}(\sqrt{p})$ ne possède aucun élément d'ordre 3. Le même résultat est vrai pour $p \equiv 3 \pmod 4$.*

[6]**Corrigendum** : dans l'énoncé du [T5, Théorème 1.2], remplacer 1/2 par 1/4.

D'après la théorie des genres, ces groupes de classes n'ont pas non plus de 2-torsion. Rappelons qu'on conjecture depuis Gauss l'existence d'une infinité de $\mathbb{Q}(\sqrt{p})$ *principaux*, et ce théorème est une timide avancée dans cette direction. Ce cas d'annulation simultanée de deux ℓ-rangs *fixés* pour une infinité de corps quadratiques est le seul connu. Paradoxalement, il est obtenu dans la seule configuration où l'on sait que leur densité est nulle (l'un des ℓ est 2). Au contraire, le modèle de Cohen-Lenstra implique l'indépendance des différents r_ℓ, et une densité positive des corps quadratiques vérifiant $r_\ell(\Delta) = k$, pour tout ℓ impair et $k \geqslant 0$. Cette conjecture n'est démontrée pour aucune paire (ℓ, k).

Donnons une idée de la démonstration[7], en commençant par un résultat de ma thèse :

Théorème 2.11 ([T2]). *Soit $\delta < 1/15$. Si q est sans facteurs carrés, on a*

$$\sum_{\substack{\Delta \leqslant X \\ q|\Delta}} \frac{3^{r_3(\Delta)} - 1}{2} = \frac{X}{12\zeta(2)} \prod_{p|q} \frac{1}{p+1} + R(X, q).$$

$$\text{où} \qquad \sum_{q \leqslant X^\delta} \mu^2(q)\, |R(X, q)| = o(X/\log X). \tag{2}$$

Ce résultat s'obtient naturellement en dénombrant des formes réduites f vérifiant les congruences issues du Corollaire 2.5, ainsi que $q \mid \mathrm{disc}(f)$. La condition $\delta < 1/15$ assure $R(X, q) = o(X)$ et donne un sens au terme d'erreur individuel $R(X, q)$; elle a pour *conséquence* l'équation (2). Le crible linéaire [38] fournit directement l'inégalité

$$\sum_{\substack{\Delta \leqslant X \\ p|\Delta \Rightarrow p > \sqrt{X}}} \frac{3^{r_3(\Delta)} - 1}{2} \leqslant \prod_{p \leqslant \sqrt{X}} \left(1 - \frac{1}{p+1}\right) \frac{X}{12\zeta(2)} (F(s) + o(1)) \sim \frac{X}{6\delta \log X}, \tag{3}$$

où $F(s) = 2e^\gamma/s$ pour $s \leqslant 2$ (γ est la constante d'Euler), et $s := \log X^\delta / \log \sqrt{X} = 2\delta \leqslant 2$. Comme $(3^{r_3(\Delta)} - 1)/2 \geqslant 1$ si $r_3(\Delta) > 0$, et 0 sinon, on obtient

$$\sum_{\substack{\Delta \leqslant X \\ p|\Delta \Rightarrow p > \sqrt{X}}} \frac{3^{r_3(\Delta)} - 1}{2} \geqslant \sum_{\substack{\Delta \leqslant X \\ p|\Delta \Rightarrow p > \sqrt{X}}} 1 - \sum_{\substack{\Delta \leqslant X \\ p|\Delta \Rightarrow p > \sqrt{X} \\ r_3(\Delta) = 0}} 1$$

Soit

$$\sum_{\substack{p \leqslant X \\ p \equiv 1 \pmod 4 \\ r_3(p) = 0}} 1 \geqslant (1 - 1/3\delta + o(1)) \sum_{\substack{p \leqslant X \\ p \equiv 1 \pmod 4}} 1 \tag{4}$$

[7] incorporant des simplifications ultérieures (non publiées).

Il suffirait donc de prouver que (2) demeure valide pour un $\delta > 1/3$. On doit procéder un peu différemment et utiliser, par rapport au Théorème 2.11 original, les idées nouvelles suivantes :

- traitement en moyenne des termes d'erreur suivant le principe
$$\sum_{q\leqslant Y} \sum_{\substack{f\in\text{Déchet}\\ q|\text{disc}(f)\\ 0<\text{disc}(f)\leqslant X}} 1 = \sum_{\substack{f\in\text{Déchet}\\ 0<\text{disc}(f)\leqslant X}} \sum_{q|\text{disc}(f)} 1 = O(\#\text{Déchet} \times X^{\varepsilon}),$$
qui permet de passer outre à une mauvaise uniformité en q dans l'estimation de la première somme intérieure.
- la condition « disc(f) est fondamental » du Corollaire 2.5 s'exprime par une coûteuse congruence adélique. Mais il suffit de cribler l'ensemble des formes réduites de discriminant inférieur à X : les formes de l'ensemble criblé sont de discriminant premier, congru à 1 (mod 4), donc automatiquement fondamental. (Elles sont aussi nécessairement irréductibles.) En substance, les estimations cruciales traitent des congruences modulo q et non plus modulo q^2, et un terme d'erreur lié à la somme
$$\sum_{p>Y} \sum_{\substack{f,\text{disc}(f)\leqslant X\\ p^2q|\text{disc}(f)}} 1$$
disparaît.
- meilleure estimation de la somme d'exponentielle associée à l'hypersurface singulière disc$(f) = 0 \pmod p$ (cas particulier explicite du théorème de stratification de Fouvry-Katz [30]).

Ces ingrédients sont tous trois nécessaires pour passer la barrière des 1/3 et permettent d'obtenir (4) pour tout $\delta < 3/8$. On obtient donc une densité de 1/9 pour cet ensemble de nombres premiers. Seul le dernier point permet d'améliorer, modestement, le domaine de validité du terme d'erreur individuel $R(X, q)$, de $q \leqslant X^{1/15-\varepsilon}$ à $q \leqslant X^{3/44-\varepsilon}$.

Il est rare de pouvoir compter des nombres premiers en utilisant uniquement un résultat de crible, en particulier à cause du phénomène de parité. Ici, le théorème des nombres premiers, à travers l'équivalent de $\pi(X; 1, 4)$, nous permet de passer outre.

3. Factorisation de polynômes sur un corps de nombres

Factoriser des polynômes univariés, en particulier sur un corps fini ou sur un corps de nombres, en général $\mathbb{Q}$, est une activité basique de tout système de calcul formel. Si on ignore toute considération de complexité, le problème est trivial : sur un corps fini le problème l'est tout autant, et la méthode d'interpolation de Kronecker ramène la factorisation dans $\mathbb{Z}[X]$ à la factorisation dans $\mathbb{Z}$, qui est un problème fini. Par ailleurs, la méthode de Kronecker ramène le cas multivarié au cas univarié, et la norme le cas d'un corps de nombres au cas rationnel.

Sur le terrain de la complexité, la situation est paradoxale : dit rapidement, les rares algorithmes dont on sait prouver qu'ils sont polynomiaux et déterministes sont impraticables. On ne connaît même pas de tel algorithme pour factoriser un polynôme quadratique $X^2 - a$ sur $\mathbb{F}_p$, à moins d'admettre GRH ou de supposer que a est petit. Pratiquement, sur un corps fini de caractéristique p, on utilise des algorithmes probabilistes bien compris et aux performances très satisfaisantes ; la partie non-déterministe se réduit au calcul des racines d'un polynôme *scindé* de $\mathbb{F}_p[X]$. Sur $\mathbb{Q}$ (et par extension, sur un corps de nombres), le problème théorique est résolu par Lenstra, Lenstra et Lovàsz [44]. Mais l'algorithme de loin le plus efficace en pratique, dû à van Hoeij [65], est de complexité polynomiale en la hauteur du polynôme P à factoriser, mais aussi hélas en le degré de son *corps de décomposition* (travail en cours de rédaction, en collaboration avec Jürgen Klüners), donc potentiellement exponentielle en le degré de P. J'ai étudié et généralisé cet algorithme dans [T10, T13], en spécifiant une variante qui règle efficacement les pathologies connues à ce jour de l'algorithme.

