VARIATIONS SUR UN THÈME DE DAVENPORT ET HEILBRONN

K. BELABAS

1. Prélude

On appelle *discriminant fondamental* un entier qui est discriminant d'un corps de degré au plus 2 sur $\mathbb{Q}$, et *discriminant quadratique*, un discriminant fondamental différent de 1. Étant donné $X \geq 0$, on notera $\Delta^+(X)$ (resp. $\Delta^-(X)$) l'ensemble des discriminants fondamentaux compris entre 0 et X (resp. $-X$ et 0). Si Δ est un discriminant quadratique, p un premier, on pose $h_p(\Delta) = p^{r_p(\Delta)}$, où $r_p(\Delta)$ est le p-rang du groupe des classes de $\mathbb{Q}(\sqrt{\Delta})$, lui-même noté $\mathrm{Cl}(\Delta)$.

Depuis Gauss, on connaît une formule explicite pour $r_2(\Delta)$, qui est essentiellement égal au nombre $\omega(\Delta)$ de diviseurs premiers de Δ (on a $r_2(\Delta) = \omega(\Delta) - 1$ ou $\omega(\Delta) - 2$). Pour $p = 3$, on peut calculer l'ordre moyen :

Théorème 1.1 (Davenport–Heilbronn [16])**.** *Pour X un réel positif, on a, au voisinage de $+\infty$, les égalités*

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

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

Pour $p \geq 5$, on ne sait essentiellement rien, mais on dispose de la conjecture suivante, issue d'un modèle probabiliste :

Conjecture 1.2 (Cohen–Lenstra [9])**.** Pour X tendant vers $+\infty$, on a les égalités

$$\sum_{\Delta\in\Delta^+(X)} h_p(\Delta) \Big/ \sum_{\Delta\in\Delta^+(X)} 1 = 1 + \frac{1}{p} + o(1)\ ,$$

$$\sum_{\Delta\in\Delta^-(X)} h_p(\Delta) \Big/ \sum_{\Delta\in\Delta^-(X)} 1 = 2 + o(1)\ .$$

En généralisant le modèle, on obtient

Date: 20 avril 2003.

Conjecture 1.3 (Cohen–Martinet [10])**.** Soit $\Delta(X; G, r_1, r_2)$ la famille des corps de nombres galoisiens, de groupe de Galois G et de signature (r_1, r_2), de discriminants compris entre $-X$ et X. Notons $n = r_1 + r_2 - 1$ le rang du groupe d'unités de $K \in \Delta$, et considérons un premier p, tel que $p \nmid |G|$. Alors, pour X tendant vers $+\infty$, on a l'égalité :

$$\sum_{K\in\Delta} h_p(\mathrm{Cl}(K)) \Big/ \sum_{K\in\Delta} 1 = 1 + \frac{1}{p^n} + o(1) \ .$$

Le théorème de Davenport et Heilbronn s'articule sur l'existence d'une application injective, préservant le discriminant, qui à tout corps cubique associe une équation (cubique!) à coefficients entiers, et dont l'image se détermine par des conditions locales simples.

Ce résultat permet de manipuler, de façon très explicite et naturelle, des familles de corps cubiques. En particulier, on obtient facilement la liste des corps cubiques de discriminant borné par une constante X. De plus, ces corps sont définis par une équation canonique qui donne, de façon immédiate, toute l'information arithmétique simple qui leur est associée : discriminant, anneau d'entiers, décomposition des idéaux premiers (voir [5]).

Par exemple, $h_3(\Delta)$ est directement lié au nombre d'extensions cubiques non ramifiées de $\mathbb{Q}(\sqrt{\Delta})$ ou, de façon équivalente, aux triplets de corps cubiques conjugués de discriminant Δ. On assimile ensuite les formes cubiques correspondantes aux points entiers d'un volume de $\mathbb{R}^4$. C'est le principe de la démonstration du Théorème 1.1. Traiter le cas suivant, à savoir le 5-rang des corps quadratiques, par des méthodes analogues nécessite l'étude de classes de formes de degré 5, à 4 variables, modulo $\mathrm{Gl}(4, \mathbb{Z})$, et paraît, pour l'instant, hors de portée.

Les heuristiques de Cohen, Lenstra, et Martinet assimilent les groupes de classes d'une famille de corps, de signature (r_1, r_2) donnée, à des quotients de groupes abéliens "génériques" par des sous-groupes à $r_1 + r_2 - 1$ générateurs. Nous allons considérer des "anneaux d'entiers" dont le groupe des classes aura le comportement générique prescrit et montrer que leur 3-rang est bien celui prédit.

Un théorème classique de Scholz lie le 3-rang du corps $\mathbb{Q}(\sqrt{\Delta})$ à celui du corps miroir $\mathbb{Q}(\sqrt{\Delta})$, par l'intermédiaire d'un "défaut de 3-primarité" $\delta(\Delta)$ valant 0 ou 1. En utilisant les heuristiques, et sous des hypothèses d'indépendance supplémentaires, Dutarte a montré que les valeurs de δ étaient équiprobables au sens de Cohen et Lenstra. En utilisant les constructions précédentes, nous montrerons que ce résultat vaut inconditionnellement, pour une moyenne un peu moins naturelle.

Comme on le verra, ces théorèmes s'obtiennent en comptant des points entiers, vérifiant une congruence adélique, dans un volume explicite. Une étude géométrique permet de contrôler le reste, pour des congruences très générales, par exemple $q|\Delta$ dans les sommes (1) et (2), où nous remplacerons le $o(1)$ par un bien meilleur terme reste.

L'étude des progressions arithmétiques évoquées plus haut permet aussi, grâce à des méthodes de crible, d'obtenir des renseignements sur $h_3(\Delta)$ en restreignant $\omega(\Delta)$, c'est-à-dire en contrôlant simultanément le 2-rang et le 3-rang (voir [3]). Par exemple, on a le

Théorème 1.4. *Pour X tendant vers $+\infty$, on a les inégalités*

$$\sum_{\substack{p\le X\\ p\equiv 1 \pmod 4}} h_3(p)\Big/ \sum_{\substack{p\le X\\ p\equiv 1 \pmod 4}} 1 \le 11\big(1+o(1)\big)\ ,$$

$$\sum_{\substack{p\le X\\ p\equiv 3 \pmod 4}} h_3(-p)\Big/ \sum_{\substack{p\le X\\ p\equiv 3 \pmod 4}} 1 \le 31\big(1+o(1)\big)\ ,$$

où tous les indices de sommation sont premiers.

Ce résultat indique simplement que le 3-rang des $\mathbb{Q}(\sqrt{p})$ n'est pas anormalement élevé (les valeurs moyennes correspondantes pour les $h_3(\Delta)$ sont respectivement 4/3 et 2). On obtient aussi les résultats typiques du crible :

Théorème 1.5. *Il existe une infinité de Δ*

- positifs *ayant au plus* 8 *facteurs premiers tels que* $h_3(\Delta)=1$,
- négatifs *ayant au plus* 26 *facteurs premiers tels que* $h_3(\Delta)=1$,
- *ayant au plus* 9 *facteurs premiers tels que* $h_3(\Delta)>1$.

