N° d'ordre : 1528.

THESE

présentée à

L'UNIVERSITE BORDEAUX I

ECOLE DOCTORALE DE MATHEMATIQUES

Par **Karim BELABAS**

POUR OBTENIR LE GRADE DE

DOCTEUR

SPECIALITE : MATHEMATIQUES PURES

VARIATIONS SUR UN THEME DE DAVENPORT ET HEILBRONN : Formes Cubiques, Corps Cubiques, et Groupes de Classes des Corps Quadratiques

---

Soutenue le 28 Juin 1996.

Après avis de :

E. FOUVRY, Professeur	Université Paris XI
H.W. LENSTRA, Professeur	Berkeley University - USA

Devant la commission d'examen formée de :

H. COHEN, Professeur	Université Bordeaux I	
E. FOUVRY, Professeur	Université Paris XI	Président
G. GRAS, Professeur	Université de Franche-Comté	
H. IWANIEC, Professeur	Rutgers University - USA	
J. MARTINET, Professeur	Université Bordeaux I	Rapporteur

- 1996 -

Remerciements

Ma reconnaissance va d'abord à Henri Cohen, qui a dirigé ma thèse depuis mon arrivée à Bordeaux, pour ses conseils, ses questions, sa disponibilité constante dont j'ai usé et abusé, et la liberté qu'il m'a laissé dans mes recherches.

Ce travail a été initié par Etienne Fouvry, dont l'intérêt ne s'est jamais démenti, qui m'a consacré beaucoup de son temps, de sa patience, de son enthousiasme, et qui a par ailleurs accepté d'être rapporteur, puis de participer au jury. Qu'il reçoive ici l'expression de ma gratitude.

Je remercie Jacques Martinet, qui a accepté de participer au jury, et tous les Algos, qui m'ont accueilli dans ce laboratoire A2X où j'ai trouvé des conditions de travail exceptionnelles.

Je remercie Hendrik Lenstra, Jr. – dont les Heuristiques développées avec Henri Cohen, constituent l'ossature et la motivation du Chapitre 3 de cette thèse – d'avoir accepté d'être rapporteur.

Je remercie Henryk Iwaniec d'avoir accepté de faire partie du jury, ainsi que pour l'intérêt qu'il a manifesté pour ce travail.

Je remercie également Georges Gras d'avoir bien voulu participer au jury.

Merci aux imprimeurs, Mauricette Jaubert et Daniel Ynbourg, pour leur gentillesse et la qualité de leur travail.

Merci enfin à mes camarades, doctorants ou non, de Bordeaux, de la rue d'Ulm ou d'ailleurs, pour leur soutien et leur amitié.

Cette thèse est dédiée à mes parents, à l'Aspirant Nadia, et à Layla.

Table des matières

Introduction

Le groupe des classes de formes quadratiques en deux variables a été introduit par Gauss, qui consacre un chapitre entier des *Disquisitiones* [**20**, Chapitre 5] à leur étude. L'extraordinaire intérêt de cette notion vient de la bijection que l'on peut établir avec le groupe des classes d'idéaux des corps quadratiques, et du rôle que la théorie du corps de classes allait associer à ce dernier (voir [**9**], par exemple, pour une très belle application de ces idées). D'autant que la loi de groupe dont Gauss a équipé les classes de formes fait de cette bijection un isomorphisme. Il devient donc possible de travailler sur le groupe des classes d'un corps quadratique $\mathbb{Q}(\sqrt{\Delta})$ en manipulant des formes quadratiques de discriminant Δ. Gauss en profite pour étudier en détail la partie 2-primaire de ces groupes. Il montre en particulier que le 2-rang est égal au nombre de diviseurs premiers du discriminant, diminué d'une unité. L'identification entre formes réduites et classes d'idéaux fournit aussi un moyen algorithmiquement raisonnable de dresser des tables de groupes des classes (Gauss lui-même en a calculé quelques unes). C'est longtemps resté le seul praticable (voir [**5**]).

Gauss décrit une procédure de "réduction", qui permet de ramener l'étude du groupe des classes à celui d'un nombre fini de formes, dont on contrôle bien les coefficients. Elle fournit même un représentant canonique pour chaque classe de discriminant *négatif*, *i.e.* pour les formes définies. Les formes indéfinies ont trop d'automorphismes et leur réduction est beaucoup plus problématique : des formes réduites distinctes peuvent être équivalentes. Dans ce dernier cas, l'ensemble de formes réduites obtenues (ce n'est même pas un groupe) est trop gros, et ne nous donne pas directement accès à un objet algébrique intéressant.

La structure du groupe des classes est très irrégulière et, même dans le cas quadratique, qui est le seul où l'on dispose d'une description explicite, on sait très peu de choses de son comportement quand le discriminant varie. Une formule de Dirichlet permet d'obtenir une majoration simple de son cardinal. Mais les minorations non triviales sont effroyablement complexes (dans le cas réel, par exemple, on ne sait que *conjecturer* que la liminf vaut 1). Considérer l'ordre moyen arrange un peu les choses, grâce aux formes quadratiques. L'ordre moyen du nombre de classes de formes définies quand le discriminant varie, se calcule simplement en comptant les formes réduites, c'est-à-dire les points entiers d'un volume défini par les inégalités de réduction ([**37**]). On en déduit le nombre de classes moyen des quadratiques imaginaires en imposant que les discriminants des classes soient fondamentaux, c'est-à-dire vérifient une congruence adélique

(essentiellement, ne pas comporter de facteurs carrés, avec un cas particulier pour $p = 2$).

Dans le cas réel, on obtient des renseignements, non plus sur le nombre de classes, mais sur le produit hR, où h est le nombre de classes et R le régulateur, sans possibilité de les dissocier. De même, dans le cas général, la plupart des résultats (Brauer-Siegel, *etc.*) ne permettent d'appréhender que le résidus de la fonction L au point $s = 1$, c'est-à-dire essentiellement ce produit hR.

Lorsque, deux siècles après Gauss, H. Davenport s'intéresse aux formes *cubiques*, leur réduction est bien connue depuis les travaux de Hermite, puis Mathews et Berwick. En particulier et contrairement au cas quadratique, toute classe de formes admet un représentant canonique, quelle que soit sa signature. Il publie une série d'articles [**12, 13, 14**], dans lesquels il donne l'ordre moyen de leur nombre de classes en calculant le volume d'un domaine fondamental. Manque une interprétation algébrique convaincante.

Elle survient, probablement au-delà de ses espérances, lorsqu'avec H. Heilbronn [**15, 16**], il construit une bijection de l'ensemble des corps cubiques, à isomorphisme près, dans une collection U de classes de formes cubiques définie par des congruences simples (mais toujours adéliques). Ils en déduisent l'ordre moyen des discriminants cubiques. Donc, et surtout, celui des sous-groupes d'indice 3 des groupes de classes de rayon des corps quadratiques. Au prix de l'introduction de congruences supplémentaires (qui, globalement, simplifient plutôt les choses !), on obtient une prise sur la partie 3-primaire du groupe des classes, plus précisément sur le 3-rang moyen. Même dans le cas réel, les unités n'interviennent pas ; le régulateur a disparu !

Comme son titre le laisse entendre, cette thèse s'articule autour de ce résultat. Nous commençons au Chapitre 1 par reprendre le travail de Davenport et Heilbronn pour établir un terme reste pour leurs formules et généraliser la moyenne aux discriminants parcourant des progressions arithmétiques. Mécaniquement, on obtient alors des estimations de crible sur le 3-rang des corps quadratiques, dont les discriminants ont peu de facteurs premiers. Nous pouvons ainsi simultanément contrôler le 2-rang et le 3-rang d'une famille de corps. C'est, en quelque sorte, une approche naï ve de la conjecture sur l'infinité du nombre de quadratiques réels principaux, mentionnée plus haut. Le lecteur se convaincra sans peine au vu des constantes qui suivent que, même en se restreignant à la 3-partie, nous sommes bien loin de la résoudre.

Au Chapitre 2, nous montrons que la bijection de Davenport et Heilbronn a une traduction algorithmique très intéressante. Couplée avec la théorie de la réduction des formes cubiques binaires, qui se révèle curieusement bien moins complexe que celle des formes quadratiques indéfinies, elle permet de décrire et de manipuler facilement des corps cubiques. Nous avons en particulier dressé des tables pour des valeurs élevées du discriminant.

Pour illustrer de nouveau la maniabilité des corps cubiques, nous calculons au Chapitre 3 le 3-rang moyen des corps de nombres galoisiens (à degré et signature fixés), sous le modèle probabiliste de Cohen-Lenstra-Martinet. Plus précisément, nous calculons le 3-rang moyen du groupe des classes d'idéaux de l'anneau des S-entiers d'une famille de corps quadratiques imaginaires, où S contient les diviseurs d'un ensemble de premiers fixés. Un tel groupe s'identifie naturellement à un quotient du groupe des classes du corps quadratique associé. Donc devrait, dans l'esprit des heuristiques de Cohen-Lenstra, se comporter comme les groupes de classes de corps de nombres, de signature liée au nombre de générateurs du quotient. Nous montrons qu'en ce qui concerne le 3-rang, cette hypothèse est vérifiée si S ne contient qu'un seul premier, grâce au théorème de Davenport et Heilbronn. Sinon, nous retrouvons bien le résultat (conjectural) prévu par les heuristiques. Incidemment, nous donnons pour ces théorèmes un bien meilleur terme de reste que celui qui découle du Chapitre 1.

Au Chapitre 4, nous montrons comment une construction explicite, due à Yamamoto, permet d'améliorer considérablement certaines estimations de crible du Chapitre 1. De plus, ces dernières ne semblent pas généralisables, sauf peut-être pour de *très* petits premiers. Ici, au contraire, le cas du ℓ-rang pour ℓ premier quelconque n'est pas sensiblement plus compliqué que le cas $\ell = 3$ (par contre, les résultats sont nettement moins bons !).

En appendice, nous donnons une démonstration complète du théorème de Davenport et Heilbronn. Celui-ci utilise de nombreux arguments "élémentaires" issus de la théorie des corps cubiques, que nous avons jugés bon de démontrer en utilisant les outils techniques qui permettent de les comprendre. Il n'est, par exemple, pas nécessaire d'introduire les conducteurs d'Artin, ou le théorème de Brauer caché dans leur définition, pour étudier une extension galoisienne de $\mathbb{Q}$ de groupe S_3 : tout peut se démontrer "à la main", avec une définition *ad hoc* des groupes de ramifications. Ces démonstrations nous ont paru suffisamment artificielles pour que nous présentions la théorie telle qu'elle se généralise. Nous étudierons donc les discriminants des corps cubiques (Annexe A), puis leurs discriminants "inessentiels" (Annexe B), dans un cadre bien plus général que ce dont nous aurons finalement besoin à l'Annexe C pour présenter la démonstration de Davenport et Heilbronn.

Ces différents chapitres faisant l'objet de publications, nous espérons que le lecteur nous pardonnera les redites, essentiellement dues au manque du temps nécessaire à la ré-écriture de l'ensemble.

CHAPITRE 1

Crible et 3-rang des Corps Quadratiques

Ce chapitre a été accepté pour publication aux *Annales de l'Institut Fourier* [**1**] et devrait paraître dans le courant de l'année.

E. Fouvry, dont les questions ont initié ce travail, a eu la gentillesse d'en relire attentivement les versions successives. Qu'il en soit ici remercié.

1. Introduction

On appelle discriminant fondamental un entier de la forme $\alpha \equiv 1(4)$ ou 4β, avec $\beta \not\equiv 1(4)$, où α et β sont sans facteurs carrés. Soit Δ un entier ; on note $h_3^*(\Delta)$ la quantité $3^{h_3(\Delta)}$, où $h_3(\Delta)$ est le 3-rang du corps quadratique $\mathbb{Q}(\sqrt{\Delta})$. On montre facilement que $h_3^*(\Delta)$ dénombre les racines cubiques de l'unité du groupe des classes de $\mathbb{Q}(\sqrt{\Delta})$.

Davenport et Heilbronn [**16**] ont calculé la valeur moyenne de ces nombres quand Δ parcourt les discriminants fondamentaux compris entre 0 et X, ou entre $-X$ et 0. Les structures très différentes des unités des corps quadratiques réels et imaginaires induisent en effet des différences de traitement appréciables ; en particulier on n'obtient pas le même résultat selon que l'on considère les $\Delta > 0$ ou les $\Delta < 0$.

Théorème 1.1 (Davenport-Heilbronn). *Si les Δ sont restreints aux discriminants fondamentaux on a, au voisinage de $+\infty$, les égalités*

$$\sum_{0<\Delta<X} h_3^*(\Delta) \Big/ \sum_{0<\Delta<X} 1 = \frac{4}{3} + o(1),$$

$$\sum_{-X<\Delta<0} h_3^*(\Delta) \Big/ \sum_{-X<\Delta<0} 1 = 2 + o(1).$$

Le but de cet article est de cribler la suite des discriminants fondamentaux affectés du poids positif $h_3^*(\Delta) - 1$ afin d'obtenir des renseignements sur la 3-partie du groupe des classes de $\mathbb{Q}(\sqrt{\Delta})$, où Δ a peu de facteurs premiers. Pour ce faire, on commence par démontrer un résultat d'équirépartition du 3-rang dans les progressions arithmétiques de raison q, qui a un intérêt propre. En effet, le résultat de Davenport-Heilbronn correspondant au cas $q = 1$, on obtient en particulier un reste en $o(1/\log^2 X \log\log^{2-\varepsilon} X)$, apparemment inédit, pour les formules du Théorème 1.1. Il n'y a aucune difficulté de principe à rendre effective la constante implicite du o (nous ne l'avons pas fait), ainsi d'ailleurs que pour tous les théorèmes démontrés dans la suite.

THÉORÈME 1.2. *Si les Δ sont restreints aux discriminants fondamentaux, alors pour tout $\varepsilon > 0$, si $q \leqslant X^{1/15-\varepsilon}$ est sans facteurs carrés, on a :*

$$\sum_{\substack{0<\Delta<X \\ q|\Delta}} [h_3^*(\Delta) - 1] = \frac{1}{\pi^2}\frac{\omega(q)}{q} \cdot X + O\big(R_\varepsilon(X,q)\big),$$

$$\sum_{\substack{-X<\Delta<0 \\ q|\Delta}} [h_3^*(\Delta) - 1] = \frac{3}{\pi^2}\frac{\omega(q)}{q} \cdot X + O\big(R_\varepsilon(X,q)\big)$$

avec

$$\omega(q) = \prod_{p|q} \frac{p}{p+1}, \quad \omega(1) = 1,$$

$$R_\varepsilon(X,q) = O\Big[\frac{X}{q\log^2 X \log\log^{2-\varepsilon} X} + X^{15/16+\varepsilon} q^{-1/16}\Big].$$

Remarque 1.3. On peut sans difficulté traiter le cas où q a un facteur carré fixé. La somme étant nulle dès que q a un facteur carré différent de 4, il suffit de généraliser légèrement la fonction ω, en la décrétant multiplicative et en posant

$$\begin{cases} \omega(p) &= p/(p+1), \\ \omega(p^\alpha) &= 0 \text{ si } \alpha \geqslant 2 \text{ et } p \text{ premier supérieur à } 2, \\ \omega(4) &= 4/3, \\ \omega(8) &= 4/3, \\ \omega(2^\alpha) &= 0 \text{ si } \alpha \geqslant 4. \end{cases}$$

On a alors le même théorème.

Puisque la fonction $\omega(p)$ vaut en moyenne 1, nous sommes dans le cadre bien connu du crible linéaire et la majoration de $R_\varepsilon(X,q)$ assure un contrôle du terme d'erreur jusqu'à $Q = X^{1/15-\varepsilon}$. Parmi la grande variété de résultats maintenant accessibles, nous avons choisi deux points de vue. Le premier dit que le 3-rang de $\mathbb{Q}(\sqrt{p})$ pour p premier n'est pas anormalement élevé. On montrera :

THÉORÈME 1.4. *Quand X tend vers l'infini, on a les inégalités*

$$\sum_{\substack{p\leqslant X \\ p=1\ (4)}} h_3^*(p) \leqslant 11\big(1+o(1)\big)\frac{X}{2\log X},$$

et

$$\sum_{\substack{p\leqslant X \\ p=3\ (4)}} h_3^*(-p) \leqslant 31\big(1+o(1)\big)\frac{X}{2\log X}.$$

Il est clair que nous aimerions remplacer les constantes 11 et 31 respectivement par 4/3 et 2, pour montrer que $\mathbb{Q}(\sqrt{\pm p})$ a un 3-rang moyen comparable à celui de $\mathbb{Q}(\sqrt{\Delta})$. Un tel résultat est totalement hors de portée des méthodes classiques de crible (phénomène de parité).

Le Théorème 1.4 entraîne une majoration du rang moyen des courbes elliptiques $y^2 = x^3 \pm p$, plus précisément :

$$\sum_{0<p<X} (\sqrt{3})^{\mathrm{rg}(y^2=x^3\pm p)} = O\Big(\frac{X}{\log X}\Big),$$

avec une constante explicite (voir [**18**] où est traité le cas de courbes $y^2 = x^3 \pm k$, avec $k \in \mathbb{Z}^*$).

Le second point de vue de nos applications est de montrer qu'il y a beaucoup de Δ ayant peu de facteurs premiers, donc tels que le 2-rang du groupe des classes soit contrôlé, et tels que sa 3-partie soit triviale, ou au contraire non triviale. Nous montrerons le :

Théorème 1.5.

- *Il existe une infinité de* Δ positifs *ayant au plus* 8 *facteurs premiers tels que* $h_3^*(\Delta) = 1$.
- *Il existe une infinité de* Δ négatifs *ayant au plus* 26 *facteurs premiers tels que* $h_3^*(\Delta) = 1$.
- *Il existe une infinité de* Δ *(qu'on peut supposer au choix positifs ou négatifs) ayant au plus* 17 *facteurs premiers tels que* $3 \mid h_3^*(\Delta)$.

Les deux premières assertions sont obtenues par une majoration du crible, la troisième par une minoration. Signalons que la clé de la démonstration consiste à compter des points à coordonnées entières dans un volume algébrique C_X explicite, vérifiant de surcroît une congruence adélique. On démontre un résultat très général (Corollaire 4.2) permettant de dénombrer les points entiers d'un semi-algébrique compact C qui vérifient une congruence modulo m, avec un reste uniforme en m.

Dans notre cas particulier, en modifiant cette congruence et ce volume, nous définirons deux ensembles A et B encadrant l'ensemble cherché. Nous appliquerons alors la majoration du crible aux points de B, et la minoration à ceux de A. Les ensembles A et B ont un nombre équivalent de points, mais leur relative simplicité par rapport à l'ensemble initial permet un bien meilleur contrôle du terme d'erreur.

Par exemple, C_X comporte une "pointe" que l'on contrôle assez mal, mais de faible volume ; d'où l'idée (due à Davenport, voir [**13**] et [**14**]) de considérer un volume tronqué $C_{X,\rho}$ et d'effectuer tous les calculs sur celui-ci. Quitte à tenir compte ensuite des points "oubliés". Dans le cadre d'une minoration, on peut supprimer ce dernier terme d'erreur. De même, lorsqu'on évaluera le nombre de corps cubiques de discriminant Δ, qui ne sont totalement ramifiés en aucune place finie ($= [h_3^*(\Delta) - 1]/2$), on le majorera en se contentant d'un nombre fini de places.

Remarquons aussi que nous montrons plus précisément la minoration

$$\sum_{\substack{|\Delta|<X\\ p|\Delta\Rightarrow p\geqslant X^{5/87-\varepsilon}}} [h_3^*(\Delta)-1] \geqslant c_\varepsilon \frac{X}{\log X}.$$

Mais il semble difficile d'en déduire un résultat de la forme

$$\sum_{\substack{|\Delta|<X\\ p|\Delta\Rightarrow p\geqslant X^{5/87-\varepsilon}\\ 3|h_3^*(\Delta)}} 1 \geqslant c_\varepsilon \frac{X}{\log X},$$

c'est-à-dire d'obtenir une proportion positive de tels discriminants. Même si, en pratique, on ne connaît pas de corps quadratique de 3-rang supérieur à 6 (exemple dû à Quer [**41**]).

Les méthodes du crible pondéré s'appliquent à la suite des Δ affectés des coefficients $h_3^*(\Delta)-1$. On calcule la valeur minimale de r telle que $\Lambda_r > 87/10$ (voir [**22**, pp. 253–254]), avec

$$\Lambda_r = r+1-\frac{\log 4}{(1+3^{-r})\log 3},$$

et l'on trouve $r=9$. Nous énonçons sans autre démonstration :

THÉORÈME 1.6. *Il existe une infinité de* Δ *(pris, au choix, positifs ou négatifs) ayant au plus* 9^* *facteurs premiers, et tels que* $3 \mid h_3^*(\Delta)$.

Remarque 1.7. Les mêmes techniques permettent de traiter l'autre résultat célèbre de Davenport et Heilbronn sur les corps cubiques, donnant cette fois-ci la densité de leurs discriminants. On obtient le même reste en $O(X/\log^2 X \log\log^{2-\varepsilon} X)$. Les cribler ne pose aucune difficulté particulière (il faut légèrement modifier §5 et changer les densités locales, qui gardent les mêmes propriétés) et on obtiendrait le même contrôle de q. Cependant, l'essentiel des résultats alors disponibles seraient triviaux puisqu'il est algébriquement très facile de calculer le discriminant des $\mathbb{Q}(\sqrt[3]{\pm p})$ (qui fournissent d'ailleurs des familles infinies où il a très peu de facteurs premiers !). Ce qui est loin d'être le cas pour le groupe des classes.

Je remercie le professeur J. -J. Risler pour la patience avec laquelle il a accueilli mes questions de néophyte en géométrie réelle, ainsi que le professeur E. Fouvry, sous la direction duquel ce travail a été réalisé, et qui m'a suggéré ce thème de recherche ainsi que beaucoup des résultats présentés ici. Je remercie également le rapporteur pour ses remarques et les simplifications significatives qu'elles ont entraînées.

*On peut nettement améliorer ce résultat, voir le Corollaire 1.5 et le Théorème 1.6.

2. Notations et définitions

On considère l'ensemble des formes cubiques binaires, primitives, irréductibles, à coefficients dans $\mathbb{Z}$. Si $F = ax^3 + bx^2y + cxy^2 + dy^3$ (éventuellement notée (a, b, c, d)) est une telle forme, on note $\Delta(F)$ son discriminant, à savoir :

$$\Delta(F) = b^2c^2 + 18abcd - 27a^2d^2 - 4b^3d - 4c^3a = \Delta(a, b, c, d).$$

Deux formes f et g sont dites équivalentes s'il existe $M \in \mathrm{GL}_2(\mathbb{Z})$ tel que $f \circ M = g$. Primitivité et irréductibilité étant conservées sous cette action de $\mathrm{GL}_2(\mathbb{Z})$, on peut définir l'ensemble des classes d'équivalences de telles formes, noté Φ. Les discriminants de deux formes équivalentes étant égaux, on définit le discriminant d'une classe F de formes cubiques, toujours noté $\Delta(F)$, comme le discriminant de l'une quelconque des formes la composant. On utilisera la notation

$$F \equiv G \pmod{p}$$

pour indiquer que tous les coefficients de $F - G$ sont divisibles par p, ou encore $p \mid F - G$.

Si p est premier impair, on note V_p l'ensemble des classes de Φ telles que $p^2 \nmid \Delta(F)$; V_2 désigne l'ensemble des classes F vérifiant $\Delta(F) = 1 \pmod 4$, ou $\Delta(F) = 8$ ou $12 \pmod{16}$. On pose alors

$$V_q = \bigcap_{p \mid q} V_p \quad \text{et} \quad V = \bigcap V_p,$$

i.e. V est l'ensemble des classes irréductibles de discriminant fondamental. Le discriminant $\Delta(F)$ étant invariant sous l'action de $\mathrm{GL}_2(\mathbb{Z})$, ces ensembles sont constitués de classes de formes cubiques. Par abus de langage on dira que $\Delta \in V_p$ si les classes de discriminant Δ appartiennent à V_p.

Les lettres grasses désigneront toujours des vecteurs (ou des fonctions vectorielles) de K^n, et $\boldsymbol{x}.\boldsymbol{y}$ est le produit scalaire usuel. K sera un anneau dépendant du contexte ($\mathbb{R}$ ou $\mathbb{Z}/k\mathbb{Z}$).

Si E est un ensemble fini, nous noterons indifféremment $|E|$ ou $\#E$ son cardinal. La lettre p, avec ou sans indice, représentera toujours un nombre premier. Le caractère ε désignera un réel positif arbitrairement petit, son emploi sous-entendra toujours "pour tout $\varepsilon > 0$ fixé", et on se permettra de noter ε toute fonction de ε vérifiant ces mêmes propriétés (par exemple, $2\varepsilon = \varepsilon\ldots$). Nous utiliserons aussi les notations usuelles suivantes :

$\mathbf{1}$	fonction constante égale à 1,
$\mu(n)$	fonction de Möbius,
$\varphi(n)$	fonction phi d'Euler,
$\tau(n)$	nombre de diviseurs de n,
$\omega(n)$	nombre de diviseurs premiers de n,
$\zeta(s)$	fonction zêta de Riemann,
$[x]$	partie entière de x,

$e(x)$	$\exp(2i\pi x)$,
(a,b)	*pgcd* de a et b,
$P^-(n)$	plus petit diviseur premier de n,
P_Y	produit des premiers inférieurs à Y,
$f*g$	convolée arithmétique de f et g, *i.e.* $$f*g(n)=\sum_{d\mid n} f(d)g\Big(\frac{n}{d}\Big),$$
γ	constante d'Euler, *i.e.* $$\gamma=\sum_1^\infty \Big(\frac{1}{k}-\log\Big(1+\frac{1}{k}\Big)\Big).$$

3. Méthode de Davenport-Heilbronn

Soit K un corps cubique de discriminant Δ dans lequel aucun premier n'est totalement ramifié. Autrement dit, Δ est un discriminant fondamental, ce qui implique que K n'est pas cyclique (voir [**23**]).

LEMME 3.1. *Le nombre de triplets de tels corps vaut :*

$$\frac{1}{2}[h_3^*(\Delta)-1].$$

PREUVE. Voir [**23**, p. 581]. Il suffit de compter les sous-groupes d'indice 3 du groupe des classes de $\mathbb{Q}(\sqrt{\Delta})$. □

On note $\mathcal{K}_3$ l'ensemble des triplets de corps cubiques non galoisiens et des corps cubiques cycliques. Davenport et Heilbronn ([**15**, démonstration du Théorème 1] et [**16**, §6 et §7]) ont établi une correspondance entre classes de formes cubiques modulo l'action de $\mathrm{GL}_2(\mathbb{Z})$ et éléments de $\mathcal{K}_3$, cette correspondance préservant le discriminant. En particulier :

LEMME 3.2. *Les triplets de corps cubiques non totalement ramifiés aux places finies sont en bijection avec les classes d'éléments de V de mêmes discriminants.*

Pour cribler, nous avons besoin d'évaluer notre somme pondérée en restreignant Δ aux progressions arithmétiques du type $\Delta\equiv 0 \pmod q$. Grâce aux deux lemmes ci-dessus, il nous suffit de compter des classes de formes cubiques dont le discriminant vérifie certaines relations de congruence (à savoir $\Delta\equiv 0 \pmod q$, et $\Delta\in V_p$ pour tout p premier).

On se donne donc S_m un sous-ensemble de $(\mathbb{Z}/m\mathbb{Z})^4$, stable modulo l'action de $\mathrm{GL}_2(\mathbb{Z})$ si on le considère comme ensemble de formes cubiques définies modulo m. Par abus de langage, nous dirons $F\in S_m$ si F modulo m appartient à S_m. En adaptant légèrement l'argument original de Davenport, on a le résultat :

THÉORÈME 3.3. *Le nombre de classes de formes cubiques irréductibles vérifiant $0\leqslant\Delta(F)\leqslant X$, $F\in S_m$, est égal, à un $O(X^{3/4+\varepsilon})$ près, à la moitié du nombre de*

points entiers appartenant à S_m contenus dans le volume C_X^+ de $\mathbb{R}^4$ défini par :

$$\begin{gathered}\Delta(a,b,c,d) \leqslant 3X,\\ |bc-9ad| \leqslant b^2-3ac \leqslant c^2-3bd,\\ a>0.\end{gathered}$$

Preuve. Voir [**13**, Lemmes 2 et 3]. Davenport considère des classes de formes cubiques strictes, *i.e.* modulo $\mathrm{SL}_2(\mathbb{Z})$, comme c'est l'usage pour les formes quadratiques. D'où l'apparition du facteur 1/2. Le $O(X^{3/4+\varepsilon})$ provient des formes réductibles dont le premier coefficient (a) est non nul, et des cas d'égalités dans les inégalités larges définissant C_X^+. □

Lemme 3.4. *Pour tout point $(a,b,c,d) \in C_X^+$, on a les majorations :*

$$\begin{aligned} |a| &< X^{1/4}, & |b| &< 2X^{1/4},\\ |ad| &< X^{1/2}, & |bc| &< 4X^{1/2},\\ |ac^3| &< 8X, & |b^3d| &< 8X,\\ c^2|bc-9ad| &< 4X. \end{aligned}$$

Preuve. C'est exactement [**13**, Lemme 1]. □

Théorème 3.5. *Le nombre de classes de formes cubiques irréductibles vérifiant $-X \leqslant \Delta(F) \leqslant 0$, $F \in S_m$, est égal, à un $O(X^{3/4+\varepsilon})$ près, à la moitié du nombre de points entiers appartenant à S_m contenus dans le volume C_X^- de $\mathbb{R}^4$ défini par :*

$$\begin{gathered}0 \leqslant -\Delta(a,b,c,d) \leqslant X,\\ d^2-a^2+ac-db \geqslant 0,\\ (a+b)(a+b+c)-ad \geqslant 0,\\ (a-b)(a-b+c)+ad \geqslant 0,\\ a>0.\end{gathered}$$

Preuve. Voir [**14**] et [**36**]. □

Aux constantes près, on a les mêmes majorations que dans le Lemme 3.4 (voir [**14**, Lemme 1]) :

Lemme 3.6. *Pour tout point $(a,b,c,d) \in C_X^-$, on a les majorations :*

$$\begin{aligned} |a| &< 2X^{1/4}, & |b| &< 3X^{1/4},\\ |ad| &< 2X^{1/2}, & |bc| &< 8X^{1/2},\\ |ac^3| &< 12X, & |b^3d| &< 12X,\\ c^2|bc-ad| &< 16X. \end{aligned}$$

Remarque 3.7. Ces deux volumes proviennent de la donnée d'un représentant "canonique" pour chaque classe de formes. On commence par associer à toute

forme cubique F un covariant quadratique, c'est-à-dire une forme quadratique binaire $Q(F)$, définie positive, telle que, pour tout $M \in \mathrm{GL}_2(\mathbb{Z})$, on ait

$$Q(F \circ M) = \lambda(F) \cdot Q(F) \circ M,$$

où $\lambda(F) \in \mathbb{C}$. On montre alors qu'il n'y a essentiellement qu'une seule forme cubique par classe dont le covariant quadratique soit réduit (au sens de la réduction des formes quadratiques définies).

Pour les classes de discriminant positif, on choisit, en suivant Hermite, le Hessien $H(F)$ pour covariant, et on impose que le premier coefficient (celui de x^3) de F soit positif. En effet, l'application $F \mapsto H(F)$ commute à l'action de $\mathrm{GL}_2(\mathbb{Z})$, donc deux formes équivalentes n'ont même Hessien que si elles diffèrent d'un automorphisme de H, *i.e.* un $g \in \mathrm{GL}_2(\mathbb{Z})$ tel que $g.H = H$. Or $\Delta = \Delta(H) = -3\Delta(F)$ et les formes quadratiques définies ont essentiellement deux automorphismes (en fait exactement autant qu'il y a d'unités dans le corps quadratique *imaginaire* $\mathbb{Q}(\sqrt{\Delta})$, c'est-à-dire 2 pour $\Delta < -4$), parmi lesquels se trouve $(x, y) \mapsto (-x, -y)$ qui change le signe de a. On obtient donc bien un unique représentant par classe, pour presque toute classe.

Par contre, dans le cas réel, les automorphismes du Hessien forment un groupe monogène infini, donc la réduction d'Hermite est inadaptée (pour tout ce qui a trait aux classes de formes quadratiques, automorphismes, réduction, nous renvoyons le lecteur au précis de Buell [**4**]). La réduction des formes de discriminant négatif (due à Mathews et Berwick, voir [**14**] et [**36**]) aboutit alors à un domaine fondamental différent.

Pour nous, le traitement sera essentiellement identique. On continuera donc la démonstration avec la notation C_X qui désignera indifféremment C_X^+ ou C_X^-. Jusqu'à la fin du §7, l'exposant $+$, resp. $-$, désignera une quantité en rapport avec les discriminants positifs, resp. négatifs ; quand ce signe ne joue pas, ou quand les résultats s'expriment identiquement modulo inversion des signes, on le remplacera par $\pm$ ou on le supprimera s'il n'y a pas d'ambiguï té.

On peut approcher le nombre de points entiers d'un compact "raisonnable" par son volume, le terme d'erreur ne faisant essentiellement intervenir que le volume de ses diverses projections sur des sous-espaces de dimension inférieure (voir [**12**]) :

THÉORÈME 3.8 (Davenport). *Soit C un compact de volume $\mathrm{Vol}(C)$ de $\mathbb{R}^n$, et soit $N(C)$ le nombre de points entiers situés dans C. On suppose que :*

- *Toute droite parallèle à l'un des axes de coordonnées intersecte C en au plus h intervalles.*
- *La même propriété reste vraie si l'on considère la projection de C sur l'un des espaces affines de dimension k d'équation $x_{i_1} = \cdots = x_{i_{n-k}} = 0$. Et ce pour tout k compris entre 1 et $n-1$.*

On note $V_k(C)$ le maximum des volumes des projections de C sur les espaces affines de dimension k définis ci-dessus ($V_0(C) = 1$ par convention). Alors on a

l'inégalité :

$$|N(C) - \mathrm{Vol}(C)| \leqslant \sum_{k=0}^{n-1} h^{n-k} \binom{n}{k} V_k(C). \tag{1}$$

Remarque 3.9. Le résultat de Davenport est plus précis : le terme $\binom{n}{k}V_k(C)$ de (1) est remplacé par la somme des volumes des projections en dimension k.

En particulier, ce théorème s'applique à tout ensemble semi-algébrique (défini par un nombre fini d'inégalités polynomiales) compact. C'est une conséquence immédiate du lemme suivant (voir par exemple [**3**, Théorème 2.3.4 et Proposition 4.4.5]) :

LEMME 3.10. *Soit $A \subset \mathbb{R}^n$ un ensemble semi-algébrique défini par*

$$\begin{cases} f_1 = \cdots = f_h = 0 \\ g_1 > 0, \ldots, g_l > 0 \end{cases}$$

- *On note d le maximum des degrés des f_i et des g_i. Alors le nombre de composantes connexes de A est fini et la borne ne dépend que de n, l et d.*
- *Si p est une projection, $p(A)$ est semi-algébrique et on peut borner uniformément le nombre et le degré des polynômes intervenant dans sa définition en fonction de ceux qui définissent A (principe de Tarski-Seidenberg).*

Ces deux bornes sont effectives.

Il se trouve que C_X n'est pas compact, quoique de volume fini. De plus, ce volume est du même ordre de grandeur que celui de sa projection sur l'hyperplan $a = 0$ (de l'ordre de X). On doit donc tronquer C_X pour pouvoir appliquer le Théorème 3.8 efficacement.

LEMME 3.11. *Soit $\rho > 0$ un nombre réel. Le nombre de points (a, b, c, d) à coordonnées entières appartenant à C_X, et vérifiant $a < X^{1/4-3\rho}$, est un $O(X^{1-\rho})$.*

PREUVE.
• $C_X = C_X^+$: c'est exactement [**13**, Lemme 4]. Ce résultat est vrai sous les seules hypothèses du Lemme 3.4.
• $C_X = C_X^-$: le calcul est identique en appliquant cette fois-ci le Lemme 3.6. □

Nous allons donc noter $C_{X,\rho}$ ($C_{X,\rho}^+$ et $C_{X,\rho}^-$ quand la distinction aura une importance) l'intersection de C_X et de la région définie par l'inégalité :

$$a \geqslant X^{1/4-3\rho}. \tag{2}$$

On appellera "pointe" la région $a < X^{1/4-3\rho}$ (la pointe à proprement parler est constituée des points où a et b sont simultanément petits).

THÉORÈME 3.12 (Davenport). *Soit $N^+(X,\rho)$, resp. $N^-(X,\rho)$, le nombre de points entiers dans le volume $C^+_{X,\rho}$, resp. $C^-_{X,\rho}$, défini ci-dessus. On note :*

$$K^+ = \frac{\pi^2}{36} \quad et \quad K^- = \frac{\pi^2}{12}.$$

On a alors l'égalité :

$$N^\pm(X,\rho) = K^\pm X + O(X^{1-\rho} + X^{3/4+3\rho}).$$

PREUVE. On reprend les calculs de Davenport. On peut borner le volume des projections de $C_{X,\rho}$ par un $O(X^{3/4+3\rho})$ (le Corollaire 4.3 montrera essentiellement $O(X^{3/4+3\rho}\log X)$, mais on peut être plus soigneux). On montre, en calquant la démonstration du Lemme 3.11, que le volume de $C_{X,\rho}$ est égal à celui de C_X à un $O(X^{1-\rho})$ près. Le volume de C_X vaut exactement KX ([**13**, erratum] pour $\Delta > 0$ et [**14**, p. 198] pour $\Delta < 0$). Le Théorème 3.8 permet alors de conclure. □

Le choix naturel que fait Davenport ($\rho = 1/16$), égalisant les deux termes d'erreur, donne un reste en $O(X^{15/16})$. Nous ferons un choix analogue en fin de démonstration.

On a en fait beaucoup mieux. Sato et Shintani [**43**] ont développé une théorie des fonctions zêta associées à certaines représentations (espaces vectoriels préhomogènes), et les premiers exemples étudiés par Shintani [**47**] sont des séries de Dirichlet dont les coefficients sont les nombres de classes de formes cubiques légèrement modifiés. Il montre l'existence de prolongements analytiques méromorphes, calcule les valeurs des résidus aux pôles (1 et 5/6), et prouve une équation fonctionnelle originale où elles interviennent toutes simultanément. Après une étude analogue des séries associées aux classes de formes quadratiques (les formes cubiques qu'il considère peuvent être réductibles), le théorème d'Ikehara suffit pour conclure, mais avec un terme d'erreur moins précis que celui de Davenport. Un théorème taubérien plus fin, essentiellement dû à Landau, modifié par Sato et Shintani ([**43**, §3]) pour tenir compte des équations fonctionnelles vérifiées par leurs fonctions zêta, permet d'obtenir le développement explicite suivant ([**48**, Théorème 4]) :

THÉORÈME 3.13 (Shintani). *Soit $X \geqslant 0$. On note $F^+(X)$, resp. $F^-(X)$, le nombre de classes de formes cubiques irréductibles, de discriminants compris entre 0 et X, resp. entre $-X$ et 0. On a l'égalité :*

$$F^\pm(X) = K^\pm X + k^\pm X^{5/6} + O(X^{2/3+\varepsilon}),$$

où k^+ et k^- sont explicites et non nuls.

Malheureusement, il semble qu'aucune démonstration élémentaire de ce résultat ne soit connue, qui ne fasse intervenir que des invariants géométriques du domaine fondamental explicite dont on dispose dans chaque cas. Comme nous avons absolument besoin de l'interprétation géométrique (notamment au §4), nous ne sommes pas en mesure d'exploiter ce résultat. Il va de soi qu'une démonstration nous permettant de remplacer notre $O(X^{15/16})$ potentiel par le $O(X^{5/6})$ optimal

améliorerait notablement les estimations du Théorème 1.2 et donc les constantes numériques présentées dans la suite.

Nous devons maintenant compter les points dont les discriminants sont fondamentaux. Davenport et Heilbronn expriment cette condition sous la forme d'une congruence modulo m, dont ils font tendre ensuite le module vers l'infini au terme d'un crible assez délicat. Comme ils n'ont pas d'uniformité sur m, ils n'obtiennent qu'une limite et pas de terme d'erreur.

Remarque 3.14. En adélisant la méthode de Shintani, Datskovsky et Wright [**11**] ont donné une généralisation des théorèmes de Davenport-Heilbronn, dénombrant les extensions cubiques de n'importe quel corps global de caractéristique différente de 2 ou 3, mais sans pouvoir obtenir autre chose qu'un équivalent, à cause d'un problème d'uniformité analogue à celui rencontré par Davenport et Heilbronn (quoique dans un cadre beaucoup moins géométrique). Sans bijection explicite avec les points entiers d'un volume généralisant $C_{X,\rho}$, il paraît difficile de généraliser les méthodes du présent article à ce contexte, et plus particulièrement celles du paragraphe suivant.

4. Congruences

Considérons un compact C de $\mathbb{R}^n$, vérifiant les hypothèses du Théorème 3.8, et un sous-ensemble S_m de $(\mathbb{Z}/m\mathbb{Z})^n$; nous voulons dénombrer les points entiers de C dont la réduction modulo m appartient à S_m. Notons

$$s(S_m, m) = \frac{|S_m|}{m^n}$$

la "densité" de S_m – on écrira $s(m)$ quand l'ensemble S_m considéré ressortira clairement du contexte. Pour tout diviseur k de m, on définit l'ensemble $S_k \subset (\mathbb{Z}/k\mathbb{Z})^n$, de cardinal $S(k)$ par réduction modulo k des éléments de S_m. On démontre facilement que $s(m)$ est multiplicative.

