DISCRIMINANTS CUBIQUES ET PROGRESSIONS ARITHMÉTIQUES

K. BELABAS & E. FOUVRY

Résumé. Nous calculons la densité des discriminants des corps sextiques galoisiens de groupe S_3, démontrant un nouveau cas de la conjecture de Malle ainsi qu'un cas particulier de sa généralisation par Ellenberg et Venkatesh. Plus généralement, nous étudions la densité des discriminants de corps cubiques dans une progression arithmétique, avec une zone d'uniformité la plus large possible.

We compute the density of discriminants of Galois sextic fields with group S_3, thereby proving a new case of Malle's conjecture as well as a special case of its generalization by Ellenberg and Venkatesh. Further, we study the density of cubic discriminants in an arithmetic progression, in the largest possible uniformity with respect to the modulus.

Table des matières

1991 *Mathematics Subject Classification.* 11R29, 11R16, 11P21.
Version 02/10/2009.

1. Introduction

Dans tout cet article, on réserve la lettre p aux nombres premiers et la lettre K aux corps de nombres tels que

$$[K : \mathbb{Q}] = 3, \quad K \subset \overline{\mathbb{Q}} \subset \mathbb{C}.$$

On note $\mathcal{K}$ cet ensemble de corps cubiques, sur lequel opère le groupe de Galois $\mathrm{Gal}\big(\overline{\mathbb{Q}}/\mathbb{Q}\big)$. On désigne par $\tilde{K}$ l'orbite de K sous cette action, de cardinal 1 ou 3 suivant que K est galoisien ou non ; on note $\tilde{\mathcal{K}}$ l'ensemble de ces orbites. Cet article étudie la suite $\mathcal{D}_3$ des discriminants des corps cubiques, c'est-à-dire la suite

$$\mathcal{D}_3 := \big(\operatorname{disc} \tilde{K}\big)_{\tilde{K} \in \tilde{\mathcal{K}}}. \tag{1}$$

La suite $\mathcal{D}_2$ des discriminants quadratiques est bien comprise : $\Delta_2 \neq 1$ est discriminant d'un corps quadratique, si et seulement si Δ_2 est de la forme $\Delta_2 = m$ ou de la forme $\Delta_2 = 4m'$ avec m et m' sans facteur carré, et $m \equiv 1$ et $m' \equiv 2, 3$ modulo 4. Enfin, si Δ_2 est un tel discriminant, il l'est pour une unique extension quadratique de $\mathbb{Q}$, incluse dans $\mathbb{C}$. La situation est plus compliquée pour les corps cubiques, car on ne dispose que de conditions nécessaires pour qu'un entier appartienne à $\mathcal{D}_3$ (Lemme 5.1) et d'une formule peu efficace pour le décompte des corps cubiques ayant pour discriminant un entier fixé (Lemme 5.3). Nous réservons dorénavant le symbole Δ_2 pour désigner un discriminant de corps quadratique. Enfin, on dit que l'entier Δ est un discriminant fondamental s'il est de la forme $\Delta = 1$ ou $\Delta = \Delta_2$.

Le premier résultat remarquable concernant la suite $\mathcal{D}_3$ est dû à Davenport et Heilbronn [14] et décrit la fonction de comptage de cette suite. Posant, pour $X < Y$ réels,

$$N(X, Y) := \operatorname{card}\left\{\tilde{K} \in \tilde{\mathcal{K}} \colon X < \operatorname{disc} \tilde{K} < Y\right\},$$

ils ont montré, pour X tendant vers l'infini, les relations

$$N(0, X) \sim \frac{1}{12\zeta(3)} X, \quad N(-X, 0) \sim \frac{1}{4\zeta(3)} X. \tag{2}$$

(Voir le récent travail de Belabas, Bhargava et Pomerance [6, Theorem 1.1] pour une formule plus précise.)

L'article de Davenport-Heilbronn contient deux importantes généralisations de la formule asymptotique (2). Un nombre premier p étant fixé, la première concerne le décompte des classes de conjugaison $\tilde{K} \in \tilde{\mathcal{K}}$ tels que K soit non galoisien, non

ramifié en p, et tels que le symbole de Frobenius $\left(p, K(\sqrt{\operatorname{disc} K})/\mathbb{Q}\right)$ ait l'une des trois valeurs fixées à l'avance Id, $A_3 \setminus \mathrm{Id}$ ou $S_3 \setminus A_3$.

La seconde généralisation donne le comportement en moyenne de la 3-torsion du groupe de classes des corps quadratiques. Plus précisément, désignons par $r_3(\Delta_2)$ le 3-rang du groupe de classes de $\mathbb{Q}(\sqrt{\Delta_2})$, et posons

$$\alpha^+ = 1 \quad \text{et} \quad \alpha^- = 3;$$

on a, pour X tendant vers l'infini, les relations ([14, Theorem 3])

$$\sum_{0<\pm\Delta_2<X} 3^{r_3(\Delta_2)} \sim \left(1 + \frac{\alpha^\pm}{3}\right) \sum_{0<\pm\Delta_2<X} 1 \tag{3}$$

dont les preuves nécessitent une étude de la suite $\mathcal{D}_3$ dans certaines progressions arithmétiques. Rappelons l'équivalence asymptotique

$$\sum_{0<\pm\Delta_2<X} 1 \sim \frac{1}{2\zeta(2)} \cdot X, \quad (X \to \infty) \tag{4}$$

et l'égalité

$$\frac{3^{r_3(\Delta_2)} - 1}{2} = \operatorname{card}\left\{\tilde{K} \in \tilde{\mathcal{K}} \colon \operatorname{disc} \tilde{K} = \Delta_2\right\}, \tag{5}$$

cas particulier des lemmes 5.3 et 5.4, et conséquence de la théorie du corps de classes. En combinant (3), (4) et (5), on obtient, pour $X \to \infty$, les relations

$$\operatorname{card}\left\{\tilde{K} \in \tilde{\mathcal{K}} \colon \operatorname{disc} \tilde{K} = \Delta_2, 0 < \pm\Delta_2 < X\right\} \sim \frac{\alpha^\pm}{2\pi^2} \cdot X, \tag{6}$$

Les résultats principaux du présent article sont des généralisations de ces théorèmes, inspirés par la conjecture de Malle [20, 21][1] et ses généralisations. Étant donnés $n \geqslant 1$, un corps de nombres $k \subset \overline{\mathbb{Q}}$, et un sous-groupe transitif $G \subset S_n$, on dit qu'une extension K de k de degré n est *de groupe* G si le groupe de Galois de la clôture galoisienne $\widehat{K}/k$, vu comme groupe de permutations sur les n k-plongements de K dans $\widehat{K}$, est isomorphe à G. En particulier, si K/k est galoisienne de groupe de Galois G, alors K/k est de groupe G. Malle s'intéresse au nombre $N_{n,k}(X, G)$ de classes d'isomorphismes d'extensions de k de degré n, de groupe G, incluses dans $\overline{\mathbb{Q}}$, dont le discriminant relatif $\mathfrak{d}_{K/k}$ est de norme inférieure à X, et propose une formule asymptotique pour $N_{n,k}(X, G)$ quand $X \to \infty$, formule ultérieurement généralisée par Ellenberg et Venkatesh [16, § 4.2].

Comme tout discriminant de corps de nombres, un élément de $\mathcal{D}_3$ s'écrit, d'une façon et d'une seule, sous la forme Δf^2 où Δ est un discriminant fondamental et $f \geqslant 1$ un entier — on précisera ce résultat général de Stickelberger au lemme 5.1 ci-dessous. Les corps cubiques non galoisiens, donc de groupe S_3, correspondent

[1] Sous sa forme la plus précise [21], la conjecture de Malle est fausse : Klüners [19] montre que le facteur logarithmique dans la prédiction est parfois inexact ; un preprint récent de Turkelli [25] propose une conjecture corrigée.

exactement au cas $\Delta \neq 1$. Pour chaque $f \leqslant X^{1/2}$, un corps cubique *galoisien* de discriminant f^2, s'il existe, est inclus dans le corps cyclotomique $\mathbb{Q}(\zeta_f)$, donc chaque tel corps est associé à un sous-groupe d'indice 3 de $\mathrm{Gal}(\mathbb{Q}(\zeta_f)/\mathbb{Q}) = (\mathbb{Z}/f\mathbb{Z})^*$; on en déduit que la contribution des corps galoisiens dans $N(-X, X)$ est en $O(X^{1/2+\varepsilon})$ pour tout $\varepsilon > 0$, et est donc négligeable (voir (8) pour un résultat plus précis). Le résultat de Davenport-Heilbronn (2) permet donc de vérifier, et préciser, la prédiction de Malle pour $N_{3,\mathbb{Q}}(X, S_3) \sim (\alpha^+ + \alpha^-)\frac{X}{12\zeta(3)}$.

Pour $n = 6$, notons $G = S_3(6)$ le groupe $G = S_3 \subset S_6$ dans sa représentation de permutation naturelle. Au lieu de compter les corps cubiques de groupe S_3, nous pouvons compter les corps sextiques qui sont leurs clôtures galoisiennes. La difficulté vient de ce que ce changement de point de vue affecte l'ordre d'énumération (par discriminant) : si un corps cubique de groupe S_3 est de discriminant Δf^2, sa clôture galoisienne, sextique de groupe S_3, est de discriminant $\Delta^3 f^4$ (Lemme 6.5). Nous démontrons ainsi

Théorème 1.1. *Quand $X \to \infty$, conformément à la conjecture de Malle, on a*

$$N_{6,\mathbb{Q}}(X, S_3(6)) \sim (\alpha^+ + \alpha^-)K \cdot X^{1/3},$$

où

$$K = \frac{1}{2\pi^2}\left(1 + \frac{2\cdot 3^{2/3} + 3^{4/3}}{36}\right)\prod_{p\neq 3}\left(1 + \frac{1}{(p+1)p^{1/3}}\right) \approx 0.124414875\ldots.$$

Bhargava et Wood [8, Theorem 2] parviennent indépendamment à un résultat analogue :

$$N_{6,\mathbb{Q}}(X, S_3(6)) \sim \left(\frac{1}{3}\prod_p c_p\right) X^{1/3},$$

où

$$c_{p\neq 3} = \left(1 + \frac{1}{p} + \frac{1}{p^{4/3}}\right)\left(1 - \frac{1}{p}\right), \quad c_3 = \left(1 + \frac{1}{3} + \frac{1}{3^{5/7}} + \frac{2}{3^{7/3}}\right)\left(1 - \frac{1}{3}\right).$$

Leur résultat est formellement différent du notre, mais une réécriture des produits eulériens montre que nos constantes $(\alpha^+ + \alpha^-)K = (\frac{1}{3}\prod c_p)$ sont bien identiques.

Le théorème 1.1 est obtenu en évaluant le cardinal de

$$\mathrm{card}\left\{\tilde{K} \in \tilde{\mathcal{K}} \colon \mathrm{disc}\,\tilde{K} = \Delta f^2, 0 < \pm\Delta^3 f^4 \leqslant X\right\}.$$

Nous y parvenons par un calcul global dans lequel seul le premier 3 joue un rôle particulier : c'est le seul p tel qu'on puisse avoir $p^2 \mid f$. Bhargava et Wood dénombrent eux les corps cubiques K en fixant le type d'isomorphisme de la $\mathbb{Q}_p$-algèbre $K \otimes_{\mathbb{Q}} \mathbb{Q}_p$, pour chaque p, en faisant appel à des tables de corps locaux pour traiter les premiers 2 et 3, et à un théorème d'uniformité de Belabas, Bhargava

et Pomerance [6] pour passer à la limite. Ceci leur permet de proposer [8, §5] une explication heuristique à la Cohen-Lenstra [2] pour leur constante.

Plus généralement, pour $X, Y \geqslant 1$, on définit

$$S(\pm X, Y) = \operatorname{card}\left\{\tilde{K} \in \tilde{\mathcal{K}} \colon \operatorname{disc}\tilde{K} = \Delta f^2, 1 \leqslant \pm\Delta \leqslant X, 1 \leqslant f \leqslant Y\right\}. \tag{7}$$

La question est de trouver un équivalent asymptotique de $S(\pm X, Y)$ lorsque $X + Y$ tend vers l'infini. Avec ces nouvelles notations, le résultat de Davenport et Heilbronn (6) s'écrit

$$S(\pm X, 1) \sim \frac{\alpha^{\pm}}{2\pi^2} X, \quad (X \to +\infty).$$

Un autre cas particulier est dû à Cohn [10], qui montre que

$$S(1, Y) \sim c_0 Y, \quad \text{avec} \quad c_0 = \frac{11\sqrt{3}}{36\pi} \prod_{p \equiv 1 \pmod 6} \left(1 - \frac{2}{p(p+1)}\right) \approx 0.158528258\ldots \tag{8}$$

Noter l'inégalité $c_0 > \alpha^+/(2\pi^2)$.

Ellenberg et Venkatesh [16], généralisant la question de Malle, conjecturent que, pour X et Y tendant vers l'infini avec une uniformité qu'il resterait à préciser, on a la relation

$$S(X, Y) \sim c_0' XY,$$

pour un $c_0' > 0$. Dans cette direction, nous montrons

Théorème 1.2. *Pour tout p premier, on pose*

$$a_p = \left(1 + \frac{1}{p}\right)^{-1}, \qquad \text{pour } p \neq 3,$$

$$a_3 = (2/3)\left(1 + \frac{1}{3}\right)^{-1} = \frac{1}{2}; \qquad \text{pour } p = 3,$$

puis on définit la fonction multiplicative

$$a_n = \mu^2(n) \prod_{p \mid n} a_p.$$

Soit $\varepsilon > 0$. On a l'égalité

$$S(\pm X, Y) = \frac{\alpha^{\pm}}{2\pi^2} X \left(1 + O_\varepsilon\Big(\frac{1}{\log X}\Big)\right) \left(\sum_{f \leqslant Y} a_f + \frac{81}{36} \cdot \sum_{\substack{f \leqslant Y/9 \\ (f,3)=1}} a_f\right),$$

[2] Quand le corps cubique K_3 varie, une classe d'isomorphisme L de $\mathbb{Q}_p$-algèbre étale apparaît comme $K_3 \otimes_{\mathbb{Q}} \mathbb{Q}_p$ avec une fréquence proportionnelle à $\frac{|\operatorname{disc} L|_p}{\operatorname{card}(\operatorname{Aut} L)}$.

uniformément pour $X \geqslant 2$ et $1 \leqslant Y \leqslant X^{\frac{1}{18}-\varepsilon}$. En particulier, si X et Y tendent vers l'infini, avec la contrainte $Y \leqslant X^{\frac{1}{18}-\varepsilon}$, on a l'équivalence asymptotique

$$S(\pm X, Y) \sim c_0' \frac{\alpha^{\pm}}{2\pi^2} XY, \quad \textit{avec} \quad c_0' = \frac{17}{15} \prod_p \left(1 - \frac{2}{p(p+1)}\right) \approx 0.53457136\ldots$$

La preuve repose sur la possibilité de compter (en moyenne) les corps cubiques à paramètre f fixé, quand Δ varie, c'est-à-dire, pour $\Delta \neq 1$, en fixant la ramification de la clôture galoisienne sur son sous-corps quadratique $\mathbb{Q}(\sqrt{\Delta})$. C'est l'uniformité en f des termes d'erreurs qui impose la contrainte $Y \leqslant X^{\frac{1}{18}-\varepsilon}$. La démarche inverse, sommer sur f à Δ fixé, est actuellement totalement impraticable par notre méthode : au lieu de compter $O_f(X)$ points dans un domaine de volume $O_f(X)$, il faudrait compter $O_\Delta(Y)$ points dans un domaine de volume $O_\Delta(Y^2)$, soit un ensemble beaucoup trop maigre. En particulier, nous ne pouvons pas retrouver ainsi le résultat de Cohn, qui repose sur la connaissance explicite de la structure des conducteurs d'une extension cubique cyclique (donnée par le lemme 5.1) et un calcul direct.