Plus précisément, si X tend vers $+\infty$, on obtient des estimations de la forme

$$\frac{X}{\log X} \ll \#\big\{\Delta\in\Delta^+(X),\ P^-(\Delta)\ge X^{1/u},\ h_3(\Delta)=1\big\} \ll \frac{X}{\log X}\ ,$$

$$\frac{X}{\log X} \ll \#\big\{\Delta\in\Delta^-(X),\ P^-(\Delta)\ge X^{1/v},\ h_3(\Delta)=1\big\} \ll \frac{X}{\log X}\ ,$$

$$\frac{X}{\log X} \ll \sum_{\substack{\Delta\in\Delta^\pm(X)\\ P^-(\Delta)\ge X^{1/w}}} (h_3(\Delta)-1) \ll \frac{X}{\log X}\ ,$$

où $P^-(\Delta)$ désigne le plus petit diviseur premier de Δ, et (u,v,w) sont des constantes, vérifiant respectivement $u<9$, $v<27$, et $w<10$.

Le dernier encadrement ne permet pas d'affirmer que les Δ produits ont une densité positive. Nous ne savons essentiellement pas en déduire mieux que

$$\#\big\{\Delta\in\Delta^\pm(X),\ \omega(\Delta)\le 9,\ h_3(\Delta)>1\big\} \gg \frac{X^{1/2}}{\log^2 X}\ .$$

Un crible direct, à partir d'une construction de Nagell [24], raffinée par Yamamoto [30], permet de faire beaucoup mieux (voir [2]). Par exemple :

Théorème 1.6. *Si ℓ est un premier impair, on définit la fonction $g(\ell)$ de la façon suivante :*

$$g(5) = 4, \quad g(4k+1) = 3k+2, \quad \textit{si } k \geq 2$$
$$g(4k+3) = 3k+3, \quad \textit{pour tout } k \geq 0.$$

Alors, il existe une infinité de discriminants fondamentaux négatifs Δ, *avec $h_\ell(\Delta) > 1$ et $\omega(\Delta) \leq g(\ell)$. De plus, on a l'inégalité*

$$\#\big\{\Delta \in \Delta^-(X),\ \omega(\Delta) \leq g(\ell), h_\ell(\Delta) > 1\big\} \gg \frac{X^{(\ell+1)/2\ell}}{\log X}\ ,$$

pour X tendant vers $+\infty$.

En particulier le cas $\ell = 3$ donne des discriminants ayant au plus 3 facteurs premiers dans le troisième point du Théorème 1.5. On obtient des résultats du même type (beaucoup moins bons, la construction étant plus complexe) pour les discriminant positifs. Cette approche ne faisant aucunement appel à notre thème, nous ne la développerons pas plus avant.

Les démonstrations seront ici réduites à leur plus simple expression. Le lecteur intéressé par les détails se reportera, respectivement, pour ce qui concerne le crible, les heuristiques, et les manipulations de corps cubiques, à [3], [1], [5], et aux bibliographies qui y figurent. Tous ces articles sont rassemblés dans [4].

Etienne Fouvry m'a fait découvrir ce théorème de Davenport et Heilbronn. Qu'il en soit remercié, ainsi que pour les très nombreuses discussions que nous avons eues à son sujet. Nous remercions aussi Georges Gras de nous avoir signalé le mémoire de Dutarte [18].

2. Thème

2.1. **La bijection fondamentale.** Considérons l'ensemble des formes cubiques binaires à coefficients entiers, qui sont primitives et irréductibles. Si $F = ax^3 + bx^2y + cxy^2 + dy^3 = (a,b,c,d)$ est une forme cubique, on définit son discriminant

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

Le groupe linéaire $\mathrm{Gl}(2,\mathbb{Z})$ agit naturellement sur cet ensemble par changement de variable, et préserve le discriminant. Baptisons Φ l'ensemble des classes pour cette action, et définissons le discriminant d'un élément de Φ comme étant le discriminant d'une forme de la classe. On définit des sous-ensembles V_p et U_p de Φ par les congruences suivantes :

$$F \in V_p \Longleftrightarrow \begin{cases} \operatorname{disc}(F) \not\equiv 0 \pmod{p^2} & \text{si } p \neq 2 \\ \operatorname{disc}(F) \equiv 1 \pmod 4 \text{ ou } \operatorname{disc}(F) \equiv 8 \text{ ou } 12 \pmod{16} & \text{si } p = 2 \end{cases}$$

$$F \in U_p \Longleftrightarrow \begin{cases} F \in V_p, \text{ ou} \\ F = \lambda(\alpha x - \beta y)^3 \pmod p \text{ et } F(\beta,\alpha) \neq 0 \pmod{p^2} \end{cases}$$

On note $U = \cap U_p$ (essentiellement, les formes dont le discriminant est celui d'un corps cubique), $V = \cap V_p$ (formes de discriminant fondamental), et $\mathcal{C}$ l'ensemble des classes d'isomorphismes de corps cubiques sur $\mathbb{Q}$. Si K est un corps cubique et $x \in K$, on note x, x', et x'' les conjugués de x dans une clôture galoisienne de K, $\mathrm{disc}(K)$ est le discriminant de K et $\sqrt{\mathrm{disc}(K)}$ une de ses racines carrées. Soit maintenant $\mathcal{B} = [1, \alpha, \beta]$ une $\mathbb{Z}$-base de $\mathbb{Z}_K$, on pose

$$F_{\mathcal{B}}(x, y) = \frac{\mathrm{N}_{K/\mathbb{Q}}\left((\beta - \beta')x - (\alpha - \alpha')y\right)}{\sqrt{\mathrm{disc}(K)}} \ .$$

Alors on a le

Théorème 2.1 (Davenport–Heilbronn [15] et [16])**.**

(1) *La classe de $F_{\mathcal{B}}$, notée F_K, ne dépend que de K.*
(2) *F_K appartient à U et* $\mathrm{disc}(F_K) = \mathrm{disc}(K)$.
(3) *$K \mapsto F_K$ est une bijection de $\mathcal{C}$ sur U.*

Le lien avec le 3-rang des corps quadratiques est le suivant :

Lemme 2.2.