3.1. **L'algorithme de van Hoeij.** On cherche donc à factoriser en produit d'irréductibles un polynôme $P \in \mathbb{Q}[X]$, qu'on peut supposer sans facteurs carrés et à coefficient entiers. Toutes les méthodes modernes reposent sur la factorisation dans $\mathbb{Q}_p[X]$ pour un premier p bien choisi, en utilisant une borne sur la taille des diviseurs rationnels de P pour déterminer la précision p-adique nécessaire au calcul. Jusqu'en 2000, on connaissait essentiellement deux méthodes :

(A) l'algorithme de Berlekamp-Zassenhaus [6, 66], qui teste un par un les facteurs modulaires pour déterminer ceux qui sont rationnels. Il est de complexité exponentielle : on construit facilement des polynômes irréductibles ayant $\Omega(\deg(P))$ facteurs sur $\mathbb{Q}_p$ uniformément en p.

(B) l'algorithme en temps polynomial (en $\deg P$ et $\log\|P\|_2$) de Lenstra, Lenstra et Lovàsz [44] qui, en substance, cherche un polynôme minimal sur $\mathbb{Z}$ d'une racine de P dans $\mathbb{C}_p$, en utilisant leur fameux algorithme LLL de réduction d'un réseau.

Mais les polynômes sur $\mathbb{Z}$ de groupe de Galois S_n, donc irréductibles et restant irréductibles modulo une densité positive de nombres premiers, sont de densité 1 [64, 31]. Ainsi le comportement exponentiel de (A) est rare ; (B) est en moyenne nettement plus lent, et extrêmement coûteux en tout état de cause. Notons tout de même que la théorie de Galois effective, qui forme une classe importante d'applications, produit fréquemment cette pathologie exponentielle.

En 2000, van Hoeij [65] introduit un algorithme révolutionnaire, qui suit l'algorithme de Zassenhaus (A), mais utilise l'ingrédient LLL de (B) pour résoudre le problème combinatoire. L'idée essentielle est une linéarisation à l'aide de sommes de Newton : trouver une combinaison valide est ramené à une famille de problèmes de programmation linéaire, la minimisation simultanée de formes linéaires sur $\mathbb{Z}$ (problème dit du sac-à-dos). Ce dernier problème est NP-dur, mais LLL donne en temps polynomial des approximations garanties de ses solutions. En créant et résolvant approximativement une suite d'instances, on *espère* converger vers la factorisation cherchée.

Dans l'algorithme (B), la matrice de changement de base donnant les « petits » vecteurs de [44] fournit les coefficients des facteurs rationnels, qu'on doit borner par des estimations souvent colossales. Dans celui de de van Hoeij, elle est à valeurs dans $\{0, 1\}$; on peut ainsi détecter de petits vecteurs à très faible précision, comme petits vecteurs de réseaux approchés.

Comme annoncé plus haut, le théorème garantissant l'arrêt en un nombre effectif d'étapes ne fournit pas une borne polynomiale. Pourtant, on ne connaît aucun exemple mettant cet algorithme en difficulté, dans la spécification précise de [T10]. Nous conjecturons que son comportement est effectivement polynomial.

3.2. **Améliorations.** Mentionnons maintenant mes contributions au sujet. Étant donné leur relative technicité, je serai bref, renvoyant le lecteur à [T13, T10].

• Une première remarque est que l'on peut utiliser les sommes de Newton pour accélérer la recombinaison naïve initiale (sur un corps de nombres arbitraire), dans l'esprit de [1], mais bien plus efficacement, en particulier en mémoire.

• van Hoeij donne en fait une famille d'algorithmes dépendant de multiples paramètres (précision p-adique, choix des S_k, niveau de troncature). J'ai proposé et étudié deux variantes spécifiques. La première, en collaboration avec Hanrot et Zimmermann, plongeait le réseau L dans $L \otimes_{\mathbb{Z}} \mathbb{R}$ et non dans un espace de dimension fixe donnée par le nombre de facteurs modulaires initial (cette méthode s'est révélée instable en grande dimension, donc sans intérêt pratique). La deuxième itère les réductions sur des approximations du *même* réseau, jusqu'à épuisement de la précision p-adique, et n'a pas de pathologie connue.

• J'ai adapté la méthode à la factorisation sur un corps de nombres F, en améliorant les algorithmes de Lenstra [43] et Roblot [56], en particulier quand le degré $[F : \mathbb{Q}]$ est grand. Par exemple, les calculs sont fait dans un ordre a priori non maximal, on supprime le goulot d'étranglement constitué par la réduction de $\mathfrak{p}^a$ (utilisant une idée apparue indépendamment dans [28], la réduction LLL partielle de Montgomery, et la technique de Lehmer-Schnorr pour les réductions LLL en virgule flottante), on démontre de meilleures bornes pour la précision a, et on adapte le sac-à-dos de van Hoeij qui élimine la pathologie exponentielle. La difficulté essentielle est la reconstruction d'un nombre algébrique à partir d'une unique approximation p-adique : à moins que p soit inerte (un tel p n'a aucune raison d'exister ; le cas échéant, ce choix rend coûteuse la factorisation sur $\mathcal{O}_F/\mathfrak{p}$), on n'a plus de relèvement canonique du corps local au corps de nombres. On démontre en particulier le

Théorème 3.1 ([T10])**.** *Soit $\mathfrak{p}$ une place finie du corps de nombres F de degré $d = [F : \mathbb{Q}]$. Soit $C > 0$ and $x \in \mathcal{O}_F$ tel que $q(x) < C$, où $(\mathcal{O}_F, q)$ est un réseau de $F \otimes_{\mathbb{Q}} \mathbb{R}$. Soit finalement (b_i) une base LLL-réduite de $\mathfrak{p}^a$, et $y \in \mathcal{O}_F$ un représentant de la classe $x + \mathfrak{p}^a$. Alors on peut reconstruire x à partir de y, pourvu que*

$$N\mathfrak{p}^a \geqslant \left(2\sqrt{C/d} \cdot (3/\sqrt{2})^{d-1}\right)^d.$$

Quand $d = 1$, on obtient le reste symetrique modulo $\mathfrak{p}^a \subset \mathbb{Z}$; en genéral,

$$x := y - P \left\lceil P^{-1} y \right\rfloor ,$$

où P est la matrice de la base (b_i) de $\mathfrak{p}^a$, en fonction d'une base arbitraire, dans laquelle est aussi exprimé le représentant y de la classe.

Ce résultat est un cas particulier d'un résultat général remplaçant $\mathfrak{p}^a \subset F \otimes_{\mathbb{Q}} \mathbb{R}$ par un sous-réseau $\Lambda \subset \mathbb{R}^d$, faisant intervenir une minoration du plus court vecteur non nul de Λ. Il améliore une estimation d'Arjen Lenstra [43]. Il est crucial pour l'algorithme de sac-à-dos que le relèvement optimal soit donné par une *formule*. Pohst [52] a proposé de déterminer des petits représentants dans toute classe de congruence par énumération dans un ellipsoïde, garantissant l'unicité du relèvement à précision moindre. Cet algorithme ne permet pas d'adapter la méthode de van Hoeij.

• [*Travaux en cours de rédaction*] Avec Jürgen Klüners, nous avons donné une borne effective pour le temps de terminaison de l'algorithme (van Hoeij en donnait une preuve non-effective). Puis, avec Klüners, Mark van Hoeij, et Allan Steel, nous avons introduit une nouvelle variante, formulée sur un corps global K arbitraire (corps de nombres ou corps de fonctions d'une variable), tout aussi efficace en pratique, mais dont on sait maintenant prouver qu'elle termine en temps polynomial.

3.3. **Deux exemples.** En conclusion, les collections de polynômes inaccessibles constituées avant 2000, comme [68], sont devenues essentiellement triviales grâce à l'algorithme de van Hoeij. Finissons par deux exemples concrets : notons SD_n le polynôme minimal de $\sqrt{p_1} + \cdots + \sqrt{p_n}$ où les p_i sont les nombres premiers consécutifs. Il est irréductible de degré 2^n, avec 2^n ou 2^{n-1} facteurs sur $\mathbb{Q}_p$, suivant que p est un carré modulo tous les p_i ou non.

Mon implantation générique prouve l'irréductibilité de SD_{10} (au mieux 512 facteurs modulaires) en environ 8 heures sur une machine à 1GHz. C'est à peu près le temps nécessaire à la factorisation de $P := (SD_7 \times SD_8)(X + Y)$ sur un corps de nombres $F = \mathbb{Q}[Y]/(T)$ de degré 50. Outre le fait que P a au moins 192 facteurs modulaires (pour deux facteurs sur F si T est générique), les ≈ 19000 coefficients d'un relèvement de P dans $\mathbb{Z}[X, Y]$ ont chacun de l'ordre de 300 chiffres décimaux.

