

BULLETIN DE LA S. M. F.

ÉTIENNE FOUVRY

Sur les propriétés de divisibilité des nombres de classes des corps quadratiques

Bulletin de la S. M. F., tome 127, n° 1 (1999), p. 95-113

http://www.numdam.org/item?id=BSMF_1999__127_1_95_0

© Bulletin de la S. M. F., 1999, tous droits réservés.

L'accès aux archives de la revue « Bulletin de la S. M. F. » (<http://smf.emath.fr/Publications/Bulletin/Presentation.html>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

**SUR LES PROPRIÉTÉS DE DIVISIBILITÉ
DES NOMBRES DE CLASSES DES
CORPS QUADRATIQUES**

PAR ÉTIENNE FOUVRY (*)

RÉSUMÉ. — On démontre qu'il y a une infinité de couples de discriminants fondamentaux positifs de la forme $(\Delta, \Delta + 4)$, tels que le groupe de classes d'idéaux de $\mathbb{Q}(\sqrt{\Delta})$ n'ait pas d'élément d'ordre 2 et tels que le groupe de classes d'idéaux de $\mathbb{Q}(\sqrt{\Delta + 4})$ n'ait pas d'élément d'ordre 3.

ABSTRACT. — ON DIVISIBILITY PROPERTIES OF CLASS NUMBERS OF QUADRATIC FIELDS. — We prove that there exist infinitely many pairs of positive fundamental discriminants of the form $(\Delta, \Delta + 4)$, such that the ideal class group of $\mathbb{Q}(\sqrt{\Delta})$ has no element of order 2 and such that the ideal class group of $\mathbb{Q}(\sqrt{\Delta + 4})$ has no element of order 3.

1. INTRODUCTION

Nous réservons la lettre p aux nombres premiers et la lettre Δ aux discriminants fondamentaux, c'est-à-dire aux entiers qui sont les discriminants d'extensions quadratiques de \mathbb{Q} . Rappelons que ces entiers ne sont divisibles par aucun carré de nombre premier impair et qu'ils sont congrus à 1, 5, 8, 9, 12 ou 13 modulo 16. Soit $\text{Cl}(\Delta)$ le groupe des classes d'idéaux de l'anneau des entiers de $\mathbb{Q}(\sqrt{\Delta})$. On désigne par $|\cdot|$ le cardinal d'un ensemble et on pose

$$h(\Delta) = |\text{Cl}(\Delta)|;$$

(*) Texte reçu le 24 avril 1998, accepté le 20 octobre 1998.

É. FOUVRY, Université de Paris-Sud, Mathématiques, Bât. 425, 91405 Orsay CEDEX.
Email : Etienne.Fouvry@math.u-psud.fr.

Classification AMS : 11N35, 11R11, 11R29, 11T23.

Mots clés : cribles, nombres de classes, corps quadratiques réels, sommes d'exponentielles.

c'est le nombre de classes. On appelle alors *p-rang* de $\mathbb{Q}(\sqrt{\Delta})$ l'entier $r_p(\Delta)$ défini par l'égalité

$$p^{r_p(\Delta)} = |C\ell(\Delta)/C\ell^p(\Delta)|.$$

Le nombre $r_2(\Delta)$ est bien connu grâce aux célèbres travaux de Gauss; il est intimement lié au nombre de facteurs premiers de Δ (voir critère 5.2 ci-dessous). Les autres $r_p(\Delta)$ sont pour l'instant très opaques, mis à part le cas particulier $p = 3$, puisque, grâce aux travaux de Davenport et Heilbronn (cf. [DH1], [DH2]), on connaît, pour $X \rightarrow \infty$, le comportement asymptotique des sommes

$$\sum_{0 < \pm\Delta \leq X} 3^{r_3(\Delta)}.$$

Toutefois les conjectures très profondes de Cohen et Lenstra [CL] prévoient, entre autres, pour les autres valeurs de p , le comportement statistique des $r_p(\Delta)$, lorsque Δ parcourt l'ensemble des discriminants fondamentaux des corps quadratiques, et prédisent l'indépendance statistique des valeurs des quantités $r_p(\Delta)$ et $r_{p'}(\Delta)$ pour p et p' nombres premiers fixés distincts; c'est dans cet esprit qu'il faut interpréter le résultat de Belabas et Fouvry [BF] qui, en poussant à l'extrême les méthodes de [Be], ont montré qu'il y a une infinité de p congrus à 1 modulo 4 tels que $r_3(p) = 0$.