- *Il y a $(h_p(\Delta) - 1)/(p - 1)$ sous-groupes d'indice p dans* $\mathrm{Cl}(\Delta)$.
- *Les sous-groupes d'indice* 3 *dans* $\mathrm{Cl}(\Delta)$ *sont en bijection avec les éléments de V (classes de formes de discriminant fondamental).*

Preuve. Le premier point est un lemme facile de théorie des groupes. Le deuxième résulte de la bijection de Davenport–Heilbronn et d'une étude des discriminants cubiques (voir [14] et [20]). □

2.2. **Réduction.** Une forme quadratique définie (A, B, C), à coefficients réels, est dite réduite si $0 \leq B \leq A \leq C$ (ce n'est pas la définition habituelle !). Il existe alors une forme réduite dans toute classe modulo $\mathrm{Gl}(2, \mathbb{Z})$, en général unique : les exceptions (dites *classes exceptionnelles*) correspondent aux cas d'égalité. On peut associer à toute forme cubique binaire F une forme quadratique définie $Q(F)$ telle que pour tout $M \in \mathrm{Gl}(2, \mathbb{Z})$, on ait

$$Q(F \circ M) = \lambda(F, M).Q(F) \circ M \ , \quad \text{ou} \quad \lambda(F, M) \in \mathbb{R} \ . \tag{3}$$

On décrète alors que $F = (a, b, c, d)$ est réduite si $Q(F)$ l'est et $a > 0$. Puis que F est exceptionnelle si $Q(F)$ l'est. Toute classe de formes cubiques contient alors une forme réduite F, et celle-ci est unique si F n'est pas exceptionnelle. En effet, si F et F' sont des formes cubiques réduites équivalentes, il en est de même des covariants quadratiques $Q(F)$ et $Q(F')$, qui sont donc égaux. Une matrice de transformation M de F en F' correspond donc à un automorphisme de $Q(F) = Q(F')$. Une étude précise montre que, sauf aux cas d'égalités, les seuls automorphismes d'une forme définie sont $\pm\mathrm{Id}$. Or $-\mathrm{Id}$ change le signe de a.

Explicitement, pour $F = (a, b, c, d)$ une forme cubique, on définit son Hessien par la formule

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

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

Un calcul immédiat montre que H_F est covariant ((3) avec $\lambda \equiv 1$) et que $\operatorname{disc}(H_F) = -3 \operatorname{disc}(F)$. Donc si $\operatorname{disc}(F) > 0$, on peut poser $Q(F) = H(F)$ et $\lambda \equiv 1$. Sinon, F admet une unique racine réelle θ et $F = ax^3+bx^2y+cxy^2+dy^3 = (x - \theta y)(Ax^2 + Bxy + Cy^2)$, où (A, B, C) est définie (et à coefficients dans $\mathbb{R}$). On prend alors $Q(F) = (A, B, C)$, $\lambda(F, M) = |a - \theta c|$. Dans les deux cas, nous pouvons exprimer que F est réduite par des inéquations polynomiales en (a, b, c, d) à coefficients *entiers* :

$$|bc - 9ad| \leq b^2 - 3ac \leq c^2 - 3bd \ , \quad \text{et} \quad a > 0$$

pour les formes de discriminants positifs, comme nous venons de le voir. Et pour les formes de discriminants négatifs (voir [23]) :

$$d^2 - a^2 + ac - db \geq 0 \ ,$$
$$(a + b)(a + b + c) - ad \geq 0 \ ,$$
$$(a - b)(a - b + c) + ad \geq 0 \ ,$$
$$a > 0 \ .$$

On peut très facilement imposer des inégalités supplémentaires (une par cas d'égalité) sur (a, b, c, d) pour avoir une forme unique, y compris pour les classes exceptionnelles (c'est le point de vue de [5] et du paragraphe suivant), ou bien contrôler le nombre de ces dernières (Lemme 3.1). Remarquons simplement que si $\operatorname{disc}(F) < 0$, aucune forme irréductible n'est exceptionnelle (tout cas d'égalité entraîne $\theta \in \mathbb{Q}$).

2.3. **Invariants.** Soit K un corps cubique. La bijection de Davenport et Heilbronn lui associe une classe de formes cubiques de même discriminant, la réduction permettant d'obtenir un représentant canonique F_K. On retrouve alors facilement (voir [5]) les invariants simples de K sur les coefficients de la forme F_K (ou de n'importe quelle autre forme de la classe) :

Théorème 2.3. *Avec les conventions précédentes, on a*

- $\operatorname{disc} K = \operatorname{disc} F_K$.
- *Si θ est une racine de F_K qui engendre K, alors $[1, a\theta, a\theta^2 + b\theta]$ est une $\mathbb{Z}$-base de l'anneau d'entiers $\mathcal{O}_K$. En particulier, $\mathcal{O}_K$ admet une base canonique.*

- *La décomposition d'un premier p dans $\mathbb{Z}_K/\mathbb{Z}$ est donnée par la factorisation de $F_K = (a, b, c, d)$ dans $\mathbb{F}_p[X, Y]$. Plus précisément, si*

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

est une décomposition en facteurs irréductibles, nous avons

$$p\mathbb{Z}_K = \prod_i \mathfrak{p}_i^{e_i} \ ,$$

où $\mathfrak{p}_i$ est premier dans $\mathbb{Z}_K$ et explicitement déterminé par T_i.

Algorithmiquement, on peut balayer simplement les formes du domaine fondamental, et les conditions locales de Davenport et Heilbronn ont une traduction agréable. Il n'est même pas nécessaire de factoriser des discriminants : savoir détecter si un entier de taille contrôlée est sans facteur carrés suffit (par exemple, en s'aidant de listes calculées une fois pour toutes).

En effet, un discriminant cubique s'écrit de manière unique sous la forme $f^2\Delta$ où Δ est fondamental. De plus, 9 est le seul facteur carré autorisé dans f, et finalement $\operatorname{pgcd}(f, \Delta) = 1$ ou 3. Si p est un nombre premier, les assertions suivantes sont équivalentes ([4] et [20]) :

- p est totalement ramifié dans $K/\mathbb{Q}$.
- p divise f.
- $F_K \notin V_p$.
- p divise le contenu f_H du Hessien de F_K.

De plus, si $p \neq 3$ et $p|f_H$, la condition $F \in U_p$ est équivalente à $p^3 \nmid \operatorname{disc} K$. En toute généralité, f et f_H ont les mêmes diviseurs premiers (on a $f = f_H$ ou $f = 3f_H$).

Une fois réglés les cas triviaux correspondant à $p = 2$ ou $p = 3$, on peut supposer $\operatorname{disc}(F)$ premier à 6. On calcule donc f_H, qui doit être sans facteurs carrés. Puis $\delta = \operatorname{pgcd}(f_H, \operatorname{disc}(F)/f_H^2)$, la division étant exacte. Finalement, on déduit facilement de ce qui précède que F représente un corps cubique si et seulement si $\operatorname{disc}(F)/f_H^2$ est sans facteurs carrés et $\delta = 1$.