4. Arithmétique de $\mathcal{O}_F$ et corps de classes

4.1. **Présentation.** La théorie du corps de classes décrit le groupe de Galois $\mathrm{Gal}(F^{ab}, F)$ de l'extension abélienne maximale F^{ab} de F. En particulier, les extensions abéliennes finies de F sont associées aux sous-groupes ouverts du groupe des classes d'idèles C_F. Le problème du corps de classes effectif est de construire l'extension associée à un tel sous-groupe, en en donnant un élément primitif sur F.

Sacrifiant l'universalité pour la facilité de traitement résultant de la finitude des objets, on aborde le problème sous la forme équivalente suivante, à la Hasse :

étant donné un diviseur $\mathfrak{f}$, et un sous-groupe de congruence $H \subset \mathrm{Cl}_{\mathfrak{f}}(F)$, on désire construire le corps de classes associé au module $(\mathfrak{f}, H)$, c'est-à-dire la sous-extension du corps de classes de rayon $\mathfrak{f}$ de F fixée par H.

Une fois admis les grands théorèmes d'existence, la mise en œuvre effective repose sur des ingrédients élémentaires : arithmétique de F et de son groupe d'idéaux fractionnaires en évitant l'explosion des coefficients, algèbre linéaire. J'ai dressé un inventaire [T12] dans l'esprit de Cohen [15, 16], des techniques nécessaires à la réalisation effective de ce programme, en particulier l'algorithmique des groupes de classes de rayon (Cohen *et al.* [17, 21]) et le calcul des corps de classes proprement dit par théorie de Kummer (Fieker [27], Cohen [16, Chapitre V]). Ma motivation initiale portait sur la suppression des phénomènes d'explosion des coefficients et d'instabilité numérique, peut-être surprenants dans un tel contexte, mais qui surgissent dès que l'on traite naïvement un exemple non trivial. Par rapport aux algorithmes classiques, la vingtaine d'algorithmes de [T12] rendent possibles le traitement de corps de grand degrés. J'en décrirai un, lié au théorème d'approximation, ainsi que la représentation des éléments de F utilisée dans la plupart de ces algorithmes.

Prendre pour but le calcul de corps de classes permet de supposer connu l'ordre maximal[8] et de se dispenser des arguments de localisation partielle liés au calcul dans des ordres non maximaux : calculer les corps de classes d'une base dont on ignore le discriminant est actuellement utopique. De même, on suppose que la partie finie du module $\mathfrak{f}$ est complètement factorisée et que le problème du logarithme discret dans $(\mathcal{O}_F/\mathfrak{f})^*$ est soluble, c'est-à-dire qu'il est soluble dans les corps résiduels associés aux places finies du support de $\mathfrak{f}$.

4.2. **Calculs** $\mathrm{mod}^*\mathfrak{f}$**.** J'illustrerai le problème de l'explosion des coefficients avec le calcul du corps de classes de Hilbert de $F = \mathbb{Q}(\sqrt{181433})$, qui est le corps de décomposition sur F de l'innocent polynôme

$$X^5 - X^4 - 77X^3 - 71X^2 + 360X - 169.$$

Les calculs s'effectuent dans l'extension cyclotomique $F(\zeta_5) =: \mathbb{Q}(\omega)$, dont le groupe des classes est $\mathbb{Z}/(3620)g_1 \oplus \mathbb{Z}/(20)g_2$, sous GRH[9]. Utiliser naïvement les algorithmes de la littérature (spécifiquement, [16, Chapitre V]) nécessite des calculs flottants à 10^5 décimales de précision relative. Ceci provient par exemple du calcul et de l'utilisation d'un générateur de l'idéal principal g_1^{3620} à partir de ses plongements, sous forme de polynôme en ω (dont on imagine la hauteur).

Suivant Buchmann, l'algorithme LLL permet une pseudo-réduction[10] dans le groupe des idéaux fractionnaires, en écrivant un idéal $\mathfrak{a}$ sous forme $\alpha(\mathfrak{a}/\alpha)$, où

[8]Si F est le corps de rupture d'un polynôme P, l'obtention de $\mathcal{O}_F$ est au moins aussi difficile que la factorisation partielle de $\mathrm{disc}(P)$ sous la forme $\mathrm{disc}(F)f^2$, qui contient une dangereuse invocation de la factorisation sur $\mathbb{Z}$.

[9]Ce qui n'a aucune importance ici : si les calculs intermédiaires sont conditionnels, il est facile de vérifier que le résultat final est correct.

[10]En fait une famille de pseudo-réductions, en fonction de la constante de Lovász et de l'ordre de troncation choisis, *cf.* [T12, §2.2.3].

$\alpha \in \mathfrak{a}$ est un élément de petite hauteur découvert par LLL dans l'image de $\mathfrak{a}$ dans $F \otimes_{\mathbb{Q}} \mathbb{R}$ par le plongement de Minkowski ([13, 20]) ; suivant les applications, on pourra trouver avantage à écrire plutôt $\mathfrak{a} = \alpha(\alpha/\mathfrak{a})^{-1}$, où $\alpha/\mathfrak{a}$ est entier. L'algorithme d'exponentiation binaire, ou ses raffinements utilisant la théorie des chaînes d'additions, transforme donc un produit d'idéaux quelconque en produit formel d'éléments du corps de base, qu'on se garde bien d'évaluer, multiplié par un idéal de petite norme[11]. Un produit formel d'éléments de F est toujours appliqué sur un domaine raisonnable comme $F \otimes_{\mathbb{Q}} \mathbb{R}$, $(\mathcal{O}_F/\mathfrak{f})^*$ ou $F^*/(F^*)^\ell$, avant évaluation, en résolvant au besoin quelques problèmes techniques de coprimalité à $\mathfrak{f}$. La dernière possibilité $F^*/(F^*)^\ell$ est introduite par la théorie de Kummer ou le problème de la racine carrée dans la dernière phase du crible algébrique (NFS, $\ell = 2$) et permet aussi des simplifications massives avant l'évaluation finale, bien que le module sous-jacent ne soit plus de type fini. Par rapport aux représentations évaluées, cette représentation formelle élimine aussi l'instabilité numérique, puisque dans les rares cas où l'on passe d'une arithmétique exacte à une arithmétique approchée, on calcule puis *multiplie* les plongements d'éléments de petite hauteur.

Adopter systématiquement ce type de représentations formelle se fait sans perte d'efficacité[12], et élimine toute explosion des coefficients, plus simplement et plus efficacement qu'avec les techniques suggérées dans la littérature, comme [16, §4.3.2]. Sous cette forme, le calcul d'un élément primitif du corps de classes de Hilbert ci-dessus est mené à bien en une poignée de secondes, temps de calcul largement dominé par les deux ou trois minutes nécessaires au calcul conditionnel de $\mathrm{Cl}(F(\zeta_5))$ et à la réduction de l'élément primitif initial sous la forme utilisable citée plus haut, via l'inévitable LLL.

Contrairement à l'estimation pessimiste de [16, p.288 (4)], ce type d'idée permet l'utilisation des résolvantes de Lagrange pour obtenir les corps de classes de F comme sous-corps de ceux de $F(\zeta_\ell)$, y compris quand ℓ est « grand ». Par exemple, il suffit d'une vingtaine de minutes pour calculer ainsi un élément primitif de l'extension de $\mathbb{Q}(\sqrt{17})$ de conducteur 311 et de degré $\ell = 13$.

4.3. **Approximation.** Les questions de coprimalité, et plus généralement d'approximation ont aussi leur importance, en particulier parce qu'elles sous-tendent la réduction d'un idéal $\mathfrak{a}$ comme $\mathcal{O}_F$-module sur *deux* générateurs, et donc la multiplication efficace des idéaux. Je me restreins ici au cas des idéaux premiers au dessus d'un premier p, voir [T12] pour le cas général. Le corps F s'identifie à $\mathbb{Q}[X]/(P)$, pour un polynôme unitaire $P \in \mathbb{Z}[X]$. Si le critère de Kummer s'applique, c'est-à-dire si l'image de $\mathbb{Z}[X]$ est maximale en p, ou encore

[11] Rigoureusement bornée à l'aide de la borne de Minkowski, de la différence entre hauteur et norme (moyenne arithmético-géométrique), et de la borne théorique entre la taille du plus court vecteur non nul et le premier vecteur d'une base LLL réduite, en $O(1)^{\text{dimension}}$.