La clé des démonstrations est une analyse de la répartition de la suite $\mathcal{D}_3$ dans les progressions arithmétiques avec la plus grande uniformité possible sur le module. C'est le second thème de notre travail et nous le mènerons plus loin que ce que requiert la démonstration des théorèmes précédents. Ce sujet est abordé dans [1, Théorème 1.2], qui étudie $r_3(\Delta_2)$ pour Δ_2 presque premier, et s'intéresse à la répartition des éléments de la suite $\mathcal{D}_3$ qui sont aussi des discriminants fondamentaux. Il montre que pour tout $\varepsilon > 0$, tout entier q sans facteur carré, on a, pour $X \to \infty$, les égalités

$$\begin{aligned}(9)\quad \operatorname{card}\left\{\tilde{K} \in \tilde{\mathcal{K}} \colon \operatorname{disc}\tilde{K} = \Delta_2, 0 < \pm\Delta_2 < X, \Delta_2 \equiv 0 \pmod{q}\right\} \\ = \frac{\alpha^{\pm}}{2\pi^2} \prod_{p \mid q} \left(\frac{p}{p+1}\right) \cdot \frac{X}{q} + O\big(R_\varepsilon(X,q)\big)\end{aligned}$$

avec

$$R_\varepsilon(X,q) = \frac{X}{q}\left\{\frac{1}{\log^2 X \log^{2-\varepsilon}\log X} + \left(\frac{q^{15}}{X^{1-\varepsilon}}\right)^{1/16}\right\}.$$

La formule (9) donne une équivalence asymptotique pour tout $\varepsilon > 0$, uniformément pour q sans facteur carré $\leqslant X^{\frac{1}{15}-\varepsilon}$. Ce domaine d'uniformité fut amélioré en $q \leqslant X^{\frac{3}{44}-\varepsilon}$ dans [3, Théorème 1]. Dans [1], l'auteur utilise des méthodes de cribles pour obtenir des résultats sur les valeurs prises par $r_3(\Delta_2)$ lorsque Δ_2 a peu de facteurs premiers. Cette démarche est alors reprise et améliorée dans [3], en considérant des formules comme (9), mais en moyenne sur q. On parvient alors à la preuve du fait qu'une proportion positive de $p \equiv 1$ modulo 4, n'appartient pas à $\mathcal{D}_3$, ou, ce qui est équivalent : l'équation $r_3(p) = 0$ est satisfaite par une proportion positive de $p \equiv 1$ modulo 4. Par contre, le problème reste ouvert pour

l'équation $r_3(p) > 0$; en d'autres termes on ne sait toujours pas si $\mathcal{D}_3$ contient une infinité de nombres premiers.

Revenons à la suite $\mathcal{D}_3$ elle-même en posant, pour $q \geqslant 1$,

$$N(X, Y; q) := \operatorname{card}\left\{\tilde{K} \in \tilde{\mathcal{K}} \colon X < \operatorname{disc} \tilde{K} < Y, \operatorname{disc} \tilde{K} \equiv 0 \pmod{q}\right\}.$$

On montrera le

Théorème 1.3. *Pour tout $\varepsilon > 0$, et tout $X \geqslant 3$, on a les égalités*

$$\begin{aligned} N(0, X; q) &= \frac{1}{12\zeta(3)} \prod_{p \mid q} \left(\frac{p^2+p}{p^2+p+1}\right) \cdot \frac{X}{q} \left(1 + O_\varepsilon\left(\frac{1}{\log X}\right)\right), \\ N(-X, 0; q) &= \frac{1}{4\zeta(3)} \prod_{p \mid q} \left(\frac{p^2+p}{p^2+p+1}\right) \cdot \frac{X}{q} \left(1 + O_\varepsilon\left(\frac{1}{\log X}\right)\right), \end{aligned} \tag{10}$$

uniformément pour q entier sans facteur carré vérifiant $1 \leqslant q \leqslant X^{\frac{1}{20}-\varepsilon}$.

En particulier (10) implique que, pour $X \to \infty$, on a les comportements asymptotiques

$$\frac{N(0, X; q)}{N(0, X)} \sim \frac{N(-X, 0; q)}{N(-X, 0)} \sim \frac{1}{q} \cdot \prod_{p \mid q} \left(\frac{p^2+p}{p^2+p+1}\right),$$

uniformément pour q sans facteur carré $\leqslant X^{\frac{1}{20}-\varepsilon}$. Puisque le facteur eulérien précédent est inférieur à 1, il n'y a pas équirépartition entre les diverses classes de congruence modulo q des valeurs de la suite $\mathcal{D}_3$.

Bien que ce soit sans influence directe sur le propos central de notre article, il est naturel de se demander quelle est la répartition de la suite $\mathcal{D}_3$ dans les autres classes de congruence. Pour X et Y réels, pour t et q entiers, avec $q \geqslant 1$, posons donc

$$N(X, Y; q, t) := \operatorname{card}\left\{\tilde{K} \in \tilde{\mathcal{K}} \colon X < \operatorname{disc} \tilde{K} < Y,\ \operatorname{disc} \tilde{K} \equiv t \pmod{q}\right\}.$$

On a donc $N(X, Y; q) = N(X, Y; q, 0)$. Par les méthodes utilisées dans la suite, il est possible de prouver qu'il existe un réel $\vartheta > 0$ tel que, pour $X \to \infty$, on ait

$$\frac{N(0, X; p, t)}{N(0, X)} \sim \frac{N(-X, 0; p, t)}{N(-X, 0)} \sim \frac{p^2}{p^3 - 1}, \tag{11}$$

uniformément pour p premier vérifiant $p \leqslant X^{\vartheta}$ et t entier non divisible par p. Le cas où q n'est pas premier nécessite l'emploi du théorème chinois. Par (11), on voit que les éléments de la suite $\mathcal{D}_3$ se répartissent harmonieusement entre les classes premières à p, mais de façon différente dans la classe $0 \bmod p$. Ce phénomène est courant en théorie des nombres, l'exemple le plus caricatural étant la suite des nombres premiers. Un autre exemple est celui de la suite des entiers sans facteur carré (et par conséquent de la suite $\mathcal{D}_2$). Indiquons simplement qu'une

des différences dans le traitement des cas $p \mid t$ et $p \nmid t$ réside dans la valeur du nombre $\Gamma(p,t)$ de solutions $(a,b,c,d) \in (\mathbb{Z}/p\mathbb{Z})^4$ à l'équation

$$\Delta(a,b,c,d) \equiv t \pmod{p}.$$

On trouve

$$\Gamma(p,t) = \begin{cases} p(p^2+p-1) & \text{pour } p \mid t, \\ p^3 - p & \text{pour } p \nmid t. \end{cases}$$

(voir par exemple [24, Lemma 1], [17, Lemme 2.1]).

La preuve du théorème 1.3 sera présentée au §3, elle comportera d'abord un calcul de facteurs locaux et empruntera certaines démarches de [1, 3]. On pourrait gagner des puissances de $\log X$, dans le terme reste de (10), par une itération de la formule d'inclusion-exclusion (35), comme il a été fait pour l'obtention de (9) qui devait être suffisamment précise pour être incorporée dans un crible. Notons que l'accent est mis sur l'uniformité en q ; pour q petit devant X, en particulier $q = O(1)$, les méthodes de [6] permettent de gagner une puissance de X.

Un dernier type de résultat aborde l'étude de $N(X,Y;q)$, non pas par une formule asymptotique du type (10), mais par des majorations ou minorations individuelles, le gain étant une plus grande uniformité sur le paramètre q. En quelque sorte, nous démontrerons des résultats de type Brun-Titchmarsh, non pas pour la suite des nombres premiers, mais pour la suite $\mathcal{D}_3$.

Nous montrerons d'abord la majoration

Théorème 1.4. *Il existe C_0, tel que, pour $X \geqslant 2$ et tout entier q sans facteur carré vérifiant $1 \leqslant q \leqslant X^{1/4}$, on ait la majoration*

$$N(-X,X;q) \leqslant C_0 \cdot \frac{X}{q} \cdot \prod_{p \mid q} \left(3 + \frac{1}{p}\right).$$

Ce théorème ne donne pas pour $N(-X,X;q)$ le bon ordre asymptotique espéré à savoir $\asymp X/q$ pour toute suite d'entiers q qui, en restant inférieurs à $X^{1/4}$, voient leur nombre de facteurs premiers tendre vers l'infini avec X. Le théorème suivant a une zone d'uniformité plus large mais, par souci de concision, on se restreint aux nombres premiers.

Théorème 1.5. *Il existe C_0, tel qu'on ait la majoration*

$$N(-X,X;p) \leqslant C_0 \cdot \frac{X}{p},$$

pour tout $X \geqslant 2$ et tout $p \leqslant X^{3/11}(\log X)^{-6/11}$.

La preuve du théorème 1.4, donnée au §4, repose sur la constatation que le décompte précédent se fait sur un certain domaine $\mathcal{F}^{\pm}(X)$ de $\mathbb{R}^4$ essentiellement constitué de segments de longueur $\gg X^{1/4}$ parallèles à l'un des axes de coordonnées. L'amélioration apportée au théorème 1.5 passe par une étude plus soigneuse du domaine $\mathcal{F}^{\pm}(X)$ et par la théorie des sommes d'exponentielles.

Pour la minoration, nous montrerons

Théorème 1.6. *Il existe deux constantes absolues c_1 et c_2 strictement positives, telles que, pour tout $X \geqslant 1$ et tout entier $q \geqslant 1$ vérifiant $v_2(q) \leqslant 3$ et $v_p(q) \leqslant 1$ pour tout $p \geqslant 3$, on ait les minorations*

$$N(0,X;q), N(-X,0;q) \geqslant c_1 \frac{\varphi(q)}{q} \cdot \frac{X}{q} - c_2 \left(\frac{X}{q}\right)^{1/2} \prod_{p|q} \left(1+p^{-1/2}\right). \tag{12}$$

(Pour p premier et q entier, $v_p(q)$ désigne la valuation p-adique de q). En particulier, il existe X_0 et $c_3 > 0$ tels que, uniformément pour q comme ci-dessus, vérifiant de plus l'inégalité $q \leqslant X \exp\bigl(-\sqrt{\log X}\bigr)$, on ait la minoration

$$N(0,X;q), N(-X,0;q) \geqslant c_3 \frac{\varphi(q)}{q} \cdot \frac{X}{q}, \tag{13}$$

pour $X > X_0$.

Remarquons que la minoration (13) a un domaine d'uniformité quasiment optimal sur q, pourvu qu'on se restreigne aux modules q sans facteur carré. Toutefois, ni (12), ni (13) ne donnent le bon ordre de grandeur asymptotique espéré pour $N(0,X;q)$ et $N(-X,0;q)$ pour une suite de modules q tels que $\liminf_{q\to+\infty} \varphi(q)/q = 0$.

Remerciements. Les auteurs remercient Manjul Bhargava, Jordan Ellenberg, Jürgen Klüners, Gunter Malle, Akshay Venkatesh et Melanie Wood pour de fructueuses discussions autour du présent travail. Le premier auteur est financé par le projet ANR ALGOL (`07-BLAN-0248`).

2. La théorie de Delone-Faddeev et Davenport-Heilbronn

Dans cette partie, nous présentons les outils nécessaires à la preuve du théorème 1.3 et regroupons les apports successifs de [15, 13, 14]. Pour une présentation générale, se reporter à [5].

Rappelons quelques conventions. Un *ordre de rang n* est un anneau intègre, libre de rang n comme $\mathbb{Z}$-module ; son *discriminant* est le discriminant d'une $\mathbb{Z}$-base quelconque. Un ordre de rang 3 est un *ordre cubique*. La forme cubique binaire $F = (a,b,c,d)$ définie par

$$F(x,y) = ax^3 + bx^2y + cxy^2 + dy^3,$$

à coefficients entiers est dite *irréductible* si elle l'est dans $\mathbb{Q}[x,y]$. Elle est dite *primitive* si $(a,b,c,d) = 1$. Le discriminant de F est par définition

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

Le groupe $\mathrm{GL}_2(\mathbb{Z})$ agit sur l'ensemble des formes cubiques par $(g\cdot F) = F((x,y)g)$, et cette action conserve le caractère primitif ou irréductible, ainsi que le discriminant. On note $\tilde{\Phi}$ l'ensemble des $\mathrm{GL}_2(\mathbb{Z})$-orbites de formes cubiques binaires entières, irréductible et primitives.

Proposition 2.1 (Delone-Faddeev [15]). *Les classes d'isomorphismes d'ordres cubiques (modulo isomorphismes d'anneau) sont en bijection avec les classes modulo* $\mathrm{GL}_2(\mathbb{Z})$ *de formes cubiques entières, irréductibles. Cette bijection préserve le discriminant.*

Parmi les ordres cubiques, les ordres maximaux sont de première importance puisque compter les corps de discriminant D prescrit revient à compter les ordres maximaux de discriminant D. Le critère de Dedekind [9, §6.1.2] permet de caractériser immédiatement les formes associées à des ordres maximaux (voir [4] ; Bhargava [7] obtient indépendamment une autre démonstration élémentaire). Nous donnons cette caractérisation dans la proposition 2.2.

Cependant, la formulation et la démonstration originale de ce résultat, due à Davenport et Heilbronn [14, Prop. 4], nécessitent l'introduction de certains ensembles de formes cubiques, stables par l'action de $\mathrm{GL}(2,\mathbb{Z})$, qui nous seront utiles dans la suite. Soit

$$\begin{cases} V_2 = \left\{F \in \mathbb{Z}^4 \colon \Delta(F) \not\equiv 0, 4 \pmod{16}\right\} \\ V_p = \left\{F \in \mathbb{Z}^4 \colon \Delta(F) \not\equiv 0 \pmod{p^2}\right\} \quad \text{si } p \geqslant 3. \end{cases} \tag{14}$$

Soit aussi U_p est l'ensemble des F qui vérifient l'une ou l'autre des propriétés (15) et (16) suivantes

$$F \in V_p, \tag{15}$$

$$\begin{cases} F(x,y) \equiv \lambda(\alpha x + \beta y)^3 \pmod{p} \text{ avec } \alpha, \beta \in \mathbb{F}_p,\ \lambda \in \mathbb{F}_p^*, \quad \text{et} \\ F(x,y) \equiv ep \pmod{p^2} \text{ a une solution avec } e \not\equiv 0 \pmod{p}. \end{cases} \tag{16}$$

Signalons que les éventualités (15) et (16) s'excluent mutuellement, que la condition $F \in U_p$ (ou $F \in V_p$) s'exprime par des congruences modulo p^2 sur ses coefficients, y compris pour $p = 2$, et qu'une définition équivalente de U_p est (voir [4])

$$U_p = \left\{F \colon p \nmid F \text{ et il n'existe pas } (a,b,c,d) \in \mathbb{Z}^4, F \sim_{\mathrm{GL}(2,\mathbb{Z})} (a, b, pc, p^2 d)\right\}.$$

On notera $\overline{U_p}$ et $\overline{V_p}$ les projections de U_p et V_p dans $\mathbb{Z}/p^2\mathbb{Z}$. Enfin, on pose

$$U = \bigcap_p U_p, \quad V = \bigcap_p V_p.$$

Notons l'inclusion $V \subset U$ et le fait que tout F appartenant à U est nécessairement primitive.

Proposition 2.2. [14, Prop. 4] *Le bijection de Delone et Faddeev induit une bijection entre classes d'isomorphismes de corps cubiques et l'ensemble* $\tilde{\Phi} \cap U$ *des classes de formes cubiques binaires irréductibles, appartenant à* U.

Par restriction, c'est une bijection entre l'ensemble des classes d'isomorphismes de corps cubiques dont le discriminant est fondamental et l'ensemble $\tilde{\Phi} \cap V$ *des classes, de formes cubiques binaires irréductibles, appartenant à* V.

Ainsi, le décompte de corps cubiques est ramené à celui de classes de formes cubiques. Ce dernier s'effectue grâce à la notion de forme réduite, qui diffère suivant le signe du discriminant.

Pour $F = (a, b, c, d)$ forme cubique de discriminant $\Delta(F)$ positif, nous posons

$$A = b^2 - 3ac, \quad B = bc - 9ad, \quad C = c^2 - 3bd,$$

qui sont les coefficients de la forme quadratique hessienne $Ax^2 + Bxy + Cy^2$ (de discriminant $-3\Delta(F) < 0$) associée à F. Par [11, p. 184], on sait ramener l'étude de $\tilde{\Phi}$ à celle des classes de formes quadratiques définies positives, modulo l'action de $\mathrm{SL}(2, \mathbb{Z})$. Plus précisément, dans chaque classe, modulo $\mathrm{SL}(2, \mathbb{Z})$, de classes de formes cubiques binaires irréductibles, de discriminant positif, il y a au moins deux éléments et au plus six dont les coefficients vérifient les inégalités $a \geqslant 1$ et

$$-A < B \leqslant A < C \quad \text{ou} \quad 0 \leqslant B \leqslant A = C \tag{17}$$

En fait, dans chaque classe il y a exactement deux formes vérifiant (17), à moins que $A = C$ et $B = 0$ (auquel cas, il y en a entre deux et quatre) ou, à moins que $A = B = C$ (auquel cas, il y en a entre deux et six).

