CRIBLE ET 3-RANG DES CORPS QUADRATIQUES

KARIM BELABAS

RÉSUMÉ. Considérons le cardinal $h_3^*(\Delta)$ de l'ensemble des racines cubiques de l'unité dans le groupe des classes de $\mathbb{Q}(\sqrt{\Delta})$, où Δ est un discriminant fondamental. Un résultat de Davenport et Heilbronn calcule la valeur moyenne de ces nombres quand Δ varie. On obtient ici géométriquement une borne explicite pour le reste, avec la possibilité supplémentaire de restreindre les Δ à des progressions arithmétiques. Des techniques de crible permettent alors d'évaluer la 3-partie des $\mathbb{Q}(\sqrt{\pm P_k})$, où P_k est pseudo-premier d'ordre k. On controle ainsi simultanément le 2-rang et le 3-rang du groupe des classes $\mathrm{Cl}(\mathbb{Q}(\sqrt{\Delta}))$. L'auteur donne en particulier une borne pour le 3-rang en moyenne des $\mathbb{Q}(\sqrt{\pm p})$, où p est premier.

ABSTRACT. Call $h_3^*(\Delta)$ the number of cube roots of unity in the class group of $\mathbb{Q}(\sqrt{\Delta})$, where Δ is a fundamental discriminant. Davenport and Heilbronn computed the mean value of these numbers when Δ tends to $\pm\infty$. The author gives a general geometric argument yielding an explicit bound for the error term, with the additional possibility of restricting Δ to arithmetic progressions. Sieve techniques then produce results about the 3-parts of the groups $\mathrm{Cl}\left(\mathbb{Q}(\sqrt{\pm P_k})\right)$, where P_k is an almost-prime of order k. In this way, one controls simultaneously both the 2-rank and the 3-rank of the class group $\mathrm{Cl}(\mathbb{Q}(\sqrt{\Delta}))$. As a special case, the author gives a bound for the mean 3-rank of the $\mathbb{Q}(\sqrt{\pm p})$, where p is prime.

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 [9] 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 $\Delta < 0$.

Date: 13 janvier 2004.

1991 *Mathematics Subject Classification.* 11P21, 11R11, 11R29, 11N36.

Key words and phrases. Lattice Points, Quadratic Extensions, Class groups, 3-Rank, Sieve.

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 [10] 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 [6] et [7]) 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 [18]).

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 [11, 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 9facteurs 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.

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 [12]).

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

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

Preuve. Voir [12, 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 ([8, démonstration du Théorème 1] et [9, §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 [6, 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 :*

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

Preuve. C'est exactement [6, 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 [7] et [17]. □

Aux constantes près, on a les mêmes majorations que dans le Lemme 3.4 (voir [7, 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 [2]). La réduction des formes de discriminant négatif (due à Mathews et Berwick, voir [7] et [17]) 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 [5]) :

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 [1, 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 [6, 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 ([6, erratum] pour $\Delta > 0$ et [7, 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 [19] ont développé une théorie des fonctions zêta associées à certaines représentations (espaces vectoriels préhomogènes), et les premiers exemples étudiés par Shintani [20] 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 ([19, §3]) pour tenir compte des équations fonctionnelles vérifiées par leurs fonctions zêta, permet d'obtenir le développement explicite suivant ([21, 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 [4] 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).

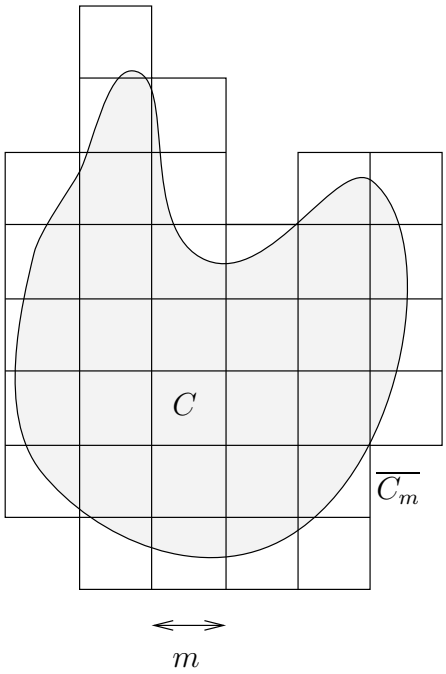

FIG. 1. Découpage de C

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

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

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*

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

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 :