[12] La seule opération rendue potentiellement plus coûteuse est le test d'égalité, qui n'est jamais utilisé. On obtient un test probabiliste d'*inégalité*, lui aussi inutile mais néanmoins efficace, par calcul modulo quelques nombres premiers.

$p \nmid [\mathcal{O}_F : \mathbb{Z}[X]/(P)]$, les diviseurs premiers $\mathfrak{p}$ de p s'écrivent $(p, P_i(X))$, où P_i est un relèvement arbitraire d'un facteur irréductible de P sur $\mathbb{F}_p[X]$. Sinon, l'algorithme de Berlekamp décompose l'algèbre étale

$$\mathcal{O}_F/I_p = \bigoplus_{\mathfrak{p}_i|p} \mathcal{O}_F/\mathfrak{p}_i$$

(algorithme de Buchmann-Lenstra), où $I_p = \cap_{\mathfrak{p}|p}\mathfrak{p}$. Pratiquement, $I_p \otimes_{\mathbb{Z}} \mathbb{Z}/(p)$ est le radical de la $\mathbb{F}_p$-algèbre $\mathcal{O}_F/(p)$, et se calcule par exemple comme noyau d'une puissance convenable du Frobenius. On obtient les $\mathfrak{p}_i/I_p$ comme $\mathbb{F}_p$-sous-espaces vectoriels de $\mathcal{O}_F/I_p$, donc comme sous $\mathbb{Z}$-modules de $\mathcal{O}_F$ engendrés par I_p et des relèvements de $\mathfrak{p}_i/I_p$. Reste à obtenir des uniformisantes π_i telles que $\mathfrak{p}_i = p\mathcal{O}_F + \pi_i\mathcal{O}_F$.

Notons $n := [F : \mathbb{Q}]$. L'algorithme standard [15, 4.7.10] choisit uniformément au hasard un élément de $\mathfrak{p}_i$ modulo p, qui est une uniformisante avec probabilité $\prod_i(1 - 1/N\mathfrak{p}_i)$. Dans le cas le pire, p est totalement décomposé et l'expression se réduit à $(1 - 1/p)^n$; si $p \ll n$, la probabilité de succès est exponentiellement faible. De plus, si $p < n$ est effectivement totalement décomposé dans F, alors on est nécesairement dans le mauvais cas où p divise l'indice. Pour prendre un cas concret, dans le corps fixe de $\mathbb{Q}(\zeta_{341})$ par le Frobenius en 2, qui est de degré 30 sur $\mathbb{Q}$, cette probabilité est donc de 2^{-30} pour chacun des 30 diviseurs premiers de 2. Le calcul d'une *unique* uniformisante requiert plusieurs jours par cette méthode.

L'algorithme déterministe [16, 1.3.10] utilisant le théorème d'approximation est censé régler ces cas problématiques. En pratique il requiert plusieurs multiplications d'idéaux (représentés par n $\mathbb{Z}$-générateurs) et un changement de base réalisant la forme normale d'une matrice de rang ng, avec $g := \#\{\mathfrak{p}_i \mid p\}$. Sur notre exemple, l'algèbre linéaire sur $\mathbb{Z}$ en dimension $30^2 = 900$ a un coût non négligeable et requiert plusieurs heures.

Dans la suite, $\mathfrak{a}$ et $\mathfrak{b}$ désignent deux idéaux entiers, premiers entre eux. J'ai proposé un algorithme déterministe élémentaire, fondé sur

- l'identité $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$, qui permet de calculer $V_i := \prod_{j\neq i} \mathfrak{p}_j$ sans multiplication, comme relèvement de l'intersection des $\mathbb{F}_p$-espace vectoriels $\mathfrak{p}_j \otimes_{\mathbb{Z}} \mathbb{F}_p$. Le calcul s'amortit sur l'ensemble des uniformisantes : obtenir l'ensemble des V_i nécessite $3g - 4$ intersections, et non $g(g - 1)$.
- l'identité de Bezout : si $\mathfrak{a} + \mathfrak{b} = \mathcal{O}_F$, l'algorithme d'Euclide (convenablement) étendu fournit $a \in \mathfrak{a}$, $b \in \mathfrak{b}$ tels que $a + b = 1$.

Il suffit d'appliquer l'identité de Bezout à $\mathfrak{a} = \mathfrak{p}_i$ et $\mathfrak{b} = V_i$ si $\mathfrak{p}_i/p$ est non ramifié : au moins l'un de $\pi_i = a$ ou $a+p$ convient. Une application du Lemme Chinois règle le cas général en essayant au plus n candidats de la forme $\pi := b\tau+a$, où τ parcourt les relèvements des générateurs de $\mathfrak{p}_i \otimes_{\mathbb{Z}} \mathbb{F}_p$. En effet π est une uniformisante si et seulement si $\tau \in \mathfrak{p}_i - \mathfrak{p}_i^2$, ce que l'un au moins des générateurs vérifie. Une implantation convenable garantit l'absence d'explosion des coefficients, et calcule par ailleurs les 30 uniformisantes de notre exemple en une demi-seconde.

Des idées analogues fournissent des versions algorithmiquement efficaces du théorème d'approximation forte sur $\mathcal{O}_F$, donc du Lemme Chinois, ainsi que la représentation d'un idéal arbitraire comme pgcd de deux idéaux principaux, et finalement la construction d'un idéal premier à $\mathfrak{f}$ dans toute classe d'idéaux.

5. K-théorie effective

Les travaux décrits dans cette section ont été menés en collaboration avec Herbert Gangl (MPIM Bonn). On note par un accent $\widehat{x}$ une quantité algorithmique, sans définition intrinsèque et déterminée expérimentalement, qui approche une quantité x rigoureusement définie.

5.1. **Motivations.** Pour un corps de nombres F, soit ζ_F la fonction zêta de Dedekind ; pour $x \in \mathbb{C}$ on définit

$$\zeta_F^*(x) := \lim_{s \to x} \frac{\zeta_F(s)}{(s-x)^{\mathrm{ord}_x\, \zeta_F}}$$

le premier coefficient non nul du développement de ζ_F au voisinage de x. Les conjectures de Lichtenbaum-Quillen [45] et Zagier relient la K-théorie de $\mathcal{O}_F$ à la cohomologie (étale) de Spec $\mathcal{O}_F$, et aux valeurs de la fonction ζ_F^* aux points entiers, généralisant la formule classique de Dirichlet

$$\zeta_F^*(0) = -\frac{\#(K_0\mathcal{O}_F)_{tor} \cdot R(K_1\mathcal{O}_F)}{\#(K_1\mathcal{O}_F)_{tor}}, \tag{5}$$

où $K_0\mathcal{O}_F = \mathbb{Z} \oplus \mathrm{Cl}(\mathcal{O}_F)$ (Steinitz), $K_1\mathcal{O}_F = \mathcal{O}_F^*$ (Bass, Milnor, Serre [4, 4.3]) et $R(\cdot)$ est l'application régulateur usuelle. Pour $n \geqslant 0$, les valeurs de $\zeta_F^*(-n)$, ou de façon équivalente par équation fonctionnelle les valeurs de $\zeta_F^*(1+n)$, seraient ainsi liées aux groupes $K_{2n}\mathcal{O}_F$ et $K_{2n+1}\mathcal{O}_F$. Par exemple, Borel [10] montre que

$$\mathrm{ord}_{-n}\, \zeta_F = \dim_{\mathbb{Q}}(K_{2n+1}\mathcal{O}_F) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

La version cohomologique de ces conjectures est démontrée pour $F/\mathbb{Q}$ abélien, à une puissance de 2 non-spécifiée près (Kolster, Nguyen-Quang-Do & Fleckinger [41], Huber & Kings [37], Burns & Greither [14]). Pour le cas particulier F abélien *réel* et $n = 1$ (conjecture de Birch-Tate), alors $K_3\mathcal{O}_F = 0$ et on obtient une égalité exacte, sans puissance de 2 parasite, qui suit de la « Conjecture Principale » d'Iwasawa (Mazur & Wiles [49], Kolster [57]) :

$$\zeta_F^*(-1) = (-1)^{r_1} \frac{\#K_2\mathcal{O}_F}{w_2(F)},$$

où r_1 est le nombre de places réelles de F et $w_k(F)$ désigne le plus grand entier n tel que $\mathrm{Gal}(F(\zeta_n)/F)$ soit d'exposant k. (Donc $w_1(F) = \#(K_1\mathcal{O}_F)_{tor}$ est le nombre de racines de l'unité de F.)