Soit, pour $X \geqslant 2$, le volume $\mathcal{F}^+(X)$ défini par

$$\mathcal{F}^+(X) = \left\{F = (a, b, c, d) \in \mathbb{R}^4 \colon a > 0, |B| \leqslant A \leqslant C, 0 < \Delta(F) \leqslant X\right\}.$$

L'ensemble $\mathcal{F}^+(X)$ nous servira de domaine fondamental pour le dénombrement de formes cubiques. D'après [11, Lemma 2, 3], on a

$$\operatorname{card}\left\{F \in \mathcal{F}^+(X) \cap \mathbb{Z}^4 \colon |B| = A \text{ ou } A = C\right\} = O(X^{3/4} \log X), \tag{18}$$

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

$$\operatorname{card}\left\{F \in \mathcal{F}^+(X) \cap \mathbb{Z}^4 \colon F \text{ réductible}\right\} = O\big(X^{\frac{3}{4}+\varepsilon}\big). \tag{19}$$

Puis, pour étudier les orbites sous l'action de $\mathrm{GL}(2, \mathbb{Z})$, au lieu de l'action de $\mathrm{SL}(2, \mathbb{Z})$, il suffit, de considérer, sur l'ensemble des formes cubiques, l'effet de la matrice $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Ceci revient à identifier, dans $\mathcal{F}^+(X)$, les points (a, b, c, d) et $(a, -b, c, -d)$. Ces points sont distincts sauf si $b = 0$ et $d = 0$, ce qui implique que la forme (a, b, c, d) est dans ce cas réductible. Le nombre de telles formes est couvert par (19). En regroupant la proposition 2.2, la discussion précédente et les relations (18) et (19), on parvient à

Proposition 2.3. *Pour tout $\varepsilon > 0$, tout entier $q \geqslant 1$ et tout $X \geqslant 2$, on a l'égalité*

$$N(0, X; q) = \frac{1}{2} \cdot \operatorname{card}\left\{F \in \mathcal{F}^+(X) \cap U \colon q \mid \Delta(F)\right\} + O_\varepsilon(X^{\frac{3}{4}+\varepsilon})$$

Le cas des discriminants négatifs est quelque peu différent. Dans [12], l'auteur suit la démarche de Mathews et Berwick [22] pour classifier les formes cubiques de discriminant négatif (voir aussi [1, Théorème 1.5]). L'idée est de factoriser, de façon unique, F sous la forme $F(x, y) = (x - \theta y)(Px^2 + Qxy + Ry^2)$ (avec θ irrationnel) et d'étudier la réduction de la forme quadratique définie $Px^2 + Qxy + Cy^2$. La conclusion est la suivante :

Soit le système d'inégalités

$$\begin{cases} d^2 - a^2 + ac - bd \geqslant 0 \\ (a+b)(a+b+c) - ad \geqslant 0 \\ (a-b)(a-b+c) + ad \geqslant 0 \\ a \geqslant 1 \end{cases} \tag{20}$$

Dans chaque classe modulo $\mathrm{SL}(2,\mathbb{Z})$ de formes cubiques irréductibles de discriminant négatif, il y a une forme et une seule dont les coefficients vérifient (20). Pour $X > 0$, le domaine fondamental sous l'action de $\mathrm{SL}(2,\mathbb{Z})$ est maintenant

$$\mathcal{F}^-(X) = \left\{F \in \mathbb{R}^4 \colon F \text{ vérifie (20)}, -X \leqslant \Delta(F) < 0\right\}.$$

Dans l'ensemble $\mathcal{F}^-(X) \cap \mathbb{Z}^4$, le nombre de formes réductibles est aussi en $O(X^{\frac{3}{4}+\varepsilon})$ ([12, Lemma 2]). De façon identique à la Proposition 2.3, nous avons maintenant

Proposition 2.4. *Pour tout $\varepsilon > 0$, tout entier $q \geqslant 1$ et tout $X \geqslant 1$, on a l'égalité*

$$N(-X, 0; q) = \frac{1}{2} \cdot \operatorname{card}\left\{F \in \mathcal{F}^-(X) \cap U \colon q \mid \Delta(F)\right\} + O_\varepsilon(X^{\frac{3}{4}+\varepsilon}).$$

3. Preuve du théorème 1.3

3.1. **Un abord heuristique.** Les ensembles U_p et V_p s'interprètent aussi comme des ensembles de formes cubiques modulo p^2. Leurs cardinaux sont calculés dans [14].

Lemme 3.1. *On a, pour tout p, les égalités*

$$\operatorname{card} \overline{U_p} = p^3(p^2-1)(p^3-1), \quad \operatorname{card} \overline{V_p} = p^4(p^2-1)^2,$$

soit

$$\operatorname{card}(\overline{U_p} \setminus \overline{V_p}) = p^3(p^2-1)(p-1) \quad \textit{et} \quad p^8 - \operatorname{card} \overline{V_p} = p^4(2p^2-1)$$

Preuve. Dans [14, lemmas 4 & 5], on calcule ces deux cardinaux, divisés par $p^4(p^4-1)$, ce qui correspond au cardinal des formes $F = (a,b,c,d) \bmod p^2$ tels que $p \nmid (a,b,c,d)$. Les résultats sont respectivement $(p^3-1)p^{-1}(p^2+1)^{-1}$ et $(p^2-1)(p^2+1)^{-1}$. □

On interprète maintenant de façon heuristique la formule (2) : par la proposition 2.3, en admettant l'indépendance des conditions locales U_p, on a

$$N(0, X) \sim \frac{1}{2} \cdot \prod_p \frac{\operatorname{card} \overline{U_p}}{p^8} \cdot \operatorname{Vol} \mathcal{F}^+(X). \tag{21}$$

Le membre de droite de (21) contient le produit de probabilités locales en p (qu'une forme modulo p^2 soit dans $\overline{U_p}$) par le volume du domaine fondamental $\mathcal{F}^+(X)$, qu'on admet être équivalent au nombre de points entiers de $\mathcal{F}^+(X)$. D'après [11, §7], on a, la relation

$$\operatorname{Vol} \mathcal{F}^+(X) = \frac{\pi^2}{36} \cdot X. \tag{22}$$

(Signalons que la constante K de [11, §7] doit être multipliée par 3, à cause du *Corrigendum.*) Le lemme 3.1 permet de calculer le produit eulérien de (21). En combinant avec (22), on a donc une preuve heuristique de (2), pour les corps cubiques de discriminants positifs.

La formule heuristique

$$N(-X,0) \sim \frac{1}{2} \cdot \prod_p \frac{\operatorname{card} \overline{U_p}}{p^8} \cdot \operatorname{Vol} \mathcal{F}^-(X)$$

conduirait aussi à la formule (2) pour les discriminants négatifs, en recourant maintenant à [12, lemmas 3, 4] :

$$\operatorname{Vol} \mathcal{F}^-(X) = \frac{\pi^2}{12} \cdot X. \tag{23}$$

Le même type d'heuristique permet d'appréhender les quantités étudiées en (6), en modifiant, comme il se doit, la proposition 2.3 pour ne compter que les corps cubiques dont le discriminant est un discriminant fondamental (voir la deuxième partie de la proposition 2.2). Heuristiquement, on a

$$\operatorname{card} \left\{ \tilde{K} \in \tilde{\mathcal{K}} \colon \operatorname{disc} \tilde{K} = \Delta_2, 0 < \pm \Delta_2 < X \right\} \sim \frac{1}{2} \cdot \prod_p \frac{\operatorname{card} \overline{V_p}}{p^8} \cdot \operatorname{Vol} \mathcal{F}^{\pm}(X),$$

La deuxième partie du lemme 3.1 et les formules (22) et (23) fournissent alors les formules (6).

Passons maintenant à une approche heuristique des formules (9) et (10) où est insérée la condition de divisibilité par q. Soit $\overline{U_p'}$ (resp. $\overline{V_p'}$) le sous-ensemble de $\overline{U_p}$ (resp. $\overline{V_p}$), constitué des formes F modulo p^2, telles que

$$\Delta(F) \equiv 0 \pmod{p}.$$

Le même genre de raisonnement permet de retrouver les formules (9) :

$$\begin{aligned} \operatorname{card} \{K \in \mathcal{K} \colon \operatorname{disc} K = \Delta_2, 0 < \pm \Delta_2 < X, \Delta_2 \equiv 0 \pmod{q}\} \\ \sim \frac{1}{2} \cdot \prod_{p \mid q} \frac{\operatorname{card} \overline{V_p'}}{p^8} \prod_{p \nmid q} \frac{\operatorname{card} \overline{V_p}}{p^8} \cdot \operatorname{Vol} \mathcal{F}^+(X) \end{aligned} \tag{24}$$

et de deviner le terme principal de (10) : on devrait avoir, pour $X \to \infty$, la relation

$$N(0, X; q) \sim \frac{1}{2} \cdot \prod_{p \mid q} \frac{\operatorname{card} \overline{U_p'}}{p^8} \prod_{p \nmid q} \frac{\operatorname{card} \overline{U_p}}{p^8} \cdot \operatorname{Vol} \mathcal{F}^+(X), \tag{25}$$

et une formule analogue pour $N(-X, 0; q)$. Le lemme suivant donne les cardinaux de $\overline{U_p'}$ et $\overline{V_p'}$ modulo p^2 :

Lemme 3.2. *Pour tout nombre premier p, on a les égalités*

$$\operatorname{card} \overline{U_p'} = p^3(p^2-1)^2, \tag{26}$$

et

$$\operatorname{card}\overline{V_p'} = p^4(p+1)(p-1)^2. \tag{27}$$

Preuve. On part de l'égalité

$$\operatorname{card}\overline{V_p'} = \operatorname{card}\overline{V_p} - \operatorname{card}\left\{F \in \overline{V_p}\colon \Delta(F) \equiv 0 \pmod p\right\}. \tag{28}$$

On utilise maintenant le fait que $\Delta(F) \not\equiv 0$ modulo p, équivaut au fait que le polynôme $F(x,y)$, modulo p, est soit irréductible de degré 3, soit produit d'un polynôme de degré 1 et d'un polynôme irréductible de degré 2, soit produit de trois polynômes distincts de degré 1. Chacun de ces trois cardinaux est calculé dans [14, lemma 1], on a donc l'égalité

$$\begin{aligned}
&\operatorname{card}\left\{F \in \overline{V_p}\colon \Delta(F) \equiv 0 \pmod p\right\}\\
&\quad = (p^8 - p^4)\left(\frac{p(p-1)}{3(p^2+1)} + \frac{p(p-1)}{2(p^2+1)} + \frac{p(p-1)}{6(p^2+1)}\right)\\
&\quad = p^5(p+1)(p-1)^2.
\end{aligned}$$

Il suffit de reporter cette égalité dans (28) et d'utiliser le lemme 3.1, pour compléter la preuve de (27).

Pour prouver (26), on écrit

$$\operatorname{card}\overline{U_p'} = \operatorname{card}\overline{V_p'} + \operatorname{card}\left\{F \in \overline{U_p}\colon F \text{ vérifie (16)}\right\}. \tag{29}$$

Modulo p, il y a $(p-1)(p+1)$ formes non nulles de la forme $F \equiv \lambda(\alpha x + \beta y)^3$. La forme $\lambda(\alpha x + \beta y)^3$ se remonte, modulo p^2 en

$$F(x,y) = \lambda(\alpha x + \beta y)^3 + p(a'x^3 + b'x^2y + c'xy^2 + d'y^3)$$

où α, β et λ sont maintenant fixés modulo p^2, et a', b', c' et d' sont définis modulo p. La forme F ci-dessus appartient à U_p si et seulement si on a $F(-\beta,\alpha) \not\equiv 0$ modulo p^2, ce qui équivaut à

$$-a'\beta^3 + b'\alpha\beta^2 - c'\alpha^2\beta + d'\alpha^3 \not\equiv 0 \pmod p. \tag{30}$$

Ayant fixé $(\alpha,\beta) \neq (0,0)$, il y a $p^4 - p^3$ quadruplets (a',b',c',d') modulo p tels que (30) soit vérifié. Grâce à la discussion précédente, on voit que le dernier terme à droite de (29) vaut $p^3(p+1)(p-1)^2$. Il suffit de regrouper cette égalité, (27) et (29) pour conclure la preuve de (26). □

Reportant (26) et (27) dans (24) et (25), on retrouve les termes principaux de (9) et (10) Ceci termine la preuve heuristique des formules (2), (6) et du théorème 1.3. Nous passons maintenant à une preuve complète de ce théorème.

3.2. **Découpage de $\mathcal{F}(X)$.** Commençons par rendre rigoureuse notre heuristique $\operatorname{card}\mathcal{F}^{\pm}(X) \approx \operatorname{Vol}\mathcal{F}^{\pm}(X)$. Comme dans [11], [1] et [3], on sépare le domaine fondamental $\mathcal{F}^{\pm}(X)$ en deux parties : soit ρ un paramètre réel vérifiant $0 < \rho < \frac{1}{12}$, on pose

$$\mathcal{F}^{\pm}(X) = \mathcal{F}^{\pm}_{\text{pointe}}(X) \cup \mathcal{F}^{\pm}_{\text{corps}}(X),$$

la pointe $\mathcal{F}^{\pm}_{\text{pointe}}(X)$ contenant les $F = (a,b,c,d) \in \mathcal{F}^{\pm}(X)$ tels que $0 < a < X^{\frac{1}{4}-3\rho}$, et le corps $\mathcal{F}^{\pm}_{\text{corps}}(X)$, les formes restantes, vérifiant donc $a \geqslant X^{\frac{1}{4}-3\rho}$.

Par [11, lemma 4] et [12, lemma 3], on a

$$\operatorname{card} \mathcal{F}^{\pm}_{\text{pointe}}(X) \cap \mathbb{Z}^4 = O\big(X^{1-\rho}\big). \tag{31}$$

Par [11, lemma 4, lemma 5] et [12, lemma 3, lemma 4], on a

$$\operatorname{card} \mathcal{F}^{\pm}_{\text{corps}}(X) \cap \mathbb{Z}^4 = \operatorname{Vol} \mathcal{F}^{\pm}(X) + O\big(X^{\frac{3}{4}+3\rho} + X^{1-\rho}\big). \tag{32}$$

Pour étudier $\mathcal{F}^{\pm}_{\text{corps}}(X)$ en contrôlant une relation de congruence, on encadre ce volume par deux ensembles d'hypercubes. Cette technique est utilisée dans [1, p. 921–923], et développée dans [3, lemmes 2.6 et 2.7]. On a

Lemme 3.3. *Pour tout $X \geqslant 2$, tout $Q \geqslant 2$, il existe deux familles finies d'indices $\mathcal{I} \subset \mathcal{J}$, des hypercubes disjoints de $\mathbb{R}^4$, $\mathcal{B}_j$ $(j \in \mathcal{J})$, dont les côtés sont parallèles aux axes de coordonnées et de longueur Q, tels que*

$$\bigcup_{i\in\mathcal{I}} \mathcal{B}_i \subset \mathcal{F}^{+}_{\text{corps}}(X) \subset \bigcup_{j\in\mathcal{J}} \mathcal{B}_j$$

et

$$\operatorname{card}\mathcal{J} - \operatorname{card}\mathcal{I} \ll Q^{-3} X^{\frac{3}{4}+3\rho} \log X + Q^{-1} X^{\frac{1}{4}+3\rho} + 1. \tag{33}$$

Un énoncé analogue est vrai pour $\mathcal{F}^{-}_{\text{corps}}$, pour une autre famille d'hypercubes.

3.3. **Début de la preuve complète du théorème 1.3.** La démarche suivie est très proche de celle et [1, §7] et [3, §5.a]. Soient q et r deux entiers premiers entre eux, sans facteur carré. Pour $Y \geqslant 2$ un paramètre, P_Y est le produit des nombres premiers $\leqslant Y$. Pour R entier premier à r et multiple de q, on désigne par $f(R,q,r,X)$ le nombre de classes de formes cubiques F de discriminant compris entre 0 et X, telles que

- la forme F est irréductible
- q divise $\Delta(F)$,
- $F \in \cap_{p|R} U_p$,
- pour tout premier $p \mid r$, on a $F \notin U_p$.