Il se trouve, de surcroît, qu'une forme réduite appartenant à U est nécessairement primitive (trivial) et irréductible (plus astucieux). Nous obtenons ainsi un algorithme, essentiellement linéaire en X, permettant de dresser les tables des corps cubiques, de signature donnée, et de discriminant borné par X. Une valeur de $X = 10^{11}$ reste tout à fait raisonnable (voir [5], où nous donnons les tables correspondantes, ainsi qu'une évaluation précise de la complexité). En comptant les corps de même discriminant, nous pouvons, par exemple, prouver ainsi que $\mathbb{Q}(\sqrt{-653329427})$, construit par Diaz y Diaz [17], est le plus petit corps imaginaire de 3-rang égal à 4 (ce que Buell [7] cite comme une conjecture). Le plus petit corps quadratique réel de 3-rang égal à 4, à savoir $\mathbb{Q}(\sqrt{58343207081})$, était semble-t-il inconnu à ce jour.

Le cas des petits discriminants Δ, avec $r_3(\Delta) \leq 3$, était bien connu, par calcul exhaustif des groupes de classes des $\mathbb{Q}(\sqrt{\Delta})$, $|\Delta| < 10^7$. Alors qu'un tel calcul s'avère impossible pour, disons $|\Delta| > 10^8$, notre algorithme permet d'étudier facilement des tranches du type $\Delta \in [X, X+Y]$, l'unique difficulté étant déterminer si approximativement Y nombres de la taille de $X+Y$ sont sans facteurs carrés (mais on n'obtient évidemment que le 3-rang, et non la structure complète !).

Ce type de méthode permet aussi d'obtenir en quelques lignes une paramétrisation des extensions cubiques d'un corps quadratique donné, ou de retrouver la formule classique donnant l'équation générale des corps cubiques cycliques (qu'on trouve par exemple dans [8, §6.4.2]) : ce sont exactement ceux dont le Hessien est de la forme $f_H(1,1,1)$.

3. Première variation

3.1. **Points entiers.** D'après le §2, il revient essentiellement au même d'étudier des classes de formes cubiques ou des points entiers dans un volume de $\mathbb{R}^4$, C^+ ou C^- suivant le signe du discriminant, défini par des équations polynomiales. La différence est quantifiée par le lemme suivant :

Lemme 3.1. *On se restreint aux classes de formes cubiques réduites, de discriminant borné par X. Le nombre de telles classes F qui sont réductibles*[1] *ou exceptionnelles est un $O(X^{3/4+\varepsilon})$, pour tout $\varepsilon > 0$.*

On tronque ces deux volumes pour obtenir

$$C^+(X) = C^+ \cap \{F : 0 \leq \operatorname{disc}(F) \leq X\} \ ,$$
$$C^-(X) = C^+ \cap \{F : -X \leq \operatorname{disc}(F) \leq 0\} \ .$$

Un principe attribué à Lipschitz indique que le nombre de points entiers dans un compact "raisonnable" est de l'ordre de grandeur de son volume. La formulation quantitative suivante est due à Davenport [12] :

Théorème 3.2. *Soit C un compact de volume $\operatorname{Vol}(C)$ de $\mathbb{R}^n$, et soit $N(C)$ le cardinal de $\mathbb{Z}^n \cap C$. 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 tout espace affine de dimension m d'équation $x_{i_1} = \cdots = x_{i_{n-m}} = 0$, pour tout m compris entre 1 et $n-1$.*

On note V_m la somme des volumes des projections de C sur les espaces affines de dimension m définis ci-dessus ($V_0 = 1$ par convention). Alors on a l'inégalité :

[1] Le heurt des terminologies est malheureux, mais difficilement évitable.

$$|N(C) - \mathrm{Vol}(C)| \leq \sum_{m=0}^{n-1} h^{n-m} V_m \ .$$

On a alors deux problèmes : les $C^{\pm}(X)$ obtenus par réduction ne sont pas compacts, quoique de volumes finis. De plus, leurs projections sur $a = 0$ ou $b = 0$ ont un volume de même ordre de grandeur que les volumes initiaux. La solution de Davenport est remarquablement simple : il tronque à nouveau $C^{\pm}(X)$, et considère

$$C^{\pm}(X, \rho) = C^{\pm}(X) \cap \left\{(a, b, c, d) : a > X^{1/4-3\rho}\right\} \ ,$$

pour un paramètre $\rho > 0$ qu'il finit par prendre égal à $\frac{1}{16}$. En contrepartie, alors que les $C^{\pm}(X)$ étaient homothétiques, ce n'est plus le cas des $C^{\pm}(X, \rho)$. On obtient tout de même sans trop de mal :

Théorème 3.3 (Davenport [13], [14])**.** *Si $H^{\pm}(X)$ (resp. $H^{\pm}(X, \rho)$) désigne le nombre de points entiers de $C^{\pm}(X)$ (resp. $C^{\pm}(X, \rho)$), on a*

$$H^{\pm}(X, \rho) = H^{\pm}(X) + O(X^{1-\rho}) \ ,$$

$$H^{\pm}(X) = K^{\pm} X + O(X^{15/16}) \ ,$$

avec $K^+ = \pi^2/72$, $K^- = \pi^2/24$.

Remarque 3.4. Shintani [27] étudie des séries de Dirichlet dont les coefficients sont essentiellement les nombres de classes de formes cubiques, en les reliant aux fonctions zêtas associées par Sato [25] à certaines représentations (espaces vectoriels préhomogènes). Ces séries se prolongent analytiquement au plan complexe (avec deux pôles simples en 1 et 5/6, où les résidus sont connus) et admettent une équation fonctionnelle originale où elles interviennent toutes simultanément. Un théorème taubérien évolué (tenant compte des équations fonctionnelles) permet alors d'obtenir un terme supplémentaire du développement de $H^{\pm}(X)$, de la forme $C^{\pm} X^{5/6}$, où $C^{\pm}$ est non nul et explicite (voir [28, Théorème 4]).

3.2. **Congruences.** Soit m un entier, on se donne un sous-ensemble S_m de classes de formes cubiques modulo m, c'est-à-dire une partie de $(\mathbb{Z}/m\mathbb{Z})^4$ stable sous $\mathrm{Gl}(2, \mathbb{Z}/m\mathbb{Z})$. On note $s(m) = |S_m|/m^4$ sa densité, qui est une fonction multiplicative. On dira qu'un point de $\mathbb{Z}^4$ appartient à S_m si c'est le cas de sa réduction modulo m. Un découpage en cubes de côté m de $C^{\pm}(X, \rho)$ permet alors de voir que le nombre de points entiers de $C^{\pm}(X, \rho) \cap S_m$ est égal à

$$s(m).H^{\pm}(X, \rho) + O(s(m) \cdot B^{\pm}(X, \rho, m)), \tag{4}$$

où $B^{\pm}(X, \rho, m)$ dénombre les points entiers des cubes rencontrant le bord de $C^{\pm}(X, \rho)$.