Imaginons que soit donnée une fonction ψ raisonnable qui à un discriminant fondamental Δ associe un autre discriminant fondamental $\psi(\Delta)$. Si cette application n'a aucune propriété arithmétique particulière, rien n'empêche de conjecturer qu'il y a indépendance statistique des valeurs $r_p(\Delta)$ et $r_{p'}(\psi(\Delta))$ pour p et p' nombres premiers fixés, distincts ou non. C'est dans cette optique que Daniel et l'auteur [DF] ont montré que, étant donnés deux entiers k et ℓ positifs, il existe une infinité d'entiers $\Delta > 0$ tels que Δ et $\Delta + 4$ soient des discriminants fondamentaux et tels que $r_2(\Delta) = k$ et $r_2(\Delta + 4) = \ell$. En fait, à cause du critère 5.2 ci-dessous, le résultat de [DF] n'est pas un énoncé de théorie algébrique mais de théorie analytique des nombres, puisque les méthodes en cause pour sa preuve sont celles que l'on met en œuvre actuellement pour résoudre des équations linéaires en nombres premiers ou presque premiers. La fonction de Möbius sera désignée par μ .

Notre intention est de prouver le :

THÉORÈME. — *Il existe une infinité de discriminants fondamentaux positifs Δ congrus à 1 modulo 4 ayant les propriétés suivantes :*

- (i) $\Delta + 4$ est lui-aussi un discriminant fondamental,
- (ii) $h(\Delta)$ est impair,

(iii) $h(\Delta + 4)$ n'est pas divisible par 3.

Plus précisément, il existe une constante $c_0 > 0$, telle que, pour X suffisamment grand, on ait l'inégalité

$$\left| \left\{ \Delta; 5 \leq \Delta \leq X, \Delta \equiv 1 \pmod{4}, \right. \right. \\ \left. \left. \mu^2(\Delta) = \mu^2(\Delta + 4) = 1, r_2(\Delta) = r_3(\Delta + 4) = 0 \right\} \right| \\ \geq c_0 \frac{X}{\log X}.$$

Cet énoncé montre une certaine indépendance entre le 2-rang de $\mathbb{Q}(\sqrt{\Delta})$ et le 3-rang de $\mathbb{Q}(\sqrt{\Delta + 4})$. L'intérêt de ce travail réside aussi dans les outils très puissants de géométrie algébrique qui apparaîtront pour majorer des sommes trigonométriques (voir lemme 2.4). Enfin signalons que, pour l'instant, on ne sait pas démontrer un énoncé analogue pour les $\Delta < 0$; à cela deux raisons : le 3-rang des corps quadratiques imaginaires est en moyenne plus grand que celui des réels et le critère pour obtenir des corps quadratiques imaginaires de nombres de classes impairs est plus restrictif.

Pour terminer, si dans la proposition 4.1, on pouvait remplacer l'exposant $\frac{1}{3} - \varepsilon$ par un exposant strictement plus grand que $\frac{1}{3}$, on aurait prouvé l'existence d'une infinité de $p \equiv 1$ modulo 4 tels que $p + 4$ soit sans facteur carré et tel que $r_3(p + 4)$ soit nul.

2. Notations. Lemmes préparatoires

a) Nombre de solutions de congruence.