(Noter que cette définition de la fonction f correspond à celle de [1] et de [3], à la différence près que V_p est remplacé par U_p.) On a donc l'égalité

$$N(0,X;q) = f(P_\infty, q, 1, X). \tag{34}$$

Par le principe d'inclusion-exclusion, on a pour tous paramètres $Y < Z$, l'égalité

$$\begin{aligned} f(P_\infty, q, 1, X) &= f\big(q\frac{P_Y}{(q,P_Y)}, q, 1, X\big) + O\Big(\sum_{\substack{Y<p\leqslant Z\\(p,q)=1}} f\big(q\frac{P_Y}{(q,P_Y)}, q, p, X\big)\Big) \\ &\quad + O\Big(\sum_{\substack{p>Z\\(p,q)=1}} f\big(q\frac{P_Y}{(q,P_Y)}, q, p, X\big)\Big) \\ &= A_1 + O(A_2) + O(A_3), \end{aligned} \tag{35}$$

par définition.

3.4. **Majoration de A_3.** Notre outil principal est

Lemme 3.4 ([3] Prop. 4.1)**.** *Soient q et n deux entiers sans facteurs carrés, premiers entre eux. Alors, pour tout ε positif, le nombre de classes de formes cubiques binaires, primitives ou non, irréductibles de discriminant D compris entre $-X$ et X divisible par n^2q, et appartenant à $\cap_{p|q}V_p$ est*

$$\ll_\varepsilon X^\varepsilon\left(\frac{X}{n^2q} + \frac{X^{15/16}}{n^{15/8}q^{1/12}} + \frac{q^{10/9}X^{1/2}}{n}\right).$$

On améliore ce lemme en

Lemme 3.5. *Soient q et n deux entiers sans facteurs carrés, premiers entre eux. Alors, pour tout ε positif, le nombre de classes de formes cubiques binaires, primitives ou non, irréductibles de discriminant D compris entre $-X$ et X divisible par n^2q est*

$$\ll_\varepsilon (qX)^\varepsilon\left(\frac{X}{n^2q} + \frac{X^{15/16}}{n^{15/8}q^{1/12}} + \frac{q^{10/9}X^{1/2}}{n}\right).$$

Preuve. On part de deux constatations : d'abord que l'ensemble des formes cubiques F est la réunion disjointe sur l'ensemble des décompositions $q = q_1q_2$ des ensembles de formes cubiques F telles que

- $F \in V_p$ pour tout $p \mid q_1$,
- $F \notin V_p$ pour tout $p \mid q_2$.

La deuxième remarque est que la condition $F \notin V_p$ pour tout $p \mid q_2$ implique $q_2^2 \mid \Delta(F)$.

On applique le lemme 3.4 avec n et q valant respectivement nq_2 et q_1. Ainsi le cardinal étudié au lemme 3.5 est

$$\ll_\varepsilon X^\varepsilon \sum_{q_1q_2=q}\left(\frac{X}{n^2q_2^2q_1} + \frac{X^{15/16}}{n^{15/8}q_2^{15/8}q_1^{1/12}} + \frac{q_1^{10/9}X^{1/2}}{nq_2}\right).$$

Dans la somme précédente, le terme est maximal pour $q_1 = q, q_2 = 1$. En sommant sur les diviseurs de q on termine la preuve du lemme. □

Le lemme 3.5 permet de majorer A_3 ; en effet, puisque $F \notin U_p$ implique $p^2 \mid \Delta(F)$, on a, pour tout $X \geqslant 2$, les relations

$$\begin{aligned} A_3 &\leqslant \sum_{\substack{p>Z \\ (p,q)=1}} f(q,q,p,X) \\ &\ll_\varepsilon (qX)^\varepsilon \sum_{Z<p\leqslant X} \left(\frac{X}{p^2 q} + \frac{X^{15/16}}{p^{15/8} q^{1/12}} + \frac{q^{10/9} X^{1/2}}{p} \right) \ll_\varepsilon \frac{1}{\log X} \cdot \frac{X}{q} \end{aligned} \tag{36}$$

avec le choix

$$Z = X^{2\varepsilon},$$

et la contrainte

$$q < X^{3/44}.$$

3.5. **Une formule pour la fonction f.** Nous inspirant toujours de [1, 3], nous montrerons la

Proposition 3.6. *Soient q, r et R trois entiers sans facteur carré, tels que $q \mid R$ et $(R, r) = 1$. Alors pour tout ρ vérifiant $0 < \rho < 1/12$, tout $X \geqslant 2$, on a l'égalité*

$$\begin{aligned} f(R,q,r,X) = \frac{\pi^2}{72} \cdot \nu(R,q,r) \cdot X + O(X^{1-\rho}) \\ + O\left(\nu(R,q,r) \big(r^2 R^2 X^{\frac{3}{4}+3\rho} \log X + r^6 R^6 X^{\frac{1}{4}+3\rho} + r^8 R^8 \big) \right), \end{aligned} \tag{37}$$

avec

$$\nu(R,q,r) = \prod_{p\mid q} \frac{1}{p} \left(1 - \frac{1}{p^2}\right)^2 \prod_{p \mid R q^{-1}} \left(1 - \frac{1}{p^2}\right) \left(1 - \frac{1}{p^3}\right) \prod_{p \mid r} \frac{1}{p^2} \left(1 + \frac{1}{p} - \frac{1}{p^3}\right).$$

Nous appliquerons cette proposition pour traiter les termes A_1 et A_2 de (35), avec R/q et r très petits par rapport à X. Pour simplifier l'exposé, nous n'utilisons pas la théorie des sommes d'exponentielles, compliquée par l'absence de transcription directe de la définition de U_p. Ceci explique le moins bon exposant de répartition obtenu par rapport à [3, Théorème 1] : 1/20 au lieu de 3/44.

Preuve. Notre point de départ est une généralisation de la proposition 2.3 : pour tout $\varepsilon > 0$, q, r et R comme ci-dessus, on a l'égalité

$$\begin{aligned} f(R,q,r,X) = \frac{1}{2} \cdot \operatorname{card} \Big\{ F \in \mathcal{F}^+(X) \colon q \mid \Delta(F), \\ F \in \bigcap_{p\mid R} U_p,\ F \notin \bigcup_{p\mid r} U_p \Big\} + O(X^{\frac{3}{4}+\varepsilon}). \end{aligned} \tag{38}$$

Comme indiqué au §3.2, on fixe ρ un paramètre réel vérifiant $0 < \rho < \frac{1}{12}$, et on sépare le domaine fondamental

$$\mathcal{F}^+(X) = \mathcal{F}^+_{\text{pointe}}(X) \cup \mathcal{F}^+_{\text{corps}}(X).$$

Appliquons le lemme 3.3 avec $Q = r^2R^2$. À l'intérieur de $\mathcal{B}_j$ ($j \in \mathcal{J}$), on a un système complet de congruences modulo R^2 et r^2. Par le théorème chinois et les lemmes 3.1 et 3.2, on voit que le nombre de F de $\mathcal{B}_j$ vérifiant les conditions de sommation à droite de (38) vaut

$$\prod_{p|q} \operatorname{card} \overline{U'_p} \prod_{p|Rq^{-1}} \operatorname{card} \overline{U_p} \prod_{p|r} (p^8 - \operatorname{card} \overline{U_p}) \\ = r^8R^8\nu(R,q,r) = \nu(R,q,r) \cdot \operatorname{card}\big(\mathcal{B}_j \cap \mathbb{Z}^4\big).$$

Sommant sur $i \in \mathcal{I}$ et $j \in \mathcal{J}$, on obtient, par (38) et (31), l'encadrement

$$\frac{\nu(R,q,r)}{2} \sum_{i\in\mathcal{I}} \operatorname{card}\big(\mathcal{B}_i \cap \mathbb{Z}^4\big) \leqslant f(R,q,r,X) + O(X^{1-\rho}) \\ \leqslant \frac{\nu(R,q,r)}{2} \sum_{j\in\mathcal{J}} \operatorname{card}\big(\mathcal{B}_j \cap \mathbb{Z}^4\big),$$

puis par (33), on a

$$f(R,q,r,X) = \frac{\nu(R,q,r)}{2}\Big(\operatorname{card}\big(\mathcal{F}^+_{\mathrm{corps}}(X) \cap \mathbb{Z}^4\big) \\ + O\big(r^2R^2X^{\frac{3}{4}+3\rho}\log X + r^6R^6X^{\frac{1}{4}+3\rho} + r^8R^8\big)\Big) + O(X^{1-\rho}). \tag{39}$$

Par (32), on termine la preuve de la proposition. □

3.6. **Fin de la preuve du théorème 1.3.** Avec les notations de (35), on choisit

$$Y = \frac{\log X}{\log\log X},$$

d'où l'inégalité

$$P_Y \ll \exp\left(\frac{10}{9} \cdot \frac{\log X}{\log\log X}\right).$$

Partant de l'égalité

$$\prod_{\substack{p\leqslant Y\\ p\nmid q}} \left(1 - \frac{1}{p^2}\right)\left(1 - \frac{1}{p^3}\right) = \zeta^{-1}(2)\zeta^{-1}(3) \prod_{p|q} \left(1 - \frac{1}{p^2}\right)^{-1}\left(1 - \frac{1}{p^3}\right)^{-1} \\ \times \left(1 + O\left(\frac{1}{Y\log Y}\right)\right),$$

valable pour tout $Y \geqslant 2$, on voit que la proposition 3.6 implique l'égalité

$$A_1 = \frac{1}{12\zeta(3)} \prod_{p|q} \left(\frac{p^2+p}{p^2+p+1}\right) \cdot \frac{X}{q}\left(1 + O\left(\frac{1}{Y\log Y}\right)\right) \\ + O(X^{1-\rho}) + O\Big(\frac{X}{q} \cdot \exp\left(\frac{9\log X}{\log\log X}\right)\Big(\frac{q^2X^{3\rho}}{X^{1/4}} + \frac{q^6X^{3\rho}}{X^{3/4}} + \frac{q^8}{X}\Big)\Big). \tag{40}$$

Pour majorer A_2, on écrit d'abord

$$A_2 \leqslant \sum_{\substack{Y<p\leqslant Z\\(p,q)=1}} f(q,q,p,X),$$

puis la proposition 3.6 entraîne l'inégalité

$$\begin{aligned} A_2 &\ll \sum_{Y<p\leqslant Z}\left(\frac{X}{qp^2}+X^{1-\rho}+\frac{1}{qp^2}\left(p^2q^2X^{\frac{3}{4}+3\rho}\log X+p^6q^6X^{\frac{1}{4}+3\rho}+p^8q^8\right)\right)\\ &\ll_\varepsilon \frac{X}{q}\Big(\frac{1}{\log X}+\frac{q^2X^{3\rho+2\varepsilon}}{X^{1/4}}+\frac{q^6X^{3\rho+10\varepsilon}}{X^{3/4}}+\frac{q^8X^{14\varepsilon}}{X}\Big)+X^{1-\rho+2\varepsilon}. \end{aligned} \tag{41}$$

En regroupant (34), (35), (36), (40) et (41), on a, pour $q\leqslant X^{3/44}$ et $0<\rho<1/12$ l'égalité

$$\begin{aligned} N(0,X;q) &= \frac{1}{12\zeta(3)}\prod_{p\mid q}\Big(\frac{p^2+p}{p^2+p+1}\Big)\cdot\frac{X}{q}\\ &\quad+O_\varepsilon\Big(\frac{X}{q}\Big(\frac{1}{\log X}+\frac{q^2X^{3\rho+2\varepsilon}}{X^{1/4}}+\frac{q^6X^{3\rho+10\varepsilon}}{X^{3/4}}+\frac{q^8X^{14\varepsilon}}{X}\Big)+X^{1-\rho+2\varepsilon}\Big). \end{aligned} \tag{42}$$

Choisissons le paramètre ρ tel que $0<\rho<3/44$ et

$$X^\rho = qX^{3\varepsilon}.$$

On voit alors que, pour $q\leqslant X^{\frac{1}{20}-3\varepsilon}$, le terme d'erreur de (42) est en $O_\varepsilon\big(\frac{X}{q\log X}\big)$. On a donc la preuve de la première partie du théorème 1.3. L'étude est analogue pour les discriminants cubiques négatifs, c'est-à-dire pour la quantité $N(-X,0;q)$. La proposition 2.4 remplace la proposition 2.3 et on utilise de nouveau le découpage du §3.2. En conclusion, la deuxième égalité de (10) se démontre comme la première, la seule différence étant que l'égalité (23) remplace (22). Ceci termine la preuve du théorème 1.3. □

4. La majoration. Preuve des théorèmes 1.4 et 1.5

4.1. **Préliminaires.** Nous cherchons à majorer la quantité $N(-X,X;q)$, ce qui nous autorise à appauvrir notablement la théorie de Davenport-Heilbronn. En particulier, au lieu de travailler avec le domaine $\mathcal{F}^\pm(X)$, nous travaillerons avec un domaine noté $\mathcal{M}(X)$, contenant $\mathcal{F}^+(X)$ et $\mathcal{F}^-(X)$, où chaque $\tilde\Phi$ a au moins un représentant.

Posons, pour $X \geqslant 2$,

$$\begin{aligned}\mathcal{M}(X) = \Big\{(a,b,c,d) \in \mathbb{R}^4 : \\ 0 < a \leqslant 2X^{1/4}, |b| \leqslant 3X^{1/4}, |ad| \leqslant 2X^{1/2}, \\ |bc| \leqslant 8X^{1/2}, \left|ac^3\right| \leqslant 12X, \left|b^3 d\right| \leqslant 12X, \\ c^2 \left|bc - 9ad\right| \leqslant 16X\Big\}.\end{aligned} \tag{43}$$

On a

Lemme 4.1 ([11] lemma 1,2)**.** *Pour $X \geqslant 2$, on a les inclusions*

$$\mathcal{F}^{\pm}(X) \subset \mathcal{M}(X),$$

et la relation

$$\operatorname{Vol} \mathcal{M}(X) = O(X).$$

D'après la proposition 2.2, et la discussion qui la suit, on a l'inégalité

$$N(0, X; q) \leqslant \operatorname{card}\left\{F \in \mathcal{F}^{+}(X) \cap \mathbb{Z}^4 : q \mid \Delta(F)\right\}, \tag{44}$$

puisqu'on compte à droite de (44) les formes irréductibles ou non, primitives ou non, et que le nombre d'orbites sous $\mathrm{SL}(2,\mathbb{Z})$ est supérieur au nombre d'orbites sous $\mathrm{GL}(2,\mathbb{Z})$. Par le lemme 4.1, (44), et une discussion analogue pour les corps de discriminants négatifs, on obtient donc

Lemme 4.2. *Pour tout $X \geqslant 2$, on a*

$$N(-X, X; q) \leqslant \operatorname{card}\left\{F \in \mathcal{M}(X) \cap \mathbb{Z}^4 : q \mid \Delta(F)\right\}.$$

Ainsi le problème du décompte grossier de corps cubiques est ramené à un décompte de points entiers à l'intérieur d'un certain volume de $\mathbb{R}^4$. Par de simples considérations géométriques et des manipulations d'inégalités, on montre maintenant que la section du volume $\mathcal{M}(X)$ par une droite parallèle à l'axe des c est soit vide soit constituée de segments de longueur suffisamment longue. Plus précisément, on a

Lemme 4.3. *Il existe une constante absolue c_4 telle que, pour tout $X \geqslant 2$, pour tout $(a,b,d) \in \mathbb{Z}^3$, l'ensemble des $c \in \mathbb{R}$ tels que $(a,b,c,d) \in \mathcal{M}(X)$ est, soit vide, soit réunion d'au plus c_4 segments, de longueur totale $\geqslant X^{1/4}$.*

Preuve. L'ensemble des c en question est l'intersection $\mathcal{I}_1 \cap \mathcal{I}_2 \cap \mathcal{E}$ des intervalles $\mathcal{I}_1 = [-8X^{1/2}/|b|, 8X^{1/2}/|b|]$ (on omet cette condition si $b = 0$), $\mathcal{I}_2 = [-(12X/a)^{1/3}, (12X/a)^{1/3}]$ et de l'ensemble semi-algébrique

$$\mathcal{E} = \left\{c : c^4(bc - 9ad)^2 \leqslant (16X)^2\right\}.$$

On constate que $\mathcal{I}_1$ et $\mathcal{I}_2$ sont des intervalles centrés en 0, de longueur $\geqslant X^{1/4}$. Il en est donc de même de $\mathcal{I}_1 \cap \mathcal{I}_2$. Enfin, on a l'implication $|c| \leqslant \frac{1}{2}X^{1/4} \Rightarrow c \in \mathcal{E}$, puisqu'on a la suite d'inégalités

$$c^4(bc - 9ad)^2 \leqslant \frac{X}{16}\left(8X^{1/2} + 18X^{1/2}\right)^2 < (16X)^2.$$