Lemme 4.1. *Reprenons les notations du* Théorème 3.8. *Nous désignons par* $\mathcal{N}(C, S_m)$ *le nombre des points entiers de* C *appartenant à* S_m. *Alors, on a l'inégalité :*

$$|\mathcal{N}(C, S_m) - s(m)\operatorname{Vol}(C)| \leqslant s(m) \sum_{k=0}^{n-1} (h.m)^{n-k} \binom{n}{k} V_k(C).$$

Preuve. Pour $\boldsymbol{x} \in S_m$, appliquons le Théorème 3.8 à la région $m^{-1}(C - \boldsymbol{x})$, obtenue par translation puis homothétie de rapport $1/m$ à partir de C :

$$|N(C) - m^{-n}\operatorname{Vol}(C)| \leqslant \sum_{k=0}^{n-1} h^{n-k} m^{-k} \binom{n}{k} V_k(C).$$

Il suffit de sommer sur $\boldsymbol{x} \in S_m$ pour obtenir le résultat. □

Le réseau $(m\mathbb{Z}^n)$ partage C en cubes de côté m. On définit l'épaississement $\overline{C_m}$ de C comme la réunion des cubes rencontrant C (la Figure 1 donne une idée de la situation en dimension 2).

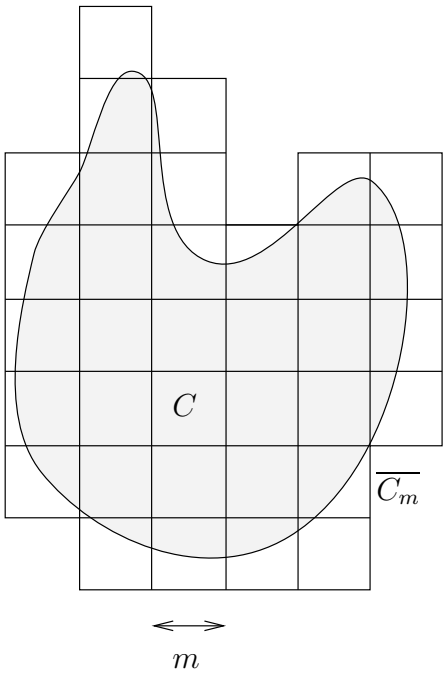


FIG. 1. Découpage de C

COROLLAIRE 4.2. *Avec les notations précédentes, on a l'inégalité :*

$$\big|\mathcal{N}(C, S_m) - s(m)\,\mathrm{Vol}(C)\big| \leqslant m\,s(m) V_{n-1}(\overline{C_m}) \cdot \big((1+h)^n - h^n\big).$$

PREUVE. Pour tout assemblage A de cubes de côté m, on a

$$m^{-k} V_k(A) \leqslant m^{-(k+1)} V_{k+1}(A).$$

En effet, les projections considérées associent à tout cube un cube de dimension inférieure, donc le nombre de cubes décroît avec la dimension. On majore les volumes de projections de C par ceux de $\overline{C_m}$ et le terme d'erreur devient

$$m\,s(m) V_{n-1}(\overline{C_m}) \sum_{k=0}^{n-1} h^{n-k} \binom{n}{k}.$$

La conclusion est alors immédiate. □

Dans le cas des formes cubiques et du volume $C_{X,\rho} \subset \mathbb{R}^4$ de Davenport, nous obtenons :

COROLLAIRE 4.3. *Le volume des projections de l'épaississement de $C_{X,\rho}$ est dominé par*

$$X^{3/4+3\rho}\log X + m^2X^{1/4+3\rho} + m^3,$$

où la constante implicite est effective.

PREUVE. La notation (a,b,c,d) désigne toujours un point de $C_{X,\rho}$. D'après les Lemmes 3.4 et 3.6, pour tout $(a,b,c,d)\in C_X$, on a

$$\begin{aligned} &a \ll X^{1/4}, && |b| \ll X^{1/4},\\ &|c| \ll X^{1/3}a^{-1/3} \ll X^{1/4+\rho}, && |c| \ll X^{1/2}|b|^{-1},\\ &|d| \ll X^{1/2}a^{-1} \ll X^{1/4+3\rho}, \end{aligned}$$

et si $b=0$, alors $ac^2|d| \ll X$. Si l'on considère un point de $C_{X,\rho}$, on a de plus $a > X^{1/4-3\rho}$. Pour $x\in\{a,b,c,d\}$, on note V_x les projections sur $x=0$ de l'épaississement $\overline{C_m}$. Comme ce sont des assemblages de cubes, d'intérieurs disjoints, aux sommets entiers, leurs volumes sont majorés par le nombre de leurs points entiers respectifs. On en tire :

$$\begin{aligned} V_a \leqslant \sum_{b,c,d} 1 \ll (X^{1/4+3\rho}+m) + &\sum_{c=1}^{X^{1/4+\rho}+m} \big(X(ac^2)^{-1}+m\big)\\ &+ \sum_{b=1}^{X^{1/4}+m} (X^{1/2}b^{-1}+m)\cdot(X^{1/4+3\rho}+m) \end{aligned}$$

(le premier terme correspond à $b=c=0$, le deuxième à $b=0$)

$$\begin{aligned} &\ll X^{3/4+3\rho}\log X + mX^{1/2+3\rho} + m^2X^{1/4+3\rho} + m^3\\ &\ll X^{3/4+3\rho}\log X + m^2X^{1/4+3\rho} + m^3, \end{aligned}$$

$$V_b \leqslant \sum_{a,c,d} 1 \ll \sum_{a=1}^{X^{1/4}+m} (X^{1/2}a^{-1}+m) \sum_{c=1}^{X^{1/4+\rho}+m} 1 \ll V_a,$$

$$V_c \leqslant \sum_{a,b,d} 1 \ll \sum_{a=1}^{X^{1/4}+m} (X^{1/2}a^{-1}+m) \sum_{b=1}^{X^{1/4}+m} 1 \ll V_b,$$

$$V_d \leqslant \sum_{a,b,c} 1 \ll (X^{1/4}+m)^2(X^{1/4+\rho}+m) \ll V_b.$$

D'où la conclusion. □

Globalement, nous obtenons donc :

PROPOSITION 4.4. *Le nombre de points entiers de $C_{X,\rho}$ appartenant à S_m vaut :*

$$s(m) \cdot N(X,\rho) + O\big(s(m) \cdot E(X,\rho,m)\big), \tag{3}$$

où $N(X,\rho)$ a été évalué au Théorème 3.12. et

$$E(X,\rho,m) = m(X^{3/4+3\rho} \log X + m^2 X^{1/4+3\rho} + m^3). \tag{4}$$

Remarque 4.5. Si $m = o(X^{1/4})$, on obtient $E \ll mX^{3/4+3\rho+\varepsilon}$. Ceci revient à s'assurer que (3) a bien un sens, c'est-à-dire qu'on a l'égalité

$$s(m) \cdot mX^{3/4} = o[s(m) \cdot N(X,\rho)].$$

D'autre part, si l'on raisonne en termes de cubes, il paraît naturel d'imposer que ceux-ci soient petits devant les dimensions de la variété (qui est essentiellement l'homothétique de rapport $X^{1/4}$ d'une variété fixe). En fait, une technique de séries de Fourier va nous permettre au §5 de diminuer artificiellement le module m de la congruence, donc le reste de notre expression, dans le cas particulier qui nous intéresse (formes dont le discriminant est fondamental et divisible par q).

Dans le lemme suivant, nous transcrivons dans nos notations les résultats de densités locales obtenues par Davenport et Heilbronn [**16**, partie 3] :

LEMME 4.6. *Pour tout p premier on a les densités :*

$$\begin{aligned}
s\left(\{F \bmod p, p \nmid F, p \mid \Delta(F)\}, p\right) &= (p+1)(p^2-1)/p^4, \\
s\left(\{F \bmod p^\alpha, p \nmid F, F \in V_p\}, p^\alpha\right) &= (p^2-1)^2/p^4, \\
s\left(\{F \bmod p^\alpha, p \nmid F, F \notin V_p\}, p^\alpha\right) &= 2(p^2-1)/p^4, \\
s\left(\{F \bmod p^\alpha, F \notin V_p\}, p^\alpha\right) &= (2p^2-1)/p^4,
\end{aligned}$$

où $\alpha = 2$ pour $p \neq 2$, et 4 sinon.

PREUVE. Davenport et Heilbronn calculaient des densités en se restreignant aux formes non divisibles par p, alors que nous avons défini nos densités en considérant toutes les formes modulo p^α ; pour passer de leurs densités aux nôtres, il suffit de les multiplier par $(1-p^{-4})$. La première égalité provient alors de [**16**, Lemme 1] : on additionne simplement les contributions de toutes les formes où p se ramifie dans le corps de décomposition de F, c'est-à-dire les deux dernières égalités du lemme. La seconde correspond exactement au [**16**, Lemme 4] et les deux dernières sont des corollaires immédiats. □

5. Sommes exponentielles

Revenons un instant sur le cheminement qui, du Lemme 4.1 et son Corollaire 4.2, à la Proposition 4.4, nous a permis de démontrer (3) : supposons que, pour un entier $v < m$, nous sachions évaluer le cardinal des points appartenant à S_m dans un cube de coté v, et non plus m. Supposons de plus que ce cardinal soit proche de $v^n|S_m|$, c'est-à-dire qu'on garde essentiellement la même densité.

Le même raisonnement nous permettrait alors d'écrire l'équation avec un terme d'erreur $E(X,\rho,v) < E(X,\rho,m)$. Nous allons voir que tout ceci est possible, avec

$$v = m^{1+\varepsilon}\prod_{p|m} p^{-1/4}.$$

Soient, donc, u et v deux entiers et $\chi_{u,v}$ la fonction caractéristique des entiers de l'intervalle $[u, u+v[$. Développons-la en série de Fourier :

$$\chi_{u,v}(a) = \frac{1}{m}\sum_{x=u}^{u+v-1}\sum_{h=0}^{m-1} e[h(a-x)/m].$$

Soit $\boldsymbol{u} = (u_1,u_2,u_3,u_4)$ et $\boldsymbol{x} = (x_1,x_2,x_3,x_4)$; on note

$$\chi_{\boldsymbol{u},v}(\boldsymbol{x}) = \prod_{i=1}^{4}\chi_{u_i,v}(x_i)$$

la fonction caractéristique des points entiers d'un cube de côté v dont les sommets sont à coordonnées entières (données par $\boldsymbol{u}$). Nous voulons évaluer le nombre de points appartenant à S_m dans un tel cube, soit :

$$\begin{aligned} F(\boldsymbol{u},v) &= \sum_{\boldsymbol{A}\in S_m}\chi_{\boldsymbol{u},v}(\boldsymbol{A}) \\ &= \frac{1}{m^4}\sum_{\boldsymbol{x}}\sum_{\boldsymbol{h}} e(-\boldsymbol{x}.\boldsymbol{h}/m)\sigma(\boldsymbol{h},m), \end{aligned}$$

où

$$\sigma(\boldsymbol{h},m) = \sum_{\boldsymbol{A}\in S_m} e(\boldsymbol{A}.\boldsymbol{h}/m).$$

En $\boldsymbol{h} = (0,0,0,0)$, on obtient $s(m)v^4$ qui serait le résultat exact si la distribution des points de S_m était uniforme. Remarquons que si h est non nul, alors

$$\Big|\sum_x e(-xh/m)\Big| \leqslant \frac{1}{\sin(\pi h/m)},$$

qui est majoré par $m/(2h)$ si $h \leqslant \frac{1}{2}m$, et par $m/[2(m-h)]$ sinon. Cette même somme vaut v si $h = 0$. Donc

$$\Big|\sum_h\sum_x e(-xh/m)\Big| \ll v + m\log m \ll m\log m.$$

Supposons que l'on sache majorer $|\sigma(\boldsymbol{h},m)|$ par $\sigma(m)$ pour tout $\boldsymbol{h}$ non nul modulo m. Nous obtenons

$$F(\boldsymbol{u},v) = s(m)v^4 + O(\sigma(m)log^4 m). \tag{5}$$

Simplifions d'abord notre problème : nous aurons uniquement besoin des m de la forme

$$\prod p^{\alpha_p}\ (\alpha_p \leqslant 2 \text{ si } p \neq 2,\ \alpha_2 \leqslant 4),$$

et S_m défini par

$$\text{“ } p \nmid \boldsymbol{A} \text{ et } \Delta(\boldsymbol{A}) \equiv 0 \pmod{p^{\alpha_p}} \text{ pour tout } p \mid m \text{ ”}$$

ou par

$$\text{“ } \Delta(\boldsymbol{A}) \equiv 0 \pmod{p^2} \text{ ”}.$$

Nous supposerons dorénavant que nous sommes dans cette situation précise. Le Lemme 4.6 assure alors

$$p^{-\alpha} \leqslant s(p^\alpha) \leqslant 2p^{-\alpha} \ (p > 2),$$

soit

$$1 \ll m \cdot s(m) \ll 2^{\omega(m)} \ll m^\varepsilon.$$

LEMME 5.1. *La fonction $\sigma(\boldsymbol{h}, m)$ est multiplicative en m.*

PREUVE. Soit $m = kl$, avec $(k, l) = 1$. On choisit u et v dans $\mathbb{Z}$ tels que $uk + vl = 1$. Alors tout $\boldsymbol{A}$ de $(\mathbb{Z}/kl\mathbb{Z})^4$ s'écrit de façon unique sous la forme :

$$\boldsymbol{A} = uk\boldsymbol{A}_l + vl\boldsymbol{A}_k,$$

où $\boldsymbol{A} \in (\mathbb{Z}/kl\mathbb{Z})^4$, $\boldsymbol{A}_l \in (\mathbb{Z}/l\mathbb{Z})^4$ et $\boldsymbol{A}_k \in (\mathbb{Z}/k\mathbb{Z})^4$. Alors

$$\begin{aligned}
\sigma(\boldsymbol{h}, kl) &= \sum_{\boldsymbol{A} \in S_{kl}} e[\boldsymbol{h}.(uk\boldsymbol{A}_l + vl\boldsymbol{A}_k)/kl] \\
&= \sum_{\boldsymbol{A}_k \in S_k} e(v\boldsymbol{h}.\boldsymbol{A}_k/k) \sum_{\boldsymbol{A}_l \in S_l} e(u\boldsymbol{h}.\boldsymbol{A}_l/l) \\
&= \sigma(\boldsymbol{h}, k)\sigma(\boldsymbol{h}, l)
\end{aligned}$$

car u (resp. v) est inversible modulo l (resp. k) et donc $\boldsymbol{A} \in S_l$ (resp. S_k) si et seulement si $u\boldsymbol{A} \in S_l$ (resp. $v\boldsymbol{A} \in S_k$). □

Remarque 5.2. Le lemme est faux si l'on ne suppose pas S_m stable par homothétie de rapport premier à m. Ici, avec les restrictions que nous venons d'adopter, c'est évidemment le cas.

Il nous reste à évaluer $\sigma(\boldsymbol{h}, p^\alpha)$ pour tous les diviseurs premiers p de m. On a facilement

$$|\sigma(\boldsymbol{h}, p^\alpha)| \leqslant \sigma(0, p^\alpha) \leqslant 2p^{3\alpha}$$

donc $\sigma(p^\alpha) = 2p^{3\alpha}$ convient, mais n'est guère satisfaisant. En effet, au vu de (5), la méthode n'a d'intérêt que si $\sigma(m) \log^4 m \ll s(m)m^{4-\varepsilon}$, soit justement $\sigma(m) \ll m^{3-\varepsilon}$.

PROPOSITION 5.3. *Si $p \nmid \boldsymbol{h}$, $p > 3$, $\alpha \in \{1, 2\}$, alors*

$$|\sigma(\boldsymbol{h}, p^\alpha)| \leqslant 4p^{3\alpha-1}.$$

PREUVE.

• On commence par traiter le cas $\alpha = 1$: le discriminant Δ est un polynôme homogène de degré 4. Considérons ses racines non triviales dans $\mathbb{F}_p^4$, c'est-à-dire dont au moins une coordonnée n'est pas nulle (à cause de la condition $p \nmid F$). Par homogénéité, les racines sont alignées sur un ensemble de droites passant par 0,

contenant toutes $p-1$ solutions non triviales. Notons Δ_1, resp. Δ_2, un système de représentants des droites de $\mathbb{F}_p^4$ contenant ces solutions, et telles que

$$\boldsymbol{A}.\boldsymbol{h} \neq 0 \pmod p, \text{ resp. } \boldsymbol{A}.\boldsymbol{h} = 0 \pmod p,$$

pour toute solution $\boldsymbol{A}$ non triviale. Alors

$$\sigma(\boldsymbol{h}, p) = \sum_{\Delta_1} \sum_{\lambda \in \mathbb{F}_p^*} e\Big(\frac{\lambda \boldsymbol{A}.\boldsymbol{h}}{p}\Big) + \sum_{\Delta_2} (p-1).$$

La somme intérieure sur λ est une progression géométrique de raison $e(\boldsymbol{A}.\boldsymbol{h}/p) \neq 1$, soit

$$\sigma(\boldsymbol{h}, p) = -\frac{1}{p-1} \#\{\boldsymbol{A} \in \mathbb{F}_p^4,\ p \nmid \boldsymbol{A},\ \Delta(\boldsymbol{A}) = 0,\ \boldsymbol{A}.\boldsymbol{h} \neq 0\} + \#\{\boldsymbol{A} \in \mathbb{F}_p^4,\ p \nmid \boldsymbol{A},\ \Delta(\boldsymbol{A}) = 0,\ \boldsymbol{A}.\boldsymbol{h} = 0\}.$$

D'après le Lemme 4.6, le premier terme est majoré en valeur absolue par

$$(p-1)^{-1} \cdot (p+1)(p^2-1) = (p+1)^2.$$

Évaluons maintenant le deuxième terme : une des coordonnées de $\boldsymbol{h}$ étant non nulle, l'équation $\boldsymbol{A}.\boldsymbol{h} = 0$ permet d'exprimer la coordonnée correspondante de $\boldsymbol{A}$ en fonction des trois autres. En substituant cette valeur dans l'équation $\Delta(\boldsymbol{A}) = 0$, on obtient une équation polynomiale modulo p, homogène, en trois variables, de degré au plus 4. Elle est non nulle : en effet, supposons l'existence d'un facteur linéaire, à coefficients entiers, $\alpha a + \beta b + \gamma c + \delta d$ dans Δ et considérons le quotient. Si $\alpha \neq 0$, son degré en a est exactement 1 et un calcul explicite montre qu'on ne peut pas obtenir le facteur $27a^2d^2$. On montre de même que δ est nul. Tous les facteurs de Δ seraient alors des multiples de b ou c, ce qui n'est manifestement pas le cas.

Une telle équation sur le corps $\mathbb{F}_p$ a au plus $4p^2$ solutions. En effet, soit un polynôme P homogène de degré d, en k variables, irréductible ; on fixe $k-1$ variables : nous obtenons un polynôme non nul en une variable, de degré au plus d qui a donc au plus d racines sur $\mathbb{F}_p$. On en déduit que P a au plus $d.p^{k-1}$ racines. Si maintenant P n'est pas irréductible sur $\mathbb{F}_p$, on le décompose en produit de P_i irréductibles de degré d_i ayant chacun au plus $d_i p^{k-1}$ racines et P en possède alors au plus $\sum d_i p^{k-1} = dp^{k-1}$.

Nous majorons donc $|\sigma(\boldsymbol{h}, p)|$ par $4p^2$.

• Cas $\alpha = 2$: On peut écrire tout élément de $(\mathbb{Z}/p^2\mathbb{Z})^4$ sous la forme $\boldsymbol{A}_0 + p\boldsymbol{A}_1$, où les coordonnées de $\boldsymbol{A}_0$ et $\boldsymbol{A}_1$ sont dans $[0, p-1]$. La formule de Taylor donne

$$\Delta(\boldsymbol{A}_0 + p\boldsymbol{A}_1) = \Delta(\boldsymbol{A}_0) + p\boldsymbol{A}_1.\operatorname{grad}_{\boldsymbol{A}_0} \Delta \pmod{p^2}.$$

Si $\Delta(\boldsymbol{A}_0) = 0 \pmod p$, on note $H_{\boldsymbol{A}_0}$ le sous-espace vectoriel de $\mathbb{F}_p^4$ défini par l'équation linéaire :

$$\boldsymbol{A}.\operatorname{grad}_{\boldsymbol{A}_0} \Delta = \frac{-\Delta(\boldsymbol{A}_0)}{p}.$$

C'est un hyperplan, sauf si $\boldsymbol{A}_0$ est singulier, auquel cas $H_{\boldsymbol{A}_0} = \emptyset$ ou $\mathbb{F}_p^4$. Nous écrivons

$$\sigma(\boldsymbol{h}, p^2) = \sum_{\substack{\Delta(\boldsymbol{A}_0)=0 \ (p) \\ (p \nmid \boldsymbol{A}_0)}} e\Big(\frac{\boldsymbol{A}_0.\boldsymbol{h}}{p^2}\Big) \sum_{\boldsymbol{A}_1 \in H_{\boldsymbol{A}_0}} e\Big(\frac{\boldsymbol{A}_1.\boldsymbol{h}}{p}\Big).$$

La deuxième somme est nulle sauf si $\operatorname{grad}_{\boldsymbol{A}_0} \Delta \neq 0 \pmod p$ et $\operatorname{grad}_{\boldsymbol{A}_0} \Delta = \lambda \boldsymbol{h}$, avec $\lambda \in \mathbb{F}_p^*$. Comme le gradient est nul quand p divise $\boldsymbol{A}_0$, la condition $(p \nmid \boldsymbol{A}_0)$ ne change rien dans l'évaluation de $\sigma(\boldsymbol{h}, p^2)$ et nous pouvons supposer, d'une part, que $\boldsymbol{A}_0$ est non singulier, et d'autre part, que $\boldsymbol{h}$ et $\operatorname{grad}_{\boldsymbol{A}_0} \Delta$ sont colinéaires. Alors, la relation d'Euler

$$\boldsymbol{A}_0 . \operatorname{grad}_{\boldsymbol{A}_0} \Delta = 4\Delta(\boldsymbol{A}_0)$$

impose $\boldsymbol{A}_0.\boldsymbol{h} = 0 \pmod p$. D'après le cas $\alpha = 1$, il y a au plus $4p^2$ solutions pour $\boldsymbol{A}_0$ et nous pouvons majorer $|\sigma(\boldsymbol{h}, p^2)|$ par $4p^5$.

D'où le résultat annoncé. □

Remarque 5.4. On peut montrer ([**33**, Théorème 5.7.0])

$$|\sigma(\boldsymbol{h}, p)| \leqslant C p^{3/2}$$

pour presque tout $\boldsymbol{h}$ (sauf sur un fermé de Zariski), avec C une constante absolue. Ou encore (voir [**32**]) que

$$p^{-4} \sum_{\boldsymbol{h} \in \mathbb{F}_p^4} |\sigma(\boldsymbol{h}, p)| \leqslant p^{3/2}.$$

Ces résultats sont nettement plus profonds que les techniques rudimentaires employées ci-dessus, mais ne permettent pas de majorer $F(\boldsymbol{u}, v)$ de façon raisonnable, même quand $\alpha = 1$. Nous devons donc nous contenter de notre $p^{3\alpha-1}$ et perdre un facteur $p^{1/2}$ par rapport au résultat optimal.

En fait, (5) n'est pas satisfaisante puisque $\boldsymbol{h}$ peut être nul modulo presque tous les diviseurs de m sans toutefois être nul modulo m. Donc on n'aura pas de majoration uniforme convenable. Il faut détailler un peu plus : on note $d \mid\mid \boldsymbol{h}$ si $\boldsymbol{h} = 0 \pmod d$ et $\boldsymbol{h}/d$ non nul modulo tout diviseur de m/d, *i.e.* si d est le pgcd des coordonnées de $\boldsymbol{h}$. Nous reprenons le calcul en utilisant les inégalités $v < m$

et $\omega(m) \ll \log m/\log\log m$:

$$\begin{aligned}
F(\boldsymbol{u},v) - s(m)v^4 &= m^{-4}\sum_{\substack{d|m\\ d\neq m}}\sum_{\boldsymbol{h},d||\boldsymbol{h}}\sum_{\boldsymbol{x}} e(-\boldsymbol{x}.\boldsymbol{h}/m)\prod_{p|d}\sigma(\boldsymbol{h},p^{\alpha_p})\prod_{p\nmid d,p|m}\sigma(\boldsymbol{h},p^{\alpha_p})\\
&\ll m^{-4}\sum_{d|m}[(v+\frac{m\log m}{d})^4 - v^4]\prod_{p|6d}\sigma(0,p^{\alpha_p})\max_{\boldsymbol{h}}\prod_{p\nmid 6d,p|m}|\sigma(\boldsymbol{h},p^{\alpha_p})|\\
&\ll m^{-4}\sum_{d|m}(v^3 m\frac{\log m}{d} + m^4\frac{\log^4 m}{d^4})\prod_{p|m}4p^{3\alpha_p-1}\prod_{p|d}p\\
&\ll 4^{\omega(m)}\log^4 m\prod_{p|m}p^{3\alpha_p-1}\\
&\ll m^{3+\varepsilon}\prod_{p|m}p^{-1}.
\end{aligned}$$

Pour ε suffisamment petit, on pose

$$v = m^{1+\varepsilon}\prod_{p|m}p^{-1/4} < m.$$

Nous pouvons supposer que ce v est entier et reprendre le raisonnement du début du §4 en appliquant une homothétie de rapport v^{-1} à $C_{X,\rho} - \boldsymbol{x}$. Le nombre de points entiers de $C_{X,\rho}$ appartenant à S_m vaut :

$$\begin{aligned}
&\frac{s(m)v^4 + O\Big(m^{3+\varepsilon}\prod_{p|m}p^{-1}\Big)}{v^4}\cdot\Big(N(X,\rho) + O\big(E(X,\rho,v)\big)\Big)\\
&\qquad = s(m)\cdot N(X,\rho) + O\Big(\frac{E(X,\rho,v)}{m^{1-\varepsilon}} + \frac{X}{m^{1+\varepsilon}}\Big)
\end{aligned}$$

en utilisant $N(X,\rho) \ll X$ et $s(m) \ll m^{\varepsilon-1}$. En remplaçant E par sa valeur (4), nous obtenons :

$$s(m)\cdot N(X,\rho) + O\Big(\frac{X}{m^{1+\varepsilon}} + E_1(X,\rho,m)\Big),$$

avec

$$E_1(X,\rho,m) = X^{\varepsilon}\Big(X^{3/4+3\rho}\prod_{p|m}p^{-1/4} + X^{1/4+3\rho}m^2\prod_{p|m}p^{-3/4} + m^3\prod_{p|m}p^{-1}\Big).$$

Si $m = o(X^{\varepsilon})$ pour tout $\varepsilon > 0$, on reprend le terme d'erreur initial de la Proposition 4.4, soit

$$s(m)E(X,\rho,m) \ll X^{1-\varepsilon}/m^{1+\varepsilon},$$

si ε est assez petit. Notons $E_2(X,\rho,m) = X^{1-\varepsilon}m^{-1-\varepsilon}$; nous avons finalement montré :

PROPOSITION 5.5. *On suppose que S_m vérifie les conditions énoncées en début du §5. On note $N^{\pm}(X,\rho,m)$ le nombre de points entiers de $C^{\pm}_{X,\rho}$ appartenant à S_m et E_1, E_2 comme ci-dessus. On a l'égalité :*

$$N^{\pm}(X,\rho,m) = s(m)N^{\pm}(X,\rho) + O(E_1(X,\rho,m) + E_2(X,\rho,m)). \tag{6}$$

6. Dénombrements préliminaires

LEMME 6.1. *Soient q,r deux entiers positifs sans facteurs carrés, et Q un multiple de q premier à r. On note $f^{\pm}(Q,q,r)$ le nombre de points entiers F de $C^{\pm}_{X,\rho}$ dont le discriminant vérifie :*

- *q divise Δ,*
- *$\Delta \in V_Q$,*
- *pour tout p premier divisant r, $\Delta \notin V_p$.*

Alors, on a

$$f(Q,q,r) = N(X,\rho)\prod_{p\mid q}\frac{1}{p+1}\prod_{p\mid r}\frac{2p^2-1}{p^4}\prod_{p\mid Q}\frac{(p^2-1)^2}{p^4}$$

$$+O\left[\sum_{k=0}^{\omega(Q)}\sum_{\substack{p_1<\cdots<p_k\\ p_i\mid Q}}(E_1+E_2)\Big(X,\rho,\frac{qr^2(p_1\dots p_k)^2}{(q,p_1\dots p_k)}\Big)\right].$$

PREUVE. C'est un simple procédé de comptage à l'aide du Lemme 4.6 et de la Proposition 5.5. Avec les notations de cette dernière, nous avons $m=(Qr)^2$. On obtient donc

$$N(X,\rho)\prod_{p\mid q}\frac{(p^2-1)(p+1)}{p^4}\prod_{p\mid r}\frac{2p^2-1}{p^4} + (E_1+E_2)(X,\rho,qr^2)$$

points entiers vérifiant $q \mid \Delta$, $p \nmid F$ pour tout $p \mid q$, et $\Delta \notin V_p$, $\forall p \mid r$. On veut retrancher les classes vérifiant de surcroît la condition "il existe $p \mid Q$ avec $\Delta \notin V_p$". Par inclusion-exclusion, il y en a :

$$\sum_k (-1)^{k-1}\sum_{\substack{p_1<\cdots<p_k\\ p_i\mid Q}}\#\Big\{F : q \mid \Delta; F \notin V_{p_1}\cup\cdots\cup V_{p_k}\cup\bigcup_{p\mid r}V_p\Big\}.$$

Donc, en faisant la distinction entre $p_i \mid q$, qui implique $p_i \nmid F$, et $p_i \mid Q$, $(p_i, q) = 1$, $f(Q, q, r)$ vaut :

$$N(X,\rho) \prod_{p|q} \frac{(p^2-1)(p+1)}{p^4} \prod_{p|r} \frac{2p^2-1}{p^4}$$
$$\times \Big[1 - \sum_{k \leqslant \omega(Q)} (-1)^{k-1} \sum_{\substack{p_1 < \cdots < p_k \\ p_i | Q}} \prod_{p_i | q} \frac{p^4}{(p^2-1)(p+1)} . \frac{2(p^2-1)}{p^4} \prod_{(p_i,q)=1} \frac{2p^2-1}{p^4}\Big]$$
$$+ O\Big[\sum_k \sum_{p_i} (E_1 + E_2)\Big(X, \rho, \frac{qr^2(p_1 \dots p_k)^2}{(q, p_1 \dots p_k)}\Big)\Big].$$

La partie entre crochets du terme principal vaut

$$1 + \sum_k \sum_{p_i} \prod_{p_i|q} \frac{-2}{p+1} \prod_{(p_i,q)=1} \frac{-(2p^2-1)}{p^4} = \prod_{p|(q,Q)} (1 - \frac{2}{p+1}) \prod_{\substack{p|Q \\ (p,q)=1}} (1 - \frac{2p^2-1}{p^4})$$
$$= \prod_{p|Q} \frac{(p^2-1)^2}{p^4} \prod_{p|q} \frac{p^4(p-1)}{(p+1)(p^2-1)^2},$$

et l'on calcule

$$\prod_{p|q} \frac{(p^2-1)(p+1)}{p^4} \cdot \frac{p^4(p-1)}{(p+1)(p^2-1)^2} = \prod_{p|q} \frac{1}{p+1}.$$

□

Corollaire 6.2. *On note P_Y le produit des nombres premiers inférieurs à Y, avec $Y = \log X / \log_3 X$. Alors, on a l'égalité :*

$$f(qP_Y, q, r) = \frac{N(X,\rho)}{\zeta^2(2)} \prod_{p|q} \frac{1}{p+1} \prod_{p|r} \frac{2p^2-1}{p^4} \Big(1 + \sum_{\substack{p>Y \\ (p,q)=1}} \frac{2}{p^2} + O(Y^{-3})\Big)$$
$$+ O\Big(X^{3/4+3\rho+\varepsilon}(qr)^{-1/4} + X^{1/4+3\rho+\varepsilon}(rq)^{13/4} + X^{\varepsilon}(qr)^5 + X^{1-\varepsilon}(qr^2)^{-1}\Big).$$

Remarque 6.3. Nous n'utiliserons ce résultat que dans les deux cas suivants :

- $qr \ll X^{1/7-\varepsilon}$, auquel cas

$$X^{1/4+3\rho+\varepsilon}(rq)^{13/4} + X^{\varepsilon}(qr)^5 \ll X^{3/4+3\rho+\varepsilon}(qr)^{-1/4}. \tag{7}$$

- $\rho = \varepsilon$ et $X^{1/7-\varepsilon} \ll qr$, ce qui implique

$$X^{1/4+3\rho+\varepsilon}(rq)^{13/4} + X^{3/4+3\rho+\varepsilon}(qr)^{-1/4} \ll X^{\varepsilon}(qr)^5. \tag{8}$$

En particulier, le terme médian $X^{1/4+3\rho+\varepsilon}(rq)^{13/4}$ sera toujours négligeable.

PREUVE. Rappelons que nous avons posé $E_2(X,\rho,m) = X^{1-\varepsilon}/m^{1+\varepsilon}$ et

$$E_1(X,\rho,m) = X^{\varepsilon}\Big(X^{3/4+3\rho}\prod_{p|m}p^{-1/4} + X^{1/4+3\rho}m^2\prod_{p|m}p^{-3/4} + m^3\prod_{p|m}p^{-1}\Big).$$

On calcule alors :

$$\begin{aligned}\sum_k \sum_{p_i|qP_Y} E_1\Big(X,&\rho,\frac{qr^2(p_1\dots p_k)^2}{(q,p_1\dots p_k)}\Big)\\ &\ll X^{\varepsilon}\Big(X^{3/4+3\rho}(qr)^{-1/4}\prod_{p|P_Y}(1+p^{-1/4})\\ &\quad + X^{1/4+3\rho}(qr)^{4-3/4}\prod_{p|P_Y}(1+p^{4-3/4}) + (qr)^{6-1}\cdot\prod_{p|P_Y}(1+p^{6-1})\Big)\\ &\ll X^{\varepsilon}(X^{3/4+3\rho}(qr)^{-1/4} + X^{1/4+3\rho}(qr)^{13/4} + (rq)^5),\end{aligned}$$

$$\begin{aligned}\sum_k \sum_{p_i|qP_Y} E_2\Big(X,&\rho,\frac{qr^2(p_1\dots p_k)^2}{(q,p_1\dots p_k)}\Big)\\ &= X^{1-\varepsilon}(qr^2)^{-1-\varepsilon}\prod_{p|qP_Y}\Big(1+\Big(\frac{(q,p)}{p^2}\Big)^{1+\varepsilon}\Big)\\ &\ll X^{1-\varepsilon}(qr^2)^{-1-\varepsilon},\end{aligned}$$

en utilisant $2^{\omega(q)} = o(X^{\varepsilon})$ et, pour tout k fixé,

$$\prod_{p|P_Y} p^k = o(X^{\varepsilon}).$$

Le terme d'erreur est donc dominé par

$$X^{\varepsilon}(X^{3/4+3\rho}(qr)^{-1/4} + X^{1/4+3\rho}(qr)^{13/4} + (qr)^5) + X^{1-\varepsilon}(qr^2)^{-1}.$$

Le terme principal s'obtient immédiatement en écrivant :

$$\prod_{p|qP_Y}\frac{(p^2-1)^2}{p^4} = \prod_p \frac{(p^2-1)^2}{p^4}\cdot\prod_{\substack{p>Y\\(p,q)=1}}\frac{p^4}{(p^2-1)^2},$$

puis en remarquant que :

$$\prod_p \frac{(p^2-1)^2}{p^4} = \frac{1}{\zeta^2(2)}$$

et finalement

$$\prod_{\substack{p>Y\\(p,q)=1}} \frac{p^4}{(p^2-1)^2} = \exp\Big(\sum_{\substack{p>Y\\(p,q)=1}} -2\log(1-1/p^2)\Big)$$
$$= 1 + \Big(\sum_{\substack{p>Y\\(p,q)=1}} 2/p^2 + O\Big(\sum_{p>Y} 1/p^4\Big)\Big).$$

□

Il ne nous manque plus qu'un dernier lemme et nous pourrons conclure :

LEMME 6.4. *Soit $q \leqslant X^{1/3-\varepsilon}$, sans facteurs carrés. Le nombre de classes de formes cubiques binaires, irréductibles, de discriminant Δ compris entre $-X$ et X, divisible par qp^2 et appartenant à V_q, est dominé par*

$$O\Big(\frac{X}{q^{1-\varepsilon}p^2} + \frac{X^{15/16+\varepsilon}}{q^{1/16}p^{30/16}}\Big).$$

PREUVE. Commençons par remarquer qu'il suffit de démontrer le théorème pour les classes primitives. On reprend [**16**, Proposition 1] où Davenport et Heilbronn démontrent que, pour $q = 1$, cette quantité est un $O(X/p^2)$. Ils commencent par compter les classes de formes F de Hessiens H réductibles (Lemme 8). Un tel Hessien aurait pour discriminant -3Δ qui serait donc un carré (dans $\mathbb{Z}$), soit $\Delta = -3\alpha^2$, avec $\alpha \in \mathbb{N}$ et $q \mid \Delta$. Alors $-3\alpha^2 \in V_l$ pour tout $l \mid q$, ce qui impose $q = 3$ ou $q = 1$. On utilise alors la majoration de Davenport-Heilbronn pour obtenir un $O(X/qp^2)$.

Nous considérons ensuite les Hessiens irréductibles, de la forme MH_1, où $M \in \mathbb{Z}$ et H_1 est primitive de discriminant $f^2\Delta$, avec Δ fondamental. Davenport et Heilbronn montrent qu'il y a au plus $O(\tau(M))$ classes de formes cubiques de Hessien MH_1 donné ([**16**, Lemme 9]). Puis au plus $O(\tau(M)3^{\omega(f)}h_3^*(\Delta))$ classes de Hessiens MH_1 ([**16**, Lemme 10]). On peut supposer $p > 2$; alors nos hypothèses impliquent $p \mid Mf$ et $q \mid \Delta$. Donc, le nombre de classes de formes cherché est dominé par

$$\sum_{\substack{M,f<X\\p\mid Mf}} M^\varepsilon f^\varepsilon \sum_{\substack{|\Delta|<\frac{X}{3M^2f^2}\\q\mid\Delta}} h_3^*(\Delta).$$

On note

$$S(X,q) = \sum_{|\Delta|<X, q\mid\Delta} [h_3^*(\Delta) - 1].$$

On majore S par le nombre de classes de formes F vérifiant $p \nmid F$ pour tout $p \mid q$, q divise $\Delta(F)$, et $|\Delta(F)| \leqslant X$. C'est-à-dire, en utilisant les Lemmes 3.11 et 4.6, le Théorème 3.12, et enfin la Proposition 5.5 :

$$O\Big(X^{1-\rho} + X\prod_{p\mid q}\frac{(p+1)(p^2-1)}{p^4} + X^{3/4+\varepsilon} + (E_2+E_1)(X,\rho,q)\Big).$$

On obtient

$$S(X,q) \ll X^{1-\rho} + X/q^{1-\varepsilon} + X^{1-\varepsilon}/q + \\ X^{3/4+3\rho+\varepsilon}q^{-1/4} + X^{1/4+3\rho+\varepsilon}q^{5/4} + X^{\varepsilon}q^2.$$

Si $q \ll X^{1/3-\varepsilon}$, les deux derniers termes sont petits devant l'anté-pénultième. On choisit $X^\rho = (Xq)^{1/16}$, ce qui rend le terme en $X^{3/4+\varepsilon}$ négligeable devant $X^{1-\rho}$ et l'on calcule :

$$S(X,q) \ll X/q^{1-\varepsilon} + X^{15/16+\varepsilon}q^{-1/16}.$$

La fin du calcul est facile. □

Remarque 6.5. A cause de ce dernier lemme nous devions mener simultanément les calculs concernant discriminants positifs et négatifs. En effet, les signes des discriminants d'une forme cubique et de son Hessien sont opposés, donc, si l'on désire se limiter à un signe fixé, la majoration fait intervenir les formes de discriminant opposé. La démonstration de Davenport-Heilbronn assure que ce terme est un $O(X/p^2)$; on a fait un peu mieux, sans toutefois atteindre l'ordre de grandeur espéré : X/p^2q.

7. Théorèmes d'équirépartition

On désigne par $\Delta^+(X)$ (resp. $\Delta^-(X)$) l'ensemble des discriminants fondamentaux positifs (resp. négatifs), inférieurs à X en valeur absolue. Notons $S^{\pm}_{X,q}$ l'ensemble des points entiers de $C^{\pm}_X$ appartenant à V, donc primitifs, et tels que q divise Δ. Les Théorèmes 3.3 et 3.5 assurent :

$$|S_{X,q}| = 2 \sum_{\substack{\Delta\in\Delta(X)\\ q|\Delta}} \frac{h_3^*(\Delta)-1}{2} + O(X^{3/4+\varepsilon}).$$

On fixe $\varepsilon > 0$ et on note

- $A^{\pm}_{X,q,\varepsilon}$ l'ensemble des points F de $C^{\pm}_{X,\varepsilon}$ appartenant à V, et tels que q divise $\Delta(F)$.
- $B^{\pm}_{X,q,\varepsilon}$ l'ensemble des points F de $C^{\pm}_X$ tels que $q \mid \Delta(F)$, appartenant à V_p pour tout les p inférieurs à X^ε ou divisant q.

On a trivialement $A_{X,q,\varepsilon} \subset S(X,q) \subset B_{X,q,\varepsilon}$.

Théorème 7.1. *Soit $\varepsilon > 0$, $Q_B = X^{1/15-\varepsilon}$, et q un entier inférieur à Q_B sans facteurs carrés. On a l'égalité*

$$\left|B^{\pm}_{X,q,\varepsilon}\right| = \frac{K^{\pm}}{\zeta^2(2)} X \prod_{p|q} \frac{1}{p+1} + R^{\pm}_B(X,q,\varepsilon),$$

où le terme d'erreur vérifie :

$$\sum_{q=1}^{Q_B} \left|R^{\pm}_B(X,q,\varepsilon)\right| = o(X/\log X).$$

Remarque 7.2. Notons

$$L(X,q,\varepsilon)=\frac{X}{q\log^2 X\log_2^{2-\varepsilon}X}$$

qui vérifie

$$\sum_{q<X}L(X,q,\varepsilon)=o\Big(\frac{X}{\log X}\Big).$$

Nous montrons en fait la majoration individuelle beaucoup plus forte :

$$\big|R_B^{\pm}(X,q,\varepsilon)\big|\ll X^{15/16+\varepsilon}q^{-1/16}+L(X,q,\varepsilon),$$

mais elle ne nous sera d'aucune utilité pour nos applications de crible.