Si F n'est pas abélien la conjecture reste ouverte. D'où l'intérêt de pouvoir faire des expérimentations numériques. Le résultat principal de [T11], en collaboration avec Herbert Gangl, est un algorithme de calcul inconditionnel de $K_2\mathcal{O}_F$, et une description de son implantation. Une première version, limitée aux corps

quadratiques imaginaires, avait été annoncée dans [T7]. L'algorithme est de complexité exponentielle en $\log|\mathrm{disc}(F)|$, et ne peut traiter que quelques dizaines de milliers de corps. À comparer cependant à Tate [62], Skałba [60], Qin [54, 55], Browkin [11] qui traitent à eux tous une quinzaine d'exemples, tous quadratiques imaginaires. On démontre ainsi des résultats du type suivant :

Théorème 5.1 ([T11]). *Soit F le corps de nombres $\mathbb{Q}[X]/(X^5-X^3-X^2+X+1)$, alors $K_2\mathcal{O}_F = (\mathbb{Z}/2\mathbb{Z})\{-1,-1\}$.*

(Le corps F n'est ni galoisien, ni totalement réel.)

Théorème 5.2 ([T11]). *Soit $F = \mathbb{Q}(\sqrt{-303})$, et $\omega := (1+\sqrt{-303})/2$, alors $K_2\mathcal{O}_F = (\mathbb{Z}/22\mathbb{Z})\{-17-3\omega, -37+\omega\}^5$.*

Théorème 5.3 ([T11]). *Soit $F = \mathbb{Q}(\sqrt{-4547})$, et soit $\omega := (1+\sqrt{-4547})/2$, alors $K_2\mathcal{O}_F$ est engendré par $\{5, 49+2\omega\}$, qui est tué par 233.*

(233 est premier, nous conjecturons que $K_2\mathcal{O}_F$ est bien d'ordre 233, sans espoir de le démontrer par nos méthodes : la certification naïve requiert le calcul du groupe des classes de l'extension cyclotomique $F(\zeta_{233})$.) Une restriction cependant : ces théorèmes sont produits par démonstration automatique, dont la transcription sur papier serait déraisonnable. Le programme ne fournit pas de certificat facilement vérifiable, rejoignant d'ailleurs en cela les algorithmes connus de calcul de $K_0\mathcal{O}_F$ et $K_1\mathcal{O}_F$.

5.2. **Calcul d'indice.** Pour donner une idée de la méthode, je décrirai d'abord l'algorithme générique de calcul d'indice, inspiré par les méthodes modernes de factorisation [15, Chapitre X], puis une variante très simplifiée de l'extension au calcul de $K_0\mathcal{O}_F$ et $K_1\mathcal{O}_F$ (due à Hafner et Mc Curley [34], puis Buchmann [13]), et enfin au §5.3, le principe de notre généralisation.

Pour calculer un groupe abélien *fini* M par générateurs et relations, on utilise quatre ingrédients :

- Un $\mathbb{Z}$-module libre A_0 dont M est un quotient
$$0 \longrightarrow \Lambda_0 \longrightarrow A_0 \longrightarrow M \longrightarrow 0$$
(le noyau Λ_0 est inconnu).
- Un sous-groupe de type *fini* $A \subset A_0$, muni d'une base explicite $\mathcal{B}$ (base de factorisation), dont M reste un quotient :
$$0 \longrightarrow \Lambda = \Lambda_0 \cap A \longrightarrow A = \mathbb{Z}^{\mathcal{B}} \longrightarrow M \longrightarrow 0$$
(le noyau Λ est inconnu).
- Un moyen de produire des éléments « bien répartis » dans Λ_0, et de les plonger dans $\mathbb{Z}^{\mathcal{B}}$ s'ils appartiennent à Λ (factorisation des éléments friables).
- Une évaluation grossière H de $h := \#M = [A : \Lambda]$, telle que $H < 2h$.

L'algorithme probabiliste suivant détermine alors Λ : produire des éléments de Λ, engendrant un sous groupe $\widehat{\Lambda} \subset \Lambda$, jusqu'à ce que

$$\widehat{h} := [A : \widehat{\Lambda}] \leqslant H, \tag{6}$$

ce qui entraîne $\widehat{h} = h$ puisque $\widehat{h}$ est un multiple entier de h, et donc $\widehat{\Lambda} = \Lambda$. On en déduit la structure de

$$M = \oplus(\mathbb{Z}/d_i\mathbb{Z})g_i, \quad d_1 \mid d_2 \mid \ldots, \quad g_i \in A$$

par réduction de Smith de Λ. La solution du logarithme discret dans A, c'est-à-dire l'écriture d'un élément de M comme produit des g_i et d'un élément de Λ, est une généralisation simple.

Pour calculer $K_0\mathcal{O}_F$ et $K_1\mathcal{O}_F$ en un temps raisonnable (sous-exponentiel en $\log|\mathrm{disc}(F)|$), on admet l'hypothèse de Riemann généralisée[13]. On étend l'idée précédente, en calculant simultanément $\widehat{\Lambda}$ comme ci-dessus, et un sous-groupe $\widehat{U}$ de $U := \mathcal{O}_F^*$: on désire calculer $M := \mathrm{Cl}(F)$,

- on choisit $A_0 := I(F)$, le groupe des idéaux fractionnaires non nuls de F,
- $\mathcal{B}$ est l'ensemble des idéaux premiers de norme inférieure à la borne de Bach [2] ; $\mathcal{B}$ engendre $\mathrm{Cl}(F)$ sous GRH.
- on produit des élément de Λ en factorisant des éléments α de petite norme dans $\mathcal{O}_F$ (par divisions successives par les idéaux de $\mathcal{B}$),
- finalement (5) donne une approximation numérique du produit hR. On calcule en pratique un produit Eulérien tronqué convergeant vers le résidu en $s = 1$. On utilise de nouveau GRH pour garantir l'approximation [3].

Les dépendances entre éléments de $\widehat{\Lambda}$, découvertes au moment du calcul de $[A : \widehat{\Lambda}]$, correspondent à une identité entre idéaux principaux $(\alpha) = (\alpha')$ dans $I(F)$, et donc à des unités $u := \alpha/\alpha' \in U$; ces éléments u engendrent un sous-groupe $\widehat{U}$ de U. Soit $\widehat{R}$ le régulateur de $\widehat{U}$, qui est un multiple entier du régulateur R ; tout comme ci-dessus, lorsque $hR < 2\widehat{h}\widehat{R}$, alors $U = \widehat{U}$ et $\Lambda = \widehat{\Lambda}$, d'où on tire $\mathrm{Cl}(F)$.

5.3. $K_2\mathcal{O}_F$**.** Cette méthode se transpose partiellement à $K_2\mathcal{O}_F$ et $K_3\mathcal{O}_F$: le théorème de Matsumoto [48] calcule

$$K_2F = F^* \otimes_{\mathbb{Z}} F^* / \{x \otimes (1-x)\},$$

et la suite de localisation identifie $K_2\mathcal{O}_F$ avec le noyau modéré de F :

$$K_2\mathcal{O}_F = \mathrm{Ker}\left(\oplus\, \partial_v : K_2F \to \oplus_v k(v)^*\right),$$

où v parcourt les places finies de F, $k(v)$ est le corps résiduel associé, et

$$\partial_v(\{a,b\}) := (-1)^{v(a)v(b)} a^{v(b)}/b^{v(a)}$$

est le symbole modéré.