Ainsi $\mathcal{E}$ est une réunion d'un nombre borné d'intervalles, dont l'un contient l'intervalle $[-\frac{1}{2}X^{1/4}, \frac{1}{2}X^{1/4}]$. Ainsi $\mathcal{I}_1 \cap \mathcal{I}_2 \cap \mathcal{E}$ vérifie bien les propriétés voulues. □

On utilise un résultat trivial de majoration du nombre de solutions à une congruence polynomiale sur un ensemble qui est essentiellement un segment :

Lemme 4.4. *Soient m et λ des constantes vérifiant $m \geqslant 1$ et $\lambda > 0$, r un entier sans facteur carré, $\mathcal{I}$ un ensemble borné de réels, qui est réunion d'au plus m intervalles et qui est de longueur totale $\ell(\mathcal{I}) \geqslant \lambda r$. Soit P un polynôme de $\mathbb{Z}[X]$ de degré $d \geqslant 1$, tel que, pour tout $p \mid r$, le polynôme P modulo p soit non constant. Il existe alors une constante $C = C(d, m, \lambda)$, telle qu'on ait l'inégalité*

$$\operatorname{card}\{n \in \mathbb{Z} \colon n \in \mathcal{I}, r \mid P(n)\} \leqslant C \cdot \frac{d^{\omega(r)}}{r} \cdot \operatorname{card}(\mathcal{I} \cap \mathbb{Z}).$$

Preuve. Cette relation est triviale si $\mathcal{I}$ ne contient aucun entier. Supposons maintenant que $\mathcal{I}$ soit réunion de m_1 ($\leqslant m$) intervalles disjoints notés $\mathcal{J}_j$ ($1 \leqslant j \leqslant m_1$). On suppose que seuls les k premiers $\mathcal{J}_j$ contiennent au moins un entier, avec $k \geqslant 1$. Ainsi les $m_1 - k$ derniers sont de longueur inférieure ou égale à 1. En découpant chaque $\mathcal{J}_j$ en intervalles de longueur r, on a trivialement, pour $1 \leqslant j \leqslant m_1$, les inégalités

$$\operatorname{card}\{n \in \mathcal{J}_j \colon r \mid P(n)\} \leqslant d^{\omega(r)} \left(\left\lfloor \frac{\operatorname{card}(\mathcal{J}_j \cap \mathbb{Z})}{r} \right\rfloor + 1 \right) \leqslant \frac{d^{\omega(r)}}{r} \operatorname{card}(\mathcal{J}_j \cap \mathbb{Z}) + d^{\omega(r)}.$$

Sommant sur les $j \leqslant m_1$, on obtient

$$\operatorname{card}\{n \in \mathbb{Z} \colon n \in \mathcal{I}, r \mid P(n)\} \leqslant \frac{d^{\omega(r)}}{r} \operatorname{card}(\mathcal{I} \cap \mathbb{Z}) + d^{\omega(r)} m_1. \tag{45}$$

Le dernier terme à droite de (45) vérifie par hypothèse

$$d^{\omega(r)} m_1 \leqslant d^{\omega(r)} m \leqslant \frac{d^{\omega(r)} m}{\lambda r} \ell(\mathcal{I}). \tag{46}$$

On a maintenant, par définition de k, les inégalités

$$\begin{aligned} \ell(\mathcal{I}) &\leqslant \sum_{1 \leqslant j \leqslant k} \ell(\mathcal{J}_j) + m \leqslant 2 \sum_{1 \leqslant j \leqslant k} \operatorname{card}(\mathcal{J}_j \cap \mathbb{Z}) + m \\ &= 2 \operatorname{card}(\mathcal{I} \cap \mathbb{Z}) + m \leqslant (2 + m) \cdot \operatorname{card}(\mathcal{I} \cap \mathbb{Z}). \end{aligned} \tag{47}$$

Il reste à regrouper (45), (46) et (47) pour terminer la preuve du lemme. □

4.2. **Preuve du théorème 1.4.** On considère le polynôme $\Delta(a, b, c, d)$ comme un polynôme en c. Modulo p, il est de degré 3 ou 2, sauf si $p \mid a$ et $p \mid b$. Dans ce dernier cas, Δ est le polynôme nul modulo p. Pour prendre en compte ces cas dégénérés, on écrit l'inégalité du lemme 4.2 sous la forme

$$N(-X, X; q) \leqslant \sum_{s \mid q} A(X, q, s), \tag{48}$$

où

$$A(X,q,s) = \operatorname{card}\Big\{(a,b,c,d) \in \mathcal{M}(X) \cap \mathbb{Z}^4 \colon (a,b,q) = s, qs^{-1} \mid \Delta(a,b,c,d)\Big\}.$$

Pour utiliser les lemmes 4.3 et 4.4, on écrit, en posant $r = qs^{-1}$, que

$$A(X,q,s) = \sum_{(a,b,d)} \operatorname{card}\big\{c \colon (a,b,c,d) \in \mathcal{M}(X) \cap \mathbb{Z}^4, r \mid \Delta(a,b,c,d)\big\}.$$

La somme est faite sur les triplets (a,b,d) vérifiant (43) (en omettant les conditions impliquant c) et la condition $(a,b,q) = s$. D'après le lemme 4.3, on voit que c décrit une réunion d'un nombre borné de segments de longueur totale $\geqslant X^{1/4}$ ($\geqslant q \geqslant r$). Puisque le polynôme Δ, considéré modulo chaque diviseur premier de r n'est pas constant, on a la majoration

$$A(X,q,s) \leqslant C \sum_{(a,b,d)} \frac{3^{\omega(r)}}{r} \operatorname{card}\big\{c \colon (a,b,c,d) \in \mathcal{M}(X) \cap \mathbb{Z}^4\big\},$$

la somme étant maintenant faite sur les (a,b,d) vérifiant (43) tels que s divise a et b. Cette dernière inégalité s'écrit aussi

$$A(X,q,s) \leqslant C\frac{3^{\omega(r)}}{r} \operatorname{card}\big\{(a,b,c,d) \in \mathcal{M}(X) \cap \mathbb{Z}^4 \colon s \mid (a,b)\big\}. \tag{49}$$

Lemme 4.5. *Il existe des constantes absolues c_5, c_6 et X_0, telles qu'on ait la majoration*

$$\operatorname{card}\big\{(a,b,c,d) \in \mathcal{M}(X) \cap \mathbb{Z}^4 \colon s \mid (a,b)\big\} \leqslant c_5\frac{X}{s^2} + c_6\frac{X^{3/4}\log X}{s},$$

pour $X \geqslant X_0$ et $s \leqslant X^{1/4}$.

Preuve. Nous reprenons le calcul de [11, p. 187], qui traite le cas particulier $s = 1$. Lorsque a, b et c sont des entiers fixés, les inégalités définissant $\mathcal{M}(X)$ impliquent que le nombre de valeurs possibles pour d est en

$$O\Big(\min\big\{X^{1/2}a^{-1}, X\,|b|^{-3}, Xa^{-1}c^{-2}\big\}\Big),$$

On somme l'expression précédente sur $c \in \mathbb{Z}$. On voit alors que a et b étant fixés, le nombre de couples (c,d) tels que (a,b,c,d) appartienne à $\mathcal{M}(X)$ est en

$$O\Big(X^{1/2}a^{-1/2}\min\big\{X^{1/4}a^{-1/2}, X^{1/2}\,|b|^{-3/2}\big\}\Big). \tag{50}$$

Il reste à sommer cette expression sur les a et b divisibles par s vérifiant $1 \leqslant a \ll X^{1/4}$, $|b| \ll X^{1/4}$. La contribution du terme $b = 0$ est en $O(X^{3/4}(\log X)s^{-1})$ sous les conditions du lemme 4.5. La sommation de (50) sur les b non nuls, divisibles par s donne un terme en

$$O\Big(X^{1/2}a^{-\frac{1}{2}} \cdot X^{1/4}a^{-\frac{1}{2}} \cdot X^{1/6}a^{1/3} \cdot s^{-1}\Big) = O\Big(X^{11/12}a^{-2/3}s^{-1}\Big).$$

Sommant sur a comme précédemment, on termine la preuve du lemme. □

Reportant la majoration du lemme 4.5 dans (49), on obtient la majoration

$$A(X,q,s) \ll \frac{3^{\omega(q)}X}{q}\cdot\frac{1}{s3^{\omega(s)}} + \frac{X^{3/4}\log X}{q}\cdot 3^{\omega(r)},$$

qui, reportée dans (48) donne la majoration

$$N(-X,X,q) \ll \frac{X}{q}\prod_{p\mid q}\Big(3+\frac{1}{p}\Big) + \frac{X^{3/4}\log X}{q}\cdot 4^{\omega(q)} \ll \frac{X}{q}\prod_{p\mid q}\Big(3+\frac{1}{p}\Big).$$

Ceci termine la preuve du théorème 1.3. □

Remarque 4.6. Le calcul précédent possède une généralisation facile, dont nous aurons besoin aux paragraphes §4.3 et §6.3. Il s'agit d'une majoration du nombre de $(a,b,c,d)\in\mathbb{Z}^4$ de la pointe

$$\Big\{(a,b,c,d)\in\mathcal{M}(X)\colon 0<a<X^{\frac{1}{4}-3\rho}\Big\},$$

tels que $q\mid\Delta(a,b,c,d)$. En restreignant, dans les calculs précédents, la sommation aux a tels que $1\leqslant a\leqslant X^{\frac{1}{4}-3\rho}$, on a la majoration

$$\begin{aligned}\operatorname{card}\Big\{&(a,b,c,d)\in\mathcal{M}(X)\cap\mathbb{Z}^4\colon\\ &1\leqslant a\leqslant X^{\frac{1}{4}-3\rho}, q\mid\Delta(a,b,c,d)\Big\} \ll \frac{X^{1-\rho}}{q}\prod_{p\mid q}\Big(3+\frac{1}{p}\Big),\end{aligned}\tag{51}$$

uniformément pour $0\leqslant\rho\leqslant 1/12$ et q sans facteur carré vérifiant $1\leqslant q\leqslant X^{1/4}$.

4.3. **Preuve du théorème 1.5.** Pour simplifier, nous supposons donc que le module est un nombre premier p. Nous découpons $\mathcal{M}(X)$ comme nous l'avons fait précédemment pour $\mathcal{F}^{\pm}(X)$. Soit ρ un réel, vérifiant $0<\rho<1/12$ et soit

$$\mathcal{M}_{\text{pointe}}(X) = \Big\{(a,b,c,d)\in\mathcal{M}(X)\colon 0<a<X^{\frac{1}{4}-3\rho}\Big\},$$

le complémentaire de cette pointe est alors

$$\mathcal{M}_{\text{corps}}(X) = \mathcal{M}(X)\setminus\mathcal{M}_{\text{pointe}}(X).$$

Le théorème 1.4 nous permet de nous restreindre au cas

$$p>2X^{1/4}.$$

Cette inégalité interdit d'appliquer le lemme 4.4 au polynôme $P(c)=\Delta(a,b,c,d)$. Toutefois l'inégalité $1\leqslant a\leqslant 2X^{1/4}<p$ montre que ce polynôme en la variable c est toujours de degré 3. Ainsi, par une majoration triviale, on a l'inégalité suivante, valable pour tout (a,b,d) vérifiant (43)

$$\begin{aligned}\operatorname{card}\big\{c\colon (a,b,c,d)\in\mathcal{M}_{\text{pointe}}(X)\cap\mathbb{Z}^4, p\mid\Delta(a,b,c,d)\big\}&\\ \leqslant \frac{3}{p}\operatorname{card}\big\{c\colon (a,b,c,d)\in\mathcal{M}_{\text{pointe}}(X)\big\}&+O(1).\end{aligned}$$

En sommant sur (a,b,d) vérifiant (43) et $1 \leqslant a \leqslant X^{\frac{1}{4}-3\rho}$, on a

$$\begin{aligned}(52)\quad &\operatorname{card}\Big\{(a,b,c,d) \in \mathcal{M}_{\text{pointe}}(X) \cap \mathbb{Z}^4 \colon p \mid \Delta(a,b,c,d)\Big\} \\ &\qquad \ll \frac{1}{p}\operatorname{card}\big(\mathcal{M}_{\text{pointe}}(X) \cap \mathbb{Z}^4\big) + \sum_{1\leqslant a\leqslant X^{\frac{1}{4}-3\rho}} \sum_{|b|\ll X^{1/4}} \sum_{|d|\ll \min(X^{1/2}a^{-1}, X|b|^{-3})} 1 \\ &\qquad \ll \frac{1}{p}\Sigma_1 + \Sigma_2,\end{aligned}$$

par définition. La relation (51) avec $q=1$, donne la majoration

$$\Sigma_1 \ll X^{1-\rho}. \tag{53}$$

Pour Σ_2, on écrit

$$\begin{aligned}(54)\quad \Sigma_2 &\ll \sum_{1\leqslant a\leqslant X^{\frac{1}{4}-3\rho}} \sum_{|b|\ll X^{1/4}} \min(X^{1/2}a^{-1}, X\,|b|^{-3}) \\ &\ll \sum_{1\leqslant a\leqslant X^{\frac{1}{4}-3\rho}} \Big\{ \sum_{b\leqslant X^{1/6}a^{1/3}} X^{1/2}a^{-1} + \sum_{b> X^{1/6}a^{1/3}} Xb^{-3}\Big\} \ll X^{\frac{3}{4}-\rho}.\end{aligned}$$

Regroupant (52), (53) et (54), on obtient

$$\operatorname{card}\big\{F \in \mathcal{M}_{\text{pointe}}(X) \cap \mathbb{Z}^4 \colon p \mid \Delta(F)\big\} \ll \frac{X^{1-\rho}}{p} + X^{\frac{3}{4}-\rho}. \tag{55}$$

Le lemme 3.3 reste valable en remplaçant $\mathcal{F}^+_{\text{corps}}(X)$ par $\mathcal{M}_{\text{corps}}(X)$. Donc pour $Q \geqslant 2$, on a l'inégalité

$$\operatorname{card}\big\{F \in \mathcal{M}_{\text{corps}}(X) \cap \mathbb{Z}^4 \colon p \mid \Delta(F)\big\} \leqslant \sum_{j\in\mathcal{J}} \operatorname{card}\big\{F \in \mathcal{B}_j \colon p \mid \Delta(F)\big\}, \tag{56}$$

et l'ensemble d'indices $\mathcal{J}$ vérifie

$$\begin{aligned}(57)\quad \operatorname{card}\mathcal{J} &= \big(\operatorname{card}\mathcal{J} - \operatorname{card}\mathcal{I}\big) + \operatorname{card}\mathcal{I} \\ &\ll Q^{-3}X^{\frac{3}{4}+3\rho}\log X + Q^{-1}X^{\frac{1}{4}+3\rho} + 1 + Q^{-4}\operatorname{Vol}\mathcal{M}_{\text{corps}}(X),\end{aligned}$$

soit encore, en utilisant le lemme 4.1,

$$\operatorname{card}\mathcal{J} \ll Q^{-4}X + Q^{-3}X^{\frac{3}{4}+3\rho}\log X, \tag{58}$$

sous l'hypothèse $Q \leqslant X^{1/4}$. Posons

$$\mathcal{B}_j = [n_1, n_1+Q] \times [n_2, n_2+Q] \times [n_3, n_3+Q] \times [n_4, n_4+Q].$$