Preuve. On pose comme précédemment $Y=\log X/\log_3 X$, P_Y le produit des p inférieurs à Y, et on note

$$V(Y)=\{F\in C_{X,\rho},q\mid \Delta(F),\Delta(F)\in V_{qP_Y}\}.$$

On veut compter le nombre de classes de formes appartenant à V_p pour tout $p\mid qP_{X^\varepsilon}$ et de discriminant divisible par q. C'est-à-dire :

$$\begin{gathered}|V(Y)|\\ -|V(Y)\cap\{\exists p,Y<p<X^\varepsilon,\ \Delta\notin V_p\}|\\ +|\{F\in C_X-C_{X,\rho},\dots\}|.\end{gathered}$$

Ou encore, en introduisant la fonction f définie au Lemme 6.1 et en utilisant le Lemme 3.11 :

$$f(qP_Y,q,1) \tag{9}$$

$$-\sum_{\substack{Y<p<X^\varepsilon\\(p,q)=1}}f(qP_Y,q,p)+O\left(\sum_{Y<p_1<p_2<X^\varepsilon}f(qP_Y,q,p_1p_2)\right) \tag{10}$$

$$+O(X^{1-\rho+\varepsilon}). \tag{11}$$

• On choisit $X^\rho=X^{1/16}q^{1/16}$. Évaluons le premier symbole de Landau (ligne (10)) à l'aide du Corollaire 6.2, sachant que, pour $q\leqslant Q_B$, nous sommes dans le cadre

de validité de (7) :

$$\begin{aligned}\sum_{Y<p_1<p_2<X^\varepsilon} & f(qP_Y,q,p_1p_2)\\ &\ll \frac{X}{q}\sum_{Y<p_1<p_2}\frac{2p_1^2-1}{p_1^4}\cdot\frac{2p_2^2-1}{p_2^4}+\sum_{Y<p_1<p_2}X^{1-\varepsilon}q^{-1}(p_1p_2)^{-2}\\ &+\sum_{p_1<p_2<X^\varepsilon}X^{3/4+3\rho+\varepsilon}(qp_1p_2)^{-1/4}\\ &\ll \frac{X}{qY^2\log^2 Y}+X^{15/16+\varepsilon}q^{-1/16}.\end{aligned}$$

Ce terme domine celui de la ligne (11).

• Le terme principal (lignes (9) et (10)) vaut :

$$\begin{aligned}(12)\quad \frac{N(X,\rho)}{\zeta^2(2)}\prod_{p|q}\frac{1}{p+1}\Big(1+\sum_{\substack{p>Y\\(p,q)=1}}\frac{2}{p^2}+O(Y^{-3})\Big)\Big(1-\sum_{\substack{Y<p<X^\varepsilon\\(p,q)=1}}\frac{2p^2-1}{p^4}\Big)\\ +O\Big(\sum_{p>Y}X^{1-\varepsilon}q^{-1}p^{-2}+\sum_{p<X^\varepsilon}\big(X^{3/4+3\rho+\varepsilon}(qp)^{-1/4}\Big).\end{aligned}$$

Le dernier O est manifestement inférieur à celui que nous venons d'évaluer. De plus,

$$\Big(1+\sum_{\substack{p>Y\\(p,q)=1}}\frac{2}{p^2}+O(Y^{-3})\Big)\Big(1-\sum_{\substack{Y<p<X^\varepsilon\\(p,q)=1}}\frac{2p^2-1}{p^4}\Big)=1+O\Big(\frac{1}{Y^2\log^2 Y}\Big).$$

• Finalement, nous appliquons le Théorème 3.12 et obtenons

$$\big|B^{\pm}_{X,q,\varepsilon}\big|=\frac{K^{\pm}X}{\zeta^2(2)}\prod_{p|q}\frac{1}{p+1}+O\Big[\frac{X}{q\log^2 X\log_2^{2-\varepsilon}X}+X^{15/16+\varepsilon}q^{-1/16}\Big].$$

L'assertion sur la moyenne des R_B se vérifie facilement. □

THÉORÈME 7.3. *Soit $\varepsilon>0$, $Q_A=X^{10/87-\varepsilon}$, et q un entier inférieur à Q_A sans facteurs carrés. On a l'égalité*

$$\big|A^{\pm}_{X,q,\varepsilon}\big|=\frac{K^{\pm}}{\zeta^2(2)}X\prod_{p|q}\frac{1}{p+1}+R_A^{\pm}(X,q,\varepsilon),$$

où le terme d'erreur vérifie

$$\sum_{q=1}^{Q_A}\big|R_A^{\pm}(X,q,\varepsilon)\big|=o(X/\log X).$$

Remarque 7.4. Nous montrons en fait les majorations individuelles beaucoup plus fortes :

$$\big|R_A^{\pm}(X,q,\varepsilon)\big| \ll X^{6/7+\varepsilon}q^{-1} + L(X,q,\varepsilon), \quad \text{si } q \ll X^{5/203},$$
$$\big|R_A^{\pm}(X,q,\varepsilon)\big| \ll X^{9/11+\varepsilon}q^{32/55} + L(X,q,\varepsilon) \text{ sinon.}$$

Mais elles ne nous seront d'aucune utilité pour nos applications.

Preuve. Notons

$$V(Y) = \big\{F \in C_{X,\varepsilon}, q \mid \Delta, \Delta \in V_{qP_Y}\big\}.$$

On veut compter le nombre de classes de formes de $C_{X,\varepsilon}$ appartenant à V dont le discriminant est divisible par q, c'est-à-dire :

$$|V(Y)| - |V(Y) \cap \{\exists p, Y < p < Z,\ \Delta \notin V_p\}| \tag{13}$$
$$-|V(Y) \cap \{\exists p, Z \leqslant p,\ \Delta \notin V_p\}|,$$

où Z est un paramètre que l'on fixera dans la suite.

• On peut facilement majorer cette quantité en ne considérant que la première ligne (13) et en posant $Z = X^{\varepsilon}$. On reprend les calculs du Théorème 7.1 pour obtenir

$$|A_{X,q,\varepsilon}| < \frac{K^{\pm}}{\zeta^2(2)} X \prod_{p|q} \frac{1}{p+1} + O\big(X^{3/4+\varepsilon}q^{-1/4} + L(X,q,\varepsilon)\big)$$

sous la condition $q = o(X^{1/7-\varepsilon})$.

• Minorons $|A_{X,q,\varepsilon}|$ par :

$$f(qP_Y, q, 1) - \sum_{\substack{Y<p<Z \\ (p,q)=1}} f(qP_Y, q, p) \tag{14}$$
$$-O\Big(\sum_{p \geqslant Z} f(qP_Y, q, p)\Big) \tag{15}$$

Le Lemme 6.4 montre que, à condition que $q \ll X^{1/3-\varepsilon}$, (15) est dominée par

$$\sum_{p \geqslant Z} \Big(\frac{X}{q^{1-\varepsilon}p^2} + X^{15/16+\varepsilon}q^{-1/16}p^{-30/16}\Big) \ll \frac{X^{1+\varepsilon}}{qZ} + \frac{X^{15/16+\varepsilon}}{q^{1/16}Z^{14/16}}.$$

L'expression (14) vaut

$$\frac{K^{\pm}}{\zeta^2(2)} X \prod_{p|q} \frac{1}{p+1} + O\big(L(X,q,\varepsilon)\big) + O\Big(X^{\varepsilon}\sum_{p<Z} X^{3/4}(qp)^{-1/4} + (qp)^5\Big),$$

le deuxième O étant dominé par $X^{3/4+\varepsilon}q^{-1/4}Z^{3/4} + X^{\varepsilon}q^5Z^6$.

- Si $q \ll X^{5/203}$, on choisit $Z = X^{1/7}q^{-1}$; alors
  $q^{-1}X^{6/7} = q^5Z^6 = X^{3/4}q^{-1/4}Z^{3/4} \gg X^{15/16}q^{-1/16}Z^{-14/16} = (Xq)^{13/16}$.

Pour $q \ll Q_A$, nous avons $Z \gg X^{\varepsilon}$, donc

$$\frac{X^{1+\varepsilon}}{qZ} = o\big(L(X,q,\varepsilon)\big),$$

et l'on obtient la minoration

$$\big|A_{X,q,\varepsilon}\big| > \frac{K^{\pm}}{\zeta^2(2)} X \prod_{p|q} \frac{1}{p+1} + O\Big(X^{6/7+\varepsilon} q^{-1} + L(X,q,\varepsilon)\Big),$$

qui donne un contrôle du terme d'erreur jusqu'à

$$q = \min(X^{5/203}, X^{1/7-\varepsilon}) = X^{5/203}.$$

- Si $q \gg X^{5/203}$, on choisit $Z = X^{3/22} q^{-81/110}$. Alors

$$X^{3/4} q^{-1/4} Z^{3/4} \ll q^5 Z^6 = X^{15/16} q^{-1/16} Z^{-14/16} = X^{9/11} q^{32/55},$$

et nous contrôlons maintenant le reste jusqu'à Q_A. □

Remarque 7.5. Le Théorème 1.2 annoncé en introduction est une conséquence immédiate des Théorèmes 7.1 et 7.3 et des remarques qui les suivent. Le terme d'erreur de la majoration dépend essentiellement de la façon dont on maîtrise la pointe, et paraît difficile à améliorer sans interprétation géométrique de la méthode de Shintani. Par contre, lors de la minoration, la géométrie n'intervient que dans le Lemme 6.4, et plus précisément dans le deuxième terme d'erreur de l'estimation :

$$\sum_{|\Delta|<X, q|\Delta} [h_3^*(\Delta) - 1] \ll \frac{X}{q^{1-\varepsilon}} + \frac{X^{15/16+\varepsilon}}{q^{1/16}}.$$

La majoration triviale par $O(X)$ donne un contrôle jusqu'à $Q = X^{1/12-\varepsilon}$. Il est possible qu'un argument algébrique, du type de celui qui permet d'isoler p, supprime ce deuxième terme. On contrôlerait alors R_A jusqu'à $Q = X^{1/7-\varepsilon}$.

Remarque 7.6. Il suffit de poser $q = 1$ pour retrouver le résultat de Davenport et Heilbronn cité en introduction. On utilise simplement le lemme suivant :

Lemme 7.7. *On a l'égalité*

$$\sum_{\Delta \in \Delta^{\pm}(X)} 1 = \frac{3}{\pi^2} X + O(X^{1/2}).$$

Preuve. Si $(a,q) = 1$, on calcule facilement le nombre d'entiers sans facteurs carrés congrus à a modulo q, par exemple en utilisant

$$\mu^2(n) = \sum_{d^2|n} \mu(d).$$

On trouve, pour q fixé, l'égalité :

$$\sum_{\substack{n=1\\ n=a\,(q)}}^{X} \mu^2(n) = \frac{1}{\zeta(2)}\frac{1}{q\prod_{p|q}(1-\frac{1}{p^2})}X\big(1+O(X^{-1/2})\big).$$

Le lemme est une application directe. □

8. Cribler le 3-rang des corps quadratiques réels

8.1. Mise en place du crible. Dorénavant, on oublie la signification première de la notation $\omega(q)$, *i.e.* le nombre de facteurs premiers de q, et on pose, comme dans le Théorème 1.2 cité en introduction,

$$\omega(q) = \prod_{p|q}\frac{p}{p+1}$$

pour tout q sans facteurs carrés.
On note

$$\mathbb{X} = \#\Big\{(a,b,c,d) \in C_X^+ \cap V\Big\} \text{ (terme principal abstrait).}$$

Rappelons que le résultat de Davenport-Heilbronn équivaut à $\mathbb{X} \sim \frac{1}{\pi^2}X$.

Tout les résultats de crible utilisés dans la suite sont extraits des articles d'Iwaniec [**31**] et [**30**]. On s'est efforcé de conserver autant que possible les mêmes notations que [**30**]. Notons que tous les résultats énoncés seraient accessibles par le crible de Selberg.

Les Théorèmes 7.1 et 7.3 s'écrivent, grâce à la Remarque 7.6 :

$$|A_{X,q,\varepsilon}| = \prod_{p|q}\frac{\omega(p)}{p}\mathbb{X} + R_A(X,q,\varepsilon),$$

$$|B_{X,q,\varepsilon}| = \prod_{p|q}\frac{\omega(p)}{p}\mathbb{X} + R_B(X,q,\varepsilon),$$

où $R_A(X,q,\varepsilon)$ et $R_B(X,q,\varepsilon)$, par abus de notation, vérifient aussi les inégalités des théorèmes.

Lemme 8.1. *Quand Y tend vers $+\infty$, on a l'égalité :*

$$\prod_{p<Y}\Big(1-\frac{\omega(p)}{p}\Big) = \frac{\pi^2}{6}\frac{e^{-\gamma}}{\log Y}\Big(1+O(\frac{1}{\log Y})\Big).$$

Preuve. La formule de Mertens donne :

$$\prod_{p<Y}\Big(1-\frac{1}{p}\Big) = \frac{e^{-\gamma}}{\log Y}\big(1+O(\log^{-1}Y)\big)$$

et donc

$$\prod_{p<Y}(1-\frac{\omega(p)}{p}) = \prod_{p<Y}\frac{p^2}{p^2-1}\cdot\prod_{p<Y}\frac{p-1}{p}$$
$$= \zeta(2)\big(1+O(Y^{-1})\big)\cdot\frac{e^{-\gamma}}{\log Y}\big(1+O(1+\log^{-1}Y)\big).$$

□

COROLLAIRE 8.2. *La condition du crible linéaire est vérifiée, puisque pour tout Y, Z vérifiant $2 \leqslant Y < Z$, on a l'inéquation :*

$$\prod_{Y\leqslant p<Z}\Big(1-\frac{\omega(p)}{p}\Big)^{-1} \leqslant \frac{\log Z}{\log Y}\Big[1+O\Big(\frac{1}{\log Y}\Big)\Big].$$

THÉORÈME 8.3. *On fixe $\varepsilon > 0$, $Q_B = X^{1/15-\varepsilon}$, $Q_A = X^{10/87-\varepsilon}$, et on pose*

$$s_B = \frac{\log Q_B}{\log Y}, \quad s_A = \frac{\log Q_A}{\log Y}.$$

On se donne un ensemble $\mathcal{P}$ de nombres premiers, puis on note

$$\mathcal{P}_Y = \prod_{\substack{p\in\mathcal{P}\\ p<Y}} p \quad et \quad S(X,\mathcal{P},Y) = \sum_{\substack{0<\Delta<X\\ (\Delta,\mathcal{P}_Y)=1}}\big[h_3^*(\Delta)-1\big].$$

On a alors les inégalités :

$$S(X,\mathcal{P},Y) < \mathbb{X}\prod_{p|\mathcal{P}_Y}\Big(1-\frac{\omega(p)}{p}\Big)F(s_B)\cdot(1+o_\varepsilon(1)) \text{ si } Y < Q_B,$$

$$S(X,\mathcal{P},Y) > \mathbb{X}\prod_{p|\mathcal{P}_Y}\Big(1-\frac{\omega(p)}{p}\Big)f(s_A)\cdot(1+o_\varepsilon(1)) \text{ si } Y < \sqrt{Q_A},$$

où F et f sont les fonctions du crible linéaire (voir [**30**] *pour leur définition exacte).*

PREUVE. $S(X,\mathcal{P},Y)$ est égal à $O(X^{3/4+\varepsilon})$ près au nombre de points de C_X^+ de discriminant premier à $\mathcal{P}_Y$, soit

$$S(X,\mathcal{P},Y) = \sum_{0<\Delta<\mathbb{X}} B(\Delta)(\mu * \mathbf{1})(\Delta,\mathcal{P}) + O(X^{3/4+\varepsilon})$$

en notant

$$B(\Delta) = \#\{F \in B_{X,1,\varepsilon}, \Delta(F) = \Delta\}.$$

Il existe deux suites $\{\mu_q^\pm\}$ d'entiers valant -1, 0, ou 1, nulles pour $q \geqslant Q$, et vérifiant l'encadrement (voir [**31**])

$$\mu^- * \mathbf{1} \leqslant \mu * \mathbf{1} \leqslant \mu^+ * \mathbf{1}.$$

On pose

$$M^+(Q,\mathcal{P},Y)=\sum_{\substack{q|\mathcal{P}_Y\\ q<Q}}\mu_q^+\frac{\omega(q)}{q}.$$

Nous avons alors :

$$\begin{aligned}S(X,\mathcal{P},Y) &\leqslant \sum_{0<\Delta<X} B(\Delta)(\mu^+ * \mathbf{1})(\Delta,P_Y)+O(X^{3/4+\varepsilon})\\ &\leqslant \sum_{\substack{q|\mathcal{P}_Y\\ q<Q}}\mu_q^+ S(X,q)+O(X^{3/4+\varepsilon})\\ &\leqslant \mathbb{X}\sum_{\substack{q|\mathcal{P}_Y\\ q<Q}}\mu_q^+\frac{\omega(q)}{q}+\sum_{\substack{q|\mathcal{P}_Y\\ q<Q}}|R_B(X,q,\varepsilon)|+O(X^{3/4+\varepsilon})\\ &= \mathbb{X}M^+(Q_B,\mathcal{P},Y)+o(X/\log X)\end{aligned}$$

d'après le Théorème 7.1, pour le choix $Q=Q_B$. Si $Y<Q_B$, on a, d'après le Lemme 3 de [**30**] :

$$M^+(Q_B,\mathcal{P},Y)<\prod_{p|\mathcal{P}_Y}\Big(1-\frac{\omega(p)}{p}\Big)\Big\{F(s_B)+O(1/\log Q_B)\Big\}.$$

Comme le produit domine $\log^{-1}X$, on obtient finalement :

$$S(X,\mathcal{P},Y)<\mathbb{X}\prod_{p|\mathcal{P}_Y}\Big(1-\frac{\omega(p)}{p}\Big)F(s_B)\big(1+o(1)\big).$$

La minoration s'effectue de façon similaire. On crible les éléments de $A_{X,1,\varepsilon}$ suivant leur discriminant, puis on applique le Théorème 7.3. □

Corollaire 8.4. *Avec les notations du Théorème 8.3, si $\mathcal{P}$ est la suite de tous les premiers, alors le Lemme 8.1 entraîne :*

$$S(X,\mathcal{P},Y)>\frac{1}{6}f(s_A)X\frac{e^{-\gamma}}{\log Y}\big(1+o(1)\big)\quad \textit{si } Y<\sqrt{Q_A}.$$

$$S(X,\mathcal{P},Y)<\frac{1}{6}F(s_B)X\frac{e^{-\gamma}}{\log Y}\big(1+o(1)\big)\quad \textit{si } Y<Q_B.$$

Remarque 8.5. Pour $0<s\leqslant 2$, on a $f(s)=0$, $F(s)=2e^{\gamma}/s$ et pour $s>2$, on a $f(s)>0$. De plus, ces deux fonctions sont monotones et convergent très rapidement vers 1. Ce sont les seules propriétés que nous utiliserons.

8.2. Applications.

PROPOSITION 8.6. *On pose*

$$A(X) = \sum_{\substack{5\leqslant p\leqslant X\\ p=1\ (4)}} h_3^*(p) + \sum_{\substack{2\leqslant p\leqslant X/4\\ p=3\ (4)}} h_3^*(4p) + \sum_{3\leqslant p\leqslant X/8} h_3^*(8p),$$

$$A_0(X) = \sum_{\substack{5\leqslant p\leqslant X\\ p=1\ (4)}} h_3^*(p).$$

Alors, on a les inégalités

$$A(X) < 11\cdot\frac{3X}{4\log X}\big(1+o(1)\big) \quad et \quad A_0(X) < 11\cdot\frac{X}{2\log X}\big(1+o(1)\big).$$

PREUVE. Notons $\mathcal{P}^2 = \{p, p\neq 2\}$ et remarquons que $A(X)$ possède, à $o(X/\log X)$ près,

$$\left(\frac{1}{2}+\frac{1}{8}+\frac{1}{8}\right)\frac{X}{\log X} = \frac{3}{4}\frac{X}{\log X} \text{ termes.}$$

alors

$$\begin{aligned} A(X) \;=\; & \sum_{\substack{5\leqslant p\leqslant X\\ p=1\ (4)}} (h_3^*(p)-1) + \sum_{\substack{2\leqslant p\leqslant X/4\\ p=3\ (4)}} (h_3^*(4p)-1) + \sum_{3\leqslant p\leqslant X/8} (h_3^*(8p)-1) \\ & + \frac{3X}{4\log X} + o(X/\log X). \end{aligned}$$

Si, dans ces trois sommes, on se restreint aux indices vérifiant $p > Q_B$, on peut les majorer par $S(X,\mathcal{P},Q_B)$. Comme, d'autre part, le Théorème 7.1 donne

$$\sum_{p<Q_B} (h_3^*(p)+h_3^*(4p)+h_3^*(8p)) \ll Q_B,$$

nous obtenons :

$$\begin{aligned} A(X) \;&<\; S(X,\mathcal{P}^2,Q_B) + O(Q_B) + \frac{3X}{4\log X} + o(X/\log X) \\ &<\; \mathbb{X}F(1)\prod_{2<p<Q_B}\Big(1-\frac{\omega(p)}{p}\Big) + \frac{3X}{4\log X}\big(1+o(1)\big) \\ &<\; \frac{1}{\pi^2}X\cdot 2e^{\gamma}\cdot\frac{3}{2}\frac{\pi^2}{6}\frac{e^{-\gamma}}{\log Q_B} + \frac{3X}{4\log X}\big(1+o(1)\big) \\ &=\; \Big(\frac{2}{3(1/15-\varepsilon)}+1\Big)\frac{3X}{4\log X}\big(1+o(1)\big). \end{aligned}$$

Pour évaluer A_0, il suffit de cribler sur tous les premiers inférieurs à Y, y compris 2. Le calcul est similaire (il n'y a plus que $X/2\log X$ termes) et l'on trouve la même

constante numérique car

$$\Big(1-\frac{\omega(2)}{2}\Big)=\frac{X}{2\log X}\Big/\frac{3X}{4\log X}=2/3.$$

□

Remarque 8.7. La minoration du crible permet d'obtenir une borne inférieure, mais on n'a aucun espoir de trouver un équivalent avec des méthodes de ce type. Rappelons aussi que la valeur moyenne de la 3-partie du groupe des classes d'un corps quadratique réel vaut 4/3. A priori, on s'attendrait à un résultat du même ordre pour les discriminants premiers. On ne connaît pas de théorème d'équirépartition de ce type, et notre 11 est bien loin des 4/3 espérés.

LEMME 8.8. *Soient a et q deux entiers premiers entre eux et $Y=X^{\eta}$, pour un $\eta>0$. On note*

$$\Phi(X,Y,a,q)=\#\big\{n<X, n\equiv a \bmod q, P^-(n)>Y\big\}.$$

Alors on a l'équivalence

$$\Phi(X,Y,a,q)\simeq_q \frac{W(u)}{\varphi(q)}\cdot\frac{X}{\log Y},$$

où $u=\dfrac{\log X}{\log Y}=\dfrac{1}{\eta}$ *et* $W(u)=\dfrac{F(u)+f(u)}{2e^{\gamma}}$ *(fonction de Buchstab).*

PREUVE. Voir [**49**, pp. 454–465] pour l'équivalent classique de $\Phi(X,Y,0,1)$. Reprendre les étapes de la démonstration en introduisant la congruence, le théorème des nombres premiers étant remplacé par Dirichlet. □

PROPOSITION 8.9. *Il existe une infinité de discriminants fondamentaux positifs n, ayant au plus 8 facteurs premiers, tels que la 3-partie du groupe des classes de $\mathbb{Q}(\sqrt{n})$ soit triviale (*i.e. $h_3^*(n)=1$*).*

PREUVE. Soit $\mathcal{P}$ l'ensemble des nombres premiers et $Y=X^{1/u}$. On note

$$\mathcal{D}=\big\{n<X, n \text{ est un discriminant fondamental}, P^-(n)>Y\big\}.$$

Supposons qu'à un nombre borné d'exceptions près, 3 divise $h_3^*(\Delta)$ pour tous les discriminants fondamentaux dont les diviseurs premiers sont plus grands que Y. Nous aurions, pour X assez grand :

$$S(X,\mathcal{P},Y)\geqslant 2\cdot|\mathcal{D}|.$$

Le nombre d'entiers divisibles par le carré d'un premier supérieur à Y est majoré par :

$$\sum_{p>Y}\frac{X}{p^2}\ll\frac{X}{Y}.$$

Fixons un petit $\varepsilon>0$; nous avons noté :

$$u=\frac{\log X}{\log Y}\quad\text{et}\quad s_B=\frac{\log Q_B}{\log Y}=u(1/15-\varepsilon).$$

Nous obtenons donc, en combinant notre remarque et le Lemme 8.8 :

$$|\mathcal{D}| = \Phi(X, Y, 1, 4) + O(X/Y) \simeq \frac{W(u)}{2}\frac{X}{\log Y}.$$

Or, pour $Y \geqslant Q_B$, on a $S(X, \mathcal{P}, Y) \leqslant S(X, \mathcal{P}, Q_B)$ par définition de la fonction de crible, et le Corollaire 8.4 donne :

$$S(X, \mathcal{P}, Y) \leqslant S(X, \mathcal{P}, Q_B) < \frac{1}{6}F(1)e^{-\gamma}\frac{X}{\log Q_B}(1 + o(1)).$$

Globalement, on aurait donc l'inégalité :

$$2\frac{W(u)}{2} \cdot \frac{X}{\log Y} < \frac{1}{6}F(1)e^{-\gamma}\frac{X}{\log Q_B}(1 + o(1)).$$

Ce qui reviendrait à :

$$\frac{F(u) + f(u)}{2}u < (5e^{\gamma} + \varepsilon)(1 + o(1)).$$

Il nous faut choisir u minimal tel que l'on obtienne une contradiction. On peut prendre u légèrement supérieur à $5e^{\gamma} \approx 8.9$.

Il existe donc une infinité de discriminants fondamentaux $n < X$ tels que $h_3^*(n) = 1$, et dont le plus petit diviseur premier soit supérieur à $X^{1/u}$. Un tel n a évidemment au plus $[u] = 8$ facteurs premiers. □

PROPOSITION 8.10. *Il existe une infinité de discriminants fondamentaux ayant au plus* 17 *facteurs premiers, et tels que* $3 \mid h_3^*(\Delta)$.

PREUVE. On crible toujours sur tous les nombres premiers plus petits que Y. Fixons $\varepsilon > 0$ tel que

$$[(10/87 - \varepsilon)(1/2 - \varepsilon)]^{-1} < 18$$

et choisissons $Y = Q_A^{1/2-\varepsilon}$. Alors $s_A = \log Q_A / \log Y > 2$, donc $f(s_A) > 0$. Soit

$$S(X, \mathcal{P}, Y) > \frac{1}{6}f(s_A)X\frac{e^{-\gamma}}{\log Y} > \alpha\frac{X}{\log X}, \quad \text{avec } \alpha > 0.$$

Mais les diviseurs premiers des discriminants comptés par $S(X, \mathcal{P}, Y)$ sont tous supérieurs à Y : il y en a donc au plus $\log X / \log Y < 18$, soit au plus 17. D'où le résultat en faisant tendre X vers $+\infty$. □

9. Cribler le 3-rang des quadratiques imaginaires

Pour cribler, il nous suffit de considérer le nouveau terme principal abstrait

$$\mathbb{X} = \sum_{-X<\Delta<0} (h_3^*(\Delta) - 1) \simeq \frac{3}{\pi^2}X.$$

On veut étudier

$$S(X, \mathcal{P}, Y) = \sum_{\substack{-X<\Delta<0 \\ (\Delta, \mathcal{P}_Y)=1}} (h_3^*(\Delta) - 1).$$

Avec ces nouvelles notations, le Théorème 8.3 reste valide, et le Corollaire 8.4 est modifié comme suit :

COROLLAIRE 9.1. *Si $\mathcal{P}$ est la suite de tous les premiers, alors*

$$S(X,\mathcal{P},Y) > \frac{1}{2}f(s_A)X\frac{e^{-\gamma}}{\log Y}(1+o(1)) \quad \textit{si } Y < \sqrt{Q_A},$$

$$S(X,\mathcal{P},Y) < \frac{1}{2}F(s_B)X\frac{e^{-\gamma}}{\log Y}(1+o(1)) \quad \textit{si } Y < Q_B,$$

puisque nous avons essentiellement multiplié par 3 le terme principal. Posons :

$$A(X) = \sum_{\substack{3\leqslant p\leqslant X\\ p=3\ (4)}} h_3^*(-p) + \sum_{\substack{5\leqslant p\leqslant X/4\\ p=1\ (4)}} h_3^*(-4p) + \sum_{3\leqslant p\leqslant X/8} h_3^*(-8p),$$

$$A_0(X) = \sum_{\substack{3\leqslant p\leqslant X\\ p=3\ (4)}} h_3^*(-p).$$

Le crible donne immédiatement les majorations :

$$A(X) < 31\cdot\frac{3X}{4\log X}(1+o(1)),$$

$$A_0(X) < 31\cdot\frac{X}{2\log X}(1+o(1)).$$

On n'a rien à changer dans les estimations du nombre de groupes des classes de 3-partie non triviale (Proposition 8.10). Par contre, la fin de la preuve de la Proposition 8.9 doit être modifiée comme suit. L'inéquation obtenue devient :

$$\frac{F(u)+f(u)}{2}u < 15e^{\gamma}+\varepsilon+o(1)$$

et on doit prendre u légèrement supérieur à $15e^{\gamma}\approx 26.7$ pour obtenir une contradiction.

D'où les résultats annoncés en introduction :

- Il existe une infinité de Δ négatifs ayant au plus 26 facteurs premiers tels que $h_3^*(\Delta)=1$.
- Il existe une infinité de Δ négatifs ayant au plus 17 facteurs premiers tels que $3 \mid h_3^*(\Delta)$.

Remarque 9.2. Il est bien connu (conjecturalement...) que les groupes de classes de corps quadratiques réels sont plus "petits" que leurs contreparties imaginaires (voir par exemple les justifications heuristiques de [**6**] ou les tables de [**4**]). Au delà des valeurs numériques, tout à fait déraisonnables puisqu'on conjecture l'existence d'une infinité de *premiers* vérifiant les mêmes conditions que nos "gros" pseudo-premiers, on retrouve ce phénomène dans nos résultats : il est plus difficile d'obtenir une 3-partie triviale dans le cas imaginaire et on a une moins bonne majoration du 3-rang moyen.

CHAPITRE 2

A Fast Algorithm to Compute Cubic Fields

Ce chapitre a été soumis pour publication à *Mathematics of Computation*. Il paraîtra aussi, sous une forme abrégée, dans les *proceedings* de ANTS II (Algorithmic Number Theory Symposium).

The classification of quadratic fields up to isomorphism is trivial: they are uniquely characterized by their discriminant, and we can compute tables as soon as we know how to test if an integer is squarefree and how to check some simple congruence modulo 16. We intend to show that *cubic* fields are essentially as easy to deal with, and we will get an equally canonical representation for them. Contrary to the quadratic case, the treatment depends on the signature but, the fundamental ideas being the same, we shall expose as much as we can before splitting cases.

Almost all results in this paper are either ancient or elementary. I would like to thank Professor H.Cohen for his interest when I first mentioned what I thought was a trivial application of some well known results. Moreover, his careful reading of successive drafts of this work and the many questions he had about it were most helpful in giving it its present shape.

1. Preliminaries

Let (a, b, c, d) denote the integral binary cubic form $F(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$. We call as usual $\mathrm{disc}(F)$ its discriminant:

$$\mathrm{disc}(a, b, c, d) = b^2c^2 - 27a^2d^2 + 18abcd - 4ac^3 - 4b^3d \ .$$

We shall say a form F is *complex* whenever $\mathrm{disc}\, F < 0$, and *real* otherwise. We call *roots* of F, the complex roots of $F(X, 1) = 0$.

A form is said to be primitive if $\gcd(a, b, c, d) = 1$, and irreducible if it is so in $\mathbb{Q}[x, y]$. The usual change of variables gives an action of $\mathrm{GL}_2(\mathbb{Z})$ on the set of binary cubic forms, which preserves discriminants, irreducibility and primitivity. We call Φ the set of classes of integral, binary cubic forms under this action. Please note that, contrary to the quadratic case, we do not restrict to $\mathrm{SL}_2(\mathbb{Z})$.

Let V_p be the subset of Φ given by the following congruence conditions:

- If $p = 2$: $\mathrm{disc}\, F \equiv 1 \pmod 4$ or $\mathrm{disc}\, F \equiv 8, 12 \pmod{16}$.
- If $p \neq 2$: $p^2 \nmid \mathrm{disc}\, F$.

So that forms in $V = \cap V_p$ have fundamental discriminants (we call an integer Δ a fundamental discriminant either if $\Delta = 1$ or if it is the discriminant of a quadratic field). Now we put $U = \cap U_p$, where $U_p \subset \Phi$ is given by: $F \in U_p$ if

- it belongs to V_p, or
- it factors as $\lambda(\alpha x + \beta y)^3$ modulo p, with $\lambda \in \mathbb{F}_p^*$, and α, β in $\mathbb{F}_p$ not both zero. Furthermore, there exists an $e \in \mathbb{F}_p^*$ such that the equation

$$F(x, y) \equiv ep \pmod{p^2}$$

has a solution in $x, y \in \mathbb{Z}/p^2\mathbb{Z}$.

Let C denote the set of non-isomorphic cubic extensions of $\mathbb{Q}$. Given $K \in C$ and $x \in K$, we call $\mathfrak{d}(x)$ the discriminant of the minimal polynomial of x, and denote by x, x', x'' the three conjugates of x in $\overline{K}$. Now put

$$F_K(x, y) = \frac{\mathrm{Norm}[(\alpha - \alpha')x - (\beta - \beta')y]}{\sqrt{\mathfrak{d}_K}} = \sqrt{\frac{\mathfrak{d}(\alpha x - \beta y)}{\mathfrak{d}_K}} \ ,$$

where $[1, \alpha, \beta]$ is any $\mathbb{Z}$-basis of the maximal order of K whose first element is 1, and $\mathfrak{d}_K$ is its absolute discriminant.

The key ingredient is the following result establishing the link between cubic forms and fields:

THEOREM 1.1 (Davenport-Heilbronn [**16**]). *Consider the following maps:*

$$\begin{aligned} \varphi_{CU} :&\ \textit{conjugacy class of } K &\longrightarrow&\ \textit{class of } F_K(x, y) \\ \varphi_{UC} :&\ \{\mathbb{Q}(\theta_1), \mathbb{Q}(\theta_2), \mathbb{Q}(\theta_3)\} &\longleftarrow&\ \textit{class of } F(x, y) \end{aligned}$$

where the θ_i are the zeros of $F(\theta, 1) = 0$. These are well defined inverse maps, and induce a discriminant preserving *bijection between the sets U and C.*

This rather abstract statement has a very nice algorithmic translation. First, reduction theory enables us to efficiently single out a *canonical* representative in each equivalence class of irreducible cubic forms. We shall discuss this in great detail in §3 (positive discriminants) and §4 (negative discriminants). We will call such forms *reduced* in the sequel. For the time being, we only need to know that if $F = (a, b, c, d)$ is reduced, then any reduced form equivalent to F is equal to F (see Lemmas 3.3 and 4.3). Hence, to a given field, we can associate a unique companion form. And second, we shall see that, as their name imply, the reduced forms have rather small coefficients, bounded in terms of their discriminant.

Denote by H_F the Hessian form associated to F:

$$H_F = -\frac{1}{4} \begin{vmatrix} \frac{\partial^2 F}{\partial x \partial x} & \frac{\partial^2 F}{\partial x \partial y} \\ \frac{\partial^2 F}{\partial x \partial y} & \frac{\partial^2 F}{\partial y \partial y} \end{vmatrix} = Px^2 + Qxy + Ry^2 \ ,$$

where

$$P = b^2 - 3ac, \quad Q = bc - 9ad, \quad \text{and} \quad R = c^2 - 3bd \ .$$

One can easily see that the Hessian is covariant with respect to $\mathrm{GL}_2(\mathbb{Z})$: we have $H_{F\circ M} = H_F \circ M$ for all $M \in \mathrm{GL}_2(\mathbb{Z})$. Moreover, a simple calculation shows that $\operatorname{disc} H_F = -3 \operatorname{disc} F$.

We summarize in the next lemma the elementary properties of the set U, which enable us to test easily whether a given form is associated to a cubic field or not.

LEMMA 1.2. *Let $F = (a, b, c, d)$ be a cubic primitive form, and (P, Q, R) its Hessian. We write $(F, p) = (1^3)$ whenever, up to a scalar factor, F is a cube modulo p.*

(1) *$(F, p) = (1^3)$ if and only if $p | \gcd(P, Q, R)$.*
(2) *If $(F, p) = (1^3)$ and $p \neq 3$, then $F \in U_p$ if and only if $p^3 \nmid \operatorname{disc}(F)$.*
(3) *If $F \in U_3$, then $3^6 \nmid \operatorname{disc}(F)$.*
(4) *If $(F, 3) = (1^3)$, the analogue of part 2. is completely described by the following algorithm :*

$$\begin{array}{rll} \textit{if} & 3|a, & F \in U_3 \Longleftrightarrow 9 \nmid a \text{ and } 3 \nmid d, \\ \textit{else if} & 3|d, & F \in U_3 \Longleftrightarrow 9 \nmid d, \\ \textit{else if} & 3|(a-d), & F \in U_3 \Longleftrightarrow a - b + c - d \equiv 0 \pmod 9, \\ \textit{else if} & 3|(a+d), & F \in U_3 \Longleftrightarrow a + b + c + d \equiv 0 \pmod 9. \end{array}$$

(5) *If a reduced form F belongs to U, then it is irreducible.*

PROOF.

- 1. One first notes that p divides $\operatorname{disc}(F)$ if and only if $(F, p) = (1^2 1)$ or (1^3), with evident notations. This is clear when the point at infinity is one of the roots, *i.e.* $F(x, 1)$ has degree at most two, so we suppose this is not the case. As the finite field $\mathbb{F}_p$ is perfect, $\operatorname{disc} F \equiv 0 \pmod p$ implies that F is reducible modulo p, two of the roots in $\overline{\mathbb{F}}_p$ being equal. As the sum of the roots is in $\mathbb{F}_p$, they all are (if $p = 2$, one uses their product instead).

  If F splits as

  $$F(x, y) \equiv (\alpha x + \beta y)^2 (\gamma x + \delta y) \pmod p \ ,$$

  one finds that $H(x, y) \equiv (\alpha x + \beta y)^2 (\alpha\delta - \beta\gamma)^2 \pmod p$. As F is primitive, α and β are not both zero modulo p, thus

  $$H(x, y) \equiv 0 \pmod p \Leftrightarrow \alpha\delta - \beta\gamma \equiv 0 \pmod p \Leftrightarrow (F, p) = (1^3) \ .$$

- 2. and 3. are exactly [**16**, Lemma 6]. Replacing F by an equivalent form, we can write $F = (a, b, c, d)$, with $F \equiv ax^3 \pmod p$. So $\operatorname{disc} F = -27a^2d^2$ modulo p^3. The form F is primitive, thus $p \nmid a$, and as $p \neq 3$, $p^3 | \operatorname{disc} F$ is equivalent to $p^2 \mid d$. Now $F(x, y) \equiv ep \pmod{p^2}$ implies that p divides x, thus $F(x, y) \equiv dy^3 \pmod{p^2}$ and our claim follows. The case $p = 3$ is left to the reader.
- 4. is trivial once one remarks that 3 must divide b and c and thus $F(x, y)$ only depends on (x, y) modulo 3.

- 5. This last assertion will be proven later (Lemmas 3.3 and 4.3).

□

We can now propose an efficient algorithm to test if a given cubic form is in the image of the Davenport-Heilbronn map:

Algorithm 1.3

Input: a cubic form $F = (a, b, c, d)$.
Output: `true` if and only if F corresponds to a cubic field.

(1) If F is not reduced, return `false`.
(2) If F is not primitive, return `false`.
(3) Compute (P, Q, R), the Hessian of F. Set $D = 4PR - Q^2 = 3\,\mathrm{disc}(F)$ and $f_H = \gcd(P, Q, R)$. Check whether F belongs to U_2 and U_3, else return `false`.
(4) If $p^2 | f_H$ with $p > 3$ return `false`.
(5) Set $t = D/f_H^2$. Remove all powers of 2 and 3 from t: at most 2^3 and 3^2. If $\gcd(t, f_H) > 1$ return `false`.
(6) If t is squarefree return `true`, else return `false`.

PROOF. We have to check that F is primitive, reduced, and belongs to U_p for all p, which implies it is irreducible. Steps 1 to 3 are straightforward, and we only have to check that a form satisfying steps 4 to 6 belongs to U_p, for all $p \geqslant 5$.

The prime divisors of f_H are exactly the ones for which $(F, p) = (1^3)$. For all of them we check in steps 4 and 5 whether p^3 divides $\mathrm{disc}\, F$ or not. Finally, in step 6, we check the other prime divisors of $\mathrm{disc}\, F$, $p \geqslant 5$: F must belong to V_p for all of them, which is the case if and only if t is squarefree. □

Remark 1.4. Step 2 is only necessary, as an "early-abort" strategy: if a prime p divides all the coefficients of F, then $p^2 | f_H$ and step 3 (if $p = 2, 3$) or 4 (if $p > 3$) would return `false` just as well. *On average*, if one uses the techniques described hereafter, this step *slows down* the algorithm.

Remark 1.5. There is a real problem lying in steps 4 and 6. Squarefree factorization of integers is presently as difficult as complete factorization, so we need to factor f_H and t and check all prime divisors for greater than one valuation. But our aim here is to compute *tables* of fields and, calling X the discriminant bound, we will need to factor X discriminants of size about X, which is not acceptable. We shall see in §5 that simple hashing techniques reduce this to a sensible amount.