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

(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 [9, 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 [9, 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 [9, 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 ([16, 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 [15]) 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 :

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

La partie entre crochets du terme principal vaut

$$\begin{aligned} 1 + \sum_k \sum_{p_i} \prod_{p_i\mid q} \frac{-2}{p+1} \prod_{(p_i,q)=1} \frac{-(2p^2-1)}{p^4} &= \prod_{p\mid(q,Q)} (1 - \frac{2}{p+1}) \prod_{\substack{p\mid Q \\ (p,q)=1}} (1 - \frac{2p^2-1}{p^4}) \\ &= \prod_{p\mid Q} \frac{(p^2-1)^2}{p^4} \prod_{p\mid q} \frac{p^4(p-1)}{(p+1)(p^2-1)^2}, \end{aligned}$$

et l'on calcule

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

□

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 :*

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

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 [9, 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 ([9, Lemme 9]). Puis au plus $O(\tau(M)3^{\omega(f)}h_3^*(\Delta))$ classes de Hessiens MH_1 ([9, 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 [14] et [13]. On s'est efforcé de conserver autant que possible les mêmes notations que [13]. 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

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

On a alors les inégalités :

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

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

où F et f sont les fonctions du crible linéaire (voir [13] *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 [14])

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

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 [13] :

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

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

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

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

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

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

Preuve. Voir [22, 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 [3] ou les tables de [2]). 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.

Références

[1] R. Benedetti & J.-J. Risler, *Real algebraic and semi-algebraic sets*, Hermann, 1990.

[2] D. A. Buell, *Binary quadratic forms*, Springer-Verlag, 1989.

[3] 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.

[4] B. Datskovsky & D. J. Wright, Density of discriminants of cubic extensions, *J. reine. angew. Math.* **386** (1988), pp. 116–138.

[5] H. Davenport, On a principle of Lipschitz, *J. Lond. Math. Soc.* **26** (1951), pp. 179–183.

[6] 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.

[7] H. Davenport, On the class number of binary cubic forms (ii), *J. Lond. Math. Soc.* **26** (1951), pp. 192–198.

[8] H. Davenport & H. Heilbronn, On the density of discriminants of cubic fields (i), *Bull. Lond. Math. Soc.* **1** (1969), pp. 345–348.

[9] H. Davenport & H. Heilbronn, On the density of discriminants of cubic fields (ii), *Proc. Roy. Soc. Lond. A* **322** (1971), pp. 405–420.

[10] 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.

[11] H. Halberstam & H. E. Richert, *Sieve methods*, Academic Press, 1974.

[12] H. Hasse, Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage, *Math. Zeitschrift.* **31** (1930), pp. 565–582.

[13] H. Iwaniec, A new form of the error term in the linear sieve, *Acta. Arith.* **37** (1980), pp. 307–320.

[14] H. Iwaniec, Rosser's sieve, *Acta. Arith.* **36** (1980), pp. 171–202.

[15] N. M. Katz, Perversity and exponential sums, *Adv. Stud. in Pure Math.* **17** (1989), pp. 210–259.

[16] N. M. Katz & G. Laumon, Transformation de Fourier et majoration de sommes exponentielles, *Publ. Math. IHES* **62** (1985), pp. 361–418.

[17] 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.

[18] 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.

[19] M. Sato & T. Shintani, On zeta functions associated with prehomogenous vector spaces, *Ann. of Math.* **100** (1974), pp. 131–170.

[20] T. Shintani, On Dirichlet series whose coefficients are class numbers of integral binary cubic forms, *J. Math. Soc. Japan* **24** (1972), pp. 132–188.

[21] 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.

[22] G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres*, Pub. Inst. Elie Cartan, 1990.

Karim Belabas
Université Bordeaux I
Département de mathématiques (A2X)
351, cours de la Libération
F-33405 Talence (France)
belabas@math.u-bordeaux.fr