Pour un ensemble de places S, on note $U_{F,S}$ l'anneau des S-unités de F et $K_2^S F$ le sous-groupe de K_2F engendré par les symboles de support $U_{F,S}$, c'est-à-dire

[13]Même sous ces hypothèses, la complexité sous-exponentielle des algorithmes reste heuristique, et n'est pas réalisée dans la variante simplifiée ci-dessous.

l'image de $U_{F,S} \otimes_{\mathbb{Z}} U_{F,S}$ dans K_2F par la projection canonique. Comme $K_2\mathcal{O}_F$ est fini (Garland [32]), $K_2\mathcal{O}_F \subset K_2^S F$ pour S assez grand, cette dernière borne étant effective (Bass & Tate [5], Groenewegen [33]). Pour un tel S, on peut alors poser $A_0 := F^* \otimes_{\mathbb{Z}} F^*$, $A := U_{F,S} \otimes_{\mathbb{Z}} U_{F,S}$, produire des relations en factorisant des tenseurs de Steinberg $x \otimes (1-x)$ dans A et tenter de déterminer l'image $K_2^S F$ de A dans K_2F, d'où on déduit $K_2\mathcal{O}_F$ avec un peu d'algèbre linéaire (c'est le noyau de $\mathrm{Ker} \oplus_{v \in S} \partial_v$ sur $K_2^S F$).

On se heurte au problème suivant : l'analogue de (5) correspond aux variantes de la conjecture de Lichtenbaum que l'on cherche à vérifier, et n'est donc disponible que lorsque F est abélien réel. Dans le cas général, on obtient seulement un groupe explicite $\widehat{K_2\mathcal{O}_F}$ dont $K_2\mathcal{O}_F$ est à priori un quotient, avec forte présomption d'égalité mais sans critère d'arrêt rigoureux. Mis à part le cas, trivial mais très fréquent, où le noyau sauvage WK_2F est nul[14], on peut souvent conclure en calculant directement le p-Sylow de $K_2\mathcal{O}_F$ pour tout p divisant $\#\widehat{K_2\mathcal{O}_F}$. On utilise pour ce faire des résultats de Tate [63] et Keune [40], sous la forme suivante : si p est un premier impair, et $r \geqslant 1$ un entier tel que p^r tue les p-Sylow de $\widehat{K_2\mathcal{O}_F}$ et des racines de l'unité locales $\mu(F_{\mathfrak{p}})$ pour tout $\mathfrak{p} \mid p$, alors

$$(\mu_{p^r} \otimes_{\mathbb{Z}} \mathrm{Cl}(\mathcal{O}_{E,p}))_{\Gamma} \simeq WK_2F \otimes_{\mathbb{Z}} \mathbb{Z}_p$$

où E est l'extension cyclotomique $F(\zeta_{p^r})$, et $\Gamma = \mathrm{Gal}(E/F)$. On peut adapter ce résultat pour $p = 2$, mais la difficulté principale vient du calcul de $\mathrm{Cl}(E)$, impraticable si p^r est grand. Si p est lui-même petit, une suite exacte analogue permet de calculer le p-rang de $K_2\mathcal{O}_F$ étant donné une présentation de $\mathrm{Cl}(F(\zeta_p))$. Ceci montre qu'il manque des relations, ou prouve la non-trivialité des générateurs de $\widehat{K_2\mathcal{O}_F} \otimes_{\mathbb{Z}} \mathbb{Z}/(p)$ dans $(K_2\mathcal{O}_F) \otimes_{\mathbb{Z}} \mathbb{Z}/(p)$. Si p est grand, aucun calcul rigoureux n'est réalisable.

Pour ces vérifications, il suffit de démontrer qu'un idéal explicite n'est pas principal dans $\mathcal{O}_E$, ce qui peut parfois se vérifier dans un sous-corps si le p-Sylow du noyau de capitulation de l'extension E/F est trivial. Cette remarque permet de traiter quelques exemples supplémentaires, mais ne règle pas le problème de fond.

Remarque 5.4. Si F est galoisien et contient une racine p-ième de l'unité, Diaz y Diaz et Soriano [24] utilisent le groupe des classes logarithmiques $\widetilde{\mathrm{Cl}}(F)$ de Jaulent [39] pour calculer $WK_2F \otimes_{\mathbb{Z}} \mu_p$. En effet, *si* $\widetilde{\mathrm{Cl}}(F)$ est fini (ce qui équivaut à la conjecture de Gross pour la tour cyclotomique de F ; donc est vrai pour F abélien), il a le même p-rang que WK_2F. Ce calcul est de difficulté comparable à celui qui est présenté ci-dessus, puisqu'il requiert le calcul de $\mathrm{Cl}(\mathcal{O}_{F(\zeta_p)})$. En l'état, il est aussi moins général.

[14] WK_2F est le sous-groupe « intéressant » de $K_2\mathcal{O}_F$. Le quotient $K_2\mathcal{O}_F/WK_2F$ étant identifié à un terme algorithmiquement élémentaire par la suite de Moore [51], son cardinal fournit une borne inférieure effective pour $\#K_2\mathcal{O}_F$.

La taille de la borne pour S pose une autre difficulté : tout comme les bornes inconditionnelles pour la taille de générateurs du groupe des classes, elle est exponentielle en $\log(\mathrm{disc}(F))$. Une étude directe, place par place[15], suivant les idées de Tate [62] améliore sensiblement la situation pratique, bien que la complexité reste exponentielle. Conceptuellement, on remplace le traitement (construction incrémentale et réductions successives sous forme normale) d'un réseau Λ de rang $O(\#S^2)$ par celui de $O(\#S)$ réseaux de rang $O(\#S)$.

Un sous-produit de l'algorithme est une solution partielle du logarithme discret, permettant de réellement calculer dans $K_2\mathcal{O}_F$. Ainsi, à la suite du Théorème 5.2, on exprime tout symbole donné en termes de S-unités (pour le S choisi dans les calculs) comme puissance du générateur. Par exemple

$$\{3\omega + 17, 2\} = (\{-17 - 3\omega, -37 + \omega\}^5)^{17}.$$

Finalement, tout comme le calcul de K_0/K_1, la méthode fournit naturellement des relations entre tenseurs de Steinberg, donc des éléments dans le groupe de Bloch $B_2(F)$, qui est très proche de $K_3\mathcal{O}_F = K_3F$ (voir Bloch [8, 9] et Suslin [61]). On obtient en particulier une base de $K_3F \otimes_{\mathbb{Z}} \mathbb{Q}$, dès qu'un régulateur convenable ne s'annule pas sur les éléments calculés. Ce genre de calcul a été systématiquement exploré par Gangl.

6. Pari/Gp

Pari/Gp [T14] est un système de calcul formel libre, sous licence gnu gpl, orienté vers la théorie des nombres. Il a été créé et développé dans les années 1984–1995 au laboratoire A2X (Bordeaux I) par Henri Cohen, ses collaborateurs (Christian Batut, Dominique Bernardi, Francisco Diaz y Diaz, Michel Olivier) et leurs étudiants, et mis à la disposition de la communauté mathématique vers 1989. Je dirige son développement, largement décentralisé maintenant, depuis 1996.

Le système se compose d'une bibliothèque C (Pari) et d'un interpréteur (Gp), noyaux historiques entièrement réécrits (soit 133000 lignes de code C, 2000 lignes de divers assembleurs), d'un compilateur (Gp2C) écrit par Bill Allombert, et

[15]Tout comme, dans le cas de $\mathrm{Cl}(\mathcal{O}_F)$, on effectue souvent un calcul heuristique en remplaçant A par un sous-groupe $A' \subset A$ de rang moindre, dont M n'est plus nécessairement un quotient. L'algorithme du logarithme discret permet de vérifier à posteriori qu'une place finie $v \in A \setminus A'$ est bien dans le sous-groupe engendré par A', validant l'hypothèse.

d'une multitude d'interfaces indépendantes[16]. PARI/GP est très portable et j'estime qu'il compte aujourd'hui au moins vingt mille utilisateurs réguliers[17].

Mon but a été de rationaliser et stabiliser le système, de le rendre aussi utilisable et prévisible que possible, y compris pour les problèmes de grande taille que la conception initiale excluait explicitement. Il a fallu aussi assurer la compatibilité avec les anciens programmes malgré les évolutions de PARI/GP, ainsi que le fonctionnement sur des architectures devenues obsolètes, tout en s'adaptant aux nouvelles machines et aux évolutions des systèmes d'exploitations. Il reste encore beaucoup à faire, notamment au niveau de la standardisation des interfaces et de la documentation, et de l'implantation systématique d'algorithmes asymptotiquement rapides.