The discriminant of a cubic field K can be uniquely factored as $f^2\Delta$, where Δ is a fundamental discriminant. The f_H appearing in step 3 of the algorithm is closely related to this one: it is known that a prime p is totally ramified in K if and only if p divides f (see [**23**]). Lemma 1.2 and Proposition 2.2 imply that this is equivalent to $p | f_H$. Thus f and f_H have the same prime divisors, but they may differ by a factor 3, if $3|\Delta$. The precise result is as follows:

LEMMA 1.6. *Let K be a cubic field, F_K its companion reduced cubic form, and Δf^2 their common discriminant. Let (P,Q,R) be the Hessian of F_K, call f_H its content and put $(P,Q,R) = f_H(P_1,Q_1,R_1)$, where (P_1,Q_1,R_1) is primitive. We have $f_H = f$ if and only if $-\frac{1}{3}(Q_1^2 - 4P_1R_1)$ is fundamental, and $f_H = 3f$ otherwise. The latter only happens when 3 divides both f and Δ. It always happens when $v_3(f) = 1$.*

PROOF. Straightforward given the preceding discussion, except for the prime 3. Lemma 1.2 tells us that $3^3 \nmid f$, and an easy computation shows that $3|f_H$ if and only if $9|f_H$. Now write that

$$f_H^2(Q_1^2 - 4P_1R_1) = -3\Delta f^2 \ ,$$

and compare the valuations at 3. □

2. Properties of the Davenport-Heilbronn cubic form

First and foremost, adjoining a root of $F(X,1)$ to $\mathbb{Q}$ yields a representative of the class of cubic fields associated to F, in the sense of Theorem 1.1. But what we want to stress here is the ease with which one recovers the simple invariants associated to K from F_K.

PROPOSITION 2.1. *Let $F_K = (a,b,c,d)$ be a representative of the class of cubic forms associated to the cubic field K by the Davenport-Heilbronn bijection. For instance, the reduced one.*

(1) *We have* $\operatorname{disc} K = \operatorname{disc} F_K$.
(2) *If θ is a root of F_K belonging to K, then $[1, a\theta, a\theta^2 + b\theta]$ is a basis of the maximal order $\mathbb{Z}_K$.*

PROOF. 1. is part of the Davenport-Heilbronn theorem, and can be easily checked from the definition of F_K anyway.

As for 2, we use an idea attributed to H. Lenstra by H. Cohen [**5**, Exercise 15, p. 216]. Let θ be an algebraic number, and $P(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n$ be its minimal primitive polynomial, with integral coefficients. One defines

$$\mathbb{Z}_\theta = \mathbb{Z}[a_0\theta, a_0\theta^2 + a_1\theta, \ldots, a_0\theta^{n-1} + \cdots + a_{n-2}\theta] \ .$$

Then $\mathbb{Z}_\theta$ is easily seen to be an algebra of finite type over $\mathbb{Z}$, and thus is an order in $\mathbb{Z}_K$. Now, if we denote the roots of P by $\theta_1, \ldots, \theta_n$, then a Van der Monde-type calculation gives

$$\operatorname{disc} \mathbb{Z}_\theta = a_0^{2n-2} \prod_{i \neq j} (\theta_i - \theta_j) = \operatorname{disc} P \ .$$

Here, we have $\operatorname{disc} F_K = \operatorname{disc} K$, so $\mathbb{Z}_\theta = \mathbb{Z}_K$. □

The next proposition is an algorithmic restatement of [**16**, Lemma 11]:

PROPOSITION 2.2. *Call θ a root of F_K belonging to K. A prime $p \in \mathbb{Z}$ decomposes in K as $F_K = (a,b,c,d)$ factors in $\mathbb{F}_p[X,Y]$. More precisely, if we take an irreducible decomposition*

$$F_K(X,Y) \equiv \prod_i T_i^{e_i}(X,Y) \pmod{p} \ ,$$

we have

$$p\mathbb{Z}_K = \prod_i \mathfrak{p}_i^{e_i}, \quad \text{with } \mathfrak{p}_i \text{ prime in } \mathbb{Z}_K \ .$$

Moreover, we can take:

- *If $p \nmid a$, then*
$$\mathfrak{p}_i = p\mathbb{Z} + T_i(\theta,1)\mathbb{Z}_K \ .$$
- *If $p|a$ but $p \nmid d$, then*
$$\mathfrak{p}_i = p\mathbb{Z} + T_i(\theta,1)/\theta^{\deg T_i}\mathbb{Z}_K \ .$$
- *If $p|a$ and $p|d$, but $p \neq 2$ or $F(X,Y) \not\equiv XY(X+Y) \pmod 2$, there exists $u \in \mathbb{Z}$ such that $u \not\equiv 0 \pmod p$, and, in the case $p \nmid c$, $u \not\equiv -b/c \pmod p$. Then we take:*
$$\mathfrak{p}_i = p\mathbb{Z} + T_i(\theta,1)/(1-u\theta)^{\deg T_i}\mathbb{Z}_K \ .$$
- *Finally, if $p = 2$ and $F(X,Y) \equiv XY(X+Y) \pmod 2$, then $2\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, with*
$$\mathfrak{p}_1 = 2\mathbb{Z}_K + a\theta\mathbb{Z}_K, \quad \mathfrak{p}_2 = 2\mathbb{Z}_K + (a\theta^2 + b\theta + 1)\mathbb{Z}_K \quad \text{and}$$
$$\mathfrak{p}_3 = 2\mathbb{Z}_K + (a\theta^2 + (a+b)\theta)\mathbb{Z}_K \ .$$

PROOF.

(1) We suppose first that $p \nmid a$ and consider

$$f(X) = a^2F(X/a,1) = (1,b,ac,a^2d) \ .$$

It is a monic irreducible integral polynomial with a root α in K. Localizing at $\mathfrak{p}$ above p in $\mathbb{Z}_K$, we find that α generates $\mathbb{Z}_{K,\mathfrak{p}}$ over $\mathbb{Z}_{(p)}$. Indeed $\mathbb{Z}[\alpha] \subset \mathbb{Z}_K$ and

$$\operatorname{disc}(\mathbb{Z}[\alpha]/\mathbb{Z}) = a^2 \operatorname{disc}(\mathbb{Z}_K/\mathbb{Z})$$

with $\gcd(a,p) = 1$. Thus, if $f(X) = \prod U_i^{e_i}(X)$, we get

$$p\mathbb{Z}_K = \prod \mathfrak{p}_i^{e_i}, \quad \text{with } \mathfrak{p}_i = p\mathbb{Z}_K + U_i(\alpha)\mathbb{Z}_K \ .$$

Now, we can take $\alpha = a\theta$ and $T_i(X,Y) = \varepsilon Y^{\deg U_i}U_i(aX/Y)$, with $\varepsilon \in \mathbb{F}_p^*$. Hence, we have

$$\mathfrak{p}_i = p\mathbb{Z}_K + T_i(\theta,1)\mathbb{Z}_K \ .$$

(2) When this is not the case, we look for an $M \in \mathrm{GL}_2(\mathbb{Z})$ such that we can apply 1. to $F \circ M$. If $p \nmid d$, we take

$$M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \ ,$$

else F has at most one non-zero root α in $\mathbb{F}_p$. If we are not in the last special case of the theorem, there exists $u \in \mathbb{F}_p^*$, $u^{-1} \neq \alpha$, so that $F(1,u)$ is not 0 mod p. Then we take

$$M = \begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix} \ .$$

As $F(1,u)$ is exactly the coefficient of x^3 in $G = F \circ M$, we are back to the preceding case. Of course, G is not reduced anymore, but still generates the field K.

(3) In the last case, p divides the coefficient of x^3 in all forms equivalent to F_K. Thus, from the definition of F_K, $p^2\mathfrak{d}_K | \mathfrak{d}(x)$ for all $x \in \mathbb{Z}_K$. This makes of p a "non-essential divisor" which, in our cubic setting, happens if and only if p equals 2 and is totally split in $K/\mathbb{Q}$ (see [**24**]). As 2 is unramified, $\operatorname{disc} F_K = \operatorname{disc} K$ is odd. We know as well that $2|a$ and $2|d$, so finally, we get $a \equiv d \equiv 0 \pmod 2$, $b \equiv c \equiv 1 \mod 2$, and F_K still factors as p.

To find an explicit decomposition, one has to split the étale algebra

$$\mathbb{A} = \mathbb{Z}_K/2\mathbb{Z}_K \approx (\mathbb{Z}/2\mathbb{Z})^3$$

whose elements are all idempotents. Now, if we put $e_1 = 1$, $e_2 = a\theta$, $e_3 = a\theta^2 + b\theta$, we find $e_2e_3 = a^2\theta^3 + ab\theta^2 = -ac\theta - ad = a\theta = e_2$ in $\mathbb{A}$, as $a\theta \in \mathbb{Z}_K$ and $c \equiv 1 \pmod 2$, $ad \equiv 0 \pmod 2$.

So e_2, $e_1 + e_3$, and $e_2 + e_3$ are the orthogonal idempotents giving the three factors.

□

3. Real cubic fields

If F is a class of positive discriminant, then $\operatorname{disc}(H_F)$ is negative. It is well known that there is a nice reduction theory for definite binary quadratic form. Recall that the Hessian is covariant with respect to the action of $\mathrm{GL}_2(\mathbb{Z})$. We shall get a canonical representative for F by specifying that its Hessian should be a reduced quadratic form, with some extra care for those forms lying on the boundary of the fundamental domain. This approach was initiated by Hermite, see [**26, 27**].

We call a quadratic form with real coefficients (P, Q, R) reduced if

$$|Q| \leqslant P \leqslant R \ ,$$

and $R > 0$ to exclude the trivial form. Beware that this is not exactly the standard notion. For instance our definition implies that $(1, -1, 1)$ is reduced,

as well as $(0,0,1)$! If $H=(P,Q,R)$ is a definite binary quadratic form, we call H^{-1} the quadratic form $(P,-Q,R)$ and $\mathrm{Aut}(H)$ the set of matrix in $\mathrm{GL}_2(\mathbb{Z})$ stabilizing H. Furthermore, we set

$$\sigma = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad .$$

LEMMA 3.1. *Let $H=(P,Q,R)$ and $H'=(P',Q',R')$ be two reduced definite binary quadratic form, such that there exists $M \in \mathrm{GL}_2(\mathbb{Z})$ with $H \circ M = H'$. Then, either $H'=H$ and $M \in \mathrm{Aut}(H)$, or $H'=H^{-1}$ and M belongs to $\mathrm{Aut}(H)\sigma$. Moreover, the only elements of $\mathrm{Aut}(H)$ are $\pm\mathrm{Id}$, except in the following special cases, which can occur simultaneously:*

- *If $P=R$,* *add* $\pm\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.
- *If $Q=0$,* *add* $\pm\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.
- *If $P=R$ and $Q=0$,* *add* $\pm\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.
- *If $P=\varepsilon Q$,* *add* $\pm\begin{pmatrix} 1 & \varepsilon \\ 0 & -1 \end{pmatrix}$.
- *If $P=\varepsilon Q=R$,* *add* $\pm\begin{pmatrix} -1 & 0 \\ \varepsilon & 1 \end{pmatrix}$, $\pm\begin{pmatrix} 0 & -1 \\ 1 & \varepsilon \end{pmatrix}$, $\pm\begin{pmatrix} \varepsilon & 1 \\ -1 & 0 \end{pmatrix}$.

Where, in the last two cases, ε is either 1 or -1.

PROOF. Being equivalent, H and H' represent the same numbers and share the same discriminant. As they are reduced, their first and last coefficients respectively correspond to their minimum over $\mathbb{Z}^2-\{(0,0)\}$ and their next minimal value. Thus they are equal. Equality of discriminants then yield $Q^2=Q'^2$. Hence $H'=H$ or $H'=H^{-1}=H\circ\sigma$, and we only need to compute $\mathrm{Aut}(H)$.

We call as usual S and T the following two generators of the modular group:

$$S=\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and let

$$M=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

be an automorphism of (P,Q,R). We call $\mathcal{F}$ the usual fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$ in Poincaré's half-plane. If $M \in \mathrm{PSL}_2(\mathbb{Z})$, it fixes a point in $\mathcal{F}$, and so is either Id, S if $H=(P,0,P)$, ST or $(ST)^2$ if $H=(P,P,P)$, TS or $(TS)^2$ if $H=(P,-P,P)$.

If $\det M=-1$, then M swaps the two complex roots τ and $\overline{\tau}$ of H. That is

$$\frac{a\tau+b}{c\tau+d}=\overline{\tau} \Rightarrow a\tau+b=c\tau\overline{\tau}+d\overline{\tau}$$

Taking imaginary parts, we get $a = -d$ and then $bP = aQ + cR$, the determinant value giving $a^2 + bc = 1$. Putting things together we get: $H(a, c) = P$. On the other hand, $H(a, c) \geqslant (P - |Q| + R) \min(a^2, c^2)$, and, as H is reduced, we have $|Q| \leqslant P \leqslant R$. It follows:

- If $ac \neq 0$, then $a^2 = c^2 = 1$ and $P = |Q| = R$. We have $a = -d = \pm 1$ and $b = 0$. If $P = \varepsilon Q$, we have $a = -\varepsilon c$, where $\varepsilon = \pm 1$.
- If $c = 0$, then $a^2 = 1$, and $bP = aQ$. This implies either $b = 0$, $Q = 0$, or $b = \varepsilon a$, $P = \varepsilon Q$, with $\varepsilon = \pm 1$.
- If $a = 0$, then $Rc^2 = P$, so $R = P$, $c^2 = 1$. We deduce $b = c = \pm 1$, $a = d = 0$.

Which concludes our proof. □

Definition 3.2. A binary integral cubic form $F = (a, b, c, d)$ of *positive* discriminant is called *reduced* whenever its Hessian (P, Q, R) is so and

- $a > 0$, $b \geqslant 0$, where $d < 0$ whenever $b = 0$.
- If $Q = 0$, $d < 0$.
- If $P = Q$, $b < |3a - b|$.
- If $P = R$, $a \leqslant |d|$, and $b < |c|$ whenever $|d| = a$.

It then comes as no surprise that:

Corollary 3.3.

(1) *Two equivalent reduced real cubic forms are equal.*
(2) *A reduced real cubic form belonging to U is irreducible.*
(3) *Any irreducible real cubic form is equivalent to a unique reduced one.*

Proof.

(1) Tedious but straightforward: as their Hessians are equal or inverse of one another, one only needs to check the possible automorphisms as listed in Lemma 3.1. Some side notes though: it is well known that the automorphisms of positive determinant of a quadratic form correspond to units in the quadratic field defined by its discriminant. These in turn act on the cubic form according to the *cube* of the unit. Thus TS and $(TS)^2$, which correspond to cube roots of unity, act trivially on any cubic form. A brute force calculation readily confirms this anyway. Also, $P = Q = R$, resp. $P = -Q = R$, if and only if F is of the form $(a, b, b - 3a, -a)$, resp. $(a, b, -b - 3a, a)$.
(2) Suppose F is reducible. Then there exists a form $G = (a, b, c, d)$ equivalent to F, with $a = 0$, $b \geqslant 0$, and $0 \leqslant c \leqslant b$, which of course belongs also to U. We are going to show that the Hessian of this last form is reduced; checking its automorphisms will then lead us to a contradiction. We compute the discriminant of G, $\Delta = b^2c^2 - 4b^3d$, and its Hessian

$$(P, Q, R) = (b^2, bc, c^2 - 3bd) \ .$$

We see that $b^2|\Delta$, thus for all odd primes p dividing b, we have $p|\gcd(P,Q,R)$ by Lemma 1.2/1. So p divides (c^2-3bd) and b, hence $p|c$, and $p^3|\Delta$. We must then have $p=3$ by Lemma 1.2/2. But $9|a$ so G cannot belong to $U_3\backslash V_3$, thus $3\nmid b$.

Now, if $2|b$, then $\Delta\equiv b^2c^2 \pmod{16}$ thus G does not belong to V_2. We must then have $2|c$, hence $16|\Delta$, which is absurd. Moreover, $b\neq 0$ else $\Delta=0$ and G does not belong to U_p, for all p. Thus $b=1$, and $c=0$ or $c=1$. It follows that the Hessian of (a,b,c,d) is either $(1,1,1-3d)$ or $(1,0,-3d)$. But $\Delta=c^2-4d>0$, so $d\leqslant -1$ and thus both $1-3d$ and $-3d$ are greater than 1. Thus both our possible Hessians are reduced, and whichever is the correct one is equal to the Hessian H_F of F or to its inverse. This implies that G is obtained from F by an automorphism of H_F, modulo σ. As the only automorphisms of H_F, as well as σ, fix a which is 0, we see that the first coefficient of F is 0, which is forbidden for a reduced form. Here is our contradiction.

(3) Any real cubic form is equivalent to a form F whose Hessian H is reduced. Now, if this Hessian has one of the aforementioned special forms, the patient reader will check that either F or $F\circ M$ is reduced, where M is an automorphism of H. Note that it is vital that F be irreducible here. More precisely, we need the trivial fact that F is reducible whenever a or d equals 0, $Q=b=0$, $P=Q$ and $b=|3a-b|$, or $P=R$, $a=|d|$ and $b=|c|$.

□

Remark 3.4. In those cases where the Hessian has some non-trivial automorphisms, we needed to fix a representative in the corresponding orbits of cubic forms. There, all the possible choices are equivalent. Furthermore, Lemma 3.5 will imply that these special cases, as listed in Lemma 3.1, occur at most $O(X^{3/4})$ times. But there is another choice we had to make, taking into account that we needed $\mathrm{GL}_2(\mathbb{Z})$ and not $\mathrm{SL}_2(\mathbb{Z})$ to operate on our set of forms. There are two natural ideas: $b\geqslant 0$ as we have just seen, or $Q\geqslant 0$. The latter one was aesthetically more pleasing because we did not have to bother with ε or σ, and things were a little more "canonical". They still are, but not in a very natural way.

In both cases, the algorithm would run roughly as follows: execute four enclosed loops for the four coefficients of the form, taking advantage of every possible inequality, testing each time if we had a field or not. And the choice $Q\geqslant 0$ now became awkward. For instance the condition $Q\geqslant 0$ could not be exploited before at least three of the four defining coefficients had been set. In fact, the general algorithm was much more complicated in this case, because the sign of b had to be considered at times, and disregarded at others. The most obvious example would be the computation of b^2 which should only be done once. Thus, the b-loop had to actually be on the absolute value of b, sometimes executing two instructions, sometimes one, depending on whether the sign of b had any importance. This led to a rather obscure and slightly less efficient program. Thus, the opposite

choice was made, but it should not be considered as the "right" one. In fact, the normalization $Q \geqslant 0$ being best-suited for theoretical purpose, we shall use it in Proposition 3.9.

We can in a very explicit way find bounds for the coefficients of a reduced form:

LEMMA 3.5. *Let $F = (a, b, c, d)$ be a reduced form whose discriminant lies in $]0, X]$. We have:*

$$|a| \leqslant \frac{2X^{1/4}}{3\sqrt{3}} \ , \tag{16}$$

$$0 \leqslant b \leqslant \frac{3a}{2} + \sqrt{\sqrt{X} - \frac{27a^2}{4}} \ . \tag{17}$$

Call P_2 the unique positive real solution of the equation

$$-4P_2^3 + (3a + 2b)^2 P_2^2 + 27a^2 X = 0 \ ,$$

then

$$\frac{b^2 - P_2}{3a} \leqslant c \leqslant b - 3a \ . \tag{18}$$

PROOF. Let $H = (P, Q, R)$ be the Hessian of F, $3\Delta = 4PR - Q^2$. Recall that

$$|Q| \leqslant P \leqslant R \ .$$

As in the classical quadratic case, we remark:

$$P^2 \leqslant PR \leqslant \Delta \leqslant X \ . \tag{19}$$

On the other hand, the formulas defining H yield:

$$P^2 = Pb^2 - 3Qab + 9Ra^2 \ .$$

This quadratic equation in b has discriminant

$$9a^2(Q^2 - 4PR) + 4P^3 = 4P^3 - 27a^2 D \ .$$

Thus it has a solution if and only if

$$a^2 \leqslant \frac{4P^3}{27D} \leqslant \frac{4P}{27} \leqslant \frac{4\sqrt{X}}{27} \ ,$$

and (16) is proved.

The largest of these two solutions is :

$$b = \frac{3Qa + \sqrt{4P^3 - 27a^2 D}}{2P} = \frac{3aQ}{2P} + \sqrt{P - \frac{27a^2 D}{4P^2}} \leqslant \frac{3a}{2} + \sqrt{P - \frac{27a^2 D}{4P^2}} \ .$$

This is an increasing function of P, which is thus maximal when $P^2 = D$. As the resulting expression increases with D, we finally obtain

$$b \leqslant \frac{3a}{2} + \sqrt{\sqrt{X} - \frac{27a^2}{4}} \ ,$$

which is (17). Note that these two bounds are actually sharp, as they are reached whenever $P = Q = R$.

The last one is a little more intricate: given a, b, P and D, we need to know at what condition there exists Q such that:

$$f(Q) = Pb^2 - 3Qab + 9a^2\left(\frac{3D+Q^2}{4P}\right) - P^2 = 0 \ , \tag{20}$$

$$-P \leqslant Q \leqslant P \leqslant \frac{3D+Q^2}{4P} \ . \tag{21}$$

Of course, $(3D+Q^2)/4P$ is equal to R, but we do not want too many variables in there. Given (20), and if we recall that both a and b are non-negative, the rightmost inequality in (21) becomes

$$Q \geqslant \frac{P}{3ab}(b^2 + 9a^2 - P) =: U \ .$$

Let's study (20) as a quadratic equation in Q: its discriminant is

$$\Delta = 4P^3 - 27a^2D \ ,$$

and we have

$$\begin{aligned} f(-P) &= P^2(3a+2b)^2 - \Delta \ , \\ f(P) &= P^2(3a-2b)^2 - \Delta \ , \\ f(U) &= \frac{P^2}{b^2}(b^2 - 9a^2 + P)^2 - \Delta \ . \end{aligned}$$

Finally, its minimum is reached at $Q_{min} = 2bP/3a > 0$, the sign of the minimal value being opposite to the sign of Δ, and thus negative.

Call respectively $P_1(D)$ and $P_2(D)$ the positive real solution of the equations:

$$-4P^3 + (3a-2b)^2P^2 + 27a^2D = 0 \ ,$$

$$-4P^3 + (3a+2b)^2P^2 + 27a^2D = 0$$

(these always exist) and $P_3(D) \leqslant P_4(D)$ the two positive solutions of

$$P^2(b^2 - 9a^2 + P)^2 - 4b^2P^3 + 27a^2b^2D = 0 \ .$$

Both P_3 and P_4 only exist when $4P^2 \geqslant 3D$, otherwise the left-hand expression remains positive. Of course, these three equations correspond to $F(P) = 0$, $F(-P) = 0$ and $F(U) = 0$ respectively. There are two cases:

- $0 \leqslant b \leqslant 3a/2$. Then $Q_{min} \leqslant P$. There is a solution in $[-P, Q_{min}]$ if and only if $f(-P) \geqslant 0$, $U \leqslant Q_{min}$, and $f(U) \geqslant 0$. And a solution in $[Q_{min}, P]$ if and only if $f(P) \geqslant 0$, and either $f(U) \leqslant 0$ or $U \leqslant Q_{min}$.
- $b > 3a/2$. Now $Q_{min} > P$, thus any solution will lie in $[-P, Q_{min}]$. The corresponding statement from the preceding case holds verbatim, save that $U \leqslant Q_{min}$ can be replaced by $U \leqslant P$, which is a little more precise but is a consequence of the other two inequalities.

Because of the trivial equality $c = (b^2 - P)/3a$, we only need to bound P. This will involve the quantities $P_i(D)$ defined above. Applying the implicit function theorem yields that $P_1(D)$, $P_2(D)$, and $P_3(D)$ are increasing with D, while $P_4(D)$ decreases. Recalling that $P^2 \leqslant D \leqslant X$, we call, we call $P_i(X) = P_i$, for all $1 \leqslant i \leqslant 4$. We have $P_1(P^2) = P_3(P^2) = 9a^2 - 3ab + b^2$ and $P_2(P^2) = P_4(P^2) = 9a^2 + 3ab + b^2$.

Remark first that, in the case $U \leqslant Q_{min}$, *i.e.* $P + b^2 - 9a^2 \geqslant 0$, we have $f(-P) \leqslant f(U)$ if and only if $P \leqslant 9a^2 + 3ab + b^2$, *i.e.* $c \geqslant -3a - b$. Now we enumerate.

Suppose first that $b > 3a/2$.

As $U \leqslant Q_{min}$, we have $P + b^2 - 9a^2 \geqslant 0$, that is $c \leqslant 2b^2/3a - 3a$. But $U \leqslant P$ yields $c \leqslant b - 3a$ which is better. We see that $P^2(b^2 - 9a^2 + P)^2 \geqslant b^2P^2(3a + 2b)^2$ if and only if $c \leqslant -3a - b$, in which case only $f(-P)$ is involved.

- If $-3a - b < c \leqslant b - 3a$, we have $P \leqslant P_3$ or $P \geqslant P_4$ and this implies $P \leqslant P_2$.
- If $c \leqslant -3a - b$, we have $P \leqslant P_2$.

Now, we consider $0 \leqslant b < 3a/2$.

- If $c > -3a + 2b^2/3a$, then $U > Q_{min}$. And we have $f(U) \leqslant 0 \leqslant f(P)$, that is $P_3(P^2) \leqslant P \leqslant P_4(P^2)$, *i.e.* $-3a - b \leqslant c \leqslant b - 3a$, and $P \leqslant P_1$, which implies that $P \leqslant P_2$.
- If $-3a - b \leqslant c \leqslant -3a + 2b^2/3a$, we need $f(U) \geqslant 0$, *i.e.* $P \leqslant P_3$ or $P \geqslant P_4$.
- If $c \leqslant -3a - b$, we still have $P \leqslant P_2$.

All of these imply that $P \leqslant P_2$. □

Remark 3.6. As far as c is concerned, we proved a much more precise statement than (18). But we will have no use for it, as it would only affect a small range of c, of the order of b, that is at most $X^{1/4}$). And we would then have to solve several extra equations involving cube roots. It turns out this is not a fair trade.

We now recall some of the densities computed by Davenport and Heilbronn in [**13**] and [**16**] :

THEOREM 3.7. *Let $H_3^+(X)$, resp. $N_3^+(X)$ denote the number of classes of equivalent cubic forms, resp. of isomorphism classes of* real *cubic fields, with positive discriminant less than X. As X tends to $+\infty$, we have:*

$$H_3^+(X) = \frac{\pi^2 X}{72} + C^+ \cdot X^{5/6} + O(X^{2/3+\varepsilon}) \approx 0.137 \cdot X \ , \tag{22}$$

$$N_3^+(X) = \frac{X}{12\zeta(3)} + o(\frac{X}{\log^2 X}) \approx 0.0693 \cdot X \ . \tag{23}$$

Remark 3.8. The non principal part in (22) is actually due to Shintani [**48**], improving on Davenport's original result [**13**]. The error term in (23) was proved in [**1**].

Once a, b, c are set as in Lemma 3.5, the coefficient d satisfies:

$$(-27a^2)d^2 + 2(9abc - 2b^3)d + (b^2c^2 - 4ac^3 - X) \leqslant 0 \tag{24}$$

as well as

$$|bc - 9ad| \leqslant b^2 - 3ac \leqslant c^2 - 3bd \ , \tag{25}$$

and the number of such (a, b, c, d) is then about $H_3^+(X)$. Now, due to

$$\frac{H_3^+(X)}{N_3^+(X)} \longrightarrow \frac{12\zeta(3)\pi^2}{72} \approx 1.97$$

as X tends to infinity, only about half of these quadruplets will be eliminated for congruence reasons. So there is very little waste among the polynomials we produce.

Our reduction theory being so explicit, it is very easy to characterize subclasses of cubic fields:

PROPOSITION 3.9. *Let K be a real cubic field, F_K be the associated reduced form,* with the normalization $Q \geqslant 0$, *and $H_K = (P, Q, R)$ its Hessian. Then*

(1) *K is cyclic* (i.e. $\mathrm{disc}(K) = f^2$) *if and only if $H_K = f_H(1, 1, 1)$.*
(2) $\mathrm{disc}(K) = 5f^2$ *if and only if $H_K = f_H(1, 1, 4)$ or $H_K = f_H(2, 1, 2)$.*
(3) $\mathrm{disc}(K) = 8f^2$ *if and only if $H_K = f_H(1, 0, 6)$ or $H_K = f_H(2, 0, 3)$.*
(4) $\mathrm{disc}(K) = 12f^2$ *if and only if $H_K = f_H(1, 0, 9)$ or $H_K = f_H(2, 2, 5)$, or $H_K = f_H(1, 0, 1)$.*
(5) *Let $\Delta > 0$ be a fundamental discriminant, then* $\mathrm{disc}(K) = \Delta f^2$ *if and only if H_K is a multiple of a primitive reduced form whose discriminant is -3Δ ($f = f_H$) or $-\Delta/3$ ($f_H = 3f$ and $3 \mid f$).*

PROOF. Part 5 is a simple consequence of Lemma 1.6 and our definition of reduced forms. The other assertions follow easily from this one. □

Due to the trivial equality

$$H(b, -3a) = P^2 \ , \tag{26}$$

we can "easily" build back the fields from a given discriminant. The preceding proposition gives all the possible Hessians. For all of them equation (26) has finitely many solutions, and given a, b and the Hessian, the cubic form is completely determined. An explicit study of the Hessian's automorphisms would even yield a complete one-to-one parametrization for the fields whose discriminant has the form Δf^2.

4. Complex cubic fields

In the complex case, our version of Hermite reduction does not work anymore: there can be many reduced forms in a given class of indefinite quadratic forms, and selecting one among these is awkward. We use instead an even simpler idea of Mathews and Berwick: if an irreducible cubic form $F = (a, b, c, d)$ has negative discriminant, it has a unique real root $\theta \notin \mathbb{Q}$, and we can factor F (in $\mathbb{R}[x, y]$!):

$$F(x, y) = (x - \theta y)(Ax^2 + Bxy + Cy^2) \ .$$

One easily computes

$$\operatorname{disc} F = (B^2 - 4AC)(A\theta^2 + B\theta + C)^2 \ .$$

As $\operatorname{disc} F < 0$, the "quadratic factor", $Q_F = (A, B, C)$, has negative discriminant and we can impose $A \geqslant 0$ by changing the signs of x and y. We have:

$$a = A, \quad b = B - \theta A, \quad c = C - \theta B \quad \text{and} \quad d = -\theta C \ .$$

Apart from a proportionality factor, (A, B, C) is covariant under $\mathrm{GL}_2(\mathbb{R})$. Indeed given

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \ ,$$

we have

$$Q_{F \circ M} = |a - \theta c| \cdot Q_F \circ M \ .$$

We define:

Definition 4.1. An integral binary complex cubic form F is *reduced* if $0 < |B| < A < C$, and

- $a > 0$.
- $b \geqslant 0$, with $d > 0$ if $b = 0$.

Note that if F is irreducible, then θ is an irrational number, and this excludes our former special cases: $B = 0$, $A = |B|$ or $A = C$. Another nice feature is that we do not have to factor F at all:

Lemma 4.2. *A complex cubic form $F = (a, b, c, d)$ is reduced if and only if:*

$$d^2 - a^2 + ac - db > 0 \ , \tag{27}$$

$$-(a - b)^2 - ac < ad - bc < (a + b)^2 + ac \ , \tag{28}$$

$$a > 0, \quad b \geqslant 0 \quad \textit{and } d > 0 \textit{ whenever } b = 0 \ . \tag{29}$$

Proof. See [**36**]. □

Lemma 4.3. (1) *A reduced complex cubic form belonging to U is irreducible.*

(2) *Any irreducible complex cubic form is equivalent to a unique reduced one.*

Proof.

(1) Just as in the proof of Corollary 3.3, a complex reducible form belonging to U is equivalent to $G = y(x^2 + \delta y^2)$ or $G' = y(x^2 + xy + \delta y^2)$, with $\delta \geqslant 1$. If a reduced form $F = (x - \theta y)(Ax^2 + Bxy + Cy^2)$ is equivalent to G or G', then (A, B, C) is equivalent to a multiple of either $(1, 0, \delta)$ or $(1, 1, \delta)$. As both are reduced, (A, B, C) is equal to one of them or their inverse, thus $B = 0$ or $A = \pm B$, all of which are forbidden.

(2) We only need to show that two reduced irreducible equivalent forms are equal. Let $F = G \circ M$, $M \in \mathrm{GL}_2(\mathbb{Z})$ be two equivalent reduced forms. Then there exists $\lambda \in \mathbb{R}_+^*$ such that $\lambda Q_F = Q_G \circ M$. We deduce $\lambda Q_F = Q_G$, thus M is an automorphism of Q_F. The proof then goes as before save that, as the forms are irreducible, all special cases are excluded.

□

The equivalent of Lemma 3.5 is much simpler :

LEMMA 4.4. *Let $F = (a, b, c, d)$ be a reduced form whose discriminant lies in $[-X, 0[$. We have:*

$$1 \leqslant a \leqslant \left(\frac{16X}{27}\right)^{1/4}, \tag{30}$$

$$0 \leqslant b \leqslant \frac{3a}{2} + \sqrt{\left(\frac{X}{3}\right)^{1/2} - \frac{3a^2}{4}}, \tag{31}$$

$$1 - b \leqslant c \leqslant U(a, b) + \left(\frac{X}{4a}\right)^{1/3}, \tag{32}$$

where $U(a, b) = b^2/3a$ if $a \geqslant 2b/3$, and $b - 3a/4$ otherwise.

PROOF. Write $F = (x - \theta y)(Ax^2 + Bxy + C)$, and recall that

$$a = A, \quad b = B - \theta A, \quad c = C - \theta B \ .$$

Setting $3\Delta = 4AC - B^2$, we have

$$|B| < A < C \quad \text{and} \quad A^2 < \Delta \ .$$

We set $D = |\operatorname{disc} F|$. From the equality $D = 3\Delta(A\theta^2 + B\theta + C)^2$, we get

$$2a\theta = -B \pm \sqrt{4a\left(\frac{D}{3\Delta}\right)^{1/2} - 3\Delta} \ .$$

The expression under the square root must be positive, so we obtain

$$16a^2 D \geqslant 27\Delta^3 \geqslant 27a^6 \tag{33}$$

and, recalling that $D \leqslant X$, we get (30). From $b = B - A\theta$, we derive

$$b = \frac{3B}{2} \mp \sqrt{a\left(\frac{D}{3\Delta}\right)^{1/2} - \frac{3\Delta}{4}} \ .$$

The square root is a decreasing function of Δ. Hence, using $|B| \leqslant a$ and $\Delta \geqslant a^2$, (31) follows.

We have $c = R - \theta B > A - \theta C > A - |\theta| A$. From $|B| < A$, we get $|b + \theta a| < a$, which implies $|\theta a| < a + b$. Thus $c > -b$, which is the left-hand side of (32). To get the right-hand side, we use the explicit formulas for b and c, which yield

$$4ac = -3B^2 + 4bB + 3\Delta =: Q(B) \ .$$

The quadratic form $Q(B)$ reaches its maximum $4b^2/3$ when $B = B_0 = 2b/3$. But, as we must have $B < A = a$, this has to be replaced by $U(a)$ whenever $B_0 > a$, and we are done. □

As before, we get a linear number of loops, and the corresponding theoretical values, as given in [**1, 14, 16, 48**], are as follows:

THEOREM 4.5. *Let $H_3^-(X)$, resp. $N_3^-(X)$, denote the number of classes of equivalent cubic forms, resp. of isomorphism classes of cubic fields, with negative discriminant greater than $-X$. As X tends to $+\infty$, we have:*

$$H_3^-(X) = \frac{\pi^2 X}{24} + C^- \cdot X^{5/6} + O(X^{2/3+\varepsilon}) \approx 0.411 \cdot X \ , \tag{34}$$

$$N_3^-(X) = \frac{X}{4\zeta(3)} + o\Big(\frac{X}{\log^2 X}\Big) \approx 0.208 \cdot X \ . \tag{35}$$

Remark 4.6. If we want an equivalent to Proposition 3.9, the complex situation is not as favorable as the real one. The possible quadratic covariants are difficult to list directly in a practical computational sense: their coefficients are not even rational. Thus we resort to Hermite reduction. Let K be a complex cubic field and suppose that $\mathrm{disc}(K) = \Delta f^2$ (Δ negative). We choose a system S of representatives for the classes (modulo $\mathrm{GL}_2(\mathbb{Z})$!) of quadratic forms of discriminant -3Δ and $-\Delta/3$. Then the canonical form F_K is equivalent to a cubic form whose Hessian H_K is a multiple of a primitive form H in S.

Now another problem arises: (26) has positive discriminant, and thus an infinite number of solutions. This can be circumvented as we only need to find the solutions (a, b) modulo the cubes in $\mathrm{Aut}\, H$. Namely, a simple computation shows that when M belongs to $\mathrm{Aut}\, H$, replacing F by $F \circ M$ multiplies $(b, -3a)$ by M^3. The cubic forms obtained can now easily be reduced in our former sense.

5. Implementation

Let P be some integer. Using an elementary sieve, we need to precompute the list of "non-squarefree" numbers $n \leqslant X$, such that there exists a prime $p \geqslant P$, with $p^2 | n$. One can trivially bound their number by:

$$\sum_{p \geqslant P} \frac{X}{p^2} \leqslant X \int_P^{+\infty} \frac{d\pi(t)}{t^2} \ .$$

The following well-known inequalities, due to Rosser and Schoenfeld [**42**, Theorem 1], give us a simple uniform bound:

$$\frac{x}{\log x}\Big(1 + \frac{1}{2\log x}\Big) \leqslant \pi(x) \leqslant \frac{x}{\log x}\Big(1 + \frac{3}{2\log x}\Big) \ ,$$

where the left-hand side is valid for $x \geqslant 59$, and the right-hand side for $x > 1$. Thus, if $P \geqslant 59$:

$$\begin{aligned}
\int_P^{+\infty} \frac{d\pi(t)}{t^2} &= -\frac{\pi(P)}{P^2} + \int_P^{+\infty} \frac{2\pi(t)dt}{t^3} \\
&\leqslant -\frac{1}{P\log P}\Big(1 + \frac{1}{2\log P}\Big) + \int_P^{+\infty} \frac{2dt}{t^2\log t} + \int_P^{+\infty} \frac{3dt}{t^2\log^2 t} \\
&= \frac{1}{P\log P}\Big(1 - \frac{1}{2\log P}\Big) + \int_P^{+\infty} \frac{dt}{t^2\log^2 t} \\
&\leqslant \frac{1}{P\log P}\Big(1 + \frac{1}{2\log P}\Big) \ .
\end{aligned}$$

Thus, depending on available memory and X, one can fix a P such that we can test if an integer bounded by X is squarefree in at most $\pi(P)$ divisions and a quick binary search, which can itself be optimized with hashing techniques. For instance, we can sort the lists according to the high-order bits of the discriminant; as we now only need to store the low-order bits, a careful implementation will keep to 32-bit integers far beyond the practical range of the algorithm. Having decided to use at most 32Mo in RAM for the hashing lists, we took $P = 97$ to compute a table up to $X = 10^{10}$ and $P = 661$ up to $X = 10^{11}$, trial division up to P still taking most of the computational time.

Call M the maximum memory one is willing to spend for the hashing lists, *i.e.* we will keep at most M 32-bit integers in RAM. We use the following initialization routine:

Sub-Algorithm 5.1 (`init`)

(1) [Initialize primes] Input X, the discriminant bound. Compute a table of primes up to $\sqrt{X}$, `p[]`, as well as their squares `pp[]`. Using a binary search, find the minimal prime p such that:

$$\frac{X}{p\log p} \cdot \left(1 + \frac{1}{2\log p}\right) \leqslant 3M \ .$$

If $p \leqslant 53$, find the minimal prime p such that

$$p^{-2} + \cdots + 53^{-2} \leqslant \frac{3M}{X} - \frac{1}{\log 59} \cdot \left(1 + \frac{1}{2\log 59}\right) \ .$$

If $p < 5$, set $p = 5$. Set `index` such that `p[index]`=p.

(2) [Initialize sieve] Put in `list[]` all the integers less than X, prime to 6, and admitting a divisor `pp[`i`]`, $i \geqslant$ `index`. Fill in boolean array `sqfull[]` up to $n = \sqrt{3X}$, such that `sqfull[`n`]` is `true` if and only if $p^2|n$ for some prime $p \geqslant 5$.

The primes 2 and 3 are special cases anyway and can be readily suppressed from the discriminant factorization: a single division modulo 72 is enough. Thus, one can restrict the lists to integers prime to 6, and there are then $6/\varphi(6) = 3$ times less numbers to keep in memory. Hence the $3 \cdot M$ instead of M in Step 1, as well as the test for $p < 5$. The bound $\sqrt{3X}$ in the definition of `sqfull` was chosen because we primarily want to test f_H with it.

The following common subroutine checks whether a reduced form belongs to U_p, for $p > 2$.

Sub-Algorithm 5.2 (`test`$(f_H, a, b, c, d, \Delta)$)
Input: (a, b, c, d) a reduced cubic form belonging to U_2, f_H and Δ respectively the content and discriminant of its Hessian (recall that $\Delta = -3\,\mathrm{disc}(a, b, c, d)$).
Output: F if it belongs to U, nothing otherwise.

(1) If (a, b, c, d) does not belong to U_3, as in Lemma 1.2, or `sqfull[`f_H`]` is `true`, then return.

(2) Set $t = \Delta/f_H^2$, and $t = t/\gcd(t, 72)$ so that now t is prime to 6. If $\gcd(t, f_H) > 1$, return.