Si m est fixé, on constate facilement que, $B^{\pm}(X, \rho, m)$ est un $o(X)$, et c'est ce qu'utilisent Davenport et Heilbronn. Mais, pour nos applications de crible, il nous faut une estimation uniforme en m.

Une première idée est d'appliquer le Théorème 3.2, en majorant le volume de nos cubes par celui d'un voisinage tubulaire (de rayon $2m$) du bord de $C^{\pm}(X,\rho)$. En reprenant le célèbre calcul de Weyl [29], une majoration explicite est possible, par des méthodes de géométrie différentielle. Cependant, le calcul s'applique à une variété (sans bord) lisse, ce qui n'est pas du tout notre cas : notre variété est l'intersection de 5 hypersurfaces. On doit donc faire un peu de chirurgie pour se ramener au cas d'une hypersurface lisse (à bord). Il faut ensuite étudier ce qui se passe là où les hypersurfaces se coupent (le bord) et envisager finalement le cas des intersections multiples. On obtient péniblement une majoration par un polynôme de degré 4 en m, le terme dominant étant de l'ordre de $X^{30\rho}m^4$: on ne peut plus prendre $\rho = 1/16$!

On peut aussi exploiter la nature algébrique du problème grâce au résultat suivant (voir [6, Théorème 2.3.4]) :

Théorème 3.5. *Soit $A \subset \mathbb{R}^n$ un ensemble semi-algébrique (*i.e. *donné par un nombre fini d'inéquations polynomiales à coefficients dans $\mathbb{R}$), 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 (effective) ne dépend que de n, l et d.

En combinant ce dernier résultat au principe de Lipschitz (Théorème 3.2) et à l'estimation (4), on peut étudier le voisinage "cubulaire" initial. Si C est un semi-algébrique compact de $\mathbb{R}^n$, le réseau $(m\mathbb{Z})^n$ en donne un découpage en cubes de côtés m. On note $\widehat{C}$ l'intérieur des cubes rencontrant la frontière de C et $\widehat{C}_i$ les projections de $\widehat{C}$ sur les hyperplans de coordonnées, pour $1 \leq i \leq n$. La Figure 1 illustre la situation, en dimension 2.

Théorème 3.6. *On reprend les notations des Théorèmes* 3.2 *et* 3.5. *On note de plus $N(C, S_m)$ le nombre de points entiers de C appartenant à S_m. Alors, il existe une constante K effective, ne dépendant que de d, l, et n, telle que l'on ait l'inégalité :*

$$\left|N(C,S_m) - s(m)\mathrm{Vol}(C)\right| \leq K(d,l,n)\cdot s(m)\, m \cdot \max_i N(\widehat{C}_i). \tag{5}$$

Pour $C = C^{\pm}(X,\rho)$, on obtient un reste global de la forme

$$s(m)\, mX^{3/4+3\rho}\log X \ ,$$

si m est un $o(X^{1/4})$. Cette dernière condition revient à imposer que le nombre de segments obtenus par projection du découpage sur un axe de coordonnées tend vers $+\infty$.

La qualité des estimations de crible que nous obtenons dépend essentiellement de la façon dont on maîtrise ce reste. Un ordre de grandeur raisonnable serait $s(m)\, mX^{5/6}$ et le résultat de Shintani indique d'ailleurs qu'il est optimal si $m = 1$.

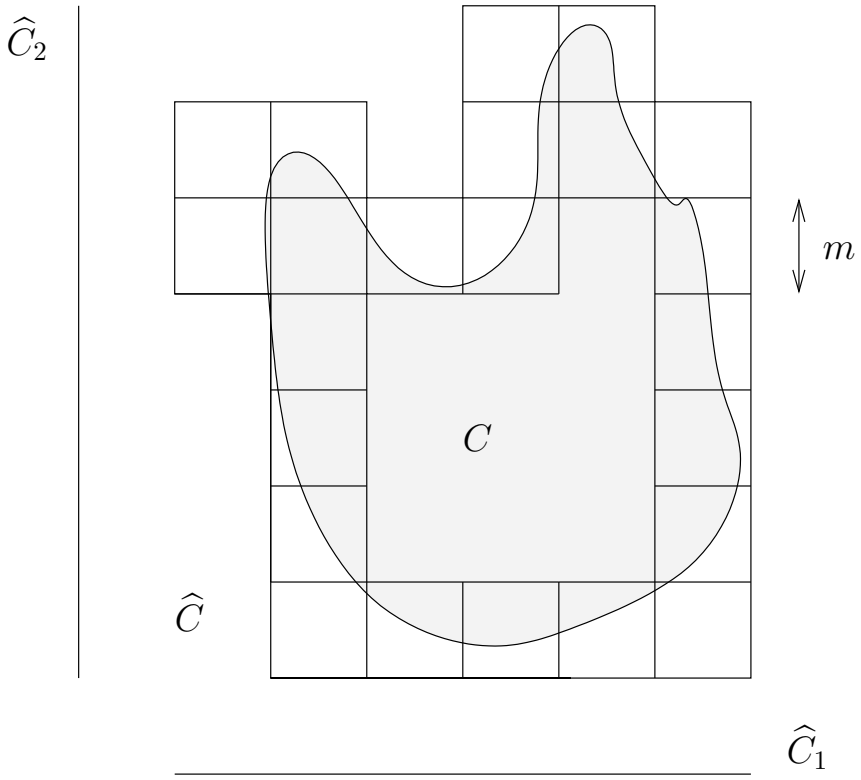

FIGURE 1. Voisinage "cubulaire".

Mais, même dans ce cas particulier, nous n'avons pu retrouver son $O(X^{5/6})$ par nos méthodes élémentaires.

D'autre part, les calculs de Shintani se prêtent effectivement à l'introduction de congruences : c'est ainsi que Datskovky et Wright [11] ont pu généraliser les théorèmes de Davenport–Heilbronn en prenant pour corps de base n'importe quel corps global de caractéristique différente de 2 ou de 3. Mais il semblerait que les fonctions zêta adéliques qu'ils utilisent ne permettent pas de maîtriser le reste (voir les remarques p. 124 de [11]).

3.3. **3-rang et progressions arithmétiques.** En supposant que l'on sache calculer les densités locales $s(p^\alpha)$ pour $p|m$, nous pouvons donner de bonnes estimations de $N\big(C^{\pm}(X,\rho), S_m\big)$ si m est petit. Si, par contre, m a de gros facteurs premiers, on utilise des résultats du type de :

Proposition 3.7. *Soit p un premier, et q un entier. On considère des corps cubiques K de discriminant $|\operatorname{disc}(K)| \leq X$.*

- *Le nombre de corps tels que $p^2|\operatorname{disc}(K)$ est un $O(X/p^2)$.*

- *Pour tout $\varepsilon > 0$, le nombre de corps tels que $p^2 q | \operatorname{disc}(K)$ est un*

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

Preuve. Le premier point se montre soit en termes de classes de formes quadratiques et des entiers qu'elles représentent [16, §4], soit en termes de corps de classes [11, §6]. Il faut essentiellement évaluer le nombre d'extensions cubiques cycliques dont p divise le conducteur (ici le corps de base est $\mathbb{Q}$ ou $\mathbb{Q}(\sqrt{\operatorname{disc}(K)})$, mais la démonstration de [11] vaut pour tout corps de nombres). Ce conducteur est lui-même borné par l'inégalité $|\operatorname{disc}(K)| \leq X$, et doit satisfaire des conditions arithmétiques assez strictes : les seuls facteurs carrés autorisés proviennent de premiers au dessus de 3, et la puissance à laquelle un tel premier intervient est uniformément bornée en fonction du corps de base.