En utilisant les caractères additifs pour détecter l'appartenance à l'intervalle $[n_i, n_i+Q]$, on a l'égalité

$$N(\mathcal{B}_j;p) := \operatorname{card}\big\{(a,b,c,d)\in\mathcal{B}_j\cap\mathbb{Z}^4 \colon p \mid \Delta(a,b,c,d)\big\}$$
$$= \frac{1}{p^4}\sum_{\mathbf{h}\,(\mathrm{mod}\ p)}\sum_{\substack{\mathbf{x}\,(\mathrm{mod}\ p)\\ \Delta(\mathbf{x})=0}}\sum_{\substack{\mathbf{t}\\ n_i\leqslant t_i\leqslant n_i+Q}} \exp\Big(2\pi i\frac{\mathbf{h}\cdot(\mathbf{x}-\mathbf{t})}{p}\Big), \tag{59}$$

où $\mathbf{h}=(h_1,\dots,h_4)\in\mathbb{F}_p^4$, $\mathbf{x}=(x_1,\dots,x_4)\in\mathbb{F}_p^4$, et $\mathbf{t}=(t_1,\dots,t_4)\in\mathbb{Z}^4$. Posons

$$S(\mathbf{h};p)=\sum_{\substack{\mathbf{x}\,(\mathrm{mod}\ p)\\ \Delta(\mathbf{x})=0}}\exp\Big(2\pi i\frac{\mathbf{h}\cdot\mathbf{x}}{p}\Big),\quad\text{et}\quad \sigma_i(h_i;p)=\sum_{n_i\leqslant t_i\leqslant n_i+Q}\exp\Big(-2\pi i\frac{h_it_i}{p}\Big).$$

L'égalité (59) devient

$$N(\mathcal{B}_j;p)=\frac{1}{p^4}\sum_{\mathbf{h}\,(\mathrm{mod}\ p)}S(\mathbf{h};p)\prod_{1\leqslant i\leqslant 4}\sigma_i(h_i;p). \tag{60}$$

On sépare le terme $\mathbf{h}=\mathbf{0}$ dont la contribution est en $O(Q^4p^{-1})$ et on utilise la majoration classique

$$\sigma_i(h_i;p)\ll\min\Big(Q,\Big\|\frac{p}{h_i}\Big\|\Big),$$

(où $\|x\|$ désigne la distance de x à l'entier le plus proche), ainsi que [3, lemme 3.2] qui donne

$$S(\mathbf{h};p)\ll p(\mathbf{h},p)(\Delta^*(\mathbf{h}),p),$$

avec $\Delta^*(h_1,h_2,h_3,h_4)=\Delta(h_1,3h_2,3h_3,h_4)$. De (60), on déduit la relation

$$N(\mathcal{B}_j;p)\ll Q^4p^{-1}+\frac{1}{p^3}\sum_{\mathbf{h}\neq\mathbf{0}}\prod_{1\leqslant i\leqslant 4}\min\Big(Q,\Big\|\frac{p}{h_i}\Big\|\Big)(p,\Delta^*(\mathbf{h})). \tag{61}$$

Pour évaluer le second terme à droite de (61), on remarque que la contribution des $\mathbf{h}\neq\mathbf{0}$ vérifiant $\Delta^*(\mathbf{h})\neq 0$ modulo p est

$$\ll\frac{1}{p^3}\Big\{\sum_{h=0}^{p-1}\min\Big(Q,\Big\|\frac{p}{h}\Big\|\Big)\Big\}^4\ll p\log^4 p \tag{62}$$

en utilisant $Q\ll p$. La contribution des $\mathbf{h}\neq 0$ modulo p, tels que $\Delta^*(\mathbf{h})=0$ modulo p se traite en constatant, que pour (h_1,h_2,h_3) fixé avec $(h_1,h_2)\neq(0,0)$, l'équation $\Delta^*(\mathbf{h})=0$ modulo p a $O(1)$ solutions en h_4. Par contre, si $(h_1,h_2)=(0,0)$, tout (h_3,h_4) est tel que $\Delta^*(\mathbf{h})=0$. Ces considérations montrent que la contribution des $\mathbf{h}$ avec $\Delta^*(\mathbf{h})=0$ au deuxième terme à droite de (61) est

$$\ll\frac{1}{p^2}\Big(Q\Big\{\sum_{h=0}^{p-1}\min(Q,\Big\|\frac{p}{h}\Big\|)\Big\}^3+Q^2\Big\{\sum_{h=0}^{p-1}\min(Q,\Big\|\frac{p}{h}\Big\|)\Big\}^2\Big)\ll Qp\log^3 p+Q^2\log^2 p,$$

soit encore

$$\ll Qp\log^3 p, \tag{63}$$

puisque $Q \ll p$. Regroupant (61), (62) et (63), on a, pour tout $j \in \mathcal{J}$, l'inégalité

$$N(\mathcal{B}_j, p) \ll Q^4 p^{-1} + p \log^4 p + Qp \log^3 p \ll Q^4 p^{-1}, \tag{64}$$

avec le choix

$$Q = p^{2/3} \log X.$$

Regroupant (55), (56), (58) et (64), on a

$$N(0, X, p) \ll \frac{X}{p} + \frac{QX^{\frac{3}{4}+3\rho} \log X}{p} + X^{\frac{3}{4}-\rho}. \tag{65}$$

On fixe ρ tel que le second terme à droite de (65) soit égal à X/p, c'est-à-dire

$$X^\rho = X^{1/12} p^{-2/9} \log^{-2/3} X,$$

cette valeur reportée dans (65) montre qu'on a la relation $N(0, X, p) \ll Xp^{-1}$, sous la contrainte $p \leqslant X^{3/11} \log^{-\frac{6}{11}} X$. Ceci termine la preuve du théorème 1.5. □

5. La minoration. Preuve du théorème 1.6

5.1. **Rappels sur les corps cubiques.** Rappelons d'abord un résultat classique de Hasse [18, §1], qui donne des conditions nécessaires pour qu'un entier appartienne à $\mathcal{D}_3$. On a

Lemme 5.1. *Soit $K \subset \mathbb{C}$ une extension cubique de $\mathbb{Q}$. Alors son discriminant est de la forme*

$$\operatorname{disc} K = \Delta f^2,$$

où Δ est un discriminant fondamental et f est un entier vérifiant

$$f = 3^e \cdot q_1 \cdots q_t,$$

avec $0 \leqslant e \leqslant 2$, $t \geqslant 0$, q_i des nombres premiers distincts et différents de 3, vérifiant la congruence $q_i \equiv \left(\frac{\Delta}{q_i}\right) \pmod 3$ (d'où $q_i \nmid \Delta$). De plus, on a les implications

$$\begin{aligned} \Delta \equiv \pm 1 \pmod 3 &\Rightarrow e \in \{0, 2\}, \\ \Delta \equiv 3 \pmod 9 &\Rightarrow e \in \{0, 1\}. \end{aligned}$$

Enfin $K(\sqrt{\Delta})$ est la clôture galoisienne de $K/\mathbb{Q}$.

Signalons que dans ce lemme, il n'y a pas de contrainte sur e lorsque $\Delta \equiv -3 \pmod 9$. Ces données se traduisent agréablement sur les classes de formes associées (voir [2, algorithm 1.3, lemma 1.6]) :

Lemme 5.2. *Soit K comme ci-dessus, F la classe de formes cubiques associée et p un nombre premier. Alors $p \mid f$ si et seulement si $F \in U_p \setminus V_p$*

Le lemme suivant donne une formule pour le nombre $m(d)$ de classes de conjugaison de corps cubiques (inclus dans $\mathbb{C}$), de discriminant égal à d. Ainsi $m(d) = 0$ si d n'est pas de la forme $d = \Delta f^2$ avec Δ et f comme dans le lemme 5.1. On a

Lemme 5.3 (Mayer [23] Theorem 1.1)**.** *Soient Δ un discriminant fondamental, $k = \mathbb{Q}(\sqrt{\Delta})$ et f un entier comme au lemme 5.1. On a alors l'égalité*

$$\sum_{f'|f} m(\Delta f'^2) = \frac{1}{2}\big(3^{\rho+t+w-\delta} - 1\big),$$

- *où ρ désigne le 3-rang du groupe des classes d'idéaux de k,*
- *où w est défini par*

$$w = \begin{cases} 0 & \text{si } e = 0 \\ 2 & \text{si } e = 2 \text{ et } \Delta \equiv -3 \pmod 9, \\ 1 & \text{sinon,} \end{cases}$$

- *et où on a posé*

$$\delta = \dim_{\mathbb{F}_3}\Big(I_{k,3}(f)/I_{k,3}(f) \cap \big(\mathbb{Q}^\times(f) k_f^\times k^\times(f)^3\big)\Big).$$

Dans cette dernière expression, on note

- *$k^\times(f)$ (resp. $\mathbb{Q}^\times(f)$) l'ensemble des éléments de $k^\times$ (resp. $\mathbb{Q}^\times$), qui sont premiers avec f,*
- *$k_f^\times = \{\gamma \in k^\times : \gamma \equiv 1 \mod {}^\times f\}$.*

Enfin on a posé $I_{k,3}(f) = I_{k,3} \cap k^\times(f)$ où $I_{k,3}$ désigne le groupe des générateurs $\alpha \in k^\times$ de tous les idéaux principaux $\alpha\mathcal{O}_k$ qui sont des cubes d'idéaux de $\mathcal{O}_k$.

Noter que [23, Theorem 1.1] spécifie que $k = \mathbb{Q}(\sqrt{\Delta})$ est un corps quadratique, mais l'énoncé vaut aussi pour $\Delta = 1$, cf [23, Introduction]. Le nombre δ défini précédemment est assez mystérieux. Heureusement, nous n'aurons besoin que d'une majoration, fournie par la preuve de Mayer :

Lemme 5.4 ([23] Remark 2, p. 837)**.** *Avec les notations du lemme précédent, on a les inégalités*

$$\delta \leqslant \begin{cases} \min(\rho, t+w) & \text{pour } \Delta < -3 \\ \min(\rho+1, t+w) & \text{pour } \Delta \geqslant -3 \end{cases}$$

5.2. **Preuve du théorème 1.6.** Soit q un entier sans facteur carré. On suppose d'abord q impair. Soit Δ un discriminant fondamental vérifiant

$$\Delta \equiv -3 \pmod 9.$$

D'après le lemme 5.3, appliqué avec les valeurs $f = 9$, $e = 2$, $t = 0$ et $w = 2$, on a l'égalité

$$\sum_{f'|9} m(\Delta f'^2) = \frac{1}{2}\big(3^{\rho+2-\delta} - 1\big). \tag{66}$$

Pour toute valeur de Δ, positive ou négative, le lemme 5.4 donne l'inégalité

$$\delta \leqslant \rho + 1,$$

qui, reportée dans (66) donne, toujours sous la condition $\Delta \equiv -3$ modulo 9, la minoration

$$\sum_{f'|9} m(\Delta f'^2) \geqslant 1. \tag{67}$$

Constatant que chaque entier d s'écrit d'au plus d'une façon $d = \Delta f'^2$, avec Δ discriminant fondamental et $f' \mid 9$, on a pour $X > 0$, les inégalités

$$\begin{aligned} N(0, X; q) &\geqslant \operatorname{card}\Big\{\tilde{K} \in \tilde{\mathcal{K}} \colon 0 < \operatorname{disc} \tilde{K} < X, q \mid \operatorname{disc} K\Big\} \\ &\geqslant \sum_{\substack{\Delta \text{ fond.}, q|\Delta \\ 0<\Delta<X/81}} \sum_{f'|9} m(\Delta f'^2) \\ &\geqslant \operatorname{card}\{\Delta \text{ fond.} \colon 0 < \Delta < X/81, \Delta \equiv -3 \pmod{36}, q \mid \Delta\}, \end{aligned}$$

la dernière ligne s'obtenant par restriction aux Δ congrus à 1 (modulo 4) et à -3 (modulo 9) et en appliquant l'inégalité (67). Ainsi, dans la partie droite de l'inégalité précédente, on peut remplacer la condition Δ *fondamental* par Δ *sans facteur carré*. On a donc l'inégalité

$$N(0, X; q) \geqslant \operatorname{card}\left\{n \colon 0 < n < \frac{X}{81}, n \equiv -3 \pmod{36}, \mu^2(n) = 1, q \mid n\right\}. \tag{68}$$

On est alors ramené à un problème de comptage d'entiers sans facteur carré dans une progression arithmétique :

Lemme 5.5. *Soit q un entier impair $\geqslant 1$, sans facteur carré, et $q' = q/(3, q)$. On a, uniformément pour $Y \geqslant 2$, l'égalité*

$$\begin{aligned} &\operatorname{card}\big\{n \colon 0 < n < Y, n \equiv -3 \pmod{36}, \mu^2(n) = 1, q \mid n\big\} \\ &\qquad = \frac{Y}{4\pi^2} \cdot \frac{\varphi(q')}{q'} \cdot \frac{1}{q'} \prod_{p|q'} \big(1 - p^{-2}\big)^{-1} + O\Big(q^{-\frac{1}{2}} Y^{1/2} \prod_{p|q} (1 + p^{-\frac{1}{2}})\Big). \end{aligned}$$

Preuve. La démarche est tout à fait classique. Soit $E(Y, q)$ le cardinal étudié. On a donc l'égalité

$$\begin{aligned} E(Y, q) &= \sum_{\substack{0<n<Y,\, q'|n \\ n\equiv -3 \pmod{36}}} \mu^2(n) \\ &= \sum_{\substack{0<n<Y,\, q'|n \\ n\equiv -3 \pmod{36}}} \sum_{\delta^2|n} \mu(\delta) = \sum_{(\delta,6)=1} \mu(\delta) \sum_{\substack{0<n<Y,\, [q',\delta^2]|n \\ n\equiv -3 \pmod{36}}} 1, \end{aligned} \tag{69}$$

où $[a, b]$ désigne le ppcm des entiers a et b. Puisque $(q'\delta^2, 36) = 1$, la dernière somme intérieure vaut

$$\begin{cases} \dfrac{Y}{36[q', \delta^2]} + O(1) & \text{pour } [q', \delta^2] \leqslant Y, \\ 0 & \text{pour } [q', \delta^2] > Y. \end{cases}$$

formule valable pour q et δ comme précédemment. Reportée dans (69), elle conduit à

$$E(Y,q)=\frac{Y}{36}\sum_{\substack{(\delta,6)=1\\ [q',\delta^2]\leqslant Y}}\frac{\mu(\delta)}{[\delta^2,q']}+O\Big(\sum_{\substack{\delta\\ [\delta^2,q']\leqslant Y}}1\Big). \tag{70}$$

On pose $\nu=(\delta^2,q')$. Puisque q est sans facteur carré, on a aussi $\nu=(\delta,q')$. On pose $\delta=\nu d$ d'où $[\delta^2,q']=d^2\nu q'$. Le terme d'erreur de (70) est

$$\ll\sum_{\nu\mid q'}\sum_{d\leqslant(Y/\nu q')^{1/2}}1\ll q^{-1/2}Y^{1/2}\sum_{\nu\mid q}\nu^{-1/2}\ll q^{-1/2}Y^{1/2}\prod_{p\mid q}(1+p^{-1/2}). \tag{71}$$

Pour le terme principal de (70), la présence de la fonction de Möbius implique $(\nu,d)=1$. D'autre part, on a $(q'\nu^{-1},d)=1$, d'où les égalités

$$\begin{aligned}\sum_{\substack{(\delta,6)=1\\ [q',\delta^2]\leqslant Y}}\frac{\mu(\delta)}{[\delta^2,q']}&=\frac{1}{q'}\sum_{\nu\mid q'}\frac{\mu(\nu)}{\nu}\sum_{\substack{(d,6q')=1\\ d\leqslant(Y/\nu q')^{1/2}}}\frac{\mu(d)}{d^2}\\&=\frac{1}{q'}\sum_{\nu\mid q'}\frac{\mu(\nu)}{\nu}\Big(\prod_{(p,6q')=1}(1-p^{-2})+O\big(\nu^{\frac12}q^{\frac12}Y^{-\frac12}\big)\Big)\end{aligned}$$

(Rappelons que q est impair sans facteur carré, donc $(q',6)=1$.) Finalement

$$\sum_{\substack{(\delta,6)=1\\ [q',\delta^2]\leqslant Y}}\frac{\mu(\delta)}{[\delta^2,q']}=\frac{6}{\pi^2}\cdot\frac{\varphi(q')}{q'}\cdot\frac{1}{q'}\prod_{p\mid 6q'}\big(1-p^{-2}\big)^{-1}+O\Big(q^{-\frac12}Y^{-1/2}\prod_{p\mid q}(1+p^{-1/2})\Big). \tag{72}$$

Reportant (71) et (72) dans (70), on conclut la preuve. □

Pour terminer la preuve de la minoration (12), il suffit d'appliquer le lemme 5.5 à la formule (68) avec $Y=X/81$. L'étude de la quantité $N(-X,0;q)$ se conduit de même.