(3) Return if t is not squarefree. The test should be done as follows: if n is small enough ($n \leqslant \sqrt{3X}$) return if `sqfull[`n`]` is `true`. Else search the sorted by construction `list` for n, then trial divide n by `pp[`i`]`, $2 \leqslant i <$ `index`, returning as soon as n is found or one `pp[`i`]` divides n.

(4) Output (a, b, c, d).

5.1. Real cubic fields. The actual algorithms are now simple to write:

Sub-Algorithm 5.3 (`is_real_field`(a, b, c, d, P, Q, R))
Input: a real cubic form $F = (a, b, c, d)$, and its reduced Hessian (P, Q, R).
Output: F, if it corresponds to a real cubic field.

(1) [Check special cases]
- if $P = Q$: if $|b| \geqslant |3a - b|$, return.
- if $P = R$: if $a > |d|$, return. If $a = |d|$ and $|b| \geqslant |c|$, return.
- if $|Q| = R$: if $4|P$ return. Execute `test`$(P, a, b, c, d, 3P^2)$, then return.

(2) Set $\Delta = 4PR - Q^2$. If $16|\Delta$ or [$\Delta \equiv 12 \pmod{16}$ and either P or R is odd], return.

(3) Set $f_H = \gcd(P, Q, R)$, then execute `test`$(f_H, a, b, c, d, \Delta)$.

Algorithm 5.4 (CRFCRF*)

*stands for Cubic Real Fields Counting Reduced Forms.

(1) Execute `init`.

(2) [Special case $b = 0$] Execute three embedded loops on a, c, d in this nesting order. Set the bounds using the reduction inequalities $a > 0$, $b \geqslant 0$ and (25), as well as (24) and Lemma 3.5. Compute the Hessian (P, Q, R), then execute `is_real_field` $(a, 0, c, d, P, Q, R)$.

(3) [General case] We now have four loops on a, b, c, d in this order, with the additional inequality $b > 0$. Compute the Hessian (P, Q, R), then execute `is_real_field` (a, b, c, d, P, Q, R).

Remark 5.5. Great care must be taken in setting the bounds for the various loops to avoid round-off errors. Also, many computations can be done at an early stage. For instance, $P = b^2 - 3ac$ can be computed before d is known. This is tedious but straightforward, so we chose not to hide the simplicity of the algorithm behind scores of auxiliary variables and explicit complicated bounds.

5.2. Complex cubic fields. Though it is now easier to test whether a form corresponds to a field, the general algorithm is a little more complicated than the previous one. First, because our reduction inequalities now involve solving (27) which is quadratic in d. And second, they do not imply anymore that the form discriminant has the expected sign: a test run of the algorithm after removing the sign condition will produce scores of counter-examples. Thus, we will have to deal with *three* quadratic inequalities instead of one.

Sub-Algorithm 5.6 (`is_complex_field`(a, b, c, d, P, Q, R))

(1) Set $\Delta = Q^2 - 4PR$. If $16|\Delta$ or [$\Delta \equiv 4 \pmod{16}$ and either P or R is odd], return `false`.

(2) Set $f_H = \gcd(|P|, |Q|, |R|)$, then execute `test`$(f_H, a, b, c, d, \Delta)$.

The shape of the algorithm is the same:

Algorithm 5.7 (CCFCCF*)

(1) Execute `init`.

(2) [Special case $b = 0$] Execute three embedded loops on a, c, d in this nesting order. The bounds are set using the reduction inequalities $a > 0$, $b \geqslant 0$ and Lemma 4.2, and the discriminant ones arising from $-X \leqslant \operatorname{disc} F < 0$ and Lemma 4.4. Compute the Hessian (P, Q, R).
Execute `is_complex_field` $(a, 0, c, d, P, Q, R)$.

(3) [General case] We now have four loops on a, b, c, d in this order, with the additional inequality $b > 0$. Compute the Hessian (P, Q, R), then execute `is_complex_field` (a, b, c, d, P, Q, R).

*stands for Cubic Complex Fields Counting Companion Forms.

5.3. General remarks. All these algorithms have been implemented in ANSI C on a DEC alpha (64-bit machine) with the help of the PARI library – see [**40**] for details on this useful number theory package.

• One can sensibly compute the number of (isomorphism class of) cubic fields up to $X \approx 10^{11}$ in this way. As one can see from Table 6.1, the overhead computations in subroutine `init` take a negligible time, thus the algorithm can easily be distributed.

• The intermediate results all fit in single precision long integers on 64-bit machines for reasonable X: say, less than 10^{12} in the real case, and 5.10^{10} in the complex case.

• It might happen that for given (a, b, c) satisfying our bounds, there does not exist d such that the form (a, b, c, d) is both reduced and has a discriminant in the expected range. One can prove the number of these "empty loops" is a $O(X^{3/4})$.

• If one compares with methods originating from Hunter's theorem, the gain is gigantic: no irreducibility check, no discriminant factorization, no search for automorphisms and thus, no need to keep all the fields found so far in memory. We get an essentially *linear* algorithm. The main loop is executed less than $C \cdot X + o(X)$ times, with $C = \pi^2/72$ in the real case and $C = \pi^2/24$ in the complex case. And all the rest is overhead computations, dominated by the main loop, save for the time spent searching the lists for non-squarefree numbers, or trial dividing to locate small square factors, which remains reasonable for the practical range of the method. As a matter of fact, sorting the fields by increasing discriminant takes much more time than actually computing them.

• It is feasible to compute fields whose discriminants lie in an interval $[X, X + Y]$, for very large X, say 10^{15}, when Y is small enough, say 10^6. We incorporate the relevant discriminant inequality in the loops and, instead of using lists of precomputed numbers, we factor the discriminant using a suitable probabilistic factorization method. The running time is then more or less the time needed to factor around Y numbers of size X. Of course, the empty loops become a problem if X is too large.

6. Results

The following tables give an idea of computational time and memory usage. First, we consider the `init` routine, which does not depend on the signature. Most of the time in there is spent building sieves. We call $P = \texttt{p[index]}$ the prime chosen to build the hashing lists. For instance, $P = 5$ means that no trial division actually takes place in `sqfree`. The "Square-full ints" column corresponds to the number of 32-bit integers stored in the lists:

	X	P	Square-full ints	Sieving time
	10^4	5	290	0.001 s
	10^5	5	2935	0.01 s
	10^6	5	29370	0.1 s
	10^7	5	293674	1.0 s
	10^8	5	2936998	7.0 s
$P > 5$	10^9	17	5474664	43 s
	10^{10}	97	6409864	356 s (5 min 56 s)
	10^{11}	661	6644929	3427 s (58 min 15 s)

TABLE 6.1. Overhead Computations.

Next, we give the data corresponding to the computation of real and complex cubic fields. Here, a is the maximal value for the first coefficient of the cubic form. They happen to be the ones given by the bound in Lemma 3.5 in the real case. And one less than the ones in Lemma 4.4 in the complex case, with the exception $X = 10^4$ where we get the exact bound. As was expected, we get a roughly linear behavior as long as $P = 5$, which quickly "diverges" as P increases. Up to the same discriminant bound, time spent for the complex computations compared to the real ones should be in the same ratio as the number of fields found: slowly decreasing in the given examples, equal to 3 at infinity due to Davenport-Heilbronn's result (not exactly so, the initializing step being exactly the same). But, as pointed out at the beginning of §5.2, the complex situation is a little worse, due to the extra square roots:

	X	# of fields	Elapsed time	a
	10^1	0	0.000 s	0
	10^2	2	0.000 s	1
	10^3	27	0.000 s	2
	10^4	382	0.005 s	3
	10^5	4,804	0.05 s	6
	10^6	54,600	0.5 s	12
	10^7	592,922	5.7 s	21
	10^8	6,248,290	64 s (1 min 04 s)	38
$P > 5$	10^9	64,659,361	774 s (12 min 54 s)	68
	10^{10}	661,448,081	18,641 s (5 h 11 min)	121
	10^{11}	6,715,824,025	714,488 s (8 days 7 h)	216

TABLE 6.2. Real cubic fields.

	X	# of fields	Elapsed time	a
	10^1	0	0.000 s	0
	10^2	7	0.000 s	1
	10^3	127	0.004 s	3
	10^4	1520	0.04 s	7
	10^5	17,041	0.3 s	14
	10^6	182,417	2.2 s	26
	10^7	1,905,514	21.3 s	49
	10^8	19,609,185	224 s (3 min 44 s)	86
$P > 5$	10^9	199,884,780	2,575 s (42 min 55 s)	155
	10^{10}	2,024,660,098	58,247 s (16 h 11 min)	276
	10^{11}	20,422,230,540	2,207,413 s (25 days 13 h)	492

TABLE 6.3. Complex cubic fields.

Such tables had previously been given by Fung-Willams [**19**] in the complex case (discriminant greater than -10^6) and Llorente-Quer [**34**] in the real case (discriminant lower than 10^7). Our results are in accordance with the former but disagree by one field with the latter. As these authors already pointed out, the density of cubic discriminants slowly increases up to the Davenport-Heilbronn limit. Recall that it is respectively $1/12\zeta(3) \approx 0.0693$ and $1/4\zeta(3) \approx 0.2080$ in the real and complex case. Thus in our computations, up to $X = 10^{11}$, the third decimal is already wrong.

But not so slowly if one considers the best proven error term in (23) or (35): $O(X/\log^2 X)$. In fact, if we write the experimental remainder as $X/\log^\alpha X$, and use the least square method to guess a "correct" value for α, we obtain an unstable behaviour: α increases steadily with the bound X, up to $\alpha \approx 3.9$ when $X = 10^{11}$. Thus, for all we know, this error term might even decrease faster than all negative powers of $\log X$.*

*And this is in fact the case, see Theorem 6.1.

CHAPITRE 3

Densités de Classes de Formes Cubiques et Calculs Heuristiques du 3-rang des Corps de Nombres

1. Introduction

Si K est un corps de nombres, on note $\mathrm{Cl}(K)$ son groupe des classes. Pour une fonction f définie sur les classes d'isomorphismes de groupes abéliens, on peut définir une "moyenne" (et donc une "probabilité" si f est la fonction caractéristique d'une propriété) sur les groupes de classes des corps de nombres, de signature et de clôture galoisienne fixée, en posant (quand la limite existe) :

$$M(f) = \lim_{x\to+\infty} \sum_{|d_K|<x} f\big(\mathrm{Cl}(K)\big) \Big/ \sum_{|d_K|<x} 1 \ ,$$

où d_K parcourt les discriminants des corps considérés. En petit degré, il est relativement facile de les calculer et $M(f)$ permet de formuler des conjectures numériques précises pour rendre compte des phénomènes apparents sur les tables – écrasante majorité de groupes cycliques, par exemple. Malheureusement, pour pratiquement toutes les fonctions f raisonnables (par exemple, la fonction caractéristique valant 1 si le groupe est cyclique, 0 sinon), on ne sait même pas si la limite existe.

Cohen et Lenstra (voir [**6**] pour une formulation précise) ont proposé un modèle probabiliste très simple pour le comportement moyen de la partie *impaire* du groupe des classes d'un corps quadratique imaginaire : on suppose que chaque groupe abélien fini G est réalisé comme groupe de classes avec une fréquence inversement proportionnelle au cardinal de son groupe d'automorphismes – ce qui permet d'expliquer simplement la prééminence des cycliques qui, à cardinal donné, sont les groupes abéliens admettant le moins d'automorphismes. Sous ces hypothèses, on peut interpréter $M(f)$ en terme de séries de Dirichlet, et un théorème taubérien élémentaire permet de prédire un comportement moyen par des calculs de résidus. Par exemple, la probabilité que cette partie impaire soit cyclique serait de

$$\frac{2\zeta(2)\zeta(3)}{3\zeta(6)\prod_{i>1}\zeta(i)(1-2^{-i})} \approx 97,76\% \ .$$

Le cas des corps quadratiques réels est traité de la même façon, en considérant cette fois des quotients d'un groupe abélien par un sous-groupe cyclique "générique" (par analogie avec l'infrastructure de Shanks qui réalise les classes de $\mathrm{Cl}(K)$

comme cycles de formes réduites). Il est à signaler qu'une fois l'hypothèse heuristique acceptée, tous les résultats sont des théorèmes et on obtient une formulation exacte de la limite. Outre l'excellent accord avec les tables, une raison sérieuse de croire en la validité du modèle est le *théorème* de Davenport-Heilbronn [**16**] donnant le nombre moyen d'éléments d'ordre 3 du groupe des classes des corps quadratiques (1/3 ou 1 suivant la signature) confirmant la prédiction. Nous ne connaissons essentiellement pas d'autre vérification (ni infirmation !).

Le traitement heuristique de la 2-composante (comme plus tard celui des "mauvais" premiers) est possible mais complexe. Nous éviterons soigneusement ce sujet dans la suite, même si les conjectures sont, là aussi, partiellement confirmées (voir [**21**]).

Une généralisation naturelle, ici très simplifiée, est présentée par Cohen et Martinet [**7**] : si K décrit les corps de nombres de signature (r_1, r_2) et de groupe de Galois Γ donnés, les groupes de classes $\mathrm{Cl}(K)$ sont supposés être "en moyenne" de la forme $G/\langle\sigma_1, \ldots, \sigma_n\rangle$, avec $n = \mathrm{rg}(\mathcal{O}_K^*) = r_1 + r_2 - 1$. En fait, cette présentation vide pratiquement leur travail de sa substance puisque Cohen et Martinet étudient des extensions relatives arbitraires (éventuellement non galoisiennes), et leur description en est considérablement compliquée.

On obtient un assez bon accord avec les tables, d'autant moins nombreuses que le degré s'élève, à condition de retirer les p-composantes correspondant aux "mauvais" nombres premiers que sont les diviseurs du degré de la clôture galoisienne. Certains de ces "mauvais" premiers devraient d'ailleurs se comporter conformément aux prédictions générales. Mais on ne dispose pas d'heuristique satisfaisante indiquant ces "bons" premiers (voir [**8**]). En l'absence de tables étendues, et en raison de la faible vitesse de convergence des limites concernées, on a déjà bien du mal à se convaincre que les prédictions sont vérifiées. Cela dit, le cas des corps quadratiques réels correspond à $n = 1$, le seul "mauvais" premier étant 2 (et il est bien "mauvais").

Soit maintenant K un corps quadratique imaginaire d'anneau d'entiers $\mathcal{O}_K$ et un ensemble $P = \{p_1, \ldots, p_n\}$ de premiers (impairs) distincts, totalement décomposés dans $K/\mathbb{Q}$, avec $p_i = \mathfrak{p}_i\mathfrak{p}_i'$. On note

$$S = S(P) = \{\mathfrak{p}_i : 1 \leqslant i \leqslant n\} \text{ et } \mathcal{O}_{K,S} = \{x \in K : v_{\mathfrak{p}}(x) \geqslant 0 \text{ si } \mathfrak{p} \notin S\} \ .$$

Nous verrons que, K étant quadratique imaginaire, les $\mathrm{Cl}(\mathcal{O}_{K,S})$ ont un comportement proche de celui que les heuristiques assignent aux groupes des classes des L tels que $\mathrm{rg}\,\mathcal{O}_L^* = n$ (voir le Lemme 4.1, avec $\mathrm{rg}\,\mathcal{O}_K^* = 0$). Comme y invite la remarque heuristique §8.b de [**7**], nous allons calculer le 3-rang moyen des $\mathcal{O}_{K,S}$ (il s'agira d'un théorème !) :

THÉORÈME 1.1. *Il existe $c > 0$ tel que*

$$\sum_{-X<\Delta_K<0} \#\left\{x \in \mathrm{Cl}(\mathcal{O}_{K,S}) : x^3 = 1, x \neq 1\right\} \Big/ \sum_{-X<\Delta_K<0} 1 = \frac{1}{3^n} + O\Big(\exp\big(-c(\log X \log\log X)^{1/2}\big)\Big) ,$$

où les Δ_K décrivent les discriminants des corps quadratiques imaginaires dans lesquels les premiers de S sont totalement décomposés.

Le cas $n = 0$ correspond au théorème de Davenport-Heilbronn sur le 3-rang des quadratiques imaginaires (avec un terme reste absent de l'original). En prenant $n = 1$, nous retrouvons bien la valeur correcte du 3-rang moyen des quadratiques réels, conformément au modèle de Cohen-Martinet.

Ce sera une conséquence immédiate d'un calcul de densité de classes de formes cubiques vérifiant une congruence adélique (comptées suivant leur discriminant). En reprenant un résultat géométrique de [**1**], nous obtenons une borne pour le terme d'erreur dans cette formule, et en particulier pour les théorèmes de densité des discriminants des corps cubiques de Davenport et Heilbronn. Un terme d'erreur moins précis apparaissait déjà en filigrane dans cet article.

2. Notations usuelles et conventions diverses

Si A est un ensemble fini, $|A|$ ou $\#A$ désigne son cardinal. Étant donnés deux entiers m et n, on note (m, n) le pgcd de m et n, c'est-à-dire le générateur positif de l'idéal de $\mathbb{Z}$ qu'ils engendrent. On note $\mu(n)$ la fonction de Möbius et $\pi(x)$ le nombre de premiers p inférieurs à x. La lettre p, indicée ou non, désigne toujours un nombre premier, et Δ un discriminant.

Si K et L sont deux corps de nombres, $K \subset L$, d'anneaux d'entiers respectifs $\mathcal{O}_K$ et $\mathcal{O}_L$, si $\mathfrak{p}$ est un premier de $\mathcal{O}_K$ et $\mathfrak{P}$ un premier de $\mathcal{O}_L$ au-dessus de $\mathfrak{p}$, on note $e(\mathfrak{P}/\mathfrak{p})$ (resp. $f(\mathfrak{P}/\mathfrak{p})$) le degré de ramification (resp. degré résiduel) de $\mathfrak{P}$ au-dessus de $\mathfrak{p}$. Dans le cas particulier d'une extension galoisienne, nous écrirons simplement $e(\mathfrak{p})$ et $f(\mathfrak{p})$. On notera L^G le sous-corps de L fixé par le sous-groupe G de $\mathrm{Gal}(L/K)$.

Si G est un $\mathbb{Z}$-module, on note $r_p(G)$ le p-rang de G, c'est-à-dire la dimension sur $\mathbb{F}_p$ de G/pG. Si A est un anneau dans lequel l'ensemble des idéaux fractionnaires non nuls forme un groupe commutatif pour la multiplication usuelle, on note $\mathrm{Cl}(A)$ le groupe des classes d'idéaux de A. Par abus de notation, si I est un idéal de A, on notera toujours I sa classe modulo les principaux. Par extension, si K est un corps de nombres d'anneau d'entiers $\mathcal{O}_K$, on notera $\mathrm{Cl}(K) = \mathrm{Cl}(\mathcal{O}_K)$ et $r_p(K) = r_p\big(\mathrm{Cl}(\mathcal{O}_K)\big)$. Lorsque $K = \mathbb{Q}(\sqrt{\Delta})$, on écrira même $\mathrm{Cl}(\Delta)$ et $r_p(\Delta)$. H_K désigne le corps de classes de Hilbert de K, *i.e.* l'extension abélienne non ramifiée maximale.

Soit q un entier tel que $p|q$ implique $p^2|q$ et $2|q$ implique $16|q$ – la lettre q désignera toujours un tel nombre dans la suite. On appelle alors discriminant

fondamental modulo q (dont on note l'ensemble DF_q) un élément de $\mathbb{Z}/q\mathbb{Z}$ que l'on peut obtenir par réduction modulo q d'un discriminant fondamental, c'est-à-dire d'un entier sans facteurs carrés autres que 4, congru à 1 modulo 4, ou de la forme 4α, avec $\alpha \equiv 2, 3 \pmod 4$. On note $D^{\pm}(X)$ l'intersection de la demi-droite $\mathbb{R}^{\pm}$ avec $\{|\Delta| \leqslant X\}$, et $DF^{\pm}(X)$ le sous-ensemble de $D^{\pm}(X)$ composé des discriminants fondamentaux. Par abus de notation, si F est une classe de n-formes de discriminant $\Delta(F)$, on écrira $F \in D^{\pm}(X)$, resp. $DF^{\pm}(X)$, pour $\Delta(F) \in D^{\pm}(X)$, resp. $DF^{\pm}(X)$. On placera un i en indice si les formes sont supposées irréductibles, et un p si elles sont primitives. Nous noterons par exemple $DF^{+}_{ip}(X)$ l'ensemble des classes de formes irréductibles et primitives, de discriminant Δ fondamental, $0 < \Delta \leqslant X$.

3. Discriminants fondamentaux et congruences

On se donne un entier q divisible par 16 et E_q un ensemble de discriminants fondamentaux modulo q. Par abus de notation, on dira qu'un entier n appartient à E_q si $n \bmod q \in E_q$.

PROPOSITION 3.1. *Si E_q ne contient pas d'éléments divisibles par 4, alors*

$$\sum_{\substack{n<X \\ n\in E_q}} \mu^2(n) = \frac{|E_q|}{q} \cdot \frac{X}{\zeta(2)} \cdot \frac{1}{\prod_{p|q}(1-1/p^2)} + O(\sqrt{X}) \ .$$

PREUVE. On utilise l'identité classique

$$\mu^2(n) = \sum_{d^2|n} \mu(d)$$

qu'il suffit de vérifier sur les p^{α} par multiplicativité ou de déduire de l'égalité des séries de Dirichlet formelles :

$$\sum \mu^2(n) n^{-s} = \frac{\zeta(s)}{\zeta(2s)} \ .$$

Alors,

$$\sum_{\substack{n<X \\ n\in E_q}} \mu^2(n) = \sum_{\substack{n<X \\ n\in E_q}} \sum_{d^2|n} \mu(d) = \sum_{d<\sqrt{X}} \mu(d) \sum_{\substack{l<X/d^2 \\ ld^2\in E_q}} 1 \ .$$

Si $(d, q) > 1$, aucun élément de E_q n'est de la forme ld^2, y compris pour $d = 2$ puisque nous avons supposé que $4 \nmid \Delta$, pour tout $\Delta \in E_q$. Si au contraire $(d, q) = 1$, alors

$$\sum_{\substack{l<X/d^2 \\ ld^2\in E_q}} 1 = \sum_{s\in E_q} \sum_{\substack{l<X/d^2 \\ ld^2=s\ (q)}} 1 = \sum_{s\in E_q} \sum_{\substack{l<X/d^2 \\ l=s/d^2\ (q)}} 1 = |E_q| \cdot \frac{X}{d^2 q} + O(1) \ .$$

Donc

$$\sum_{\substack{n<X\\ n\in E_q}} \mu^2(n) = \frac{|E_q|}{q} X \sum_{\substack{d<\sqrt{X}\\ (d,q)=1}} \frac{\mu(d)}{d^2} + O(\sqrt{X}) \ ,$$

et la suite est facile. □

COROLLAIRE 3.2. *Pour tout ensemble E_q de discriminants fondamentaux modulo q, on a :*

$$\sum_{\substack{0<n<X\\ n\in E_q}} \mu^2(n) = \frac{|E_q|}{q} \cdot \frac{X}{\zeta(2)} \cdot \frac{1}{\prod_{p|q}(1-1/p^2)} + O(\sqrt{X}) \ .$$

PREUVE. On note $\frac{1}{4}E_q = \{n \bmod \frac{q}{4} : 4n \in E_q\}$ et $E_q^0 = \{n \in E_q : 4 \nmid n\}$. Il nous suffit alors d'écrire

$$\sum_{\substack{0<n<X\\ n\in E_q}} \mu^2(n) = \sum_{\substack{0<n<X\\ n\in E_q^0}} \mu^2(n) + \sum_{\substack{0<n<X/4\\ n\in \frac{1}{4}E_q}} \mu^2(n)$$

et d'utiliser la Proposition 3.1 alliée au résultat trivial : $|E_q^0| + |\frac{1}{4}E_q| = |E_q|$. □

Remarque 3.3. Se donner q divisible par 16 oblige éventuellement à rajouter la congruence "$n \in DF_{16}$" à l'ensemble E_q que l'on désirait étudier, mais permet d'énoncer le résultat de façon simple. Quoi qu'il en soit, on vérifie facilement qu'il y a exactement 6 discriminants fondamentaux modulo 16, à savoir $\{1, 5, 8, 9, 12, 13\}$.

COROLLAIRE 3.4. *On se donne un ensemble $S = \{p_1, \ldots, p_n\}$ de nombres premiers impairs distincts et on note $\mathcal{K}_S$ l'ensemble des corps quadratiques où les p_i sont totalement décomposés. On a l'égalité :*

$$\sum_{\substack{\Delta\in DF^+(X)\\ \mathbb{Q}(\sqrt{\Delta})\in\mathcal{K}_S}} 1 = \frac{3X}{\pi^2} \prod_{p\in S} \frac{p}{2(p+1)} + O(\sqrt{X}) = \sum_{\substack{\Delta\in DF^-(X)\\ \mathbb{Q}(\sqrt{\Delta})\in\mathcal{K}_S}} 1 \ .$$

PREUVE. On pose $q = 16\prod p_i^2$. Un premier impair p est totalement décomposé dans $\mathbb{Q}(\sqrt{\Delta})$ si et seulement si Δ est un des $\frac{p-1}{2}$ carrés non nuls modulo p, ce qui implique $\Delta \in DF_{p^2}$. On pose alors $E_q = \{\Delta \in DF_q : \forall p \in S, \left(\frac{\Delta}{p}\right) = 1\}$ et on obtient l'égalité :

$$\frac{|E_q|}{q} = \frac{6}{16} \prod_{p\in S} \frac{p-1}{2p} \ .$$

La conclusion est alors immédiate. □

Remarque 3.5. Si $S = \emptyset$, on retrouve le résultat classique :

$$\sum_{\Delta\in DF^-(X)} 1 = \frac{3X}{\pi^2} + O(\sqrt{X}) = \sum_{\Delta\in DF^+(X)} 1 \ .$$

4. Formes cubiques et 3-rang

Soit K un corps de nombres, $\mathcal{O}_K$ son anneau d'entiers, et $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ un ensemble de premiers non associés de $\mathcal{O}_K$. Considérons alors, comme dans l'introduction,

$$\mathcal{O}_{K,S} = \{x \in K : \forall \mathfrak{p} \notin S, v_{\mathfrak{p}}(x) \geqslant 0\} \ ,$$

et notons $\langle S \rangle$ le sous-groupe de $\mathrm{Cl}(K)$ engendré par les $\mathfrak{p}_i$.

LEMME 4.1. *Pour tout $\mathbb{Z}$-module A, on note* $\mathrm{rg}(A)$ *la dimension du $\mathbb{Q}$-espace vectoriel $A \otimes_{\mathbb{Z}} \mathbb{Q}$.*

i. $\mathrm{rg}\, \mathcal{O}_{K,S}^* = \mathrm{rg}\, \mathcal{O}_K^* + |S|$.
ii. $\mathrm{Cl}(\mathcal{O}_{K,S}) \simeq \mathrm{Cl}(K)/\langle S \rangle \simeq \mathrm{Gal}(H_K^{\langle S \rangle}/K)$.

PREUVE.

i. Les éléments de $\mathcal{O}_{K,S}^*$ sont les S-unités de K. Le théorème de Dirichlet donne immédiatement le résultat.
ii. On vérifie que l'ensemble des idéaux de $\mathcal{O}_{K,S}$, c'est-à-dire l'ensemble des idéaux de $\mathcal{O}_K$ premiers à chacun des $\mathfrak{p}_i$ est un groupe commutatif, donc la notation $\mathrm{Cl}(\mathcal{O}_{K,S})$ est licite. On considère le morphisme canonique

$$\begin{array}{rccc} \varphi & : & \mathrm{Cl}(\mathcal{O}_K) & \to & \mathrm{Cl}(\mathcal{O}_{K,S}) \\ & & I & \mapsto & I\mathcal{O}_{K,S} \end{array}$$

Si $\mathcal{I} \in \mathrm{Cl}(\mathcal{O}_{K,S})$, alors $\varphi(\mathcal{I} \cap \mathcal{O}_K) = \mathcal{I}$, donc φ est surjectif. Supposons maintenant que la classe d'un idéal entier I appartienne à $\mathrm{Ker}\, \varphi$. On en déduit l'existence de $\alpha \in \mathcal{O}_K$ tel que $I\mathcal{O}_{K,S} = \alpha\mathcal{O}_{K,S}$. En prenant les valuations, on vérifie que $\frac{1}{\alpha} I \in \langle S \rangle$, donc $\mathrm{Ker}\, \varphi \subset \langle S \rangle$. Comme l'inclusion réciproque est banale, le premier isomorphisme est démontré.

L'application d'Artin, qui, à tout premier $\mathfrak{p}$, associe l'automorphisme de Frobenius $(\mathfrak{p}, H_K/K)$, donne un isomorphisme de $\mathrm{Cl}(K)$ sur $\mathrm{Gal}(H_K/K)$. Le théorème de Galois permet de conclure.

□

On pose maintenant $K = \mathbb{Q}(\sqrt{\Delta})$, S un ensemble de premiers de $\mathcal{O}_K$, et $\mathcal{O}_{K,S}$ défini comme dans l'énoncé du Lemme 4.1. Un lemme élémentaire de théorie des groupes montre que, si G est un groupe abélien fini, il y a

$$\frac{p^{r_p(G)} - 1}{p - 1}$$

sous-groupes d'indice p dans G (par dualité, un sous-groupe d'indice p correspond à $p-1$ caractères d'ordre p, et la p-torsion de $\hat{G} \simeq G$ est isomorphe à G/pG). On a donc

$$\frac{3^{r_3(\mathcal{O}_{K,S})} - 1}{2}$$

extensions cubiques de K incluses dans $H_K^{\langle S \rangle}$, donc dans H_K.

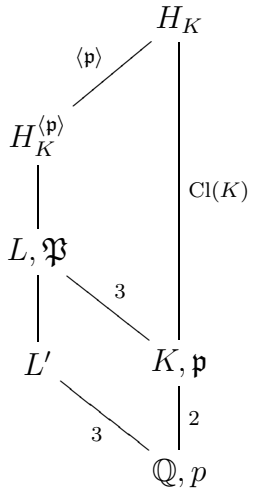
Les extensions cubiques cycliques non ramifiées de K sont galoisiennes sur $\mathbb{Q}$ et correspondent bijectivement aux classes d'isomorphismes de corps cubiques qui ne sont totalement ramifiées en aucune place finie (voir [**23**, p. 581]). Il est équivalent de dire que le discriminant commun aux éléments de la classe est fondamental*. La bijection s'obtient simplement en associant à un triplet la clôture galoisienne commune.

On note Φ l'ensemble des classes de formes cubiques binaires à coefficients dans $\mathbb{Z}$, primitives et irréductibles, et $\Phi(\Delta)$ l'ensemble des éléments de Φ dont le discriminant est Δ. Davenport et Heilbronn [**16**] ont montré l'existence d'une bijection préservant le discriminant entre, d'une part, un sous-ensemble (explicite !) de Φ et, d'autre part, les classes d'isomorphismes de corps cubiques. En particulier, si le discriminant Δ est fondamental, $\Phi(\Delta)$ correspond aux triplets de corps cubiques de discrimants Δ. Donc, d'après ce qui précède, aux sous-groupes d'indice 3 de $\mathrm{Cl}(K)$.

Nous devons donc identifier les extensions cubiques non ramifiées de K fixées par les Frobenius associés aux $\mathfrak{p}_i$ (notés $(\mathfrak{p}_i, H_K/K)$) et voir ce qu'il en advient par la bijection de Davenport-Heilbronn. La caractérisation est particulièrement simple :

LEMME 4.2. *Soit p un nombre premier totalement décomposé dans $K/\mathbb{Q}$ et $\mathfrak{p}$ un premier de $\mathcal{O}_K$ au-dessus de p. Une extension cubique de K incluse dans H_K est fixée par $(\mathfrak{p}, H_K/K)$ si et seulement si, modulo p, la classe de formes cubiques qui lui est associée se décompose en trois facteurs linéaires deux à deux non proportionnels (*i.e. *F est totalement décomposée modulo p).*

PREUVE. Soit L une extension cubique non ramifiée de K et $\mathfrak{P}$ un idéal premier de $\mathcal{O}_L$ au-dessus de p. On obtient le schéma suivant :



*ce qui implique qu'ils ne sont pas cycliques et qu'on a bien un triplet de corps cubiques (non galoisiens) dans chaque classe.

On sait que $(\mathfrak{p}, H_K/K)$ est trivial sur L si et seulement si $f(\mathfrak{P}/\mathfrak{p}) = 1$, c'est-à-dire, p étant totalement décomposé dans $K/\mathbb{Q}$, si $\mathfrak{p}$ est totalement décomposé dans L/K. On voit facilement que cette dernière condition est équivalente à ce que p soit totalement décomposé dans $L'/\mathbb{Q}$ où L' est l'un des trois corps cubiques (non galoisiens) inclus dans L. On désigne par F_L la classe de formes cubiques associée à la clôture galoisienne L de L' (ou encore au triplet de corps conjugués à L'). On sait d'après [**16**, Lemme 11] que, pour déterminer le type de décomposition d'un premier p dans $L'/\mathbb{Q}$, il suffit de factoriser F_L modulo p et d'appliquer le critère de Dedekind (bien que F_L ne soit pas en général unitaire !). Le résultat s'ensuit. □

On notera $(F, p) = (111)$ pour "F est totalement décomposée modulo p".

COROLLAIRE 4.3. *Soit S une famille de nombres premiers. Considérons les extensions cubiques non ramifiées des corps quadratiques où les éléments de S se décomposent totalement. Elles correspondent aux classes de formes F dont le discriminant est fondamental, vérifiant $(F, p) = (111)$ pour tout $p \in S$.*

PREUVE. Une forme de discriminant Δ fondamental correspond à une extension cubique non ramifiée de $\mathbb{Q}(\sqrt{\Delta})$. Au vu du lemme précédent, il suffit de remarquer que si $(F, p) = (111)$, le discriminant de F est un carré de $\mathbb{F}_p^*$ (puisque c'est le carré du produit des différences des racines), et donc p est totalement décomposé dans $\mathbb{Q}(\sqrt{\Delta})/\mathbb{Q}$. □

5. Formes cubiques et congruences

On désire compter les classes de formes cubiques vérifiant une relation de congruence donnée. Pour que la question ait un sens, il faut que celle-ci soit compatible à l'action de $Gl_2(\mathbb{Z})$, ce qui est par exemple le cas si la condition ne porte que sur le discriminant. Nous reprenons la démonstration proposée dans [**1**] pour la congruence particulière : $\Delta(F)$ *est fondamental et q divise Δ (q fixé).*

Essentiellement, on compte des points entiers dans un volume $C_X^{\pm}$ (suivant que les discriminants sont positifs ou négatifs) que l'on découpe en hypercubes de côté égal au module de la congruence. Ici, on va s'autoriser une condition adélique. Si l'on désire de surcroît privilégier une congruence modulo q et contrôler le terme d'erreur en fonction de q, les calculs se compliquent notablement. C'est le point de vue de [**1**], et nous renvoyons le lecteur à cet article pour un tel calcul (ne prétendant d'ailleurs aucunement à l'optimalité).

On se donne, pour tout p premier, un ensemble E_p de classes de formes modulo p^{α_p}, avec $\alpha_p \leqslant 4\alpha$ pour presque tout p. Par abus de langage, on écrira $F \in E_p$ si $F \bmod p \in E_p$. On note

$$E = \bigcap E_p, \quad E_q = \bigcap_{p|q} E_p, \quad s(p) = \frac{|E_p|}{p^{\alpha_p}} \quad \text{et} \quad t(p) = 1 - s(p) \ .$$

LEMME 5.1. *Soit $m = o(X^{1/4})$. Pour tout $\varepsilon > 0$, le nombre de classes de formes cubiques $F \in D_i^{\pm}(X)$ telles que $F \in E_p$ pour tout $p \mid m$ vaut*

$$H^{\pm} \prod_{p|m} s(p)X + O(m^{1/4}X^{15/16+\varepsilon}) \ ,$$

en posant

$$H^{+} = \frac{\pi^2}{72} \quad \text{et} \quad H^{-} = \frac{\pi^2}{24} \ .$$

PREUVE. On reprend les résultats et les notations de [**1**] : les classes de formes irréductibles de $\cap E_p$ correspondent, à un $O(X^{3/4+\varepsilon})$ près, à la moitié des points entiers du volume $C_X^{\pm}$ vérifiant la même congruence (Théorèmes 3.3 et 3.5). Si $m = o(X^{1/4})$, les points entiers d'une troncature $C_{X,\rho}^{\pm}$ de $C_X^{\pm}$ vérifiant la congruence sont en nombre

$$H^{\pm} \prod_{p|m} s(p)X + O(X^{1-\rho+\varepsilon} + mX^{3/4+3\rho+\varepsilon})$$

(Théorème 3.11 et Proposition 4.2) et les points du complémentaire de $C_{X,\rho}^{\pm}$ dans $C_X^{\pm}$ sont de cardinal dominé par $X^{1-\rho+\varepsilon}$ (Lemme 3.11). On pose

$$X^{\rho} = X^{1/16}m^{-1/4}$$

et le lemme est démontré. □

COROLLAIRE 5.2. *On se donne $Y > 0$ et on note $f^{\pm}(r)$ le nombre d'éléments $F \in D_i^{\pm}(X)$ tels que, pour tout premier p, on ait*

- *$p \mid r$ implique $F \bmod p \notin E_p$,*
- *$p \leqslant Y$ implique $F \bmod p \in E_p$.*

Alors, pour tout $\varepsilon > 0$, on a

$$f^{\pm}(r) = H^{\pm} \prod_{p \leqslant Y} s(p) \prod_{p|r} t(p) \cdot X + O(X^{15/16+\varepsilon} e^{\alpha Y} r^{\alpha}) \ .$$

PREUVE. Notons

$$P_Y = \prod_{p \leqslant Y} p \ .$$

En appliquant le lemme précédent, on obtient

$$f^{\pm}(r) = H^{\pm} \prod_{p \leqslant Y} s(p) \prod_{p|r} t(p)X + O\Big(X^{15/16+\varepsilon} \prod_{p|rP_Y} p^{\alpha_p/4}\Big) \ ,$$

et la conclusion est immédiate. □

THÉORÈME 5.3. *Hypothèses : il existe $C > 0$ et $u > 1$ tel que*

- *le nombre de classes de formes appartenant à $D^{\pm}(X)$, mais pas à E_p, est un $O(Xp^{-u})$,*
- *les formes de E_p sont non nulles modulo p,*
- *$t(p) \leqslant Cp^{-u}$.*

Alors le nombre de classes de formes communes à $D_{ip}^{\pm}(X)$ et E vaut :

$$H^{\pm}\prod_{p} s(p)X + O\Big(X\exp\big(-c(\log X\log\log X)^{1/2}\big)\Big)\ ,$$

pour un $c>0$ bien choisi.

Preuve. On note

$$S^{\pm}(Y) = \{F\in D_i^{\pm}(X) : \forall p\leqslant Y, F\in E_p\}\ .$$

Nous voulons compter le nombre de classes de formes appartenant à E_p pour tout p, donc primitives d'après notre deuxième hypothèse. Autrement dit,

$$\begin{aligned}\#S(Y) - \#\{F\in S(Y) : \exists p,\ Y<p<Z,\ F \bmod p\notin E_p\}\\ -\#\{F\in S(Y) : \exists p,\ Z\leqslant p,\ F\notin E_p\}\ ,\end{aligned}$$

où Z est un paramètre que l'on fixera dans la suite. Ou encore, avec les notations du corollaire précédent :

$$f(1) - \sum_{k\geqslant 1}\sum_{\substack{p_1<\cdots<\mathfrak{p}_k\\ Y<p_i<Z}} (-1)^{k-1} f(p_1\dots p_k) - O\Big(\sum_{p\geqslant Z} f(p)\Big)\ . \tag{36}$$

Le symbole de Landau est dominé par XZ^{1-u} grâce à notre première hypothèse. On introduit un paramètre K, et l'on décompose le terme principal sous la forme

$$f(1) - \sum_{1\leqslant k<K}\sum_{\substack{p_1<\cdots<\mathfrak{p}_k\\ Y<p_i<Z}} (-1)^{k-1} f(p_1\dots p_k) + O\Bigg(\sum_{\substack{p_1<\cdots<p_K\\ Y<p_i<Z}} f(p_1\dots p_K)\Bigg)\ .$$

Soit, en utilisant le Corollaire 5.2,

$$\begin{aligned}H^{\pm}\prod_{p\leqslant Y} s(p)X\Bigg[1 - \sum_{k=1}^{K-1}\sum_{\substack{p_1<\cdots<\mathfrak{p}_k\\ Y<p_i<Z}} (-1)^{k-1} t(p_1\dots p_k)\Bigg]\\ + O\Bigg(X^{15/16+\varepsilon}e^{\alpha Y}K\sum_{p_1<\cdots<p_K<Z}(p_1\dots p_K)^{\alpha}\Bigg)\ .\end{aligned}$$

Ou encore, en utilisant notre troisième hypothèse,

$$\begin{aligned}H^{\pm}\prod_{p\leqslant Y} s(p)X\Bigg[1 + \sum_{k\geqslant 1}\sum_{\substack{p_1<\cdots<\mathfrak{p}_k\\ Y<p_i<Z}} (-1)^{k} t(p_1\dots p_k)\Bigg]\\ + O\Bigg(XC^K\Big(\sum_{p>Y} p^{-u}\Big)^K + X^{15/16+\varepsilon}e^{\alpha Y}K\Big(\sum_{p<Z} p^{\alpha}\Big)^K\Bigg)\ .\end{aligned}$$

Soit

$$H^{\pm}\prod_{p<Z} s(p)X + O\Big(X\big(CY^{1-u}/\log Y\big)^K + X^{15/16+\varepsilon}e^{\alpha Y}KZ^{K(1+\alpha)}\Big)\ .$$

Finalement, en utilisant de nouveau la première hypothèse pour évaluer la vitesse de convergence de $\prod s(p)$, la quantité (36) vaut

$$H^{\pm}\prod s(p)X + O\Big(XY^{K(1-u)} + X^{15/16+\varepsilon}e^{\alpha Y}KZ^{K(1+\alpha)} + XZ^{1-u}\Big) \ .$$

On choisit $Y = \log X/\log_3 X$ et on suppose $K = o(X^{\varepsilon})$. Le terme reste, divisé par X, est dominé par

$$(37)\quad (\log X)^{K(1-u)} + X^{-1/16+\varepsilon}Z^{K(1+\alpha)} + Z^{1-u} \\ = e^{K(1-u)\log_2 X} + e^{(-1/16+\varepsilon)\log X + K(1+\alpha)\log Z} + e^{(1-u)\log Z} \ .$$

Afin d'égaliser les deux premiers termes, on pose

$$K = \frac{(1/16-\varepsilon)\log X}{(\alpha+1)\log Z + (u-1)\log_2 X} \ .$$

On choisit maintenant $\log Z = \lambda(\log X \log_2 X)^{1/2}$, avec $\lambda = (16(\alpha+1))^{-1/2}$, et l'on en déduit

$$K \sim \lambda(1-16\varepsilon)\left(\frac{\log X}{\log_2 X}\right)^{1/2} \ .$$

D'où le résultat, avec $c = \lambda(u-1) - \varepsilon$. □

La preuve montre que tout $c < c_0$ convient, avec

$$c_0 = \frac{u-1}{4(\alpha+1)^{1/2}} \ .$$

Si les E_p sont fixés et "raisonnables", des techniques de sommes d'exponentielles permettent d'augmenter légèrement cette valeur. C'est en particulier le cas pour le corollaire suivant. Il suffit de reprendre les calculs de [**1**] – nous avons conservé la valeur donnée par le Théorème 5.3.