Le deuxième point utilise nos estimations géométriques, mais reprend essentiellement la preuve du premier (voir [3]). □

Si $v < m$, on peut évaluer le nombre de points d'un cube de côté v appartenant à S_m en développant en série de Fourier la fonction caractéristique de l'intervalle $[0, v]$. Apparaissent alors les sommes d'exponentielles :

$$\sigma(\boldsymbol{h}, m) = \sum_{\boldsymbol{A} \in S_m} e^{2i\pi(\boldsymbol{A}.\boldsymbol{h}/m)} \ ,$$

où $\boldsymbol{h} \in (\mathbb{Z}/m\mathbb{Z})^4 - \{0\}$. En les majorant, nous pouvons remplacer m par v dans le reste de (5), si v n'est pas trop petit. Finalement, on peut exploiter l'encadrement trivial :

$$N(C(X, \rho), S_{mn}) \leq N(C(X), S_{mn}) \leq N(C(X), S_n) \ .$$

Globalement, on obtient le type de théorème suivant, où seules la majoration des sommes exponentielles et les densités locales font intervenir la congruence considérée :

Théorème 3.8. *Fixons un $\varepsilon > 0$, et $K^{\pm}$ comme au Théorème 3.3. On note S_q l'ensemble des discriminants fondamentaux divisibles par q. Quand X tend vers $+\infty$, on a les inégalités :*

$$\sum_{\substack{\Delta \in \Delta^{\pm}(X) \\ \Delta \in S_q}} \frac{h_3(\Delta) - 1}{2} \leq \frac{K^{\pm} X}{\zeta^2(2)} \prod_{p|q} \frac{1}{p+1} + O\left(\frac{X \log_3^2 X}{q \log^2 X \log_2^2 X} + X^{15/16+\varepsilon} q^{-1/16}\right) \ ,$$

$$\sum_{\substack{\Delta \in \Delta^{\pm}(X) \\ \Delta \in S_q}} \frac{h_3(\Delta) - 1}{2} \geq \frac{K^{\pm} X}{\zeta^2(2)} \prod_{p|q} \frac{1}{p+1} + O\left(\frac{X \log_3^2 X}{q \log^2 X \log_2^2 X} + X^{13/16+\varepsilon} q^{13/16}\right) \ .$$

La minoration est valable si $q < X^{3/29-\varepsilon}$ et la majoration si $q < X^{1/15-\varepsilon}$.

Remarquons aussi que, puisque $\Delta^{\pm}(X) = 3X/\pi^2 + O(\sqrt{X})$, le cas $q = 1$ donne le résultat de Davenport et Heilbronn, avec un terme reste plus précis. En fait, en menant les calculs sans se soucier de l'uniformité en q, on obtient dans [1] un bien meilleur résultat :

Théorème 3.9. *On* fixe q, X *tendant vers* $+\infty$. *Pour tout ensemble* S_q *de discriminants fondamentaux, vus modulo* q, *on a l'égalité*

$$\sum_{\substack{\Delta\in\Delta^{\pm}(X)\\ \Delta\in S_q}} \frac{h_3(\Delta)-1}{2} = \frac{K^{\pm}X}{\zeta^2(2)}\frac{|S_q|}{q^4\prod_{p|q}(1-p^{-2})^2} + o(X.L(X)) \ , \tag{6}$$

$$o\grave{u} \quad L(X) = \exp\big(-c(\log X \log\log X)^{\frac{1}{2}}\big) \ ,$$

pour une constante c *convenable* ($c < 24^{-\frac{1}{2}}$ *suffit).*

(On peut contrôler q, mais la qualité des termes d'erreurs dépend alors fortement de la congruence considérée.) On peut donc remplacer dans le Théorème 1.1 les $o(1)$ par des $o(L(X))$. Les mêmes techniques permettent d'obtenir sans difficulté des densités de discriminants cubiques ne provenant pas forcément d'extensions non ramifiées de corps quadratiques, avec le même terme d'erreur.

Cette vitesse de convergence est considérablement plus élevée que ne le laissaient prévoir les précédents calculs en machine (voir par exemple les commentaires de [19] et [22]).

3.4. **Cribles.** Un crible est une "boîte noire" prenant en entrée une suite d'entiers $\mathcal{A}$ et une suite de premiers $\mathcal{P}$. Si l'on dispose de renseignements sur la répartition des éléments de $\mathcal{A}$ dans les progressions arithmétiques, on obtient en sortie une estimation du nombre d'éléments de $\mathcal{A}$ qui ne sont divisibles par aucun élément de $\mathcal{P}$.

On utilise ici une généralisation simple : on crible les Δ qui sont des discriminants fondamentaux, affectés du poids positif $h_3(\Delta) - 1$. Le Théorème 3.8 fournit les renseignements nécessaires sur la répartition dans les progressions arithmétiques. Le cadre est particulièrement favorable (crible linéaire), et l'on obtient le résultat suivant :

Théorème 3.10. *On fixe* $\varepsilon > 0$, $Q_B = X^{1/15-\varepsilon}$ *et* $Q_A = X^{3/29-\varepsilon}$ *(données par le Théorème 3.8), et on pose*

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

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

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

On note finalement

$$\mathbb{X}^{\pm} = \#\{(a,b,c,d) \in C^{\pm}(X) \cap V\} \sim \frac{2K^{\pm}}{\zeta^2(2)} X \ .$$

On a alors les inégalités :

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

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

où F et f sont les fonctions du crible linéaire (voir [21] *pour leur définition exacte).*

Les théorèmes de crible cités en introduction sont des corollaires plus ou moins directs de ce dernier résultat (à l'exception du Théorème 1.6).

4. Deuxième variation

Cohen, Lenstra, et Martinet ont proposé un modèle probabiliste pour le comportement moyen de la partie impaire du groupe des classes d'un corps de nombres (voir [9] pour le cas quadratique et [10] pour la généralisation en degré quelconque – et à des extensions éventuellement non galoisiennes). Cette description implique en particulier que les groupes de classes des corps de nombres galoisiens se comportent en moyenne comme ceux de quadratiques imaginaires, quotientés par un sous-groupe à n générateurs "aléatoires", si le groupe des unités est de rang n. Les conjectures citées au §1 résultent alors d'une deuxième hypothèse sur la structure des $\mathrm{Cl}(\Delta)$, pour $\Delta < 0$.