5.3. **Cas où q est pair.** Par hypothèse, on sait que $1\leqslant v_2(q)\leqslant 3$ et $v_p(q)\leqslant 1$ pour tout $p\geqslant 3$. Si $q'\mid q$, on a l'inégalité évidente

$$N(0,X;q)\leqslant N(0,X;q'),$$

donc il suffit de montrer l'inégalité (12) pour $q=8q_1$ avec q_1 impair et sans facteur carré, quitte à modifier les valeurs des constantes c_1 et c_2. On a toujours l'inégalité

$$N(0,X;q)\geqslant \operatorname{card}\{\Delta \text{ fond.}\colon 0<\Delta<X/81,\Delta\equiv -3 \pmod 9, q\mid\Delta\}.$$

On pose alors $\Delta=8\Delta_1$ avec Δ_1 sans facteur carré, $q_1\mid\Delta_1$ et $\Delta_1\equiv 3$ modulo 4. L'analogue dans ce cas de l'inégalité (68) est

$$N(0,X;q)\geqslant \operatorname{card}\big\{n_1\colon 0<n_1<X/648, n_1\equiv 3 \pmod{36}, \mu^2(n_1)=1, q_1\mid n_1\big\}.$$

La preuve est alors identique au cas q impair.

5.4. **Preuve de** (13)**.** C'est une application classique des estimations de Chebychev. On a d'abord

$$\frac{\varphi(q)}{q} \gg \frac{1}{\log\log q} \gg \frac{1}{\log\log X}$$

et

$$\log \prod_{p\mid q}(1+p^{-\frac{1}{2}}) = \sum_{p\mid q}\log(1+p^{-\frac{1}{2}}) \ll \sum_{p\ll \log q} p^{-\frac{1}{2}} \ll \frac{\log^{\frac{1}{2}} q}{\log\log q}.$$

Par ces calculs et l'hypothèse $q \leqslant X\exp(-\sqrt{\log X})$, on voit que, (12) implique la minoration de $N(0,X;q)$ et $N(-X,0;q)$ par

$$\frac{\varphi(q)}{q}\cdot\frac{X}{q}\Big\{c_1' - (\log\log X)\Big(\frac{q}{X}\Big)^{1/2}\exp\Big(c_2'\frac{\log^{1/2} X}{\log\log X}\Big)\Big\} \geqslant c_3'\frac{\varphi(q)}{q}\cdot\frac{X}{q},$$

pour certaines constantes c_1', c_2' et $c_3' > 0$, ce qui est l'inégalité (13). La preuve du théorème 1.6 est ainsi complète. □

6. Un calcul hybride. Preuve des théorèmes 1.2 et 1.1

6.1. **Preuve du théorème 1.2.** Nous nous concentrons uniquement sur le cas des discriminants positifs. Pour calculer la fonction $S(X,Y)$ définie en (7), on introduit, pour f entier et $X \geqslant 1$, l'ensemble fini

$$\begin{aligned}\Xi(f,X) := \Big\{F \in \tilde{\Phi}\colon F \text{ irréductible}, 1 \leqslant \operatorname{disc} F \leqslant X,\\ p \mid f \Rightarrow F \in U_p \setminus V_p,\\ p \nmid f \Rightarrow F \in V_p\Big\}.\end{aligned}$$

On note

$$\xi(f,X) := \operatorname{card}\big\{F \in \Xi(f,X)\colon 3^4 \nmid \operatorname{disc} F\big\},$$
$$\xi_3(f,X) := \operatorname{card}\big\{F \in \Xi(f,X)\colon 3^4 \mid \operatorname{disc} F\big\}.$$

Si f est restreint aux entiers sans facteurs carrés, les ensembles $\Xi(f,X)$ sont 2 à 2 disjoints et forment une partition des éléments de U de discriminant inférieur à X. Plus précisément :

Lemme 6.1. *Pour tout $X \geqslant 1$ et tout $Y \geqslant 1$, on a l'égalité*

$$S(X,Y) = \sum_{f\leqslant Y}\mu^2(f)\xi(f,Xf^2) + \sum_{f'\leqslant Y/9}\mu^2(3f')\xi_3(f',X(9f')^2).$$

Preuve. Si Δf^2 est le discriminant d'un corps cubique K, le lemme 5.1 implique que f est sans facteur carré autre que 3^2, que $3^3 \nmid f$ et que $9 \mid f$ si et seulement si $3^4 \mid \operatorname{disc} K$. On conclut en utilisant le lemme 5.2 : la première somme tient compte des f divisibles par 3 mais pas par 3^2, la deuxième de ces derniers uniquement (de la forme $f = 9f'$, f' premier à 3). □

Le nombre premier 3 jouant un rôle particulier, complétons de suite le lemme 3.1 pour le calcul de ξ_3 :

Lemme 6.2. *On a l'égalité*

$$\operatorname{card}\left\{F \in \overline{U_3}\colon 3^4 \mid \operatorname{disc} F\right\} = \frac{1}{39}\operatorname{card}\overline{U_3} = \frac{1}{36}\operatorname{card}\overline{V_3}.$$

Preuve. Comptons ces formes F. Comme $3^4 \mid \operatorname{disc} F$, on a $F \in \overline{U_3} \setminus \overline{V_3}$, donc cette forme est le cube d'un facteur linéaire modulo 3 ; si l'on suppose la racine triple en 0 (parmi les 4 choix possibles dans $\mathbb{P}^1(\mathbb{F}_3)$), la condition de 3-maximalité sur $(a, 3\beta, 3\gamma, 3\delta)$ est $3 \nmid a\delta$. Sous ces conditions, puisque

$$D = \operatorname{disc}(a, 3\beta, 3\gamma, 3\delta) = 3^5 \cdot 2a\beta\gamma\delta - 3^5a^2\delta^2 + 3^4\beta^2\gamma^2 - 3^4 \cdot 4\beta^3\delta - 3^3 \cdot 4a\gamma^3,$$

on obtient que $v_3(D) = 3$ si et seulement si $3 \nmid \gamma$, $v_3(D) \geqslant 4$ sinon. Le cardinal cherché est donc

$$4 \cdot 6 \cdot 3 \cdot 1 \cdot 2 = 2^4 3^2$$

où les termes correspondent respectivement aux 4 choix de racines dans $\mathbb{P}^1(\mathbb{F}_3)$, à $a \in (\mathbb{Z}/3^2\mathbb{Z})^*$, $\beta \in \mathbb{Z}/3\mathbb{Z}$, $\gamma \equiv 0 \pmod 3$, et $\delta \in (\mathbb{Z}/3\mathbb{Z})^*$. On conclut à l'aide du lemme 3.1. □

Corollaire 6.3. *On a les égalités*

$$\operatorname{card}\left\{F \in \overline{U_3}\colon 3^4 \nmid \operatorname{disc} F\right\} = \frac{38}{39}\operatorname{card}\overline{U_3},$$

$$\operatorname{card}\left\{\overline{U_3} \setminus \overline{V_3}\right\} = \frac{3}{39}\operatorname{card}\overline{U_3},$$

$$\operatorname{card}\left\{F \in \overline{U_3} \setminus \overline{V_3}\colon 3^4 \nmid \operatorname{disc} F\right\} = \frac{2}{39}\operatorname{card}\overline{U_3}.$$

Preuve. Les deux premières sont immédiates. Pour la troisième, il suffit de remarquer que les conditions $3^4 \mid \operatorname{disc} F$ et $F \in \overline{V_3}$ s'excluent mutuellement, et correspondent respectivement à $\frac{1}{39}\operatorname{card}\overline{U_3}$ et $\frac{36}{39}\operatorname{card}\overline{U_3}$ formes. □

Pour $X \geqslant 1$, puis f, r et s des nombres entiers sans facteur carré, premiers entre eux deux à deux et tels que $3 \mid fr$, on pose

$$\begin{aligned} G(f,r,s,X) = \operatorname{card}\Big\{F \in \tilde{\Phi}\colon\ & F \text{ irréductible}, 1 \leqslant \operatorname{disc} F \leqslant X, \\ & p \mid f \Rightarrow F \in U_p \setminus V_p, \text{ ainsi que } 3^4 \nmid \operatorname{disc} F \text{ si } p = 3, \\ & p \mid r \Rightarrow F \in V_p, \\ & p \mid s \Rightarrow F \notin V_p\Big\}. \end{aligned}$$

On a donc l'égalité

$$\xi(f, X) = G\left(f, \frac{P_\infty}{(f, P_\infty)}, 1, X\right),$$

en notant que si $3 \nmid f$, on a $3 \mid r$, soit $F \in V_3$; ce qui implique bien $3^4 \nmid \operatorname{disc} F$. Le principe d'inclusion-exclusion donne, comme pour (35), l'égalité suivante, valable

pour $Y < Z$,

$$\begin{aligned}\xi(f,X) &= G(f,\frac{P_Y}{(f,P_Y)},1,X) + O\Big(\sum_{\substack{Y<p\leqslant Z\\(p,f)=1}} G(f,\frac{P_Y}{(f,P_Y)},p,X)\Big)\\ &\quad + O\Big(\sum_{\substack{p>Z\\(p,f)=1}} G(f,\frac{P_Y}{(f,P_Y)},p,X)\Big) \qquad (73)\\ &= G_1 + O(G_2) + O(G_3),\end{aligned}$$

par définition.

6.2. **Majoration de G_3.** On constate que si F est compté dans $G(f,r,s,X)$ on a $f^2s^2 \mid \Delta(F)$. Par conséquent, par le lemme 3.5, on a

$$\begin{aligned}G_3 &\ll_\varepsilon X^{\varepsilon/2}\Big(\sum_{Z<p<X}\big(\frac{X}{f^2p^2} + \frac{X^{15/16}}{f^{15/8}p^{15/8}} + \frac{X^{1/2}}{fp}\big)\Big)\\ &\ll_\varepsilon X^\varepsilon\Big(\frac{X}{f^2Z} + \frac{X^{15/16}}{f^{15/8}Z^{7/8}} + \frac{X^{1/2}}{f}\Big),\end{aligned}$$

soit encore, pour tout $\varepsilon > 0$,

$$G_3 \ll_\varepsilon \frac{X^{1+\varepsilon}}{f^2Z}, \qquad (74)$$

uniformément pour $f \geqslant 1$, $Z \geqslant 1$ satisfaisant

$$fZ \leqslant X^{1/2}. \qquad (75)$$

6.3. **Une formule générale pour la fonction G.** La démarche est proche de celle suivie au §3.5. Nous montrons

Proposition 6.4. *Pour $X \geqslant 2$, Pour f, r et s entiers premiers entre eux deux à deux, sans facteur carré, vérifiant $3 \mid fr$ et $fs < X^{1/4}$, pour ρ vérifiant $0 < \rho < \frac{1}{12}$, et pour tout $\varepsilon > 0$, on a l'égalité*

$$\begin{aligned}G(f,r,s,X) =& \frac{\pi^2}{72}\cdot\gamma(f,r,s)\cdot X + O(X^{\frac34+\varepsilon})\\ &+ O\Big(\gamma(f,r,s)\big(f^2r^2s^2X^{\frac34+3\rho}\log X + f^6r^6s^6X^{\frac14+3\rho} + f^8r^8s^8\big)\Big)\\ &+ O\Big(\frac{X^{1-\rho}}{fs}\prod_{p\mid fs}\Big(3+\frac1p\Big)\Big),\end{aligned}$$

avec

$$\gamma(f,r,s) = (2/3)^{v_3(f)}\prod_{p\mid f}\frac{1}{p^2}\Big(1-\frac1p\Big)\Big(1-\frac{1}{p^2}\Big)\prod_{p\mid r}\Big(1-\frac{1}{p^2}\Big)^2\prod_{p\mid s}\frac{1}{p^2}\Big(2-\frac{1}{p^2}\Big).$$

Notons que les arguments de [6] permettraient d'améliorer le terme d'erreur en X aux prix de complications techniques que nous avons préféré éviter.

Preuve. Notre point de départ est toujours une généralisation de la proposition 2.3 et un découpage de $\mathcal{F}^+(X)$ en une pointe et un corps, comme indiqué au §3.2. Pour tout $0 < \rho < 1/12$ et tout $\varepsilon > 0$, on a

$$G(f,r,s,X) = \frac{1}{2}\Big(G_{\text{corps}} + G_{\text{pointe}}\Big) + O(X^{\frac{3}{4}+\varepsilon}), \tag{76}$$

où

$$G_\bullet = \operatorname{card}\big\{F \in \mathcal{F}_\bullet^+(X)\colon F \in \cap_{p|f}(U_p \setminus V_p), F \in \cap_{p|r} V_p, F \notin \cup_{p|s} V_p\big\}.$$

Le terme d'erreur $O(X^{\frac{3}{4}+\varepsilon})$ provient des formes réductibles ou de celles telles que $|B| = A$ ou $A = C$. Pour majorer G_{pointe}, on part de la majoration triviale

$$G_{\text{pointe}} \leqslant \operatorname{card}\big\{F \in \mathcal{F}_{\text{pointe}}^+(X) \cap \mathbb{Z}^4\colon fs \mid \Delta(F)\big\}.$$

(On pourrait améliorer la majoration en conservant le critère plus fort de divisibilité $(fs)^2 \mid \Delta(F)$, au prix d'une analyse plus fastidieuse). Puisqu'on a l'inclusion

$$\mathcal{F}_{\text{pointe}}^+(X) \subset \Big\{(a,b,c,d) \in \mathcal{M}(X)\colon 0 < a \leqslant X^{\frac{1}{4}-3\rho}\Big\},$$

on a, par (51) avec $q = fs$, la majoration

$$G_{\text{pointe}} \ll \frac{X^{1-\rho}}{fs} \prod_{p|fs}\Big(3 + \frac{1}{p}\Big), \tag{77}$$

uniformément pour $1 \leqslant fs \leqslant X^{1/4}$.

L'étude de G_{corps} se conduit comme celle de la proposition 3.6. On encadre l'ensemble $\mathcal{F}_{\text{corps}}^+(X)$ par deux ensembles d'hypercubes $\mathcal{B}_i$ $(i \in \mathcal{I})$ et $\mathcal{B}_j$ $(j \in \mathcal{J})$ avec $\mathcal{I} \subset \mathcal{J}$. La longueur des côtés de ces hypercubes vaut maintenant $Q = (frs)^2$. Notons $e := v_3(f) \in \{0,1\}$. Dans chaque $\mathcal{B}_j$, le nombre de $F = (a,b,c,d) \in \mathbb{Z}^4$ vérifiant

$$\begin{aligned} p \mid f &\;\Rightarrow\; F \in U_p \setminus V_p, \quad \text{ainsi que } 3^4 \nmid \operatorname{disc} F \text{ si } p = 3,\\ p \mid r &\;\Rightarrow\; F \in V_p,\\ p \mid s &\;\Rightarrow\; F \notin V_p \end{aligned}$$

vaut, par le théorème chinois, le lemme 3.1 et le corollaire 6.3

$$\begin{aligned} &\Big(\operatorname{card}\big\{F \in \overline{U_3} \setminus \overline{V_3}\colon 3^4 \nmid \operatorname{disc} F\big\} / \operatorname{card}(\overline{U_3} \setminus \overline{V_3})\Big)^e \\ &\qquad \prod_{p|f} \operatorname{card}(\overline{U_p} \setminus \overline{V_p}) \prod_{p|r} \operatorname{card} \overline{V_p} \prod_{p|s} (p^8 - \operatorname{card} \overline{V_p}) \\ &= (2/3)^e (frs)^8 \prod_{p|f} \frac{1}{p^2}\Big(1 - \frac{1}{p}\Big)\Big(1 - \frac{1}{p^2}\Big) \prod_{p|r}\Big(1 - \frac{1}{p^2}\Big)^2 \prod_{p|s} \frac{1}{p^2}\Big(2 - \frac{1}{p^2}\Big) \\ &= \operatorname{card}\big(\mathcal{B}_j \cap \mathbb{Z}\big) \cdot \gamma(f,r,s). \end{aligned}$$

Raisonnant comme pour la formule (39) et en utilisant (76) et (77), on a, pour tout $\varepsilon > 0$, l'égalité

$$G(f,r,s,X) = \frac{\gamma(f,r,s)}{2}\Big(\operatorname{card}\mathcal{F}^+_{\text{corps}}(X) + O\Big(QX^{\frac{3}{4}+3\rho}\log X + Q^3X^{\frac{1}{4}+3\rho} + Q^4\Big)\Big) + O\Big(\frac{X^{1-\rho}}{fs}\prod_{p\mid fs}\Big(3+\frac{1}{p}\Big)\Big) + O(X^{\frac{3}{4}+\varepsilon}).$$