Corollaire 5.4. *On fixe n et on se donne E_n tel que $\Delta(E_n) \subset DF_n$, où $\Delta(E_n)$ est l'ensemble des discriminants des formes de E_n. On note $r_3(\Delta)$ le 3-rang de $\mathbb{Q}(\sqrt{\Delta})$. Alors, pour tout $c < 24^{-1/2}$, on a l'égalité*

$$\sum_{\substack{\Delta\in DF^{\pm}(X)\\ \Delta\in\Delta(E_n)}} \frac{3^{r_3(\Delta)}-1}{2} = \frac{K^{\pm}X}{\zeta^2(2)}\prod_{p\mid n}\frac{s(p)}{(1-p^{-2})^2} \\ + O\Big(X\exp\big(-c(\log X\log\log X)^{1/2}\big)\Big) \ .$$

Preuve. On a pris comme E_p les classes correspondant aux discriminants fondamentaux, appartenant à E_n si $p \mid n$. Les calculs de Davenport et Heilbronn [**16**] montrent que si $n = 1$, les hypothèses du Théorème 5.3 sont satisfaites avec $s(p) = (1-p^{-2})^2$, et $4\alpha = u = 2$. On calcule alors

$$\prod s(p) = \zeta^{-2}(2)\prod_{p\mid n}\frac{s(p)}{(1-p^{-2})^2} \ .$$

□

6. Applications

THÉORÈME 6.1. *Notons $N_3^+(X)$ le nombre de corps cubiques réels de discriminant inférieur à X, et $N_3^-(X)$ le nombre de corps cubiques imaginaires de discriminant supérieur à $-X$. Alors, pour tout $c < 24^{-1/2}$, on a les égalités :*

$$N_3^+(X) = \frac{X}{12\zeta(3)} + O\Big(X \exp\big(-c(\log X \log\log X)^{1/2}\big)\Big) \ .$$

et

$$N_3^-(X) = \frac{X}{4\zeta(3)} + O\Big(X \exp\big(-c(\log X \log\log X)^{1/2}\big)\Big) \ .$$

PREUVE. On utilise les résultats de [**16**]. Les hypothèses du Théorème 5.3 sont satisfaites avec $s(p) = (1-p^{-3})(1-p^{-2})$ et $4\alpha = u = 2$. Puisque

$$\prod s(p) = \zeta^{-1}(3)\zeta^{-1}(2) \ ,$$

le résultat s'ensuit. □

Remarque 6.2. Les valeurs moyennes du Théorème 6.1 avaient déjà été calculées par Davenport et Heilbronn [**16**] sans reste explicite. Nous nous sommes d'ailleurs largement inspirés de leur méthode. À titre d'exemple, $N_3^+(10^{11}) = 6,715,824,025$, soit une densité expérimentale de 0.0672 pour les cubiques réels, à comparer avec $1/12\zeta(3) \approx 0.0693$. Pour les cubiques complexes, on trouve respectivement $N_3^-(10^{11}) = 20,422,230,540$, et $1/4\zeta(3) \approx 0.2080$ (voir les tables de [**2**]). Une régression linéaire sur ces données expérimentales, en échantillonnant sur une centaine d'intervalles $[0, X/100], \ldots, [99X/100, X]$ pour différentes valeurs de X, fournit une constante c comprise entre 0.6 et 0.7 (alors que $24^{-1/2} \approx 0.2$). Cela dit, en supposant le reste de la forme $X/\log^\alpha X$, le même type de calculs fournit $3 < \alpha < 4$, alors que nous venons de voir que l'erreur est bien plus faible – en particulier, elle est $o(X/\log^\alpha X)$ pour tout α. Ce résultat n'est donc probablement pas significatif.

THÉORÈME 6.3. *On se donne $\{p_1, \ldots, p_n\}$ un ensemble de nombres premiers impairs distincts. Pour tout corps quadratique imaginaire K de discriminant Δ_K, on choisit un ensemble $E_K = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ de premiers de $\mathcal{O}_K$, tel que chaque $\mathfrak{p}_i$ soit au-dessus d'un p_i. Alors, pour tout $c < 24^{-1/2}$,*

$$\sum_{\substack{\Delta \in DF^-(X) \\ e(\mathfrak{p}_i)=f(\mathfrak{p}_i)=1}} \big(3^{r_3(\Delta)} - 1\big) = \frac{3X}{\pi^2} \cdot \prod_{p \in \{p_1,\ldots,p_n\}} \frac{p}{6(p+1)} + O\Big(X \exp\big(-c(\log X \log\log X)^{1/2}\big)\Big) \ .$$

PREUVE. Posons $n = \prod p_i^2$ et notons $\Delta(F)$ le discriminant de la forme F ; on considère l'ensemble :

$$E_p = \{F \bmod p : (F,p) = (111)\} \ .$$

Une telle forme possède un coefficient dominant dans $\mathbb{F}_p^*$ et 3 racines distinctes dans $\mathbb{P}^1(\mathbb{F}_p)$, soit respectivement $p+1$, p et $p-1$ choix possibles. On en déduit

$$\#\big\{F \bmod p^2 : (F,p) = (111)\big\} = \frac{1}{6}p^5(p-1)(p^2-1) \ ,$$

puis

$$\frac{|E_n|}{n^4} = \prod_{p|n} \frac{(p-1)(p^2-1)}{6p^3} \ .$$

Le Corollaire 5.4 donne alors :

$$\sum_{\substack{\Delta \in DF^-(X) \\ \mathbb{Q}(\sqrt{\Delta}) \in \mathcal{K}_S}} \big(3^{r_3(\Delta)} - 1\big) = \frac{3X}{\pi^2} \prod_{p|n} \frac{p}{6(p+1)} + O\Big(X \exp\big(-c(\log X \log\log X)^{1/2}\big)\Big) \ .$$

□

D'où on déduit, en utilisant le Corollaire 3.4 et l'égalité facile

$$3^{r_3(\Delta)} = \#\{x \in \mathrm{Cl}(\Delta), x^3 = 1\} \ ,$$

le Théorème 1.1 annoncé en introduction.

CHAPITRE 4

Sur le ℓ-rang des Corps Quadratiques Imaginaires de Discriminant Pseudo-Premier

Ce chapitre doit beaucoup à une idée de D. Heath-Brown qui m'a été signalée par E. Fouvry. Elle fournit une estimation clé permettant d'appliquer un crible efficace aux familles que nous considérons.

1. Introduction

Soit ℓ un nombre premier. Si $K = \mathbb{Q}(\sqrt{\Delta})$ est un corps quadratique, on note $\mathrm{Cl}(\Delta)$ le groupe des classes de K. C'est un groupe abélien fini, et l'on définit son ℓ-rang $r_\ell(\Delta) = \dim_{\mathbb{F}_\ell} \mathrm{Cl}(\Delta)/\mathrm{Cl}(\Delta)^\ell$. Yamamoto [**51**] a montré par une construction explicite qu'il existe une infinité de corps quadratiques imaginaires (resp. réels) $\mathbb{Q}(\sqrt{\Delta})$, dont le ℓ-rang soit supérieur à 2 (resp. 1). Il généralisait une idée de Nagell [**39**] applicable aux seuls corps imaginaires, qui fournissait un ℓ-rang supérieur à 1.

Pour $\ell = 2$, Gauss avait déjà obtenu un 2-rang arbitrairement grand, en montrant que $r_2(\Delta)$ est égal au nombre de diviseurs premiers (comptés sans multiplicité) du discriminant de $\mathbb{Q}(\sqrt{\Delta})$. Pour $\ell = 3$, Craig [**10**] et Diaz y Diaz [**17**] ont obtenu des familles infinies de corps de 3-rang supérieur ou égal à 4. Pour $\ell = 5$ ou 7, on sait encore obtenir une infinité de corps de ℓ-rang plus grand que 2 (voir Mestre [**38**]). Si $\ell > 7$, on ne sait pas faire mieux que la construction de Yamamoto, bien que les conjectures de Cohen et Lenstra [**6**] fournissent une densité positive (explicite !) de corps quadratiques de ℓ-rang donné. L'idée de Nagell, adaptée par Yamamoto, est la suivante :

THÉORÈME 1.1. *Soit ℓ un premier impair, $K = \mathbb{Q}(\sqrt{\Delta})$ un corps quadratique et x, y deux entiers premiers entre eux, vérifiant $\Delta = y^2 - 4x^\ell$. Soit $\mathfrak{a}$ l'idéal de K engendré par x et $(y + \sqrt{\Delta})/2$. Nous avons*

$$\mathfrak{a}^\ell = \left(\frac{x + \sqrt{\Delta}}{2}\right) .$$

Supposons qu'il existe un diviseur premier s de x, $s \equiv 1 \pmod{\ell}$ tel que y ne soit pas une puissance ℓ-ième modulo s, et que l'unité fondamentale de K soit une puissance ℓ-ième modulo les diviseurs de s dans K. Alors $\mathfrak{a}$ n'est pas principal.

COROLLAIRE 1.2. *Soit $K = \mathbb{Q}(\sqrt{\Delta})$,* Δ négatif *qui n'est pas de la forme $-3f^2$, $\mathfrak{a}$ et s comme ci-dessus. Alors $\mathfrak{a}$ est d'ordre ℓ dans* $\mathrm{Cl}(\Delta)$.

Le cas réel est plus ennuyeux à cause de l'existence d'unités non triviales : si l'on désigne par E_K le groupe des unités de K, E_K/E_K^ℓ n'a aucune raison d'être réduit à la classe neutre. Yamamoto considére l'équation diophantienne

$$\Delta = y_1^2 - 4x_1^\ell = y_2^2 - 4x_2^\ell,$$

en supposant que les solutions vérifient certaines congruences, qui interdisent notamment les solutions évidentes $x_1 = x_2$, $y_1 = \pm y_2$. Il introduit ensuite deux idéaux dans $\mathrm{Cl}(\Delta)$ dont l'un au moins est d'ordre ℓ si le corps est réel, et qui engendrent un sous-groupe isomorphe à $\mathbb{Z}/\ell\mathbb{Z}\times\mathbb{Z}/\ell\mathbb{Z}$ sinon (on obtient alors un ℓ-rang supérieur à 2). Il construit ensuite une famille de solutions ne dépendant plus que d'un seul paramètre t. Si t vérifie une congruence fixée, il exhibe un polynôme explicite Q_ℓ, de degré $2\ell-1$, tel que pour tout Δ de la forme $Q_\ell(t)$, $r_\ell(\Delta) \geqslant 1$ si $\Delta > 0$ et $r_\ell(\Delta) \geqslant 2$ sinon.

Les résultats de Craig et Diaz y Diaz sont des raffinements de cette idée, ne s'appliquant qu'au cas $\ell = 3$. Ceux de Mestre proviennent d'une interprétation géométrique : il construit ses corps à partir de courbes elliptiques définies sur $\mathbb{Q}$, ayant un point de ℓ-torsion. Le théorème de Mazur interdit donc toute généralisation à $\ell > 7$.

Dans une autre direction, Davenport et Heilbronn [**16**] ont montré indirectement l'existence d'une infinité de corps quadratiques de 3-rang nul en calculant les valeurs moyennes

$$\lim_{X\to+\infty} \sum_{0<\Delta<X} 3^{r_3(\Delta)} \Big/ \sum_{0<\Delta<X} 1 = \frac{4}{3}\ ,$$

$$\lim_{X\to+\infty} \sum_{-X<\Delta<0} 3^{r_3(\Delta)} \Big/ \sum_{-X<\Delta<0} 1 = 2\ ,$$

où Δ parcourt les discriminants fondamentaux. En effet, si dans l'un de ces deux cas, il n'y avait qu'un nombre fini de corps de 3-partie triviale, la moyenne correspondante serait supérieure à 3. Mais, à notre connaissance, on ne sait ni construire explicitement de telles familles infinies, ni démontrer un résultat analogue pour $\ell > 3$.

Nous baptisons P_g un entier ayant au plus g diviseurs premiers (comptés avec multiplicité). Nous noterons par exemple $n = P_g$ pour indiquer que l'entier n a au plus g facteurs premiers. Nous avons montré dans [**1**], en appliquant un crible assez délicat au résultat de Davenport-Heilbronn, donc toujours de façon indirecte, que l'on pouvait obtenir des familles infinies de $\mathbb{Q}(\sqrt{P_g})$ de 3-rang nul, avec $g = 8$ dans le cas réel, $g = 26$ dans le cas imaginaire. Ces mêmes méthodes montraient l'existence d'une infinité de P_9 tels que $r_3(P_9) \geqslant 1$. Pour X assez grand, nous obtenions

$$\sum_{|n|<X,\, n=P_9} \left(3^{r_3(n)} - 1\right) \geqslant c\,\frac{X}{\log X}\ , \quad c > 0,$$

où l'on peut, au choix, restreindre la somme aux n positifs ou négatifs. Nous ne savons pas évaluer $3^{r_3(\Delta)}$ autrement que par la majoration grossière :

$$3^{r_3(\Delta)} \leqslant |\operatorname{Cl}(\Delta)| \ll \Delta^{1/2}\log(\Delta) \ .$$

On peut gagner un facteur $2^{\omega(\Delta)}$ en tenant compte de la partie 2-primaire. De plus, si Δ est positif, le $\log(\Delta)$ est superflu. Le résultat reste cependant désastreux puisque les $3^{r_3(\Delta)}$ sont bornés en moyenne. On en déduit tout de même :

$$\left|\left\{n : n = P_9, |n| < X, r_3(n) \geqslant 1\right\}\right| \geqslant c\,\frac{X^{1/2}}{\log^2 X} \ , \quad c > 0, \tag{38}$$

où les n peuvent être pris positifs ou négatifs.

La construction de Yamamoto permet d'améliorer ce dernier résultat en utilisant le résultat de crible suivant, dû à Richert (voir [**22**, Théorème 9.7]) :

Théorème 1.3. *Soit $F(n)$ un polynôme irréductible, de degré $g \geqslant 1$, à coefficients entiers. On note $\rho(p)$ le nombre de solutions dans $\mathbb{F}_p$ de l'équation $F(x) \equiv 0 \bmod p$, et l'on suppose que $\rho(p) < p$ pour tout p, ce qui implique que F est primitif. Alors, il existe $c_F > 0$ tel que, pour X assez grand, on ait*

$$\left|\left\{n : 1 \leqslant n \leqslant X, F(n) = P_{g+1}\right\}\right| \geqslant c_F\,\frac{X}{\log X} \ .$$

On peut supposer que n vérifie une congruence fixée.

Corollaire 1.4. *Soit F un polynôme vérifiant les hypothèses du théorème précédent. Alors, il existe une infinité de discriminants fondamentaux Δ de la forme $\operatorname{disc}\mathbb{Q}(\sqrt{F(n)}\,)$, tels que $\Delta = P_{g+1}$ ou $4P_{g+1}$. Si l'équation $F(x) \equiv 1 \bmod 4$ admet une solution, $\Delta = P_{g+1}$ suffit.*

Preuve. D'après le théorème de Tchebotarev, il existe une infinité de p premiers tel que $F(x) \equiv 0 \bmod p$ ait une solution x_0. Il suffit, en effet, de choisir p totalement décomposé dans le corps de décomposition de F*. Si un tel p ne divise pas le coefficient dominant de F, alors F est totalement décomposé modulo p.

Supposons qu'il n'existe qu'un nombre fini de Δ vérifiant les hypothèses de l'énoncé. On choisit un premier impair p qui ne divise aucun de ces nombres, ni le discriminant de F, ni son coefficient dominant, et tel que $F(x_0) \equiv 0 \bmod p$. Comme p ne divise pas $\operatorname{disc}(F)$, il existe un unique relèvement de x_0 en une solution modulo p^2 (et plus généralement à $\mathbb{Z}_p$). Donc il existe $p-1$ relèvements de x_0 modulo p^2 tels que $F(x) \equiv 0 \bmod p$ et $F(x) \not\equiv 0 \bmod p^2$. On applique maintenant le Théorème 1.3, en imposant que n soit l'un de ces relèvements x modulo p^2. Si $F(x) = 1$ est soluble modulo 4, on exige aussi que n en soit solution. Alors $v_p(F(n)) = 1$ pour tous les n ainsi obtenus. Donc p se ramifie dans $\mathbb{Q}(\sqrt{F(n)})$, dont le discriminant vérifie pourtant nos hypothèses. Contradiction. La condition $F(n) \equiv 1 \bmod 4$ permet simplement d'affirmer que ce discriminant est égal à la partie sans facteurs carrés F'de $F(n)$, et non à $4F'$. □

*Dans ce cas particulier, la densité analytique se calcule d'ailleurs élémentairement, sans faire appel au résultat général.

Si l'on pouvait assurer que les $F(n)$ produits par le Théorème de Richert sont *sans facteurs carrés* (le crible indique seulement que $p^2|F(n)$ implique $p \geqslant X$), on obtiendrait des minorations du nombre de ces Δ, quand n est dans l'intervalle $[-X, X]$. Elles seraient de la forme $cX^{1/g}/\log X$, avec $c > 0$. Les techniques du §3 (crible à carrés) permettent d'obtenir une minoration explicite, mais catastrophique : en $\log\log X$.

Corollaire 1.5. *Il existe une infinité de discriminants fondamentaux Δ tel que l'une quelconque des conditions suivantes soit vérifiée :*

- $\Delta = P_{2\ell} > 0 \quad$ *et* $\quad r_\ell(\Delta) \geqslant 1.$
- $\Delta = P_{2\ell} < 0 \quad$ *et* $\quad r_\ell(\Delta) \geqslant 2.$
- $\Delta = P_{\ell+1} < 0 \quad$ *et* $\quad r_\ell(\Delta) \geqslant 1.$

C'est une application immédiate de ce qui précède. Pour les deux premières inégalités, on considère le polynôme $Q_\ell(n)$, évoqué page 80, que l'on peut construire de façon à ce que $Q_\ell(n) \equiv 1 \bmod 4$ ait une solution et $\rho(p) < p$ pour tout p (prendre $S_1 = S_2 = S_3 = \varnothing$, $(a, b) = 2$ et $a \equiv 0 \bmod 4$, $b \equiv 2 \bmod 4$ dans la construction du Théorème 2 de [**51**]). Son terme dominant est en $n^{2\ell-1}$, et nous pouvons donc rendre $Q_\ell(n)$ positif ou négatif si $|n|$ est grand. Plus précisément, nous appliquons le Corollaire 1.4 à $Q_\ell(n)$ ou $Q_\ell(-n)$, pour n positif.

Pour la dernière assertion, on utilise $y^2 - 4x^\ell$, pour y impair fixé. On ne peut malheureusement pas considérer ce dernier comme polynôme en y (et appliquer le résultat d'Iwaniec [**29**] qui fournirait des P_2 pour y assez grand) puisque nous devons nous restreindre à ses valeurs *négatives*.

Dans le cas imaginaire, on peut faire largement mieux en faisant varier y. Nous montrerons (voir le Corollaire 2.5) :

Théorème 1.6. *Si ℓ est un premier impair, on définit la fonction $g(\ell)$ de la façon suivante :*

$$g(5) = 4, \quad g(4k+1) = 3k+2, \quad \textit{si } k \geqslant 2$$

$$g(4k+3) = 3k+3, \quad \textit{pour tout } k \geqslant 0.$$

Alors, il existe une infinité de discriminants fondamentaux négatifs *P_g, avec $r_\ell(P_g) \geqslant 1$ et $g = g(\ell)$. De plus, il existe $c > 0$, tel que*

$$\left|\left\{\Delta : \Delta = P_g, -X \leqslant \Delta \leqslant -1, r_\ell(\Delta) \geqslant 1\right\}\right| \geqslant c\,\frac{X^{(\ell+1)/2\ell}}{\log X} \ ,$$

où l'on peut supposer que les Δ sont des discriminants fondamentaux.

Remarquons que, par rapport à (38) ou au Corollaire 1.5, nous améliorons très nettement le degré des pseudo-premiers obtenus, ainsi que la minoration de leur cardinal.

2. Préliminaires

Fixons un premier impair ℓ, puis l'entier $\mu = (\ell-1)/2$ et considérons la région C_K de $\mathbb{R}^2$ définie par $0 < y^{1/\mu} \leqslant x \leqslant K$. Le nombre $N(K)$ de points entiers de C_K vérifie

$$N(K) = \sum_{x=1}^{K} \sum_{y=1}^{x^\mu} 1 = \frac{K^{\mu+1}}{\mu+1} + O(K) \ .$$

Soit s le plus petit premier impair congru à 1 modulo ℓ, ce qui implique que $x \mapsto x^\ell$ n'est pas un automorphisme de $\mathbb{F}_s^*$. On considère la suite $\mathbf{A}_\ell(K)$ des entiers de la forme $\Delta = y^2 - 4x^\ell$, $(x,y) \in C_K$, vérifiant la condition

$(*)$ $\qquad s|x$ et y n'est pas une puissance ℓ-ième modulo s.

Ces entiers sont négatifs, minorés par $-4K^\ell$, et le Théorème 1.1 assure que $\mathbb{Q}(\sqrt{\Delta})$ a un ℓ-rang supérieur à 1, sauf pour les Δ de la forme $-3f^2$. Les Δ ainsi obtenus sont en bijection avec les points entiers de C_K vérifiant $(*)$, à un nombre fini près indépendant de K. En effet, supposons $y_1^2 - 4x_1^\ell = y_2^2 - 4x_2^\ell$, et $x_1 < x_2$. Alors nous avons

$$x_2^{\ell-1} \geqslant y_2^2 - y_1^2 = 4(x_2^\ell - x_1^\ell) \geqslant 4(x_2^\ell - (x_2-1)^\ell) = 4\ell x_2^{\ell-1}(1+o(1)) \ ,$$

soit une contradiction si x_2 est assez grand.

Lemme 2.1. *On considère q premier à s, sans facteurs carrés, et la congruence modulo $m = sq$: "(x,y) vérifie $(*)$ et $q|(y^2-4x^\ell)$". Soit $S(m)$ son nombre de solutions. Alors*

$$S(m) = \frac{(s-1)(\ell-1)}{s\ell}\, m \ .$$

Preuve. Notons $\mathfrak{S}(q)$ le nombre de couples de solutions (x,y) de l'équation $y^2 - 4x^\ell \equiv 0 \bmod q$. Alors $\mathfrak{S}(q)$ est multiplicative et $S(m) = S(s)\mathfrak{S}(q)$. On trouve $(s-1)/\ell$ puissances ℓ-ièmes dans $\mathbb{F}_s^*$ donc, par définition,

$$S(s) = s - 1 - (s-1)/\ell = (s-1)(\ell-1)/\ell \ .$$

On suppose maintenant $p \neq s$. Soit (x,y) une solution de l'équation $y^2 - 4x^\ell = 0$ dans $\mathbb{F}_p$. Ceci implique que x est un carré puisque $x = 0$ ou $x = (2^{-1}x^{-\mu}y)^2$, soit $x = u^2$ et $y = \pm 2u^\ell$. Donc $(u^2, 2u^\ell)$, $u \in \mathbb{F}_p$, paramètre les solutions de la congruence et $\mathfrak{S}(p) = p$. □

On note E_m l'ensemble des solutions dénombrées par $S(m)$ et $N(K, E_m)$ le nombre d'éléments de C_K appartenant à E_m. On voit facilement, en découpant C_K en carrés de côté m (voir [**1**, Corollaire 4.2]), que l'on a l'égalité

$$N(K, E_m) = \frac{S(m)}{m^2} N(K) + O(K^\mu + m) \ , \tag{39}$$

ce qui donne un contrôle du reste (moyen) jusqu'à $m = K$. On peut faire un peu mieux en appliquant une technique de sommes d'exponentielles. On note $\omega(n)$ le nombre de diviseurs premiers de n (comptés sans multiplicité).

PROPOSITION 2.2. *Soit u_1, u_2, et v des entiers tels que $v = o(m^{1-\varepsilon})$ pour un $\varepsilon > 0$. On note $F(u_1, u_2, v)$ le nombre de points de E_m contenus dans le carré de côté v : $]u_1, u_1 + v] \times]u_2, u_2 + v]$. Alors*

$$F(u_1, u_2, v) = \frac{S(m)}{m^2}\, v^2 + O(\ell^{\omega(m)} m^{1/2} \log^2 m) \ . \tag{40}$$

PREUVE. La fonction caractéristique des entiers de l'intervalle $]u, u + v]$ est donnée par :

$$\chi_{u,v}(a) = \frac{1}{m} \sum_{k=u+1}^{u+v} \sum_{\gamma=0}^{m-1} e\left(\frac{\gamma(a-k)}{m}\right) \ .$$

Donc,

$$F(u_1, u_2, v) = \sum_{x,y \in E_m} \chi_{u_1,v}(x)\chi_{u_2,v}(y) = \frac{1}{m^2} \sum_{\gamma,\delta=0}^{m-1} S(m, \gamma, \delta)\theta_\gamma \psi_\delta \ ,$$

où

$$S(m, \gamma, \delta) = \sum_{x,y \in E_m} e\left(\frac{\gamma x + \delta y}{m}\right) \ ,$$

$$\theta_\gamma = \sum_{k=u_1+1}^{u_1+v} e\left(\frac{-\gamma k}{m}\right) \ll \min\left(v, \left\lfloor (\gamma/m)^{-1} \right\rceil\right) \ ,$$

$$\psi_\delta = \sum_{l=u_2+1}^{u_2+v} e\left(\frac{-\delta l}{m}\right) \ll \min\left(v, \left\lfloor (\delta/m)^{-1} \right\rceil\right) \ .$$

Ici, $\lfloor x \rceil$ désigne l'entier le plus proche de x. Si $\gamma = \delta = 0$, nous obtenons exactement le terme principal de (40). Pour majorer les autres termes, tout se passe comme si $S(m, \gamma, \delta)$, comme fonction de m, était multiplicative. En effet, soient α et β deux entiers premiers entre eux et a, b tels que $a\alpha + b\beta = 1$ (donc par exemple $(a\gamma, \beta) = (\gamma, \beta)$ et $(a\delta, \beta) = (\delta, \beta)$). Alors

$$\begin{aligned} S(\alpha\beta, \gamma, \delta) &= \sum_{x,y \in E_\beta} e\left(\frac{\gamma a x + \delta a y}{\beta}\right) \cdot \sum_{x,y \in E_\alpha} e\left(\frac{\gamma b x + \delta b y}{\alpha}\right) \\ &= S(\beta, a\gamma, a\delta) S(\alpha, b\gamma, b\delta) \ . \end{aligned}$$

On trouve, en appliquant récursivement le procédé,

$$S(m, \gamma, \delta) = \prod_{p|m} S(p, c_p, d_p) \ ,$$

où les c_p, d_p sont des entiers modulo p vérifiant $(c_p, p) = (\gamma, p)$ et $(d_p, p) = (\delta, p)$. Le théorème Chinois permet de les relever en deux entiers c et d tels que $(c, m) = (\gamma, m)$ et $(d, m) = (\delta, m)$. Nous verrons au Lemme 3.2 que, si $p \neq s$,

$$|S(p, c, d)| \leqslant \ell \cdot (p, c, d)^{1/2} p^{1/2} = \ell \cdot (p, \gamma, \delta)^{1/2} p^{1/2} \ ,$$

soit

$$S(m,\gamma,\delta) \leqslant \ell^{\omega(m)}(m,\gamma,\delta)^{1/2}m^{1/2} \ .$$

Nous obtenons donc, en utilisant $\omega(m)v \ll m$:

$$\begin{aligned}
F(u_1,u_2,v) - \frac{S(m)}{m^2}v^2 &= \frac{1}{m^2}\sum_{\substack{\lambda|m\\ \lambda\neq m}}\sum_{\substack{\gamma,\delta=0\\ (m,\gamma,\delta)=\lambda}}^{m-1} S(m,c,d)\theta_\gamma\psi_\delta \\
&\ll \frac{\ell^{\omega(m)}m^{1/2}}{m^2}\sum_{\substack{\lambda|m\\ \lambda\neq m}}\sum_{\substack{\gamma,\delta=0\\ (m,\gamma,\delta)=\lambda}}^{m-1} \lambda^{1/2}|\theta_\gamma\psi_\delta| \\
&\ll \ell^{\omega(m)}m^{-3/2}\sum_{\lambda|m}\lambda^{1/2}\left(v\Big(\sum_{\substack{\gamma=1\\ \lambda|\gamma}}^{m-1}\frac{m}{\gamma}+\sum_{\substack{\delta=1\\ \lambda|\delta}}^{m-1}\frac{m}{\delta}\Big)+\sum_{\substack{\gamma=1\\ \lambda|\gamma}}^{m-1}\frac{m}{\gamma}\sum_{\substack{\delta=1\\ \lambda|\delta}}^{m-1}\frac{m}{\delta}\right) \\
&\ll \ell^{\omega(m)}m^{-3/2}\big(v\omega(m)\cdot m\log m + m^2\log^2 m\big) \\
&\ll \ell^{\omega(m)}m^{1/2}\log^2 m \ .
\end{aligned}$$

□

Lemme 2.3. *On a l'égalité*

$$N(K,E_m) = \frac{S(m)}{m^2}N(K) + O\big(R(K,q)\big) \ ,$$

où $R(K,q)$ vérifie

$$\sum_{q\leqslant K^\alpha(\log K)^{-C}} \mu^2(q)3^{\omega(q)}|R(K,q)| \ll \frac{K^{\mu+1}}{\log^2 K} \ , \tag{41}$$

pour $\alpha = 4/3$, et $C > 0$ convenable.

Preuve. On reprend le raisonnement qui nous a permis d'obtenir (39), cette fois avec des carrés de côté v :

$$N(K,E_m) = v^{-2}\left(\frac{(s-1)(\ell-1)}{s\ell m}\,v^2 + O\big(\ell^{\omega(m)}m^{1/2}\log^2 m\big)\right)\times \left(\frac{K^{\mu+1}}{\mu+1} + O\big(K^\mu v + v^2\big)\right).$$

Le choix $v = \ell^{\omega(m)}m^{3/4}\log^2 m$ donne

$$R(K,q) = \frac{K^{\mu+1}}{\ell^{\omega(q)}q\log^2 q} + K^\mu\ell^{\omega(q)}q^{-1/4}\log^2 q + \ell^{2\omega(q)}q^{1/2}\log^4 q \ ,$$

qui vérifie bien (41) quand $q \geqslant X^\varepsilon$. Les $q \ll X^\varepsilon$ se traitent facilement en gardant la forme initiale du terme d'erreur de (39) : $R(X,q) = K^\mu + m$. □

Nous allons appliquer un crible linéaire pondéré aux éléments de $\mathbf{A}_\ell(K)$ (Théorème 9.3 de [**22**]) dont l'énoncé, légèrement adapté, est le suivant :

THÉORÈME 2.4. *Soit $\mathbf{A}(X)$ un ensemble fini d'entiers, paramétré par X. Notons $\mathbf{A}_q$ le nombre d'éléments de $\mathbf{A}$ divisibles par q et*

$$||\mathbf{A}||_\infty = \max_{a\in\mathbf{A}} |a| \ .$$

On suppose qu'il existe une fonction ν multiplicative telle que

$$|\mathbf{A}_q| = \frac{\nu(q)}{q}X + R_q \ ,$$

et qui vérifie les conditions suivantes :

$$(\Omega_1) \qquad 0 \leqslant \frac{\nu(p)}{p} \leqslant 1 - \frac{1}{A_1} \ .$$

$$(\Omega_2^*(1)) \qquad -\log\log 3X \ll \sum_{v\leqslant p<w} \frac{\nu(p)}{p}\log p - \log\frac{w}{v} \ll 1 \ .$$

$$(\Omega_3^*(\alpha)) \qquad \sum_{p\geqslant X^{\alpha/4}} |\mathbf{A}_{p^2}| = o\left(\frac{X}{\log X}\right) \ .$$

Il existe C tel que

$$(R_1(1,\alpha)) \qquad \sum_{q<X^\alpha(\log X)^{-C}} \mu^2(q)3^{\omega(q)}|R_q| \ll \frac{X}{\log^2 X} \ .$$

On pose

$$\Lambda_r = r + 1 - \frac{\log 4}{(1+3^{-r})\log 3} \ ,$$

et on choisit le r entier ($\geqslant 2$) minimal tel que

$$\Lambda_r > \frac{\log||\mathbf{A}||_\infty}{\log(X^\alpha)} \ .$$

Alors le nombre d'éléments de $\mathbf{A}$ sans facteurs carrés, ayant au plus r facteurs premiers, et dont les diviseurs premiers sont supérieurs à $X^{\alpha/4}$, est minoré par $cX/\log X$, où c est une constante strictement positive.

PREUVE. Nous avons remplacé la condition Ω_3 de Halberstam et Richert par la condition $\Omega_3^*(\alpha)$, un peu plus générale. De plus, nous avons utilisé la condition $R(1,\alpha)$ définie page 236 (*op. cit.*), plus proche de nos applications, et non la version moins précise (p. 64) indiquée dans l'index. La démonstration est identique. □

COROLLAIRE 2.5. *Si ℓ est un premier impair, on définit la fonction $g(\ell)$ comme au Théorème 1.6 :*

$$g(5) = 4, \quad g(4k+1) = 3k+2, \textit{ si } k \geqslant 2,$$
$$g(4k+3) = 3k+3, \quad \textit{pour tout } k \geqslant 0.$$

On note $\mathbf{A}_\ell = \cup \mathbf{A}_\ell(K)$. Alors $\mathbf{A}_\ell$ contient une infinité d'entiers sans facteurs carrés, ayant au plus $g(\ell)$ diviseurs premiers. Il existe $c > 0$ tel que

$$\big|\big\{\Delta : \Delta = P_{g(\ell)}, -K^\ell \leqslant \Delta \leqslant 1, r_\ell(\Delta) \geqslant 1\big\}\big| \geqslant c\,\frac{K^{\mu+1}}{\log K} \ .$$

De plus, on peut supposer que ces Δ sont des discriminants fondamentaux.

Preuve. Avec les notations du théorème, nous avons $\mathbf{A} = \mathbf{A}(K)$, $\nu(p) = 1$ pour tout $p \neq s$, $\nu(s) = 0$, et

$$X = \frac{(s-1)(\ell-1)}{s\ell}\,\frac{K^{\mu+1}}{\mu+1} \ ,$$

soit $||A||_\infty \ll X^{\ell/(\mu+1)}$.

Les conditions Ω_1 et $\Omega_2^*(1)$ sont trivialement satisfaites et le Lemme 2.3 prouve $R_1(1, 4/3(\mu+1))$, avec C convenable. Nous allons montrer $\Omega_3^*(z)$ pour tout $z > 0$ au paragraphe suivant (voir (49)). Nous devons calculer le plus petit entier r vérifiant

$$r + 1 - \frac{\log 4}{(1+3^{-r})\log 3} > \frac{3\ell}{4} \ .$$

Écrivons $3\ell/4 = [3\ell/4] + u/4$, où $u = 3$ si $\ell \equiv 1 \pmod 4$ et $u = 1$ sinon. Puisque

$$1/4 < 2 - \log(4)/\log(3)(1+3^{-r}) < 3/4$$

pour tout $r \geqslant 5$, on doit prendre $r = [3\ell/4]+2$ dans le premier cas et $r = [3\ell/4]+1$ dans le deuxième, dès que $[3\ell/4] \geqslant 4$. Les cas particuliers $\ell = 3$ et $\ell = 5$ se traitent ensuite sans difficultés.

Le Théorème 2.4 permet donc de conclure à l'existence d'une infinité de (x, y) satisfaisant aux conditions du Théorème 1.1, tels que $\Delta = y^2 - 4x^\ell$ ait au plus $g(\ell)$ facteurs premiers. En effet, x et y sont premiers entre eux puisque Δ est sans facteurs carrés. De plus, comme 2 ne divise pas Δ, y est impair et $\Delta \equiv 1 \pmod 4$. Donc, Δ est bien un discriminant fondamental. □

Sans le Lemme 2.3, qui utilise l'estimation de Weil de certaines sommes d'exponentielles associées aux courbes algébriques (Théorème 3.1), nous aurions un exposant de répartition $\alpha = 1/(\mu+1)$, et non $\alpha = 4/3(\mu+1)$, dans le théorème précédent. Le gain est d'autant plus considérable que ℓ est grand.

3. Preuve de $\Omega_3^*(z)$, Crible à carrés

Nous voulons montrer que, pour $z > 0$, on a l'inégalité

$$\sum_{p > K^z} \#\big\{(x,y) : 0 < y^{1/\mu} < x < K, 4x^\ell - y^2 \equiv 0 \bmod p^2\big\} \ll_z \frac{K^{\mu+1}}{\log^2 K} \ .$$

Nous pouvons supposer $p > s$. La majoration triviale $|\mathbf{A}_{p^2}| \ll K^\ell/p^2$ permet de restreindre la somme aux $p \leqslant K^{\mu+\varepsilon}$. On cherche les solutions modulo p^2 de

$4x^\ell = y^2$ sous la forme $(x_0 + px_1, y_0 + py_1)$, où (x_0, y_0) parcourt les solutions modulo p, *i.e.* les $(u^2, 2u^\ell)$, et $(x_1, y_1) \in \mathbb{F}_p^2$. La formule de Taylor donne

$$u^\ell(\ell u^{\ell-2}x_1 - y_1) \equiv 0 \pmod{p} \ .$$

Si $u = 0$, nous avons $p|x$. Comme $x \neq 0$ et $x \leqslant K$, nous avons $p \leqslant K$ et au plus $K/p \cdot K^\mu/p$ solutions pour (x, y). Sinon, y est déterminé modulo p^2 quand x est fixé. On obtient alors au plus $K \cdot K^\mu/p^2$ solutions si $p^2 \leqslant K^\mu$, au plus K sinon. Finalement,

$$\sum_{K^z<p<Y} |\mathbf{A}_{p^2}| \ll \sum_{K^z<p<Y} \left(K + \frac{K^{\mu+1}}{p^2}\right) \ll K^{\mu+1-z} + KY \ , \tag{42}$$

Nous contrôlons donc la somme pour $p < K^{\mu-\varepsilon}$ et $p > K^{\mu+\varepsilon}$, pour tout $\varepsilon > 0$. L'idée naturelle consisterait à introduire des sommes d'exponentielles, comme au Lemme 2.2 mais, pour les $p \approx K^\mu$ récalcitrants, elles sont trop courtes, et on contrôle mal leurs oscillations.

Nous allons suivre un article de Heath-Brown [**25**], qui introduit un crible à carrés très ingénieux. Lui-même simplifie une idée de Hooley [**28**], qui utilisait le grand crible pour parvenir à ses fins. On majore simplement le nombre des carrés dans une suite par celui des entiers n dont le symbole de Legendre $\left(\frac{n}{p}\right)$ vaut 1 pour une famille $\mathcal{P}$ de premiers bien choisis, beaucoup plus petits que K^μ. Il ne reste plus alors qu'à majorer une somme d'exponentielles avec caractère, modulo de *petits* premiers.

Considérons donc

$$\begin{aligned}\sum_{p>Y} |\mathbf{A}_{p^2}| &= \sum_{p>Y} \#\left\{(x,y) : p^2|4x^\ell - y^2\right\} \\ &\leqslant \sum_u \mu^2(u) \sum_v \#\left\{(x,y) : 4x^\ell - y^2 = uv^2\right\},\end{aligned}$$

où $0 < y < K^\mu$, $0 < x < K$ et $u \ll U = K^\ell/Y^2$. Notons $w_u(n)$ la fonction définie par

$$w_u(mu) = \#\left\{(x,y) : u|(4x^\ell - y^2), 4x^\ell - y^2 = m\right\},$$

et $w_u(n) = 0$ si $u \nmid n$. Ce poids vérifie la propriété

$$\sum_n w_u(n^2) = \sum_v \#\left\{(x,y) : 4x^\ell - y^2 = uv^2\right\}.$$

On choisit

$$\mathcal{P}_u = \{p : p \nmid u, Q < p \leqslant 2Q\},$$

pour un Q que l'on prendra dans la suite de l'ordre de X^ε. Nous avons $P = |\mathcal{P}_u| \sim Q/\log Q$ et la somme sur v vaut (voir [**25**, Théorème 1])

$$\sum_n w_u(n^2) \ll \frac{1}{P}\sum_n w_u(n) + \frac{1}{P^2}\sum_{\substack{p\neq q\\ p,q\in\mathcal{P}_u}}\left|\sum_n w_u(n)\left(\frac{n}{pq}\right)\right| \ .$$

La contribution de la première somme se majore trivialement :

$$\frac{1}{P}\sum_{n,u} w_u(n) \ll \frac{1}{P}\#\left\{(x,y) : 0<y<K^\mu, 0<x<K\right\} \ll \frac{K^{\mu+1}}{P} \ . \tag{43}$$

Pour le deuxième terme, il faut évaluer

$$\sum_{p\neq q}\left|\sum_n w_u(n)\left(\frac{n}{pq}\right)\right| = \sum_{p\neq q}\left|\sum_{x,y}\left(\frac{(4x^\ell - y^2)u}{pq}\right)\right| \ , \tag{44}$$

où la dernière somme s'effectue sur les $0<y<K^\mu$, $0<x<K$, $u|4x^\ell - y^2$ et nous pouvons supposer que u est sans facteurs carrés.