Fixons n premiers impairs distincts $p_1, \dots, p_n$ et considérons la famille Δ_S des corps quadratiques imaginaires K (qu'on identifiera avec leurs discriminants par abus de langage), dans lesquels les p_i sont totalement décomposés. Pour chacun de ces K, d'anneau d'entiers $\mathcal{O}_K$, on fixe un diviseur $\mathfrak{p}_{i,K}$ de p_i pour tout i, puis l'on pose $S_K = \{\mathfrak{p}_{1,K}, \dots, \mathfrak{p}_{n,K}\}$ (pour alléger les notations, on omettra parfois le K en indice dans la suite). On note

$$\mathcal{O}_{K,S} = \{x \in K : v_{\mathfrak{q}}(x) < 0 \Longrightarrow \mathfrak{q} \in S_K\}$$

les S_K-entiers de K. Les idéaux fractionnaires de $\mathcal{O}_{K,S}$ (en bijection avec ceux de $\mathcal{O}_K$ qui sont étrangers à S) forment un groupe commutatif, et les idéaux principaux un sous-groupe. On définit comme d'habitude le groupe des classes de $\mathcal{O}_{K,S}$ en effectuant le quotient.

Lemme 4.1. *Les $\mathcal{O}_{K,S}$ ont le comportement que les heuristiques assignent aux corps de nombres galoisiens dont le rang des unités est n :*

- $\mathrm{rg}\, \mathcal{O}_{K,S}^* = \mathrm{rg}\, \mathcal{O}_K + |S_K| = n$.
- $\mathrm{Cl}(\mathcal{O}_{K,S}) = \mathrm{Cl}(K)/\langle \mathfrak{p}_1, \dots, \mathfrak{p}_n \rangle$.

Preuve. Le premier point résulte du théorème de Dirichlet sur les S-unités. Le deuxième vient en étudiant le morphisme canonique $I \mapsto I\mathcal{O}_{K,S}$ qui, à tout idéal de $\mathcal{O}_K$, associe un idéal de $\mathcal{O}_{K,S}$. □

Donc, si H_K désigne le corps de classe de Hilbert de K, et H_K^S les points fixes par les Frobenius en les $\mathfrak{p}_i$, le groupe de Galois de H_K^S/K est $\mathrm{Cl}(\mathcal{O}_{K,S})$. Reprenons la preuve présentée au paragraphe 2 :

Lemme 4.2. *Soit K un élément de Δ_S :*

- *Il y a $(h_p(\mathcal{O}_{K,S})-1)/(p-1)$ sous-groupes d'indice p dans $\mathrm{Cl}(\mathcal{O}_{K,S})$.*
- *Les sous-groupes d'indice 3 dans $\mathrm{Cl}(\mathcal{O}_{K,S})$ sont en bijection avec les extensions cubiques cycliques de K, où les Frobenius $(\mathfrak{p}_i, H_K/K)$ agissent trivialement.*
- *Une extension cubique cyclique L de K est fixée par $(\mathfrak{p}, H_K/K)$ si et seulement si, modulo p, la forme cubique qui lui est associée est non nulle et se décompose en 3 facteurs linéaires premiers entre eux.*
- *Dans ce cas, on a automatiquement $F \in V_p$ et l'ensemble S_p correspondant a pour cardinal $\frac{1}{6}(p+1)p(p-1)^2$.*
- *Les extensions cubiques cycliques non ramifiées d'un corps quadratique où p se décompose totalement correspondent aux formes de S_p.*

Preuve. Les deux premiers points sont immédiats. Le Frobenius agit trivialement si et seulement si $\mathfrak{p}$ est totalement décomposé dans L/K, c'est-à-dire si p l'est dans l'un des sous-corps cubiques de L. Le troisième point résulte donc du Théorème 2.3.

Soit F la forme cubique associée, elle n'a pas de facteurs carrés modulo p donc p ne divise pas $\mathrm{disc}(F)$, ce qui implique $F \in V_p$. Un dénombrement élémentaire des différents choix, pour les 3 racines distinctes (dans $\mathbb{P}^1(\mathbb{F}_p)$) et le coefficient dominant (dans $\mathbb{F}_p^*$), donne alors le quatrième point.

Enfin, si une forme appartient à S_p, son discriminant Δ est un carré modulo p (c'est le carré du produit des différences des racines), et p est totalement décomposé dans $\mathbb{Q}(\sqrt{\Delta})/\mathbb{Q}$. Comme la réciproque résulte des points précédents, le lemme est démontré. □

Les éléments de Δ_S sont les discriminants fondamentaux qui ne sont pas résidus quadratiques modulo $p \in S$. On montre facilement les égalités

$$|\Delta^{\pm}(X)| = \frac{3X}{\pi^2} + O(\sqrt{X}) \ ,$$

$$|\Delta^{\pm}(X) \cap \Delta_S| = \prod_{p\in S} \frac{p}{2(p+1)} \cdot \frac{3X}{\pi^2} + O(\sqrt{X}) \ .$$

(il suffit de reprendre le calcul classique du nombre d'entiers sans facteurs carrés inférieurs à X, et d'incorporer des congruences). On en déduit immédiatement, à l'aide du lemme précédent et de (6), que

$$\sum_{\Delta\in\Delta^-(X)\cap\Delta_S}\frac{h_3(\Delta)-1}{2} = \frac{K^-}{\zeta^2(2)}\prod_{p\in S}\frac{\frac{1}{6}(1+p)p(p-1)^2}{p^4(1-p^{-2})^2}X+O(X.L(X))$$
$$= \frac{1}{2}\cdot\frac{1}{3^n}|\Delta^-(X)\cap\Delta_S|+O(X.L(X))$$

Soit

$$\sum_{\Delta\in\Delta^-(X)\cap S_p}h_3(\Delta)\Big/\sum_{\Delta\in\Delta^-(X)\cap S_p}1=(1+3^{-n})+O(L(X)), \tag{7}$$

ce qui correspond au comportement des quadratiques *réels* (Théorème 1.1) si n est égal à 1. Pour $n>1$, on retrouve bien la valeur du 3-rang prévue par les heuristiques.

5. Final

Soit l'ensemble Ω des $\mathrm{Cl}(\Delta)$, $\Delta>0$, dont on considère une partie A. Suivant Cohen–Lenstra, notons, quand la limite existe,

$$P(A)=\lim_{X\to+\infty}\sum_{\Delta\in\Delta^+(X)}1_A(\mathrm{Cl}(\Delta))\Big/\sum_{\Delta\in\Delta^+(X)}1\ ,$$

où 1_A désigne la fonction caractéristique de A. P est seulement finiment additive, et n'est donc pas une mesure sur Ω. Nous écrirons néanmoins que $\mathrm{Cl}(\Delta)\in A$ avec "probabilité" $P(A)$.