J'ai modifié ou implanté l'essentiel des algorithmes, fonction par fonction. Les algorithmes des parties précédentes ont tous occasionné des réécritures majeures du noyau existant : du calcul multiprécision à l'arithmétique polynomiale, en passant par l'algèbre linéaire. La partie mathématiquement significative (originale) de ces travaux est décrite aux §3, §4. PARI/GP a toujours été considéré comme un système extrêmement rapide. Il l'est environ deux fois plus aujourd'hui qu'en 1996 sur la batterie de tests standards, et utilise moins de mémoire ; les gains sont en général de plusieurs ordres de grandeur sur les exemples non-triviaux, voir par exemple [46] qui se limite au calcul formel.

PARI/GP est une œuvre collective, qui incorpore les contributions de nombreux auteurs depuis 1996, en particulier Bill Allombert, Henri Cohen, Louis Granboulan, Guillaume Hanrot, Gerhard Niklasch, Xavier Roblot, et Ilya Zakharevitch. L'historique général mis en place en Novembre 1997, après une première réécriture complète, mentionne 36 auteurs différents et m'attribue 1632 modifications substantielles du système depuis cette date (sur un total de 2103 au 14/05/2003).

[16] Interfaces utilisateur (Emacs, TEXmacs, PariGUIde), interfaces langages (Perl, Python, CLISP, C++), interfaces système (`dlopen()` et modules dynamiques), interfaces graphiques (Qt, gnuplot, X-Windows)...

[17] On comptabilise $\approx$ 80000 téléchargements entre novembre 2000 et avril 2003 depuis les deux serveurs principaux, sachant que d'autres sites le proposent, qu'il est inclus dans au moins deux distributions Linux majeures (SuSE, Debian) ainsi que dans la distribution Fink pour Mac OS X/Darwin, et que les utilisateurs intensifs récupèrent directement des version de développement sans être comptabilisés.

Liste des travaux présentés

disponibles à l'adresse `http://www.math.u-psud.fr/~belabas/pub/`.

[T1] Computing cubic fields in quasi-linear time, in *Ants II, Bordeaux*, LNCS, no. 1122, Springer-Verlag, 1995, pp. 17–25.

[T2] Crible et 3-rang des corps quadratiques, *Ann. de l'Inst. Fourier* **46** (1996), pp. 909–949.

[T3] A fast algorithm to compute cubic fields, *Math. Comp.* **66** (1997), pp. 1213–1237.

[T4] (avec H. Cohen), Binary cubic forms and cubic number fields, in *Computational perspectives on number theory (Chicago, IL, 1995)* (Providence, RI), Amer. Math. Soc., Providence, RI, 1998, pp. 191–219.

[T5] On the mean 3-rank of quadratic fields, *Compositio Mathematica* **118** (1999), pp. 1–9.

[T6] (avec E. Fouvry), Sur le 3-rang des corps quadratiques de discriminant premier ou presque premier, *Duke Math. J.* **98** (1999), no. 2, pp. 217–268.

[T7] (avec H. Gangl) Determining $K_2\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ for $0 > d \geqslant -151$, appendice à [11] (2000), pp. 1681–1683.

[T8] (avec S. Hersonsky et F. Paulin), Counting horoballs and rational geodesics, *Bull. London Math. Soc.* **33** (2001), no. 5, pp. 606–612.

[T9] On quadratic fields with high 3-rank, 16 pages, à paraître dans *Mathematics of Computation*.

[T10] A relative van Hoeij algorithm over number fields, 27 pages, à paraître au *Journal of Symbolic Computation*.

[T11] (avec H. Gangl), Generators and relations for $K_2\mathcal{O}_F$, 30 pages, à paraître à *K-Theory*.

[T12] Topics in computational algebraic number theory, 37 pages, à paraître au *Journal de Théorie de Nombres de Bordeaux*.

Rapport technique

[T13] (avec G. Hanrot et P. Zimmermann), Tuning and generalizing van Hoeij's algorithm, Rapport de recherche 4124, INRIA, 2001, 13 pages.

Logiciel

[T14] Pari/Gp, `http://pari.math.u-bordeaux.fr`, 35 versions publiques depuis 1997. Voir aussi `http://www.math.u-psud.fr/~belabas/pari/`

Liste des autres travaux cités

[1] J. Abbott, V. Shoup & P. Zimmermann, Factorization in $\mathbb{Z}[x]$: the searching phase, in *ISSAC'2000* (C. Traverso, ed.), ACM Press, 2000, pp. 1–7.

[2] E. Bach, Explicit bounds for primality testing and related problems, *Math. Comp.* **55** (1990), no. 191, pp. 355–380.

[3] E. Bach, Improved approximations for Euler products, in *Number theory (Halifax, NS, 1994)* (Providence, RI), Amer. Math. Soc., Providence, RI, 1995, pp. 13–28.

[4] H. Bass, J. Milnor & J.-P. Serre, Solution of the congruence subgroup problem for $\mathrm{SL}_n\,(n \geqslant 3)$ and $\mathrm{Sp}_{2n}\,(n \geqslant 2)$, *Inst. Hautes Études Sci. Publ. Math.* (1967), no. 33, pp. 59–137.

[5] H. Bass & J. Tate, The Milnor ring of a global field, 349–446. Lecture Notes in Math., Vol. 342, Springer, 1973, pp. 349–446. Lecture Notes in Math., Vol. 342.

[6] E. R. Berlekamp, Factoring polynomials over large finite fields, *Math. Comp.* **24** (1970), pp. 713–735.

[7] M. Bhargava, Higher composition laws, Ph.D. thesis, Princeton University, 2001.

[8] S. Bloch, Applications of the dilogarithm function in algebraic K-theory and algebraic geometry, in *Proceedings of the International Symposium on Algebraic Geometry (Kyoto Univ., Kyoto, 1977)* (Tokyo), Kinokuniya Book Store, 1978, pp. 103–114.

[9] S. Bloch, *Higher regulators, algebraic K-theory, and zeta functions of elliptic curves*, American Mathematical Society, Providence, RI, 2000.

[10] A. Borel, Stable real cohomology of arithmetic groups, *Ann. Sci. École Norm. Sup. (4)* **7** (1974), pp. 235–272 (1975).

[11] J. Browkin, Computing the tame kernel of quadratic imaginary fields, *Math. Comp.* **69** (2000), no. 232, pp. 1667–1683, With an appendix by K. Belabas and H. Gangl.

[12] J. A. Buchmann & H. W. Lenstra, Jr., Approximating rings of integers in number fields, *J. Théor. Nombres Bordeaux* **6** (1994), no. 2, pp. 221–260.

[13] J. Buchmann, A subexponential algorithm for the determination of class groups and regulators of algebraic number fields, in *Séminaire de Théorie des Nombres, Paris 1988–1989*, Progr. Math., vol. 91, Birkhäuser, 1990, pp. 27–41.

[14] D. Burns and C. Greither, On the equivariant Tamagawa conjecture for Tate motives, *Inventiones Mathematicae* **153** (2003), no. 2, 303–359.

[15] H. Cohen, *A course in computational algebraic number theory*, Springer-Verlag, 1993.

[16] H. Cohen, *Advanced topics in computational number theory*, Springer-Verlag, 2000.

[17] H. Cohen, F. Diaz y Diaz & M. Olivier, Computing ray class groups, conductors and discriminants, *Math. Comp.* **67** (1998), no. 222, pp. 773–795.

[18] H. Cohen & H. W. Lenstra, Jr., Heuristics on class groups of number fields, in *Number theory, Noordwijkerhout 1983* (Berlin), Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 33–62.