Puisque le symbole de Legendre est multiplicatif, avec $|\left(\frac{u}{pq}\right)| = 1$, nous pouvons supprimer u dans la somme intérieure. Nous écrivons alors celle-ci sous la forme

$$\begin{aligned}\sum_{x,y}\left(\frac{4x^\ell - y^2}{pq}\right) &= \sum_{\alpha,\beta=0}^{upq-1}\left(\frac{4\alpha^\ell-\beta^2}{pq}\right)\sum_{\substack{x<K\\ x=\alpha\ (upq)}} 1 \sum_{\substack{y<K^\mu\\ y=\beta\ (upq)}} 1\\ &= \frac{1}{(upq)^2}\sum_{\alpha,\beta=0}^{upq-1}\left(\frac{4\alpha^\ell-\beta^2}{pq}\right)\cdot\sum_{\gamma=0}^{upq-1}\sum_{k<K} e\left(\frac{\gamma(\alpha-k)}{upq}\right)\cdot\sum_{\delta=0}^{upq-1}\sum_{l<K^\mu} e\left(\frac{\delta(\beta-l)}{upq}\right)\\ &= \frac{1}{(upq)^2}\sum_{\gamma,\delta=0}^{upq-1} S(u,pq;\gamma,\delta)\theta_\gamma\psi_\delta \ ,\end{aligned}$$

avec des notations proches de celles de la Proposition 2.2 :

$$S(u,pq;\gamma,\delta) = \sum_{\substack{\alpha,\beta=0\\ u|4\alpha^\ell-\beta^2}}^{upq-1}\left(\frac{4\alpha^\ell-\beta^2}{pq}\right)e\left(\frac{\gamma\alpha+\delta\beta}{upq}\right) \ , \tag{45}$$

$$\theta_\gamma = \sum_{k<K} e\left(\frac{-\gamma k}{upq}\right) \ll \min\left(K, \left\lfloor(\gamma/upq)^{-1}\right\rceil\right) \ ,$$

$$\psi_\delta = \sum_{l<K^\mu} e\left(\frac{-\delta l}{upq}\right) \ll \min\left(K^\mu, \left\lfloor(\delta/upq)^{-1}\right\rceil\right) \ .$$

En notant r un diviseur premier générique de u, S se factorise sous la forme

$$S_2(p,c,d)\cdot S_2(q,c,d)\cdot\prod_{r|u} S_1(r,c,d) \ ,$$

où

$$S_2(p,c,d) = \sum_{\alpha,\beta=1}^{p} \left(\frac{4\alpha^\ell - \beta^2}{p}\right) e\left(\frac{c\alpha + d\beta}{p}\right) ,$$

$$S_1(r,c,d) = \sum_{\substack{\alpha,\beta=1 \\ r|4\alpha^\ell-\beta^2}}^{r} e\left(\frac{c\alpha + d\beta}{r}\right) ,$$

et c, d sont des entiers vérifiant

$$(c, upq) = (\gamma, upq), \quad (d, upq) = (\delta, upq) .$$

Nous pouvons majorer S_1 et S_2 grâce au théorème de Weil (voir [**50**] où, par exemple, [**44**] pour une présentation élémentaire) :

THÉORÈME 3.1 (Weil). *Soit ψ un caractère additif non trivial de $\mathbb{F}_q$, et $g(X)$ un polynôme de $\mathbb{F}_q[X]$, non nul, de degré n, avec $n < q$ et $(n,q) = 1$. Alors*

$$\left| \sum_{x\in\mathbb{F}_q} \psi(g(x)) \right| \leqslant (n-1)\sqrt{q} . \tag{46}$$

LEMME 3.2. *On a l'inégalité*

$$|S_1(p,c,d)| \leqslant (\ell-1)p^{1/2}\,(p,c,d)^{1/2} .$$

PREUVE. Si $(p,c,d) = p$ ou $p \leqslant \ell$, le résultat est trivial puisqu'il n'y a que p couples de solutions à la congruence. Nous pouvons donc supposer que $(p,c,d) = 1$ et $p > \ell$ (donc $p \neq 2$). Alors

$$S_1(p,c,d) = \sum_{\substack{\alpha,\beta \\ 4\alpha^\ell=\beta^2\ (p)}} e\left(\frac{c\alpha + d\beta}{p}\right) .$$

De même qu'au Lemme 2.1, nous pouvons écrire $\alpha = u^2$, $\beta = 2u^\ell$, d'où

$$S_1(p,c,d) = \sum_{u\in\mathbb{F}_p} e\left(\frac{cu^2 + du^\ell}{p}\right) \leqslant (\ell-1)p^{1/2}$$

en appliquant le Théorème 3.1 au polynôme $g(u) = cu^2 + du^\ell$ (de degré inférieur à ℓ, et non nul modulo p puisque $(p,c,d) = 1$). □

LEMME 3.3. *On a l'inégalité*

$$|S_2(p,c,d)| \leqslant \ell p^{3/2} .$$

PREUVE. Si $p \leqslant \ell$, le résultat est trivial, donc nous pouvons supposer que $p > \ell$. Le terme correspondant à $\alpha = 0$ est nul si $(d,p) = 1$ et vaut $\left(\frac{-1}{p}\right)p$ sinon. Si $\alpha \neq 0$, on remplace β par $2\alpha^\mu\beta$, puis α par $\alpha + \beta^2$. Soit

$$|S_2(p,c,d)| \leqslant p + \left| \sum_{\alpha\neq\beta^2} \left(\frac{\alpha}{p}\right) e\left(\frac{(\alpha+\beta^2)(c + 2d(\alpha+\beta^2)^{(\ell-3)/2}\beta)}{p}\right) \right| . \tag{47}$$

Si $p|(c,d)$, on utilise $\sum \left(\frac{\alpha}{p}\right) = 0$, pour majorer S_2 par $2p$ (en fait, le calcul est explicite : la somme est nulle si -1 est un carré modulo p, et vaut $-2p$ sinon). Dans le cas contraire, nous majorons par

$$p + \sum_{\alpha \neq 0} (\ell - 1) p^{1/2} \leqslant \ell p^{3/2} \ .$$

□

Remarque 3.4. Si $\ell = 3$ ou $p|d$, la somme de (47) est produit de deux sommes indépendantes, l'une étant tordue par le caractère multiplicatif $\left(\frac{\alpha}{p}\right)$. Dans ces cas, on obtient facilement le bon ordre de grandeur $S_2(p,c,d) \ll p$ en appliquant la généralisation du théorème de Weil aux sommes avec caractères. La borne grossière du lemme nous suffira.

Nous obtenons donc la majoration

$$S(u, pq; \gamma, \delta) \ll (pq)^{3/2} \, \ell^{\omega(u)} u^{1/2} (u, \gamma, \delta)^{1/2} \ . \tag{48}$$

D'autre part,

$$\sum_{\gamma,\delta=0}^{upq-1} (u,\gamma,\delta)^{1/2} |\psi_\delta \theta_\gamma| \ll K^{\mu+1} u^{1/2} + (K + K^\mu) \sum_{\gamma=1}^{upq-1} \frac{upq}{\gamma} (u,\gamma)^{1/2} + \sum_{\gamma,\delta=1}^{upq-1} \frac{(upq)^2}{\gamma\delta} (u,\gamma,\delta)^{1/2} \ ,$$

les trois termes de la somme correspondant respectivement aux cas : γ et δ nuls, un seul des deux nuls, tous deux non nuls. Nous utilisons la majoration triviale

$$\sum_{\gamma=1}^{upq-1} \frac{(u,\gamma)^{1/2}}{\gamma} \leqslant \sum_{d|u} d^{1/2} \sum_{d|\gamma} \gamma^{-1} \leqslant \sum_{d|u} d^{-1/2} \sum_{\gamma \leqslant UQ^2} \gamma^{-1} \ll 2^{\omega(u)} \log K \ ,$$

pour finalement majorer (44) par

$$\sum_{1 \leqslant u < U} \frac{Q^3 u^{1/2} (4\ell)^{\omega(u)} \log^2 K}{u^2 Q^4} \Big(K^{\mu+1} u^{1/2} + u Q^2 K^\mu + (uQ^2)^2 \Big) \ll (\log K)^{4\ell+2} \left(Q^{-1} K^{\mu+1} + U^{1/2} Q K^\mu + Q^3 U^{3/2} \right).$$

D'après (43) et ce qui précède, nous obtenons la majoration globale

$$\sum_{p > Y} |\mathbf{A}_{p^2}| \ll (\log K)^{4\ell+2} (Q^{-1} K^{\mu+1} + U^{1/2} Q K^\mu + Q^3 U^{3/2}) \ .$$

En tenant compte de (42), la majoration devient

$$\sum_{p > K^z} |\mathbf{A}_{p^2}| \ll K^{\mu+1-z} + YK + (\log K)^{4\ell+2} \left(Q^{-1} K^{\mu+1} + U^{1/2} Q K^\mu + Q^3 U^{3/2} \right) \ .$$

Pour ε assez petit, on choisit $Q = K^{\varepsilon}$ et $Y = K^{\mu-\varepsilon}$, soit $U = K^{\ell}/Y^2 = K^{1+2\varepsilon}$. Nous obtenons finalement

$$\sum_{p>K^z} |\mathbf{A}_{p^2}| \ll K^{\mu+1-\varepsilon} \ , \tag{49}$$

et $\Omega_3(\varepsilon)$ est démontrée. Nous laissons au lecteur patient le soin d'effectuer un choix optimal pour nos paramètres.

ANNEXE A

Discriminants des Corps Cubiques

Pour cette section, la référence incontournable est *Corps Locaux* [**45**]. Nous utilisons librement les résultats élémentaires de la théorie des caractères, tels qu'ils sont par exemple décrits dans la première partie du livre de Serre [**46**].

Notre présentation est fortement influencée par les notes d'une série d'exposés de J. Martinet sur la théorie du corps de classes [**35**]. Nous remercions par ailleurs ce dernier d'avoir bien voulu relire l'interprétation que nous en avons faite.

1. Ramification

Si L/K est une extension de corps de nombres, on écrit $\mathfrak{d}_{L/K}$ son discriminant, et $\mathfrak{D}_{L/K}$ sa différente. Dans le cas absolu $K = \mathbb{Q}$, on notera d_L le discriminant d'une base d'entiers de $L/\mathbb{Q}$, soit $\mathfrak{d}_{L/\mathbb{Q}} = d_L\mathbb{Z}$. $\mathbb{Z}_K$ désigne l'anneau d'entiers du corps K. Si $\mathfrak{p}$ est un idéal premier de $\mathbb{Z}_K$, et $\mathfrak{P} \subset \mathbb{Z}_L$ est un diviseur premier de $\mathfrak{p}$, on note respectivement $f(\mathfrak{P}/\mathfrak{p})$ et $e(\mathfrak{P}/\mathfrak{p})$ les degrés résiduels et de ramification.

On suppose maintenant l'extension galoisienne, de groupe $G = \mathrm{Gal}(L/K)$. Pour tout $i \geqslant -1$, on définit le i-ème groupe de ramification

$$G_i(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in G : v_{\mathfrak{P}}(\sigma(x) - x) \geqslant i + 1, \forall x \in \mathbb{Z}_{L_{\mathfrak{P}}}\} \ .$$

Théorème 1.1. *On note p la caractéristique (commune !) des corps résiduels $\mathbb{Z}_K/\mathfrak{p}$ et $\mathbb{Z}_L/\mathfrak{P}$,* i.e. *le générateur positif de l'idéal $\mathfrak{p} \cap \mathbb{Z}$. On a les résultats*

(1) *Les G_i forment une filtration décroissante finie de G,* i.e. *il existe $g \geqslant 0$ tel que pour tout $i \geqslant g$, $G_i = \{1\}$. De plus, les G_i sont des sous-groupes distingués de G_{-1}.*
(2) $|G_{-1}| = e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p})$, $|G_0| = e(\mathfrak{P}/\mathfrak{p})$.
(3) *G_0/G_1 est un groupe cyclique, d'ordre premier à p.*
(4) *G_1 est un p-groupe. De plus G_1 est trivial si et seulement si p ne divise pas $e(\mathfrak{P}/\mathfrak{p})$. On dira dans ce cas que la ramification est modérée, et sauvage sinon.*
(5) $v_{\mathfrak{P}}(\mathfrak{D}_{L/K}) \leqslant e(\mathfrak{P}/\mathfrak{p}) - 1 + v_{\mathfrak{P}}(e(\mathfrak{P}/p))$.
(6) *On a les égalités :*

$$v_{\mathfrak{P}}(\mathfrak{D}_{L/K}) = \sum_{i \geqslant 0} \big(|G_i| - 1\big) \ , \quad \text{et} \quad v_{\mathfrak{p}}(\mathfrak{d}_{L/K}) = \frac{[L:K]}{e(\mathfrak{P}/\mathfrak{p})} v_{\mathfrak{P}}(\mathfrak{D}_{L/K}) \ .$$

Preuve. Tous ces résultats sont démontrés en détail dans [**45**] :

(1) I.§7 Corollaire à la Proposition 21 et IV.§1 Proposition 1.
(2) IV.§1 Proposition 1 et III.§7 Proposition 13.

(3) IV.§2 Corollaire 3 à la Proposition 1.
(4) IV.§2 Corollaire 1 à la Proposition 1.
(5) III.§7 Proposition 13.
(6) IV.§1 Proposition 4.

□

2. Conducteurs

Considérons la situation suivante (on se restreint au cas des corps de nombres) :

$$\begin{array}{c} M \\ | \\ H \\ | \\ G \quad M^H = L \\ | \\ K \end{array}$$

On suppose que M/K est galoisienne, de groupe G. Soit α un générateur de L sur K, de polynôme minimal f. Le groupe G opère sur les $[L : K]$ racines de f. Considérons la représentation de permutation (complexe) associée : (ρ_G, V), de dimension $[L : K]$, ainsi que la représentation triviale de H, (ρ_H, W), de dimension 1, de caractère 1_H, correspondant à α (*i.e.* $W = \mathbb{C}\alpha$).

Soit $\sigma \in G$, $\sigma\alpha$ ne dépend que de la classe à gauche de σ modulo H. Posons $W_\sigma = \sigma.W$: ce sont des sous-espaces vectoriels de dimension 1 de V, engendrés par les conjugués de α. Les W_σ sont donc permutés par G et, comme G est un groupe de Galois, l'action est transitive. De plus, $[G : H] = [L : K]$, donc

$$V = \bigoplus_{\sigma \in G/H} W_\sigma \ .$$

Par définition, ceci signifie que (ρ_G, V) est induite par (ρ_H, W). Donc le caractère de (ρ_G, V) est donné par la formule

$$\mathrm{Ind}_H^G 1_H(g) = \frac{1}{|H|} \sum_{\sigma \in G} 1_H(\sigma^{-1} g \sigma) \ ,$$

pour tout $g \in G$, où 1_H se prolonge par 0 en dehors de H. La formule de Frobenius donne explicitement le caractère de (G, V) : si χ est un caractère de G et ψ un caractère de H, on a

$$< \chi, \mathrm{Ind}_H^G \psi >_G = < \chi_{|H}, \psi >_H \ ,$$

où

$$< \chi, \psi >_G = \frac{1}{|G|} \sum_{\sigma \in G} \chi(\sigma) \overline{\psi(\sigma)} \ ,$$

et $z \mapsto \overline{z}$ représente la conjugaison complexe. Par exemple, le caractère de la représentation régulière (qui est l'induit de $\{1\}$ à G du caractère trivial), est donné par

$$r_G = \sum_{\chi} \chi(1) \cdot \chi \ , \tag{50}$$

où χ parcourt l'ensemble des caractères irréductibles de G – qui forment une base de l'espace des fonctions centrales sur G, orthonormée pour le produit hilbertien $< \ , >_G$.

Donnons nous maintenant $\rho : G \to \mathrm{GL}_n(V)$, une représentation complexe arbitraire de G, de caractère χ. Si $\mathfrak{p}$ est un idéal premier de $\mathbb{Z}_K$, on pose

$$n(\mathfrak{p}, \chi) = \frac{1}{|G_0|} \sum_i |G_i| \, \mathrm{codim}_{\mathbb{C}}(V^{G_i}) \ ,$$

où les G_i sont les groupes de ramifications associés à l'un quelconque des $\mathfrak{P} \in \mathbb{Z}_M$ au-dessus de $\mathfrak{p}$. Comme le laisse supposer la notation, ce nombre ne dépend de ρ que par l'intermédiaire du caractère χ (pour tout sous-groupe H de G, on a $< \chi_{|H}, 1_H >_H = \dim_{\mathbb{C}} V^H$, soit $\mathrm{codim}(V^H) = \chi(1) - < \chi_{|H}, 1_H >_H$), et ne dépend pas du $\mathfrak{P}$ choisi (changer de $\mathfrak{P}$ ne change pas la classe de conjugaison de G_i et les caractères sont des fonctions centrales).

Les $n(\mathfrak{p}, \chi)$ sont des entiers (voir [**45**], Théorème 1' et Corollaire 1 à la Proposition 2), et l'on pose

$$\mathfrak{F}(\chi, M/K) = \prod \mathfrak{p}^{n(\mathfrak{p}, \chi)} \ ,$$

où $\mathfrak{p}$ parcourt l'ensemble de idéaux premiers de $\mathbb{Z}_K$. C'est bien un idéal de $\mathbb{Z}_K$ (appelé conducteur d'Artin du caractère χ) puisque $n(\mathfrak{p}, \chi) = 0$ si $G_0 = \{1\}$, c'est-à-dire si $\mathfrak{p}$ n'est pas ramifié. Il n'y a donc qu'un nombre fini de facteurs.

Le conducteur $\mathfrak{F}$ vérifie banalement les égalités

$$\mathfrak{F}(\chi_1 + \chi_2) = \mathfrak{F}(\chi_1).\mathfrak{F}(\chi_2) \ , \quad \mathfrak{F}(1_G, M/K) = \mathbb{Z}_K \ ,$$

et un peu moins banalement ([**45**], VI.§3, Proposition 6) la formule d'induction

$$\mathfrak{F}(\mathrm{Ind}_H^G \chi, M/K) = N_{L/K}\big(\mathfrak{F}(\chi, M/L)\big) \cdot \mathfrak{d}_{L/K}^{\chi(1)} \ ,$$

où χ est un caractère de H et $N_{L/K}$ désigne la norme relative (rappelons que $L = M^H$). En appliquant ce résultat à $\chi = 1_H$, on obtient :

$$\mathfrak{F}(\mathrm{Ind}_H^G 1_H, M/K) = \mathfrak{d}_{L/K} \ .$$

Exemple : Si $H = \{1\}$, soit $L = M$, le caractère induit est donné par (50) et on retrouve la Führerdiskriminantenproduktformel d'Artin et Hasse :

$$\mathfrak{d}_{M/K} = \prod_{\chi} \mathfrak{F}(\chi)^{\chi(1)} \ ,$$

où χ parcourt l'ensemble des caractères irréductibles de $\mathrm{Gal}(M/K)$.

3. Corps cubiques galoisiens

Soit L/K une extension cubique galoisienne. Le groupe de Galois $G = \mathrm{Gal}(L/K)$, engendré par σ, possède trois caractères irréductibles :

$$1_G, \quad \chi : \sigma \mapsto \exp(2i\pi/3), \quad \text{et} \quad \overline{\chi} \ .$$

On vérifie immédiatement que $\mathfrak{F}(\chi, L/K) = \mathfrak{F}(\overline{\chi}, L/K)$*. Nous en déduisons

$$\mathfrak{d}_{L/K} = \mathfrak{F}(\chi, L/K)^2 = \mathfrak{f}^2 \ .$$

Soit $\mathfrak{p}$ un idéal premier de K ramifié dans l'extension et $\mathfrak{P} \subset \mathbb{Z}_L$ un de ses diviseurs premiers. Si $\mathfrak{p} \nmid 3$, alors $p \nmid e(\mathfrak{P}/\mathfrak{p})$ et la ramification est modérée, soit $v_\mathfrak{p}(\mathfrak{d}_{L/K}) = 2$. Si $\mathfrak{p}|3$, on a $v_\mathfrak{p}(\mathfrak{d}_{L/K}) \leqslant 2 + v_\mathfrak{p}(3)$. Et même

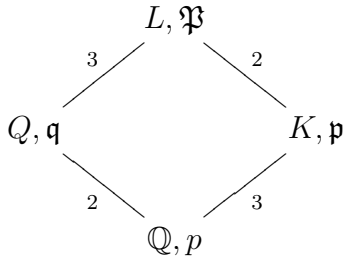
$$v_\mathfrak{p}(\mathfrak{d}_{L/K}) \leqslant 2 + 2[v_\mathfrak{p}(3)/2] \ ,$$

puisque $\mathfrak{d}_{L/K}$ est un carré.

Plaçons-nous dans le cas $K = \mathbb{Q}$, et écrivons $\mathfrak{d}_{L/K} = f^2\mathbb{Z}$. Si $\mathfrak{p} = 3\mathbb{Z}$, nous avons la majoration $v_\mathfrak{p}(\mathfrak{d}_{L/K}) \leqslant 2 + 2[3/2] = 4$. D'autre part, 3 divise $e(\mathfrak{P}/\mathfrak{p})$ donc la ramification est sauvage (soit $G_1 \neq \{1\}$). Donc, $v_\mathfrak{p}(\mathfrak{d}_{L/K}) = 4$.

4. Corps cubiques non galoisiens

Soit $K/\mathbb{Q}$ une extension cubique non galoisienne et $L/\mathbb{Q}$ sa clôture galoisienne. On voit facilement que $G = \mathrm{Gal}(L/\mathbb{Q}) \simeq S_3$, donc les classes de conjugaisons sont données par 1, les transpositions (τ, τ', τ'') et les 3-cycles (σ, σ^2). La situation est donc la suivante :



où L/K, L/Q, $L/\mathbb{Q}$ et $Q/\mathbb{Q}$ sont galoisiennes, $Q = L^\sigma$ et $K = L^\tau$. La table des caractères de S_3 se calcule sans difficultés :

	1	τ	σ
1_G	1	1	1
χ	1	-1	1
ψ	2	0	-1

On en déduit les formules d'induction

$$\mathrm{Ind}_\tau^G 1_\tau = 1_G + \psi \quad , \quad \mathrm{Ind}_\sigma^G 1_\sigma = 1_G + \chi \ ,$$

où, par abus de langage, on note encore x le sous-groupe engendré par x. Donc

$$\mathfrak{d}_{Q/\mathbb{Q}} = \mathfrak{F}(\chi, L/\mathbb{Q}), \quad \mathfrak{d}_{K/\mathbb{Q}} = \mathfrak{F}(\psi, L/\mathbb{Q}) \ ,$$

*De façon générale, si χ se déduit de χ' par un automorphisme de $\mathbb{Q}(\chi)$, on a $\mathfrak{F}(\chi) = \mathfrak{F}(\chi')$.

$$\text{(51)} \qquad \text{et} \quad \mathfrak{d}_{L/\mathbb{Q}} = \mathfrak{F}(\chi, L/\mathbb{Q})\mathfrak{F}^2(\psi, L/\mathbb{Q}) = \mathfrak{d}_{K/\mathbb{Q}}^2 \mathfrak{d}_{Q/\mathbb{Q}} \ ,$$

cette dernière égalité étant donnée par la Führerdiskriminantenproduktformel. Les formules de transitivité du discriminant s'écrivent

$$\begin{aligned} \mathfrak{d}_{L/\mathbb{Q}} &= N_{Q/\mathbb{Q}}(\mathfrak{d}_{L/Q})\mathfrak{d}_{Q/\mathbb{Q}}^3 \\ &= N_{K/\mathbb{Q}}(\mathfrak{d}_{L/K})\mathfrak{d}_{K/\mathbb{Q}}^2 \end{aligned}$$

et, d'après l'étude du cas galoisien, $\mathfrak{d}_{L/Q} = \mathfrak{f}^2$ est un carré. On en déduit

$$\text{(52)} \qquad \mathfrak{d}_{K/\mathbb{Q}} = d_K\mathbb{Z} = \mathfrak{d}_{Q/\mathbb{Q}} N_{Q/\mathbb{Q}}(\mathfrak{f}) = d_Q N_{Q/\mathbb{Q}}(\mathfrak{f}) \ .$$

Comme, d'autre part, $K/\mathbb{Q}$ n'est pas galoisienne, d_K n'est pas un carré, et $Q = \mathbb{Q}(\sqrt{d_K})$. On en déduit $d_Q = d_K$ modulo $(\mathbb{Q}^*)^2$, donc $N_{Q/\mathbb{Q}}(\mathfrak{f})$ est un carré et

$$\text{(53)} \qquad d_K = d_Q f^2 \ ,$$

avec $f \in \mathbb{Z}$.

On peut donner une interprétation agréable de ce dernier résultat. En effet, considérons plus généralement une suite d'extensions $A \subset Q \subset L$, où L/Q est abélienne, de conducteur $\mathfrak{f}$, et Q/A cyclique, de groupe de Galois engendré par τ. L/A est galoisienne si et seulement si $\tau(L) = L$, où l'on continue de noter τ un de ses prolongements. D'après la théorie du corps de classes, L correspond à un sous-groupe de congruence H de Q, de conducteur $\mathfrak{f}$. Mais $\tau(L)$ est le corps de classes associé à $\tau(H)$. Donc L/A est galoisienne si et seulement si $\tau(H) = H$, d'après le théorème d'unicité de Takagi.

Ici, $L/\mathbb{Q}$ est galoisienne, donc $\tau(H) = H$ et $\tau(\mathfrak{f}) = \mathfrak{f}$, soit $N_{Q/\mathbb{Q}}(\mathfrak{f}) = \mathfrak{f}^2$. En comparant (52) et (53), on obtient $f\mathbb{Z}_Q = \mathfrak{f}$. Donc le conducteur $\mathfrak{f}$ est principal, engendré par l'entier $f \in \mathbb{Z}$. On peut bien sûr obtenir le même résultat, de façon plus artificielle, en étudiant les groupes de ramifications, par épuisement des cas.

On fixe un premier p de $\mathbb{Q}$, ramifié dans $L/\mathbb{Q}$. On notera génériquement ses diviseurs comme dans le schéma de début de section (*i.e.* la lettre $\mathfrak{p}$ représente un idéal premier de $\mathbb{Z}_K$ au-dessus de p). Soit $v_L = v_p(d_L)$, $v_K = v_p(d_K)$, $v_Q = v_p(d_Q)$, et $v_f = v_p(f)$, alors (51) s'écrit

$$\text{(54)} \qquad v_L = 4v_f + 3v_Q \ ,$$

au vu de (53).

Théorème 4.1.

(1) *$p|f$ si et seulement si p est totalement ramifié dans $K/\mathbb{Q}$.*
(2) *$p|(f, d_Q)$ implique $p = 3$.*
(3) *$p^2|f$ n'est possible que si $p = 3$, et alors $3^3 \nmid f$. En particulier, si $p \neq 3$, alors $p^3 \nmid d_K$.*

Preuve.

(1) Puisque $f\mathbb{Z}$ est le conducteur de L/Q, p divise f si et seulement si $\mathfrak{q}$ est ramifié dans L/Q, soit $3|e(\mathfrak{P}/p)$, ce qui équivaut à $e(\mathfrak{p}/p) = 3$.

(2) Si p divise f et d_Q, L/Q et $Q/\mathbb{Q}$ sont ramifiées en $\mathfrak{q}$ et $\mathfrak{p}$. Elles sont galoisiennes donc $e(\mathfrak{P}/p) = 6$, soit $G_0 = S_3$. Comme G_0/G_1 est cyclique, G_1 n'est pas trivial. Comme c'est un p-groupe, on en déduit $p = 2$ ou $p = 3$. Supposons $p = 2$; autrement dit, G_1 est engendré par une transposition. Comme il est distingué dans G_{-1}, $G_{-1} \neq S_3$ et $G_{-1} = G_0 = G_1$. Dans ce cas, nous obtenons $e(\mathfrak{P}/p) = |G_0| = 2$. Donc, la seule possibilité est $p = 3$.

(3) Si $p^2|f$, alors $p^4|N_{Q/\mathbb{Q}}(\mathfrak{f}) = \mathfrak{f}^2$ et $\mathfrak{p}^2|\mathfrak{f}$. Donc $\mathfrak{p}|3$ et $p = 3$. Si 3 divise d_Q, *i.e.* si $G_0 = S_3$, on a $e(\mathfrak{P}/3) = 6$ et $v_L \leqslant 6 - 1 + 6 = 11$. Sinon $e(\mathfrak{P}/3) = 3$ et $v_L \leqslant 2(3 - 1 + 3) = 10$. En appliquant (54), on en déduit $v_f \leqslant 2$ dans les deux cas.

□

On peut obtenir ces résultats sans référence explicite aux conducteurs d'Artin, en se contentant d'examiner toutes les suites de groupes de ramifications possibles, à la lumière du Théorème 1.1. C'est ce que fait, Hasse dans [**23**].

ANNEXE B

Diviseurs Inessentiels du Discriminant

Nous donnons un critère, dû à Hensel, permettant de déterminer facilement si un idéal premier $\mathfrak{p}$ est diviseur inessentiel. Ce qui suit est une paraphrase de Hasse [**24**].

1. Définitions

On considère l'extension de corps de nombres

$$\begin{array}{c} L, \mathfrak{P} \\ \Big| n \\ K, \mathfrak{p} \end{array}$$

où $p = \prod \mathfrak{P}^{e_\mathfrak{P}}$, $e_\mathfrak{P} f_\mathfrak{P} = n_\mathfrak{P}$, et $\sum n_\mathfrak{P} = n$. On note $k(\mathfrak{p})$ le corps résiduel $\mathbb{Z}_K/\mathfrak{p}\mathbb{Z}_K$, et $\mathfrak{d}_{L/K}$ le discriminant de L/K.

Nous écrivons $L = K(\theta)$, $\theta \in \mathbb{Z}_L$, et $g \in \mathbb{Z}_K[X]$ le polynôme minimal de θ. Sur le complété $K_\mathfrak{p}$ de K en $\mathfrak{p}$, g se factorise en produit de facteurs irréductibles : $g = \prod g_\mathfrak{P}$, où les $g_\mathfrak{P} \in \mathbb{Z}_{K_\mathfrak{p}}[X]$ sont unitaires. On décompose $g_\mathfrak{P}$ sur une clôture algébrique $\overline{K_\mathfrak{p}}$ de $K_\mathfrak{p}$:

$$g_\mathfrak{P}(X) = \prod_{\nu=0}^{n_\mathfrak{P}-1} (X - \theta_{\mathfrak{P},\nu}) \ .$$

Afin de fixer un plongement du complété de L en $\mathfrak{P}$ dans $\overline{K_\mathfrak{p}}$, on choisit $\theta_{\mathfrak{P},0} = \theta_\mathfrak{P}$, puis $L_\mathfrak{P} = K_\mathfrak{p}(\theta_\mathfrak{P})$.

On appelle discriminant de θ, noté $d(\theta)$, le discriminant de son polynôme minimal g. Soit $d_\mathfrak{P}$ le discriminant de $L_\mathfrak{P}/K_\mathfrak{p}$ et

$$d_\mathfrak{p} = \prod_\mathfrak{P} d_\mathfrak{P} = d_{L/K} \cdot \mathbb{Z}_{K_\mathfrak{p}} \ .$$

Si $R(P,Q)$ désigne le résultant des polynômes P et Q, nous avons

$$\begin{aligned} d(\theta) &= \prod_\mathfrak{P} \prod_{\nu \neq \nu'} (\theta_{\mathfrak{P},\nu} - \theta_{\mathfrak{P},\nu'}) \prod_{\mathfrak{P} \neq \mathfrak{P}'} \prod_{\nu,\nu'} (\theta_{\mathfrak{P},\nu} - \theta_{\mathfrak{P}',\nu'}) \\ &= \prod_\mathfrak{P} d_\mathfrak{P}(\theta_\mathfrak{P}) \prod_{\mathfrak{P} \neq \mathfrak{P}'} R(g_\mathfrak{P}, g_{\mathfrak{P}'}) \ , \end{aligned}$$

où $d_\mathfrak{P}$ désigne le discriminant (dans $L_\mathfrak{P}/K_\mathfrak{p}$) de $\theta_\mathfrak{P}$. Aussi bien $d_\mathfrak{P}(\theta_\mathfrak{P})$ que $R(g_\mathfrak{P}, g_{\mathfrak{P}'})$ sont des éléments de $\mathbb{Z}_{K_\mathfrak{p}}$.

On note $A_{\mathfrak{P}}$ le déterminant de la matrice de passage d'une base d'entiers de $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ à la base de puissances $(1, \ldots, \theta_{\mathfrak{P}}^{n_{\mathfrak{P}}-1})$. Soit $d_{\mathfrak{P}}(\theta_{\mathfrak{P}}) = A_{\mathfrak{P}}^2 d_{\mathfrak{P}}$ et

$$\prod_{\mathfrak{P}} d_{\mathfrak{P}}(\theta_{\mathfrak{P}}) = d_{\mathfrak{p}} \prod_{\mathfrak{P}} A_{\mathfrak{P}}^2 \ .$$

D'où, en choisissant une relation d'ordre arbitraire sur les $\mathfrak{P}$,

$$d(\theta) = d_{\mathfrak{p}} \prod_{\mathfrak{P}} A_{\mathfrak{P}}^2 \prod_{\mathfrak{P}<\mathfrak{P}'} R^2(g_{\mathfrak{P}}, g_{\mathfrak{P}'}) = d_{\mathfrak{p}} m_{\mathfrak{p}}^2(\theta) \tag{55}$$

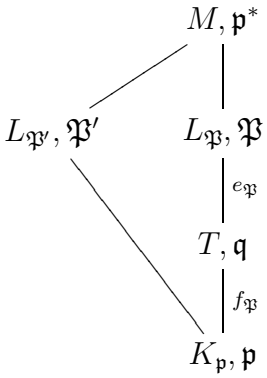
pour tout $\mathfrak{p}$. Et donc $d(\theta) = m^2(\theta)\mathfrak{d}_{L/K}$, avec $m(\theta) \in \mathbb{Z}_{K_{\mathfrak{p}}} \cap K = \mathbb{Z}_K$. Si $\mathbb{Z}_K$ est principal, il existe une base d'entiers relative et le résultat est trivial.

Définition 1.1. On dit que $\mathfrak{p}$ est *diviseur inessentiel* du discriminant (außerwesentliche Diskriminantenteiler) si $\mathfrak{p}$ divise $m(\theta)$, quel que soit $\theta \in \mathbb{Z}_L$. Autrement dit, d'après et avec les notations de (55), les deux assertions suivantes sont équivalentes :

- L'idéal premier $\mathfrak{p}$ n'est pas diviseur inessentiel du discriminant.
- Les $A_{\mathfrak{P}}$ et les $R(g_{\mathfrak{P}}, g_{\mathfrak{P}'})$ sont tous des unités de $\mathbb{Z}_{K_{\mathfrak{p}}}$.

2. Théorèmes

On considère la situation locale :



où M désigne la clôture normale de $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ (qui contient donc tous les $L_{\mathfrak{P}'}$). Puisque $k(\mathfrak{P}) = k(\mathfrak{q})$, on peut choisir dans T un relèvement $\omega_{\mathfrak{P}}$ de $\theta_{\mathfrak{P}}$ mod $\mathfrak{P}$.

Lemme 2.1. *Les assertions suivantes sont équivalentes :*

(1) $A_{\mathfrak{P}} \in \mathbb{Z}_{K_{\mathfrak{p}}}^*$.
(2) $1, \theta_{\mathfrak{P}}, \ldots, \theta_{\mathfrak{P}}^{n-1}$ *est une base d'entiers de* $L_{\mathfrak{P}}/K_{\mathfrak{p}}$.
(3) $\theta_{\mathfrak{P}} \bmod \mathfrak{P}$ *est un élément primitif de* $k(\mathfrak{P})/k(\mathfrak{p})$. *De plus, si* $e_{\mathfrak{P}} > 1$, *alors* $\theta_{\mathfrak{P}} = \omega_{\mathfrak{P}} + \pi_{\mathfrak{P}} \pmod{\mathfrak{P}^2}$, *où* $\pi_{\mathfrak{P}}$ *est une uniformisante de* $L_{\mathfrak{P}}$.

Preuve.

- $1 \Leftrightarrow 2$ est immédiat.

- $2 \Rightarrow 3$. $\theta_{\mathfrak{P}}$ est un élément primitif de $\mathbb{Z}_{L_{\mathfrak{P}}}/\mathbb{Z}_{K_{\mathfrak{p}}}$, donc de $k(\mathfrak{P})/k(\mathfrak{p})$. Supposons $e_{\mathfrak{P}} > 1$ et écrivons
$$\theta_{\mathfrak{P}} \equiv \omega_{\mathfrak{P}} + \alpha_{\mathfrak{P}} \pmod{\mathfrak{P}^2} \ ,$$
avec $\alpha_{\mathfrak{P}} \in \mathfrak{P}$. Comme $(1, \dots, \theta_{\mathfrak{P}}^{n-1})$ est une $\mathbb{Z}_{K_{\mathfrak{p}}}$-base d'entiers, une uniformisante de $L_{\mathfrak{P}}$ s'écrit
$$\pi_{\mathfrak{P}} = R(\theta_{\mathfrak{P}}), \quad R \in \mathbb{Z}_{K_{\mathfrak{p}}}[X] \ .$$
Soit, par la formule de Taylor,
$$\pi_{\mathfrak{P}} \equiv R(\omega_{\mathfrak{P}}) + \alpha_{\mathfrak{P}} R'(\omega_{\mathfrak{P}}) \mod \mathfrak{P}^2 \ ,$$
et donc $R(\omega_{\mathfrak{P}}) \in \mathfrak{P} \cap T = \mathfrak{q}$. D'où, puisque $e_{\mathfrak{P}} > 1$, $R(\omega_{\mathfrak{P}}) \equiv 0 \pmod{\mathfrak{P}^2}$, soit $v_{\mathfrak{P}}(\alpha_{\mathfrak{P}}) = 1$.
- $3 \Rightarrow 2$. Si $\theta_{\mathfrak{P}}$ est un élément primitif de l'extension résiduelle et $\pi_{\mathfrak{P}}$ une uniformisante de $\mathbb{Z}_{L_{\mathfrak{P}}}$, alors les $\theta_{\mathfrak{P}}^i \pi_{\mathfrak{P}}^j$, $0 \leqslant i < f_{\mathfrak{P}}$, $0 \leqslant j < e_{\mathfrak{P}}$ forment une base de $\mathbb{Z}_{L_{\mathfrak{P}}}/\mathbb{Z}_{K_{\mathfrak{p}}}$ (c'est une conséquence immédiate du lemme de Nakayama, [**45**, III.§6, Lemme 3]). Donc, si $e_{\mathfrak{P}} = 1$, il n'y a rien à démontrer. Sinon, on note R un relèvement sur T du polynôme minimal de $\theta_{\mathfrak{P}} \pmod{\mathfrak{P}}$. Comme l'extension de corps résiduels est séparable, $R'(\omega_{\mathfrak{P}}) \notin \mathfrak{P}$ et le calcul précédent montre que $R(\theta_{\mathfrak{P}})$ est une uniformisante. Donc $\mathbb{Z}_{L_{\mathfrak{P}}} = \mathbb{Z}_{K_{\mathfrak{p}}}[\theta_{\mathfrak{P}}]$.

□

LEMME 2.2. *Supposons que $\theta_{\mathfrak{P}}$ et $\theta_{\mathfrak{P}'}$ satisfont aux propriétés* 1,2,3 *du lemme précédent. Les assertions suivantes sont alors équivalentes :*

(1) $R(g_{\mathfrak{P}}, g_{\mathfrak{P}'}) \in \mathbb{Z}_{K_{\mathfrak{p}}}^*$.
(2) *$\theta_{\mathfrak{P}}$ et $\theta_{\mathfrak{P}'}$ modulo $\mathfrak{p}^*$ ne sont pas racines d'un même polynôme irréductible à coefficients dans $k(\mathfrak{p})$ (*i.e. *ne sont pas conjugués au-dessus de $k(\mathfrak{p})$).*

PREUVE. $R(g_{\mathfrak{P}}, g_{\mathfrak{P}'})$ n'est pas une unité de $\mathbb{Z}_{K_{\mathfrak{p}}}$ si et seulement si $R(g_{\mathfrak{P}}, g_{\mathfrak{P}'}) = 0$ dans $k(\mathfrak{p})$, *i.e.* si $g_{\mathfrak{P}}$ et $g_{\mathfrak{P}'}$, vus modulo $\mathfrak{p}$, ont une composante irréductible commune. Or, $\mathbb{Z}_{K_{\mathfrak{p}}}[\theta_{\mathfrak{P}}] = \mathbb{Z}_{L_{\mathfrak{P}}}$, donc $g_{\mathfrak{P}}$ se décompose modulo $\mathfrak{p}$ comme le premier $\mathfrak{p}$ dans $L_{\mathfrak{P}}/K_{\mathfrak{p}}$. Il en est de même de $g_{\mathfrak{P}'}$, soit
$$g_{\mathfrak{P}} \equiv P_{\mathfrak{P}}^{e_{\mathfrak{P}}} \pmod{\mathfrak{p}}, \quad g_{\mathfrak{P}'} \equiv P_{\mathfrak{P}'}^{e_{\mathfrak{P}'}} \pmod{\mathfrak{p}} \ ,$$
où $P_{\mathfrak{P}}$, resp. $P_{\mathfrak{P}'}$, est un polynôme irréductible de degré $f_{\mathfrak{P}}$, resp. $f_{\mathfrak{P}'}$, à coefficients dans $k(\mathfrak{p})$. La conclusion s'ensuit. Remarquons que, d'après la preuve, $f_{\mathfrak{P}} \neq f_{\mathfrak{P}'}$ impose $R(g_{\mathfrak{P}}, g_{\mathfrak{P}'}) \notin \mathfrak{p}$. □

THÉORÈME 2.3 (Hensel). *Soit $\mathfrak{p}$ un premier de K, on note $r(f)$ le nombre d'idéaux premiers $\mathfrak{P}$ au-dessus de $\mathfrak{p}$, de degré résiduel f. On pose $q = N_{K/\mathbb{Q}}(\mathfrak{p}) = |k(\mathfrak{p})|$. Alors, $\mathfrak{p}$ est diviseur inessentiel du discriminant si et seulement s'il existe f tel que*
$$r(f) > \frac{1}{f} \sum_{d|f} \mu(d) q^{f/d}. \tag{56}$$

Remarque 2.4. Le membre de droite dénombre les polynômes irréductibles de degré f sur $k(\mathfrak{p})$. En effet, partitionnons les éléments de $\mathbb{F}_{q^f}$ suivant le degré de leur corps de définition. Une extension de corps finis est séparable, donc chaque polynôme irréductible de degré d a bien d racines distinctes. D'où, si a_d désigne le nombre de polynômes irréductibles de degré d sur $\mathbb{F}_q$, on en déduit

$$q^f = \sum_{d|f} d a_d \ .$$

La conclusion est immédiate par inversion de Möbius.