Si Δ est un discriminant fondamental positif, on définit le défaut $\delta(\Delta)$ par l'équation

$$r_3(-3\Delta)=r_3(\Delta)+1-\delta(\Delta),\quad\text{soit}\quad h_3(-3\Delta)=h_3(\Delta)3^{1-\delta(\Delta)}\ .$$

Un résultat classique de Scholz [26] énonce que $\delta(\Delta)$ ne prend que les valeurs 0 et 1. Sous le modèle de Cohen–Lenstra, Dutarte [18] parvient, modulo des hypothèses supplémentaires d'indépendance, à la conjecture suivante :

Conjecture 5.1. On a l'égalité $P(\{\mathrm{Cl}(\Delta):\delta(\Delta)=0, r_3(\Delta)=a\})=3^{-(a+1)}$, pour tout $a\geq 0$.

D'où l'on déduit que $P(\{\mathrm{Cl}(\Delta):\delta(\Delta)=0, r_3(\Delta)\leq a\})$ tend vers $1/2$ quand a tend vers $+\infty$. On parvient donc à la conjecture raisonnable :

$$P(\{\mathrm{Cl}(\Delta):\delta(\Delta)=0\})=P(\{\mathrm{Cl}(\Delta):\delta(\Delta)=1\})=1/2\ .$$

Théorème 5.2. *Pour X tendant vers $+\infty$, on a l'égalité*

$$\sum_{\substack{\Delta\in\Delta^+(X)\\ \delta(\Delta)=0}}h_3(\Delta)\Big/\sum_{\Delta\in\Delta^+(X)}h_3(\Delta)=\frac{1}{2}+O(L(X))\ .$$

Autrement dit, $\delta(\Delta)$ est équiréparti pour la loi obtenue en munissant la probabilité P du poids $h_3(\Delta)$.

Preuve. Écrivons

$$\begin{aligned}\sum_{\Delta\in\Delta^+(X)} h_3(-3\Delta) &= \sum_{\substack{\Delta\in\Delta^+(X)\\ 3\nmid\Delta}} h_3(-3\Delta) + \sum_{\substack{\Delta\in\Delta^+(X)\\ 3\mid\Delta}} h_3(-3\Delta)\\ &= \sum_{\substack{\Delta\in\Delta^-(3X)\\ 3\mid\Delta}} h_3(\Delta) + \sum_{\substack{\Delta\in\Delta^-(X/3)\\ 3\nmid\Delta}} h_3(\Delta)\ .\end{aligned}$$

Or, on déduit de (6), en utilisant la densité donnée au Théorème 3.8, que

$$\sum_{\substack{\Delta\in\Delta^-(X)\\ 3\mid\Delta}} \frac{h_3(\Delta)-1}{2} = \frac{K^-X}{4\zeta^2(2)} + o(X.L(X))\ .$$

Soit

$$\begin{aligned}\sum_{\Delta\in\Delta^+(X)} \frac{h_3(-3\Delta)-h_3(\Delta)}{2} &= \frac{K^-}{\zeta^2(2)}\left(\frac{3X}{4}+\frac{X}{3}(1-\frac{1}{4})\right) - \frac{K^+X}{\zeta^2(2)} + o(X.L(X))\\ &= \frac{X}{\pi^2} + o(X.L(X))\ ,\end{aligned}$$

D'où l'on tire, par définition de $\delta(\Delta)$, et grâce au Théorème 1.1 :

$$\sum_{\Delta\in\Delta^+(X)} h_3(\Delta)\frac{3^{1-\delta(\Delta)}-1}{2}\Big/ \sum_{\Delta\in\Delta^+(X)} h_3(\Delta) = \frac{1}{2} + O(L(X))\ .$$

On conclut en remarquant que $(3^{1-\delta(\Delta)}-1)/2$ est la fonction caractéristique de la propriété $\delta(\Delta)=0$. □

Bibliographie

[1] K. Belabas, Densités de classes de formes cubiques et calculs heuristiques du 3-rang des corps de nombres, en préparation.

[2] K. Belabas, Sur le ℓ-rang des corps quadratiques imaginaires de discriminant pseudo-premier, en préparation.

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

[4] K. Belabas, Variations sur un thème de Davenport et Heilbronn, Thèse de Doctorat d'État, Université Bordeaux I, 1996.

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

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

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

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

[9] 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.

[10] H. Cohen & J. Martinet, Études heuristiques des groupes de classes des corps de nombres, *J. reine angew. Math.* **404** (1990), pp. 39–76.
[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, Thèse de Doctorat d'État, Orsay, 1978.
[18] P. Dutarte, Compatibilité avec le Spiegelungssatz de probabilités conjecturales sur le p-rang du groupe des classes, in *Number theory, 1983–1984* (Besançon), Univ. Franche-Comté, Besançon, 1984, pp. Exp. No. 4, 11.
[19] G. W. Fung & H. G. Williams, On the computation of complex cubic fields, with discriminant $D \geq -10^6$, *Math. Comp.* **55** (1990), pp. 313–325, errata *ibid* **63** (1994), p. 433.
[20] H. Hasse, Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage, *Math. Zeitschrift.* **31** (1930), pp. 565–582.
[21] H. Iwaniec, A new form of the error term in the linear sieve, *Acta. Arith.* **37** (1980), pp. 307–320.
[22] P. Llorente & J. Quer, On totally real cubic fields with discriminant $d < 10^7$, *Math. Comp.* **50** (1988), pp. 581–594.
[23] 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.
[24] T. Nagell, Über die Klassenzahl imaginär-quadratisher Zahlkörper, *Abh. Math. Sem. Univ. Hamburg* **1** (1922), pp. 140–150.
[25] M. Sato & T. Shintani, On zeta functions associated with prehomogenous vector spaces, *Ann. of Math.* **100** (1974), pp. 131–170.
[26] A. Scholz, Über die Beziehung der Klassenzahlen quadratisher Körper zueinander, *J. reine angew. Math.* **166** (1932), pp. 201–203.
[27] T. Shintani, On Dirichlet series whose coefficients are class numbers of integral binary cubic forms, *J. Math. Soc. Japan* **24** (1972), pp. 132–188.
[28] 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.
[29] H. Weyl, On the volume of tubes, *Am. Jour. of Math.* **61** (1939), pp. 461–472.
[30] Y. Yamamoto, On unramified Galois extensions of quadratic number fields, *Osaka J. Math.* **7** (1970), pp. 57–76.

Max Planck Institut für Mathematik
Gottfried-Claren-Str. 26
53225 Bonn (Allemagne)
karim@mpim-bonn.mpg.de

Université Bordeaux I
Département de mathématiques (A2X)
351, cours de la Libération
33405 Talence (France)