En utilisant (32), dont les termes d'erreur sont absorbés dans ceux déjà présents, on termine la preuve de la proposition. □

6.4. **Étude de la formule** (73)**.** On applique la proposition 6.4 avec

$$s = 1, \quad r = \frac{P_Q}{(f,P_Q)}, \quad \text{et} \quad Q = \frac{\log X}{\log\log X},$$

et X suffisamment grand pour que $Q \geqslant 3$ (ce qui garantit $3 \mid fr$). Posant $e := v_3(f) \in \{0,1\}$, on a alors

$$\begin{aligned}
\gamma(f,r,1) &= \frac{(2/3)^e}{f^2}\prod_{p\mid f}\Big(1-\frac{1}{p}\Big)\Big(1-\frac{1}{p^2}\Big)\prod_{\substack{p\leqslant Q\\ p\nmid f}}\Big(1-\frac{1}{p^2}\Big)^2\\
&= \frac{(2/3)^e}{f^2}\prod_{p\mid f}\Big(1-\frac{1}{p}\Big)\Big(1-\frac{1}{p^2}\Big)\prod_{p\nmid f}\Big(1-\frac{1}{p^2}\Big)^2\Big(1+O\Big(\frac{1}{Q\log Q}\Big)\Big)\\
&= \frac{(2/3)^e}{f^2\zeta(2)^2}\prod_{p\mid f}\Big(1-\frac{1}{p}\Big)\Big(1-\frac{1}{p^2}\Big)\Big(1-\frac{1}{p^2}\Big)^{-2}\Big(1+O\Big(\frac{1}{\log X}\Big)\Big)\\
&= \frac{(2/3)^e}{f^2\zeta(2)^2}\prod_{p\mid f}\Big(1+\frac{1}{p}\Big)^{-1}\Big(1+O\Big(\frac{1}{\log X}\Big)\Big).
\end{aligned}$$

On parvient ainsi à l'égalité suivante, valable pour tout $\varepsilon > 0$, tout $0 < \rho \leqslant 1/12$ et tout $f \leqslant X^{1/4}$ sans facteur carré :

$$G_1 = \frac{(2/3)^e}{2\pi^2}\prod_{p\mid f}\Big(1+\frac{1}{p}\Big)^{-1}\cdot\frac{X}{f^2}\Big(1+O\Big(\frac{1}{\log X}\Big)\Big) + O\Big(\big(X^{\frac{3}{4}+3\rho}+f^4X^{\frac{1}{4}+3\rho}+f^6\big)X^{\varepsilon}\Big) + O\Big(\frac{X^{1-\rho+\varepsilon}}{f}\Big). \tag{78}$$

Pour majorer G_2, nous utilisons la majoration $\gamma(f,r,p) \leqslant 2/(f^2p^2)$ qui donne

$$G(f,\frac{P_Q}{(f,P_Q)},p,X) \ll \frac{X}{f^2p^2} + X^{\varepsilon}\big(X^{\frac{3}{4}+3\rho}+f^4p^4X^{\frac{1}{4}+3\rho}+f^6p^6\big) + \frac{X^{1-\rho+\varepsilon}}{fp},$$

Sommant sur les premiers p satisfaisant $Q < p \leqslant Z = X^{2\varepsilon}$, on a

$$G_2 \ll \frac{X}{f^2\log X} + X^{\frac{3}{4}+3\rho+3\varepsilon} + f^4X^{\frac{1}{4}+3\rho+11\varepsilon} + f^6X^{15\varepsilon} + \frac{X^{1-\rho+2\varepsilon}}{f}. \tag{79}$$

Regroupant (73), (74), (78) et (79), on a

$$\xi(f,X)=\frac{(2/3)^e}{2\pi^2}\prod_{p\mid f}\Big(1+\frac{1}{p}\Big)^{-1}\cdot\frac{X}{f^2}\Big(1+O\Big(\frac{1}{\log X}\Big)\Big) + O\left(X^{\frac{3}{4}+3\rho+3\varepsilon}+f^4X^{\frac{1}{4}+3\rho+11\varepsilon}+f^6X^{15\varepsilon}+\frac{X^{1-\rho+2\varepsilon}}{f}\right). \tag{80}$$

On démontre de même en utilisant le lemme 6.2 que, pour $3\nmid f$, on a

$$\xi_3(f,X)=\frac{1}{36}\cdot\frac{1}{2\pi^2}\prod_{p\mid f}\Big(1+\frac{1}{p}\Big)^{-1}\cdot\frac{X}{f^2}\Big(1+O\Big(\frac{1}{\log X}\Big)\Big) + O\left(X^{\frac{3}{4}+3\rho+3\varepsilon}+f^4X^{\frac{1}{4}+3\rho+11\varepsilon}+f^6X^{15\varepsilon}+\frac{X^{1-\rho+2\varepsilon}}{f}\right). \tag{81}$$

Pour tout p premier, on pose

$$a_p=\Big(1+\frac{1}{p}\Big)^{-1}, \qquad \text{pour } p\neq 3,$$
$$a_3=(2/3)\Big(1+\frac{1}{3}\Big)^{-1}=\frac{1}{2}; \qquad \text{pour } p=3,$$

puis on définit la fonction multiplicative

$$a_n=\mu^2(n)\prod_{p\mid n}a_p.$$

et on reporte (80) et (81) dans la formule du lemme 6.1. Choisissant $\rho=1/20$, on obtient

$$S(X,Y)=\frac{X}{2\pi^2}\Big(1+O\Big(\frac{1}{\log X}\Big)\Big)\left(\sum_{f\leqslant Y}a_f+\frac{81}{36}\cdot\sum_{\substack{f\leqslant Y/9\\(f,3)=1}}a_f\right) + O\Big(X^{15\varepsilon}\sum_{f\leqslant Y}\big\{(Xf^2)^{9/10}+f^4(Xf^2)^{2/5}+f^6+f^{-1}(Xf^2)^{19/20}\big\}\Big). \tag{82}$$

Le terme d'erreur de (82) est dominé par

$$\big(X^{9/10}Y^{14/5}+X^{\frac{2}{5}}Y^{29/5}+Y^7+X^{19/20}Y^{19/10}\big)X^{15\varepsilon}\ll\frac{XY}{\log X}, \tag{83}$$

sous l'hypothèse $1\leqslant Y\leqslant X^{(1/18)-1000\varepsilon}$. Regroupant (82) et (83), on termine la preuve de la première partie du théorème 1.2. La seconde s'obtient en considérant la série de Dirichlet $H(s)=\sum_{n=1}^{\infty}a_nn^{-s}$. La fonction $H(s)$ vérifie l'égalité

$$H(s)=\zeta(s)\frac{1+(1/2)3^{-s}}{1+(3/4)3^{-s}}\prod_p\left(1-\frac{1}{(p+1)p^s}-\frac{p}{(p+1)p^{2s}}\right),\quad(\operatorname{Re}s>1).$$

Un théorème taubérien donne, pour $Y \to \infty$, le comportement asymptotique

$$\sum_{n \leqslant Y} a_n \sim (H/\zeta)(1) \cdot Y.$$

De même, en corrigeant par la contribution du facteur eulérien en 3,

$$1 + \frac{a_3}{3} = \frac{7}{6},$$

on obtient

$$\sum_{\substack{n \leqslant Y \\ 3 \nmid n}} a_n \sim \frac{6}{7}(H/\zeta)(1) \cdot Y,$$

soit

$$\sum_{f \leqslant Y} a_f + \frac{81}{36} \cdot \sum_{\substack{f \leqslant Y/9 \\ (f,3)=1}} a_f \sim (H/\zeta)(1) \cdot \left(1 + \frac{81}{36} \cdot \frac{6}{7} \cdot \frac{1}{9}\right) \cdot Y = c_0' \cdot Y,$$

avec

$$c_0' = \frac{17}{14}\left(\frac{1+1/6}{1+1/4}\right) \prod_p \left(1 - \frac{2}{p(p+1)}\right) = \frac{17}{15} \prod_p \left(1 - \frac{2}{p(p+1)}\right).$$

□

6.5. **Preuve du théorème 1.1.** Il suffit de relier le problème des corps de groupe $S_3(6)$ à ce que nous venons de faire :

Lemme 6.5. *Soit K un corps cubique non galoisien, de discriminant Δf^2, avec Δ fondamental, $\Delta \neq 1$. Si L est la clôture galoisienne de $K/\mathbb{Q}$, alors* $\operatorname{disc} L = \Delta^3 f^4$.

Preuve. Soit $k = \mathbb{Q}(\sqrt{\Delta})$; Hasse [18, §3] montre que $\mathfrak{d}_{L/k} = f^2 \mathcal{O}_k$. Le résultat suit en ce qui concerne l'*idéal* discriminant. On vérifie que $\operatorname{disc} L$ et Δ ont même signe, puisque le nombre de places complexes de L et de k ont même parité. □

On se concentre sur le cas $\Delta > 0$. Puisque $\Delta^3 f^4 \leqslant X$ si et seulement si $(\Delta f^2)^3 \leqslant X f^2$, le nombre de corps sextiques L, galoisiens de groupe S_3 et discriminant $0 < \operatorname{disc} L \leqslant X$ est (cf. lemme 6.1)

$$\sum_f \mu^2(f) \xi\Big(f, (Xf^2)^{1/3}\Big) + \sum_f \mu^2(3f) \xi_3\Big(f, \big(X(9f)^2\big)^{1/3}\Big) + O(X^{1/2}),$$

où le terme reste provient de (8). Notons que ces deux sommes sont finies avec $f \leqslant X^{1/4}$. La technique est maintenant classique : on fixe $\varepsilon > 0$ très petit ; pour

$f > X^{5\varepsilon}$, on utilise le lemme 3.5 et, comme au (36), on obtient la majoration

$$\begin{aligned}\sum_{f>X^{5\varepsilon}} \xi\Big(f,(Xf^2)^{1/3}\Big)+\xi_3\Big(f,\big(X(9f)^2\big)^{1/3}\Big)&\\ \ll_\varepsilon X^\varepsilon \sum_{X^{5\varepsilon}<f\leqslant X^{1/4}} \left(\frac{(Xf^2)^{1/3}}{f^2}+\frac{(Xf^2)^{15/48}}{f^{15/8}}+\frac{(Xf^2)^{1/6}}{f}\right)&\\ \ll \frac{X^{1/3}}{\log X},&\end{aligned}$$

si ε est suffisamment petit. Pour $f \leqslant X^{5\varepsilon}$, on utilise de nouveau (80) et (81), pour obtenir

$$\begin{aligned}(84)\quad &\frac{1}{2\pi^2}\left(\sum_{f\leqslant X^{5\varepsilon}}\frac{a_f}{f^2}(Xf^2)^{1/3}+\frac{1}{36}\sum_{\substack{f\leqslant X^{5\varepsilon}\\(f,3)=1}}\frac{a_f}{f^2}(X(9f)^2)^{1/3}\right)\left(1+O\left(\frac{1}{\log X}\right)\right)\\ &+\sum_{f\leqslant X^{5\varepsilon}} O\left((Xf^2)^{\frac14+\rho+\varepsilon}+f^4(Xf^2)^{\frac{1}{12}+\rho+4\varepsilon}+f^6(Xf^2)^{5\varepsilon}+\frac{(Xf^2)^{(1-\rho+2\varepsilon)/3}}{f}\right),\end{aligned}$$

pour tout $0<\rho\leqslant 1/12$. Pour le choix $\rho=3\varepsilon$, le terme d'erreur est $\ll X^{1/3}/\log X$. Comme les deux séries en f sont convergentes, on obtient

$$S(X,Y)=KX^{1/3}\left(1+O\left(\frac{1}{\log X}\right)\right),$$

où

$$\begin{aligned}K &= \frac{1}{2\pi^2}\left(\sum_f\frac{a_f}{f^{4/3}}+\frac{3^{4/3}}{36}\sum_{(f,3)=1}\frac{a_f}{f^{4/3}}\right)\\ &= \frac{1}{2\pi^2}\left(1+\frac{a_3}{3^{4/3}}+\frac{3^{4/3}}{36}\right)\prod_{p\neq 3}\left(1+\frac{1}{(p+1)p^{1/3}}\right)\\ &= \frac{1}{2\pi^2}\left(1+\frac{2\cdot 3^{2/3}+3^{4/3}}{36}\right)\prod_{p\neq 3}\left(1+\frac{1}{(p+1)p^{1/3}}\right).\end{aligned}$$

La preuve pour les discriminants négatifs est analogue, avec une constante multipliée par 3. □

Références

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

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

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

[4] K. Belabas, On quadratic fields with large 3-rank, *Math. Comp.* **73** (2004), no. 248, pp. 2061–2074.
[5] K. Belabas, Paramétrisation de structures algébriques et densités de discriminants [d'après Bhargava], *Astérisque* (2005), no. 299, pp. 267–299, Séminaire Bourbaki. Vol. 2003/2004.
[6] K. Belabas, M. Bhargava, & C. Pomerance, Error estimates for the Davenport-Heilbronn theorems, *Duke Math. Journal* à paraître ; disponible sur `http://www.math.u-bordeaux1.fr/~belabas/pub/#BBP`.
[7] M. Bhargava, A simple proof of the Davenport-Heilbronn theorem, 1999, preprint.
[8] M. Bhargava & M. M. Wood, The density of discriminants of S_3-sextic number fields, *Proc. Amer. Math. Soc.* **136** (2008), no. 5, pp. 1581–1587.
[9] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993.
[10] H. Cohn, The density of abelian cubic fields, *Proc. Amer. Math. Soc.* **5** (1954), pp. 476–477.
[11] 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.
[12] H. Davenport, On the class number of binary cubic forms (ii), *J. Lond. Math. Soc.* **26** (1951), pp. 192–198.
[13] H. Davenport & H. Heilbronn, On the density of discriminants of cubic fields (i), *Bull. Lond. Math. Soc.* **1** (1969), pp. 345–348.
[14] H. Davenport & H. Heilbronn, On the density of discriminants of cubic fields (ii), *Proc. Roy. Soc. Lond. A* **322** (1971), pp. 405–420.
[15] B. N. Delone & D. K. Faddeev, *The theory of irrationalities of the third degree*, Translations of Mathematical Monographs, vol. 10, American Mathematical Society, 1964.
[16] J. S. Ellenberg & A. Venkatesh, Counting extensions of function fields with bounded discriminant and specified Galois group, in *Geometric methods in algebra and number theory* (Boston, MA), Progr. Math., vol. 235, Birkhäuser Boston, Boston, MA, 2005, pp. 151–168.
[17] É. Fouvry, Sur les propriétés de divisibilité des nombres de classes des corps quadratiques, *Bull. Soc. Math. France* **127** (1999), no. 1, pp. 95–113.
[18] H. Hasse, Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage, *Math. Zeitschrift.* **31** (1930), pp. 565–582.
[19] J. Klüners, A counterexample to Malle's conjecture on the asymptotics of discriminants, *C. R. Math. Acad. Sci. Paris* **340** (2005), no. 6, pp. 411–414.
[20] G. Malle, On the distribution of Galois groups, *J. Number Theory* **92** (2002), no. 2, pp. 315–329.
[21] G. Malle, On the distribution of Galois groups. II, *Experiment. Math.* **13** (2004), no. 2, pp. 129–135.
[22] 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.
[23] D. C. Mayer, Multiplicities of dihedral discriminants, *Math. Comp.* **58** (1992), no. 198, pp. 831–847, S55–S58.
[24] J. Nakagawa & K. Horie, Elliptic curves with no rational points, *Proc. Amer. Math. Soc.* **104** (1988), no. 1, pp. 20–24.
[25] S. Turkelli, Connected components of Hurwitz schemes and Malle's conjecture, 2008, `http://arxiv.org/abs/0809.0951`.

Karim Belabas, Université de Bordeaux, IMB – UMR 5251, 351 cours de la Libération, F-33405 Talence (France) • *E-mail*: `Karim.Belabas@math.u-bordeaux.fr`

Étienne Fouvry, Mathématiques – Bâtiment 425, Université de Paris-Sud F-91405 Orsay Cedex (France) • *E-mail* : Etienne.Fouvry@math.u-psud.fr