Preuve. La condition est suffisante d'après le Lemme 2.2. Réciproquement, supposons que pour tout f, $r(f)$ soit au plus égal au nombre de polynômes irréductibles de degré f sur $k(\mathfrak{p})$. Grâce aux Lemmes 2.1 et 2.2, on peut alors choisir dans chaque $\mathbb{Z}_L/\mathfrak{P}^{e_\mathfrak{P}}$ un $\theta_\mathfrak{P}$ de façon à satisfaire les congruences

$$A_\mathfrak{P} \not\equiv 0 \pmod{\mathfrak{p}}, \quad \text{et } R(g_\mathfrak{P}, g_{\mathfrak{P}'}) \not\equiv 0 \pmod{\mathfrak{p}}, \text{ pour tout } \mathfrak{P}' \ .$$

Le lemme d'approximation permet alors d'obtenir un θ dans $\mathbb{Z}_L$ congru à chacun des $\theta_\mathfrak{P}$ modulo $\mathfrak{P}^{e_\mathfrak{P}}$, donc tel que $\mathfrak{p}$ ne divise pas $m(\theta)$. □

Corollaire 2.5. *Si $N_{K/\mathbb{Q}}(\mathfrak{p}) \geqslant [L : K]$, $\mathfrak{p}$ n'est pas un diviseur inessentiel du discriminant.*

Preuve. Notons $q = N_{K/\mathbb{Q}}(\mathfrak{p})$. Il suffit de remarquer que $r(f) \leqslant [L : K]/f$, puis que

$$\sum_{d|f} \mu(d) q^{f/d}$$

est un entier strictement positif, divisible par q. □

Corollaire 2.6. *Soit K un corps cubique. Un premier est diviseur inessentiel du discriminant de K si et seulement s'il est égal à 2 et se décompose totalement dans $K/\mathbb{Q}$.*

Preuve. Supposons que p soit diviseur inessentiel. D'après le corollaire précédent, on a $p = 2$. Comme $r(f) \leqslant 1$ pour $f > 1$, le critère ne peut être mis en défaut que pour $f = 1$ et $r(1) > 2$, soit $r(1) = 3$. La réciproque est immédiate. □

ANNEXE C

La Bijection de Davenport et Heilbronn

1. Formes cubiques

On considère l'ensemble Φ des formes cubiques binaires, primitives, et irréductibles à coefficients dans $\mathbb{Z}$, c'est-à-dire de la forme

$$F(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$$

avec $pgcd(a,b,c,d) = 1$ et F irréductible sur $\mathbb{Q}$. Le groupe $\Gamma = \mathrm{GL}_2(\mathbb{Z})$ agit naturellement à gauche sur Φ par changement de variable : $\gamma.F = F \circ \gamma$, pour $\gamma \in \Gamma$. Étant donné une factorisation de F sur $\mathbb{C}$:

$$F = \prod_i (\alpha_i x + \beta_i y) \ ,$$

on définit le discriminant de F par

$$\begin{aligned} \mathrm{disc}(F) &= \prod_{i<j} (\alpha_i\beta_j - \alpha_j\beta_i)^2 \\ &= b^2c^2 + 18abcd - 27a^2d^2 - 4b^3d - 4c^3a \ . \end{aligned} \tag{57}$$

La deuxième écriture montre que c'est un entier indépendant de la factorisation, la première qu'il est invariant sous l'action de Γ (on obtient un facteur $\det^6(\gamma)$ en remplaçant F par $\gamma.F$). Parler du discriminant d'un élément de $\Gamma\backslash\Phi$ a donc un sens.

2. L'injection F_K

Elle est introduite par Davenport et Heilbronn dans [**15**], et leur permet de majorer la densité des discriminants cubiques par celle des discriminants des classes *formes* cubiques, précédemment calculée par Davenport [**13, 14**].

Soit K un corps cubique de discriminant absolu d_K. On choisit $B = (1, \alpha, \beta)$ une $\mathbb{Z}$-base de $\mathbb{Z}_K$, ainsi qu'une racine carrée $\sqrt{d_K}$ de d_K. $L = \mathbb{Q}(\sqrt{d_K})$ est alors la clôture galoisienne de $K/\mathbb{Q}$. Pour tout $u \in K$, on note u' et u'' ses conjugués et on désigne par

$$d(u) = [(u-u')(u'-u'')(u''-u)]^2$$

le discriminant du polynôme minimal de u. Posons alors

$$d^{1/2}(u) = (u-u')(u'-u'')(u''-u) \ ,$$

puis, pour tout (x, y) dans $\mathbb{Q}$,

$$F_B(x,y) = \frac{d^{1/2}(\alpha x + \beta y)}{d_K^{1/2}} \quad . \tag{58}$$

PROPOSITION 2.1.

(1) $\mathrm{disc}(F_B) = d_K$
(2) *F_B est une forme cubique binaire, à coefficients entiers.*
(3) *La classe de F_B est bien déterminée, indépendante de la racine carrée et de la base d'entiers, du type $(1, \alpha, \beta)$, choisie.*
(4) *F_B est irréductible sur $\mathbb{Q}$.*
(5) *F_B est primitive.*
(6) *Soient K et K' deux corps cubiques, puis $B = (1, \alpha, \beta)$ et $B' = (1, \alpha', \beta')$ des bases d'entiers de K et K' respectivement. Alors K et K' sont conjugués si et seulement si F_B et $F_{B'}$ sont équivalentes.*

PREUVE. On note $F_B = ax^3 + bx^2y + cxy^2 + dy^3$.

(1) Si l'on considère la forme $d^{1/2}(\alpha x + \beta y)$, chacun des 3 facteurs de (57) vaut exactement d_K. Le discriminant étant homogène de degré 4, il nous reste à multiplier par $\left(d_K^{-1/2}\right)^4$, pour obtenir le discriminant de F_K, soit d_K.
(2) Les coefficients de F_B sont invariants par $\mathrm{Gal}(L/\mathbb{Q})$, donc rationnels. Si x et y sont entiers, $\mathbb{Z}[x\alpha + y\beta] \subset \mathbb{Z}_K$. Donc $d(x\alpha + y\beta) = \gamma^2 d_K$, où $\gamma = [\mathbb{Z}_K : \mathbb{Z}[x\alpha + y\beta]]$ est *entier* et $F(x, y) = \pm\gamma \in \mathbb{Z}$. Donc $a = F(1, 0)$ et $d = F(0, 1)$ sont entiers, de même que $b - c = F(1, -1) - a + d$ et $b + c = F(1, 1) - a - d$. Donc b et c sont des demi-entiers, égaux modulo $\mathbb{Z}$. D'après le point précédent, le discriminant de F_B est entier, donc celui de $2F_B$ est un multiple de 16, et vaut $16b^2c^2$ modulo 8 par un calcul direct. Donc b et c sont entiers.
(3) Changer de racine carrée revient à multiplier par -1, c'est-à-dire à faire agir $-\mathrm{Id}$ sur F_B. Remplaçons maintenant $B = (1, \alpha, \beta)$ par $B' = (1, \alpha', \beta') = (1, \alpha, \beta)M$, où $M \in \mathrm{GL}_3(\mathbb{Z})$. Ce qui s'écrit encore $(\alpha', \beta') = (\alpha, \beta)\gamma + (u, v)$, pour un $\gamma \in \Gamma$. On en déduit

$$\alpha' x + \beta' y = (\alpha', \beta') \begin{pmatrix} x \\ y \end{pmatrix} = (\alpha, \beta)\gamma \begin{pmatrix} x \\ y \end{pmatrix} + (ux + vy) \quad ,$$

soit $F_{B'} = \gamma.F_B$ puisque $d^{1/2}(\lambda + q) = d^{1/2}(\lambda)$ pour tout $q \in \mathbb{Q}$.
(4) F_B étant de degré 3, elle est réductible si et seulement si elle a un facteur linéaire. Supposons qu'il existe un couple de rationnels (x, y) vérifiant $F_B(x, y) = 0 = d(x\alpha + y\beta)$. Le polynôme minimal de $x\alpha + y\beta$ est alors scindé sur $\mathbb{Q}$ et $x\alpha + y\beta \in \mathbb{Q}$. Soit $x = y = 0$ puisque $[1, \alpha, \beta]$ est $\mathbb{Z}$-libre.
(5) Supposons que p premier divise tous les coefficients de F_B, ce qui implique $p^4 | \mathrm{disc}(F_B) = d_K$ donc que p est ramifié. De plus, p divise

$d(x)/d_K$, pour tout x dans $\mathbb{Z}_K$, donc p est un diviseur inessentiel du discriminant. D'après le Corollaire 2.6, $p = 2$ et 2 est totalement décomposé dans $K/\mathbb{Q}$, donc non ramifié. D'où une contradiction.

(6) L'implication est évidente. Supposons donc que F_B et $F_{B'}$ soient équivalentes. Le polynôme cubique $F_B(x, 1)$ est irréductible, à coefficients rationnels, donc ses zéros engendrent les extensions cubiques de $\mathbb{Q}$ incluses dans la clôture normale de $K/\mathbb{Q}$, donc en particulier K. Deux formes équivalentes engendrant les mêmes corps, nous en déduisons que K et K' sont conjugués. □

Ces résultats permettent d'associer à tout corps cubique K une classe de $\Gamma\backslash\Phi$ de même discriminant, notée F_K. Celle-ci est donnée par l'image d'une F_B par la projection canonique, pour une $\mathbb{Z}$-base B arbitraire de $\mathbb{Z}_K$ (de la forme $[1, \alpha, \beta]$). C'est même une injection au vu du point 6, à condition de considérer les corps cubiques à conjugaison près.

3. L'image de F_K

Un an après avoir introduit F_K, Davenport et Heilbronn [**16**] trouvent un critère remarquablement simple qui leur permet de déterminer son image, donc en particulier de calculer la densité des discriminants cubiques. Pour chaque p premier, on définit un sous-ensemble V_p de $\Gamma\backslash\Phi$ de la façon suivante. Si $p \neq 2$, $F \in V_p$ si $p^2 \nmid \mathrm{disc}(F)$, et sinon, $F \in V_2$ si

$$\mathrm{disc}(F) \equiv 1 \pmod 4 \quad \text{ou} \quad \mathrm{disc}(F) \equiv 8, 12 \pmod{16} \ .$$

On introduit de même un ensemble U_p : $F \in U_p$ si $F \in V_p$, ou si F modulo p est de la forme $\lambda(\alpha x + \beta y)^3$, $\lambda \in \mathbb{F}_p^*$ – on notera $(F, p) = (1^3)$ – et qu'il existe $e \not\equiv 0 \pmod p$, tel que $F(x, y) \equiv ep \pmod{p^2}$ ait une solution. On pose finalement $U = \cap U_p$.

Remarque 3.1. On montre facilement (remarque de H. Cohen) que, si $p \nmid F$, $F \notin U_p$ si et seulement si $F(x, y) \equiv (\delta x - \gamma y)^2(cx + dy) \pmod p$, avec

$$F(\gamma, \delta) \equiv 0 \pmod{p^2} \ .$$

Théorème 3.2. *On note $\mathcal{K}$ l'ensemble des corps cubiques cycliques et des triplets d'extensions cubiques non galoisiennes de $\mathbb{Q}$. Alors $K \mapsto F_K$ est une bijection de $\mathcal{K}$ sur U.*

Ceci résulte immédiatement des trois lemmes suivants :

Lemme 3.3. *F_K appartient à U.*

Preuve. Fixons un premier p. Nous allons utiliser les résultats de l'Appendice A, en particulier que d_K s'écrit $f^2\Delta$, où Δ est un discriminant fondamental, $(f, \Delta) = 1$ ou 3, et $p^2 \nmid f$ si $p \neq 3$. Rappelons (Chapitre 2, Proposition 2.2) que p se décompose dans $K/\mathbb{Q}$ de la même façon que F_K se factorise modulo p. On sait aussi que, si $p \neq 3$, $F \notin V_p$ et $(F, p) = (1^3)$, alors $F \in U_p$ si et seulement si $p^3 \nmid \mathrm{disc}(F)$ (Chapitre 2, Lemme 1.2).

Écrivons donc $\mathrm{disc}(F_K) = d_K = f^2\Delta$. Nous voulons montrer que $F_K \in U_p$. Si p ne divise pas f, alors $F \in V_p \subset U_p$ donc nous pouvons supposer que $p|f$. Donc p est totalement ramifié ($p = \mathfrak{p}^3$), et F_K a bien le type de décomposition attendu.

Si $p \neq 3$, alors $p^3 \nmid d_K$, donc $F \in U_p$. Reste le cas ennuyeux, $p = 3$. Notons N et Tr respectivement la norme et la trace absolues. Un calcul immédiat montre que

$$d^{1/2}(\alpha^2) = d^{1/2}(\alpha)\,\mathrm{N}(\mathrm{Tr}(\alpha) - \alpha) \ .$$

Choisissons un $\alpha \in \mathfrak{p}$, $\alpha \notin \mathfrak{p}^2$, alors l'ordre $\mathbb{Z}[\alpha]$ est 3-maximal (l'extension est totalement ramifiée en 3 donc, localement, l'anneau d'entiers est engendré par une uniformisante, voir la démonstration du Lemme 2.1), soit $v_3(d(\alpha)) = v_3(d_K)$. De plus $\mathrm{Tr}(\alpha) \in \mathfrak{p} \cap \mathbb{Z} = 3\mathbb{Z}$, donc

$$\mathrm{N}(\mathrm{Tr}(\alpha) - \alpha) \equiv -\,\mathrm{N}(\alpha) \equiv \pm 3 \pmod 9 \ ,$$

puisque $\mathrm{N}(\mathfrak{p}) = 3$. Nous venons d'obtenir un entier α^2 tel que

$$d^{1/2}(\alpha^2)/d_K^{1/2} \equiv \pm 3 \pmod 9 \ .$$

Donc F_K représente un entier congru à 3 modulo 9, et $F_K \in U_3$. □

Définition 3.4. Deux formes F_1 et F_2 sont dites *rationnellement* équivalentes s'il existe $\gamma \in M_2(\mathbb{Z})$, de déterminant non nul, telle que $F_1 \circ \gamma = \lambda F_2$, où λ est un rationnel non nul.

Lemme 3.5. *Pour toute forme F de Φ, il existe un corps cubique K tel que F et F_K soient rationnellement équivalentes.*

Preuve. On a $F = a(x - \lambda y)(x - \lambda' y)(x - \lambda'' y)$ dans une clôture algébrique de $\mathbb{Q}$. F est irréductible, donc λ engendre un corps cubique K. Écrivons $F_K = a_K(x - \nu y)(x - \nu' y)(x - \nu'' y)$, où $\nu \in K$ (si K est cyclique, on prend un conjugué au hasard, sinon ν est unique). K est un $\mathbb{Q}$-espace vectoriel de dimension 3, donc il existe k, l, m, n quatre entiers non tous nuls tels que $l + k\lambda - m\nu - n\lambda\nu = 0$. Cette égalité reste valide si l'on remplace ν et λ par leurs conjugués. En utilisant $\lambda = (m\nu - l)/(k - n\nu)$, on obtient

$$F_K(kx + ly, mx + ny) = \rho(x - \lambda y)(x - \lambda' y)(x - \lambda'' y) = (\rho/a)F \ ,$$

où $\rho = a_K\,\mathrm{N}(k - n\nu) \in \mathbb{Q}$. De plus, si $kn - lm$ était nul, λ ou ν serait rationnel, d'où la conclusion. □

Lemme 3.6. *Si F_1 et F_2 rationnellement équivalentes sont dans U, elles sont équivalentes.*

Preuve. Supposons $F_1 \circ \gamma = \lambda F_2$. Remplacer F_1 (resp. F_2) par une forme équivalente revient à multiplier γ à gauche (resp. à droite) par une matrice de $Gl_2(\mathbb{Z})$. La théorie des diviseurs élémentaires (forme normale de Smith) nous ramène au cas

$$\gamma = \begin{pmatrix} \alpha m & 0 \\ 0 & \alpha \end{pmatrix}, \quad m \in \mathbb{Z}_{>0}$$

et en remplaçant λ par λ/α^3, on peut prendre $\alpha = 1$. Si $m = 1$, alors $\lambda = 1$ et ces formes sont équivalentes. Sinon, il existe p premier tel que $m = p^l m_0$ et $\lambda = p^k \lambda_0$, avec m_0 et λ_0 premiers à p, et $l > 0$. On a $F_1(p^l m_0 x, y) = p^k \lambda_0 F_2(x, y)$, ce qui nous donne :

$$\begin{cases} a_1 &= \tau_a a_2 p^{k-3l} \\ b_1 &= \tau_b b_2 p^{k-2l} \\ c_1 &= \tau_c c_2 p^{k-l} \\ d_1 &= \tau_d d_2 p^k \end{cases}$$

où les τ_x sont des rationnels premiers à p. Si $k - l > 0$, alors p/c_1, et p^2/d_1 ; sinon, p/b_2, et p^2/a_2. Par symétrie, on peut se restreindre au premier cas : p/c_1, p^2/d_1, ce qui implique $p^2 | \operatorname{disc}(F_1)$. Si $p > 2$, ceci implique directement que $F \notin V_p$, sinon, un calcul direct montre que $\operatorname{disc}(F_1) \equiv b^2 c^2 \pmod{16}$, soit $F_1 \notin V_2$. Donc $F_1 \notin V_p$ dans tous les cas.

Puisque $F_1 \in U_p$, nous avons $(F_1, p) = (1^3)$, donc p divise b_1. La congruence $F_1(x, y) \equiv ep \pmod{p^2}$ implique alors $x \equiv 0 \pmod{p}$, puis $e \equiv 0 \pmod{p}$. Cette dernière absurdité achève la démonstration. □

ANNEXE D

Exemples

1. Corps Cubiques Réels

La table qui suit donne les cent premiers corps cubiques réels, classés par discriminants. De gauche à droite : le discriminant, la forme cubique canonique définissant le corps (nous avons écrit $F(x,1)$ au lieu de $F(x,y)$), son Hessien sous la forme $f_H(P_1,Q_1,R_1)$, où (P_1,Q_1,R_1) est primitive, et enfin le facteur f du discriminant ($\mathrm{disc}(F) = f^2\Delta$, où Δ est un discriminant fondamental). Les discriminants marqués d'une étoile sont ceux des corps cubiques cycliques, *i.e.* ceux dont le Hessien est de la forme $(P, \pm P, P)$.

Disc	$F(X)$	Hessien	f
49∗	X^3+X^2-2X-1	$7(1,1,1)$	7
81∗	X^3-3X-1	$9(1,1,1)$	9
148	X^3+X^2-3X-1	$2(5,3,6)$	2
169∗	X^3+X^2-4X+1	$13(1,-1,1)$	13
229	X^3-4X-1	$(12,9,16)$	1
257	X^3+2X^2-3X-1	$(13,3,15)$	1
316	X^3+2X^2-3X-2	$(13,12,21)$	1
321	X^3+X^2-4X-1	$(13,5,19)$	1
361∗	X^3+2X^2-5X+1	$19(1,-1,1)$	19
404	X^3+X^2-5X+1	$2(8,-7,11)$	2
469	X^3+2X^2-4X-1	$(16,1,22)$	1
473	X^3-5X-1	$(15,9,25)$	1
564	X^3+2X^2-4X-2	$2(8,5,14)$	2
568	X^3+4X^2-X-2	$(19,14,25)$	1
621	X^3+3X^2-3X-2	$9(2,1,3)$	3
697	X^3+3X^2-4X-1	$(21,-3,25)$	1
733	X^3+2X^2-6X+1	$(22,-21,30)$	1
756	X^3-6X-2	$18(1,1,2)$	6
761	X^3+X^2-6X+1	$(19,-15,33)$	1
785	X^3+2X^2-5X-1	$(19,-1,31)$	1
788	X^3+4X^2-2X-2	$2(11,5,14)$	2
837	X^3-6X-1	$9(2,1,4)$	3
892	X^3+5X^2-2	$(25,18,30)$	1
940	X^3+3X^2-4X-2	$(21,6,34)$	1
961∗	$2X^3+X^2-5X-2$	$31(1,1,1)$	31
985	X^3+X^2-6X-1	$(19,3,39)$	1
993	X^3+2X^2-5X-3	$(19,17,43)$	1
1016	X^3+X^2-6X-2	$(19,12,42)$	1
1076	X^3+3X^2-5X-1	$2(12,-3,17)$	2

1101	X^3+5X^2-X-2	$(28,13,31)$	1
1129	X^3+3X^2-4X-3	$(21,15,43)$	1
1229	X^3+2X^2-6X-1	$(22,-3,42)$	1
1257	X^3+2X^2-7X+1	$(25,-23,43)$	1
1300	X^3+3X^2-7X+1	$10(3,-3,4)$	10
1304	$2X^3+3X^2-4X-2$	$(33,24,34)$	1
1345	X^3-7X-1	$(21,9,49)$	1
1369∗	X^3+4X^2-7X+1	$37(1,-1,1)$	37
1373	X^3+3X^2-5X-2	$(24,3,43)$	1
1384	X^3+5X^2-2X-2	$(31,8,34)$	1
1396	X^3+2X^2-6X-2	$2(11,3,24)$	2
1425	X^3+4X^2-3X-3	$5(5,3,9)$	5
1436	X^3+6X^2+X-2	$(33,24,37)$	1
1489	X^3+4X^2-5X-1	$(31,-11,37)$	1
1492	X^3+4X^2-4X-2	$2(14,1,20)$	2
1509	X^3+2X^2-6X-3	$(22,15,54)$	1
1524	X^3+X^2-7X-1	$2(11,1,26)$	2
1556	X^3+5X^2-X-3	$2(14,11,23)$	2
1573	X^3+X^2-7X-2	$11(2,1,5)$	11
1593	X^3+3X^2-6X-1	$9(3,-1,5)$	3
1620	X^3+6X^2-2	$18(2,1,2)$	18
1708	X^3+4X^2-3X-4	$(25,24,57)$	1
1765	X^3+5X^2-3X-2	$(34,3,39)$	1
1772	$2X^3+X^2-6X-2$	$(37,30,42)$	1
1825	X^3+2X^2-7X-1	$5(5,-1,11)$	5
1849∗	$2X^3+X^2-7X+2$	$43(1,-1,1)$	43
1901	X^3+4X^2-4X-3	$(28,11,52)$	1
1929	X^3+5X^2-2X-3	$(31,17,49)$	1
1937	X^3+X^2-8X+1	$(25,-17,61)$	1
1940	X^3-8X-2	$2(12,9,32)$	2
1944	X^3+3X^2-6X-2	$27(1,0,2)$	9
1957	X^3+2X^2-8X+1	$(28,-25,58)$	1
2021	X^3-8X-1	$(24,9,64)$	1
2024	X^3+4X^2-5X-2	$(31,-2,49)$	1
2057	X^3+3X^2-8X+1	$11(3,-3,5)$	11
2089	$2X^3+3X^2-5X-2$	$(39,21,43)$	1
2101	X^3+4X^2-6X-1	$(34,-15,48)$	1
2177	X^3+2X^2-7X-3	$(25,13,67)$	1
2213	X^3+7X^2+3X-2	$(40,39,51)$	1
2228	$2X^3+2X^2-6X-1$	$2(20,3,21)$	2
2233	X^3+X^2-8X-1	$(25,1,67)$	1
2241	X^3+3X^2-6X-3	$9(3,1,7)$	3
2292	$2X^3+4X^2-4X-3$	$2(20,19,26)$	2
2296	X^3+7X^2+2X-2	$(43,32,46)$	1
2300	X^3+X^2-8X-2	$5(5,2,14)$	5
2349	X^3+6X^2-3	$9(4,3,6)$	9
2429	$2X^3+X^2-7X+1$	$(43,-25,46)$	1
2505	X^3+4X^2-5X-3	$(31,7,61)$	1
2557	X^3+X^2-9X+2	$(28,-27,75)$	1
2589	$2X^3+5X^2-3X-3$	$(43,39,54)$	1
2597	X^3+2X^2-8X-1	$7(4,-1,10)$	7

2636	$2X^3 - 7X - 1$	$(42, 18, 49)$	1
2673	$X^3 - 9X - 3$	$27(1, 1, 3)$	9
2677	$X^3 + 3X^2 - 7X - 2$	$(30, -3, 67)$	1
2700	$X^3 + 6X^2 - 3X - 2$	$45(1, 0, 1)$	15
2708	$X^3 + 4X^2 - 6X - 2$	$2(17, -3, 30)$	2
2713	$X^3 + 6X^2 - X - 3$	$(39, 21, 55)$	1
2777	$X^3 + 5X^2 - 6X - 1$	$(43, -21, 51)$	1
2804	$X^3 + X^2 - 9X + 1$	$2(14, -9, 39)$	2
2808	$X^3 - 9X - 2$	$9(3, 2, 9)$	3
2836	$X^3 + 2X^2 - 8X - 2$	$2(14, 1, 38)$	2
2857	$X^3 + 2X^2 - 9X + 1$	$(31, -27, 75)$	1
2917	$X^3 + 5X^2 - 5X - 2$	$(40, -7, 55)$	1
2920	$2X^3 + 4X^2 - 5X - 2$	$(46, 16, 49)$	1
2941	$2X^3 + X^2 - 7X - 1$	$(43, 11, 52)$	1
2981	$X^3 + 5X^2 - 3X - 4$	$(34, 21, 69)$	1
2993	$X^3 + 5X^2 - 4X - 3$	$(37, 7, 61)$	1
3021	$X^3 + 2X^2 - 8X - 3$	$(28, 11, 82)$	1
3028	$X^3 + 3X^2 - 7X - 3$	$2(15, 3, 38)$	2
3124	$2X^3 + 6X^2 - 2X - 3$	$2(24, 21, 29)$	2
3132	$2X^3 + 3X^2 - 6X - 2$	$9(5, 2, 6)$	3

2. Corps Cubiques Complexes

Cette table donne les cent premiers corps cubiques imaginaires, classés par discriminant. Les notations sont analogues à celles de la table précédente.

Disc	$F(X)$	Hessien	f
-23	$X^3 + X^2 + 2X + 1$	$(-5, -7, 1)$	1
-31	$X^3 + X + 1$	$(-3, -9, 1)$	1
-44	$X^3 + 2X^2 + 2X + 2$	$2(-1, -7, -4)$	2
-59	$X^3 + 2X + 1$	$(-6, -9, 4)$	1
-76	$X^3 + X^2 + 3X + 1$	$2(-4, -3, 3)$	2
-83	$X^3 + X^2 + X + 2$	$(-2, -17, -5)$	1
-87	$X^3 + 2X^2 + 3X + 3$	$(-5, -21, -9)$	1
-104	$2X^3 + 2X^2 + 3X + 1$	$(-14, -12, 3)$	1
-107	$X^3 + X^2 + 3X + 2$	$(-8, -15, 3)$	1
-108	$X^3 + 3X^2 + 3X + 3$	$18(0, -1, -1)$	6
-116	$X^3 + X^2 + 2$	$(1, -18, -6)$	1
-135	$X^3 + 3X + 1$	$9(-1, -1, 1)$	3
-139	$X^3 + 2X^2 + 2X + 3$	$(-2, -23, -14)$	1
-140	$X^3 + 2X + 2$	$2(-3, -9, 2)$	2
-152	$2X^3 + 3X^2 + 4X + 2$	$(-15, -24, -2)$	1
-172	$2X^3 + 2X + 1$	$2(-6, -9, 2)$	2
-175	$X^3 + X^2 + 2X + 3$	$5(-1, -5, -1)$	5
-199	$X^3 + X^2 + 4X + 1$	$(-11, -5, 13)$	1
-200	$X^3 + 2X^2 + 3X + 4$	$5(-1, -6, -3)$	5
-204	$X^3 + X^2 + X + 3$	$2(-1, -13, -4)$	2
-211	$2X^3 + X^2 + 3X + 1$	$(-17, -15, 6)$	1
-212	$X^3 + X^2 + 4X + 2$	$(-11, -14, 10)$	1
-216	$X^3 + 3X + 2$	$9(-1, -2, 1)$	3
-231	$X^3 + 2X^2 + X + 3$	$(1, -25, -17)$	1

-239	X^3+3X^2+2X+3	$(3,-21,-23)$	1
-243	X^3+3X^2+3X+4	$27(0,-1,-1)$	9
-244	$2X^3+2X^2+3X+2$	$(-14,-30,-3)$	1
-247	X^3+3X^2+4X+5	$(-3,-33,-29)$	1
-255	X^3+X^2+3	$(1,-27,-9)$	1
-268	$2X^3+4X^2+4X+3$	$2(-4,-19,-10)$	2
-283	X^3+4X+1	$(-12,-9,16)$	1
-300	$2X^3+2X^2+4X+1$	$10(-2,-1,1)$	10
-307	X^3+2X^2+4X+5	$(-8,-37,-14)$	1
-324	$2X^3+3X+1$	$9(-2,-2,1)$	9
-327	$3X^3+3X^2+4X+1$	$(-27,-15,7)$	1
-331	X^3+X^2+3X+4	$(-8,-33,-3)$	1
-335	X^3+2X^2+5X+5	$(-11,-35,-5)$	1
-339	X^3+2X^2+3	$(4,-27,-18)$	1
-351	X^3+3X+3	$9(-1,-3,1)$	3
-356	$2X^3+X^2+2X+2$	$(-11,-34,-2)$	1
-364	X^3+4X+2	$2(-6,-9,8)$	2
-367	X^3+2X^2+3X+5	$(-5,-39,-21)$	1
-379	X^3+X^2+X+4	$(-2,-35,-11)$	1
-411	X^3+X^2+5X+2	$(-14,-13,19)$	1
-419	$2X^3+X^2+3X-1$	$(-17,21,12)$	1
-424	$3X^3+4X^2+5X+2$	$(-29,-34,1)$	1
-431	$2X^3+X^2+3X+2$	$(-17,-33,3)$	1
-436	X^3+3X^2+4X+6	$(-3,-42,-38)$	1
-439	X^3+2X^2-X+3	$(7,-29,-17)$	1
-440	$2X^3+X+2$	$(-6,-36,1)$	1
-451	$2X^3+3X^2+5X+3$	$(-21,-39,-2)$	1
-459	$2X^3+3X^2+3X+3$	$9(-1,-5,-2)$	3
-460	X^3+X^2+5X+3	$2(-7,-11,8)$	2
-472	$2X^3+4X^2+5X+4$	$(-14,-52,-23)$	1
-484	X^3+2X^2+5X+6	$11(-1,-4,-1)$	11
-491	X^3+2X^2+2X+5	$(-2,-41,-26)$	1
-492	X^3+2X^2+4X+6	$2(-4,-23,-10)$	2
-499	X^3+4X+3	$(-12,-27,16)$	1
-503	$2X^3+5X^2+5X+4$	$(-5,-47,-35)$	1
-515	X^3+4X^2+4X+5	$(4,-29,-44)$	1
-516	$3X^3+3X^2+4X+2$	$(-27,-42,-2)$	1
-519	$3X^3+5X^2+6X+3$	$(-29,-51,-9)$	1
-524	X^3+X^2+3X+5	$2(-4,-21,-3)$	2
-527	X^3+5X+1	$(-15,-9,25)$	1
-543	X^3+X^2+2X+5	$(-5,-43,-11)$	1
-547	$3X^3+2X^2+4X+1$	$(-32,-19,10)$	1
-563	X^3+X^2+5X+4	$(-14,-31,13)$	1
-567	$3X^3+3X+1$	$9(-3,-3,1)$	9
-588	X^3+2X^2+6X+6	$14(-1,-3,0)$	14
-620	$2X^3+4X+1$	$2(-12,-9,8)$	2
-628	$2X^3+5X^2+6X+5$	$(-11,-60,-39)$	1
-643	X^3+3X^2+X+4	$(6,-33,-35)$	1
-648	$2X^3+3X+2$	$9(-2,-4,1)$	9
-652	$2X^3+2X^2+4X+3$	$2(-10,-23,-1)$	2
-655	X^3+2X^2+X+5	$(1,-43,-29)$	1

-671	X^3+3X^2+2X+5	$(3,-39,-41)$	1
-675	X^3+3X^2+3X+6	$45(0,-1,-1)$	15
-676	$2X^3+2X^2+5X+2$	$13(-2,-2,1)$	13
-679	X^3+3X^2+4X+7	$(-3,-51,-47)$	1
-680	$2X^3+2X^2+5X+1$	$(-26,-8,19)$	1
-687	X^3+2X^2+5X+7	$(-11,-53,-17)$	1
-695	X^3+4X^2+5X+7	$(1,-43,-59)$	1
-696	X^3+2X^2-X+4	$(7,-38,-23)$	1
-707	X^3+3X^2+5X+8	$(-6,-57,-47)$	1
-716	$3X^3+X^2+3X-1$	$2(-13,15,6)$	2
-728	X^3+X^2+6X+2	$(-17,-12,30)$	1
-731	X^3+2X^2+4X+7	$(-8,-55,-26)$	1
-743	X^3+5X+3	$(-15,-27,25)$	1
-744	$2X^3+X^2+4X-1$	$(-23,22,19)$	1
-748	X^3+2X^2+2X+6	$2(-1,-25,-16)$	2
-751	X^3+X^2+6X+1	$(-17,-3,33)$	1
-755	X^3+2X^2+6X+7	$(-14,-51,-6)$	1
-756	$2X^3+3X^2+6X+3$	$9(-3,-4,1)$	3
-759	X^3+X^2+6X+3	$(-17,-21,27)$	1
-771	X^3+X^2+3X+6	$(-8,-51,-9)$	1
-780	X^3+4X^2+4X+6	$2(2,-19,-28)$	2
-804	X^3+X^2+4X+6	$(-11,-50,-2)$	1
-808	X^3+X^2+2X+6	$(-5,-52,-14)$	1
-812	$2X^3+4X^2+6X+5$	$2(-10,-33,-12)$	2
-815	$3X^3+4X^2+5X+3$	$(-29,-61,-11)$	1

Bibliographie

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

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

[3] R. Benedetti & J.-J. Risler, *Real algebraic and semi-algebraic sets*, Hermann, 1990.

[4] D. A. Buell, *Binary quadratic forms*, Springer-Verlag, 1989.

[5] H. Cohen, *A course in computational algebraic number theory*, third ed., Springer-Verlag, 1996.

[6] 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.

[7] H. Cohen & J. Martinet, Études heuristiques des groupes de classes des corps de nombres, *J. reine angew. Math.* **404** (1990), pp. 39–76.

[8] H. Cohen & J. Martinet, Heuristics on class groups : some good primes are not too good, *Math. Comp.* **207** (1994), pp. 329–334.

[9] D. Cox, *Primes of the form* $x^2 + ny^2$, Wiley-Interscience, 1989.

[10] M. Craig, A construction for irregular discriminants, *Osaka J. Math* **14** (1977), pp. 365–402.

[11] B. Datskovsky & D. J. Wright, Density of discriminants of cubic extensions, *J. reine. angew. Math.* **386** (1988), pp. 116–138.

[12] H. Davenport, On a principle of Lipschitz, *J. Lond. Math. Soc.* **26** (1951), pp. 179–183.

[13] H. Davenport, On the class number of binary cubic forms (i), *J. Lond. Math. Soc.* **26** (1951), pp. 183–192, errata *ibid* **27** (1951), p. 512.

[14] H. Davenport, On the class number of binary cubic forms (ii), *J. Lond. Math. Soc.* **26** (1951), pp. 192–198.

[15] H. Davenport & H. Heilbronn, On the density of discriminants of cubic fields (i), *Bull. Lond. Math. Soc.* **1** (1969), pp. 345–348.

[16] H. Davenport & H. Heilbronn, On the density of discriminants of cubic fields (ii), *Proc. Roy. Soc. Lond. A* **322** (1971), pp. 405–420.

[17] F. Diaz y Diaz, Sur le 3-rang des corps quadratiques réels, *Prépublications de la faculté d'Orsay*, 1978.

[18] E. Fouvry, Sur le comportement en moyenne du rang des courbes $y^2 = x^3 + k$, in *Séminaire de Théorie des Nombres Paris, 1990–91*, Birkäuser, 1993, pp. 61–83.

[19] G. W. Fung & H. G. Williams, On the computation of complex cubic fields, with discriminant $D \geqslant -10^6$, *Math. Comp.* **55** (1990), pp. 313–325, errata *ibid* **63** (1994), p. 433.

[20] C. F. Gauss, *Arithmetische Untersuchungen (Disquisitiones Arithmeticae)*, Chelsea, 1889.

[21] F. Gerth III, The 4-class ranks of quadratic fields, *Invent. Math.* **77** (1984), pp. 489–515.

[22] H. Halberstam & H. E. Richert, *Sieve methods*, Academic Press, 1974.

[23] H. Hasse, Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage, *Math. Zeitschrift.* **31** (1930), pp. 565–582.

[24] H. Hasse, *Zahlentheorie*, Akademie-Verlag GmbH, 1949.

[25] D. R. Heath-Brown, The square sieve and consecutive square-free numbers, *Math. Annalen* **266** (1984), pp. 251–259.

[26] C. Hermite, Note sur la réduction des formes homogènes à coefficients entiers et à deux indéterminées, *J. reine. angew. Math.* **36** (1848), pp. 357–364.

[27] C. Hermite, Sur la réduction des formes cubiques à deux indéterminées, *C.R. Acad. Sci. Paris* **48** (1859), pp. 351–357.

[28] C. Hooley, On the representations of a number as the sum of four cubes, *Proc. London Math. Soc.* **36** (1978), pp. 117–140.

[29] H. Iwaniec, Almost-primes represented by quadratic polynomials, *Inv. Math.* **47** (1978), pp. 171–188.

[30] H. Iwaniec, A new form of the error term in the linear sieve, *Acta. Arith.* **37** (1980), pp. 307–320.

[31] H. Iwaniec, Rosser's sieve, *Acta. Arith.* **36** (1980), pp. 171–202.

[32] N. M. Katz, Perversity and exponential sums, *Adv. Stud. in Pure Math.* **17** (1989), pp. 210–259.

[33] N. M. Katz & G. Laumon, Transformation de Fourier et majoration de sommes exponentielles, *Publ. Math. IHES* **62** (1985), pp. 361–418.

[34] P. Llorente & J. Quer, On totally real cubic fields with discriminant $d < 10^7$, *Math. Comp.* **50** (1988), pp. 581–594.

[35] J. Martinet, *Une introduction à la théorie du Corps de Classes (notes de M. Olivier)*, Publ. Ecole doct. de Math. de Bordeaux, 1991.

[36] G.-B. Mathews, On the reduction and classification of binary cubics which have a negative discriminant, *Proc. London Math. Soc.* **10** (1912), pp. 128–138.

[37] F. Mertens, Über einige asymptotische Gesetze der Zahlentheorie, *J. reine. angew. Math.* **77** (1874), pp. 289–338.

[38] J.-F. Mestre, Courbes elliptiques et groupes de classes d'idéaux de certains corps quadratiques, *J. reine. angew. Math.* **343** (1983), pp. 23–35.

[39] T. Nagell, Über die Klassenzahl imaginär-quadratisher Zahlkörper, *Abh. Math. Sem. Univ. Hamburg* **1** (1922), pp. 140–150.

[40] PARI/GP, version `2.1.5`, Bordeaux, 2003, `http://pari.math.u-bordeaux.fr/`.

[41] J. Quer, Corps quadratiques de 3-rang 6 et courbes elliptiques de rang 12, *C.R. Acad. Sci. Paris Série I Math.* **305** (1987), pp. 215–218.

[42] J.-B. Rosser & L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois J. Math.* **6** (1962), pp. 64–94.

[43] M. Sato & T. Shintani, On zeta functions associated with prehomogenous vector spaces, *Ann. of Math.* **100** (1974), pp. 131–170.

[44] W. M. Schmidt, *Equations over finite fields, an elementary approach*, Lect. notes in Math., no. 536, Springer-Verlag, 1976.

[45] J.-P. Serre, *Corps locaux*, Hermann, 1968.

[46] J.-P. Serre, *Représentations linéaires des groupes finis*, Hermann, 1978.

[47] T. Shintani, On Dirichlet series whose coefficients are class numbers of integral binary cubic forms, *J. Math. Soc. Japan* **24** (1972), pp. 132–188.

[48] T. Shintani, On zeta-functions associated with the vector space of quadratic forms, *J. Fac. Sci. Univ. Tokyo, Sec. Ia* **22** (1975), pp. 25–66.

[49] G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres*, Pub. Inst. Elie Cartan, 1990.

[50] A. Weil, On some exponential sums, *Proc. Nat. Acad. Sci. USA* **34** (1948), pp. 204–207.

[51] Y. Yamamoto, On unramified Galois extensions of quadratic number fields, *Osaka J. Math.* **7** (1970), pp. 57–76.