[19] H. Cohen & J. Martinet, Études heuristiques des groupes de classes des corps de nombres, *J. reine angew. Math.* **404** (1990), pp. 39–76.
[20] H. Cohen, F. Diaz y Diaz & M. Olivier, Subexponential algorithms for class group and unit computations, *J. Symbolic Comput.* **24** (1997), no. 3-4, pp. 433–441, Computational algebra and number theory (London, 1993).
[21] H. Cohen, F. Diaz y Diaz & M. Olivier, Algorithmic methods for finitely generated abelian groups, *J. Symbolic Comput.* **31** (2001), no. 1-2, pp. 133–147, Computational algebra and number theory (Milwaukee, WI, 1996).
[22] H. Davenport & H. Heilbronn, On the density of discriminants of cubic fields (ii), *Proc. Roy. Soc. Lond. A* **322** (1971), pp. 405–420.
[23] B. N. Delone & D. K. Faddeev, *The theory of irrationalities of the third degree*, Translations of Mathematical Monographs, vol. 10, American Mathematical Society, 1964.
[24] F. Diaz y Diaz & F. Soriano, Approche algorithmique du groupe des classes logarithmiques, *J. Number Theory* **76** (1999), no. 1, pp. 1–15.
[25] P. Dutarte, Compatibilité avec le Spiegelungssatz de probabilités conjecturales sur le p-rang du groupe des classes, in *Number theory, 1983–1984* (Besançon), Univ. Franche-Comté, Besançon, 1984, pp. Exp. No. 4, 11.
[26] V. Ennola & R. Turunen, On totally real cubic fields, *Math. Comp.* **44** (1985), no. 170, pp. 495–518.
[27] C. Fieker, Computing class fields via the Artin map, *Math. Comp.* **70** (2001), no. 235, pp. 1293–1303 (electronic).
[28] C. Fieker & C. Friedrichs, On reconstruction of algebraic numbers, in *Algorithmic number theory (Leiden, 2000)*, LNCS, vol. 1838, Springer, 2000, pp. 285–296.
[29] D. Ford, S. Pauli & X.-F. Roblot, A fast algorithm for polynomial factorization over $\mathbb{Q}_p$, *J. Théor. Nombres Bordeaux* **14** (2002), no. 1, pp. 151–169.
[30] E. Fouvry & N. Katz, A general stratification theorem for exponential sums, and applications, *J. Reine Angew. Math.* **540** (2001), pp. 115–166.
[31] P. X. Gallagher, The large sieve and probabilistic Galois theory, in *Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972)*, Amer. Math. Soc., Providence, R.I., 1973, pp. 91–101.
[32] H. Garland, A finiteness theorem for K_2 of a number field, *Ann. of Math. (2)* **94** (1971), pp. 534–548.
[33] R. Groenewegen, Bounds for computing the tame kernel, *Math. Comp.*, à paraître, `http://www.math.leidenuniv.nl/reports/2002-13.shtml`.
[34] J. L. Hafner & K. S. McCurley, A rigorous subexponential algorithm for computation of class groups, *J. Amer. Math. Soc.* **2** (1989), no. 4, pp. 837–850.
[35] H. Hasse, Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage, *Math. Zeitschrift.* **31** (1930), pp. 565–582.
[36] S. Hersonsky & F. Paulin, Diophantine approximation for negatively curved manifolds, *Math. Z.* **241** (2002), no. 1, pp. 181–226.
[37] A. Huber & G. Kings, Bloch-Kato Conjecture and Main Conjecture of Iwasawa theory for Dirichlet characters, *Duke Math. J.*, **119** (2003), no. 3, 393–464.
[38] H. Iwaniec, Rosser's sieve, *Acta. Arith.* **36** (1980), pp. 171–202.
[39] J.-F. Jaulent, Classes logarithmiques des corps de nombres, *J. Théor. Nombres Bordeaux* **6** (1994), no. 2, pp. 301–325.

[40] F. Keune, On the structure of the K_2 of the ring of integers in a number field, *K-Theory* **2** (1989), no. 5, pp. 625–645.

[41] M. Kolster, T. Nguyen-Quang-Do & V. Fleckinger, Twisted S-units, p-adic class number formulas, and the Lichtenbaum conjectures, *Duke Math. J.* **84** (1996), no. 3, pp. 679–717, errata : *Duke Math. J.* **90** (1997), no. 3, pp. 641–643.

[42] Y. Lee, Cohen-Lenstra heuristics and the Spiegelungssatz : number fields, *J. Number Theory* **92** (2002), no. 1, pp. 37–66.

[43] A. K. Lenstra, Lattices and factorization of polynomials over algebraic number fields, (Berlin), LNCS, vol. 144, Springer, Berlin, 1982, pp. 32–39.

[44] A. K. Lenstra, H. W. Lenstra, Jr. & L. Lovász, Factoring polynomials with rational coefficients, *Math. Ann.* **261** (1982), no. 4, pp. 515–534.

[45] S. Lichtenbaum, Values of zeta-functions, étale cohomology, and algebraic K-theory, in *Algebraic K-theory, II : "Classical" algebraic K-theory and connections with arithmetic (Proc. Conf., Battelle Memorial Inst., Seattle, Wash., 1972)* (Berlin), Springer, Berlin, 1973, pp. 489–501. Lecture Notes in Math., Vol. 342.

[46] R. Lewis & M. Wester, Comparison of polynomial-oriented computer algebra systems. *cf.* `http://www.math.u-psud.fr/~belabas/pari/`

[47] G. Malle, On the distribution of Galois groups, *J. Number Theory* **92** (2002), no. 2, pp. 315–329.

[48] H. Matsumoto, Sur les sous-groupes arithmétiques des groupes semi-simples déployés, *Ann. Sci. École Norm. Sup. (4)* **2** (1969), pp. 1–62.

[49] B. Mazur & A. Wiles, Class fields of abelian extensions of $\mathbb{Q}$, *Invent. Math.* **76** (1984), no. 2, pp. 179–330.

[50] Centre de calcul formel MEDICIS, `http://www.medicis.polytechnique.fr`.

[51] C. C. Moore, Group extensions of p-adic and adelic linear groups, *Inst. Hautes Études Sci. Publ. Math. No.* **35** (1968), pp. 157–222.

[52] M. Pohst, *Computational algebraic number theory*, DMV Seminar, vol. 21, Birkhäuser, Basel, 1993.

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

[54] H. Qin, Computation of $K_2\mathbb{Z}[\sqrt{-6}]$, *J. Pure Appl. Algebra* **96** (1994), no. 2, pp. 133–146.

[55] H. Qin, Computation of $K_2\mathbb{Z}[(1+\sqrt{-35})/2]$, *Chinese Ann. Math. Ser. B* **17** (1996), no. 1, pp. 63–72.

[56] X.-F. Roblot, Polynomial Factorization Algorithms over Number Fields, 2002, *J. Symbolic Computation*, à paraître.

[57] J. Rognes & C. Weibel, Two-primary algebraic K-theory of rings of integers in number fields, *J. Amer. Math. Soc.* **13** (2000), no. 1, pp. 1–54, Appendix A by Manfred Kolster.

[58] A. Scholz, Über die Beziehung der Klassenzahlen quadratisher Körper zueinander, *J. reine angew. Math.* **166** (1932), pp. 201–203.

[59] R. Schoof, Elliptic curves over finite fields and the computation of square roots mod p, *Math. Comp.* **44** (1985), no. 170, pp. 483–494.

[60] M. Skałba, Generalization of Thue's theorem and computation of the group K_2O_F, *J. Number Theory* **46** (1994), no. 3, pp. 303–322.
[61] A. A. Suslin, K_3 of a field, and the Bloch group, *Trudy Mat. Inst. Steklov.* **183** (1990), pp. 180–199, 229, Galois theory, rings, algebraic groups and their applications (Russian).
[62] J. Tate, Appendix, in *Algebraic K-theory II*, Lecture Notes in Math., vol. 342, Springer-Verlag, 1973, pp. 429–446.
[63] J. Tate, Relations between K_2 and Galois cohomology, *Invent. Math.* **36** (1976), pp. 257–274.
[64] B. L. van der Waerden, Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt, *Monatsh. Math. Phys.* (1936), no. 43, pp. 133–147.
[65] M. van Hoeij, Factoring polynomials and the knapsack problem, *J. Number Theory* **95** (2002), no. 2, pp. 167–189.
[66] H. Zassenhaus, On Hensel factorization I, *Journal of Number Theory* (1969), pp. 291–311.
[67] H. Zassenhaus, Ein Algorithmus zur Berechnung einer Minimalbasis über gegebener Ordnung, in *Funktionalanalysis, Approximationstheorie, Numerische Mathematik (Oberwolfach, 1965)* (Basel), Birkhäuser, Basel, 1967, pp. 90–103.
[68] P. Zimmermann, Polynomial factorization challenges : a collection of polynomials difficult to factor, 1996, `http://www.loria.fr/~zimmerma/mupad/`.

N° d'impression 2559
4ème trimestre 2003