On note

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

le discriminant de la forme cubique

$$F = (a, b, c, d) = ax^3 + bx^2y + cxy^2 + dy^3.$$

Nous aurons besoin du :

LEMME 2.1. — Pour ℓ entier et q entier sans facteur carré, on désigne par $\rho(q, \ell)$ le nombre de solutions à l'équation

$$\Delta(a, b, c, d) \equiv \ell \pmod{q}.$$

La fonction $\rho(q, \ell)$ est multiplicative et vérifie les égalités

$$\rho(p, \ell) = \begin{cases} p(p^2 + p - 1) & \text{si } p \mid \ell, \\ p^3 - p & \text{si } p \nmid \ell. \end{cases}$$

Le cas de $\rho(p, \ell)$ pour $p \nmid \ell$ est prouvé dans [NaHo, prop. 1] et celui de $\rho(p, 0)$ dans [Be, lemme 4.6], lui-même hérité de [DH2, lemma 1]. \square

LEMME 2.2. — Pour p nombre premier impair, on désigne par $p^8\xi(p)$ le nombre de solutions à l'équation

$$\Delta(a, b, c, d) \equiv 0 \pmod{p^2}$$

et par $16^4\xi(2)$ le nombre de solutions aux congruences

$$\Delta(a, b, c, d) \in \{0, 2, 3, 4, 6, 7, 10, 11, 13, 14, 15\} \pmod{16}.$$

Pour tout p , on a alors l'égalité

$$\xi(p) = \frac{2}{p^2} - \frac{1}{p^4}.$$

L'ensemble des congruences ci-dessus constitue l'ensemble des congruences interdites à un discriminant fondamental, et dans le cas de $p = 2$, puisqu'on a toujours $\Delta(a, b, c, d) \equiv 0$ ou 1 modulo 4 , il revient au même de considérer l'ensemble plus petit $\{0, 4\}$ (modulo 16).

La valeur de la fonction ξ , qui, par le principe d'inclusion-exclusion nous permettra d'accéder à des valeurs de la fonction $\Delta(a, b, c, d)$ qui sont des discriminants fondamentaux, est extraite de [DH2, lemma 1] et se retrouve dans [Be, lemme 4.6]. \square

b) Sommes d'exponentielles.

Soit, pour q et r entiers ≥ 1 , la somme

$$\begin{aligned} S(\mathbf{h}; q, r^2) &= S(h_1, h_2, h_3, h_4; q, r^2) \\ &= \sum_{(a, b, c, d) \bmod qr^2} \exp\left(2\pi i \frac{ah_1 + bh_2 + ch_3 + dh_4}{qr^2}\right) \end{aligned}$$

la somme étant faite sur les (a, b, c, d) modulo qr^2 tels que

$$\Delta(a, b, c, d) + 4 \equiv 0 \pmod{q} \quad \text{et} \quad \Delta(a, b, c, d) \equiv 0 \pmod{r^2}.$$

Cette somme trigonométrique vérifie la relation de multiplicativité croisée :

LEMME 2.3. — Si q_1, q_2 et r sont des entiers premiers entre eux deux à deux, on a l'égalité

$$S(\mathbf{h}; q_1q_2, r^2) = S(\overline{q_1r^2} \mathbf{h}; q_2, 1) S(\overline{q_2r^2} \mathbf{h}; q_1, 1) S(\overline{q_1q_2} \mathbf{h}; 1, r^2),$$

valable pour tout quadruplet d'entiers \mathbf{h} . On a désigné par $\overline{q_1r^2}$ l'inverse multiplicatif de q_1r^2 modulo q_2 ; les quantités $\overline{q_2r^2}$ et $\overline{q_1q_2}$ le sont de façon similaire.

C'est une application itérée du théorème chinois. \square

Le point important de la preuve sera de majorer la somme

$$S(\mathbf{h}; q) = S(\mathbf{h}; q, 1) = \sum_{\substack{(a,b,c,d) \pmod q \\ \Delta(a,b,c,d)+4 \equiv 0 \pmod q}} \exp\left(2\pi i \frac{ah_1 + bh_2 + ch_3 + dh_4}{q}\right),$$

puisque nous majorerons trivialement les sommes $S(\mathbf{h}; 1, r^2)$. Le lemme suivant est dû essentiellement à Katz et Laumon [KaLa], et repose sur des méthodes très avancées de géométrie algébrique. Nous l'utiliserons sous la forme qu'en a donnée l'auteur [Fo]. Nous nous restreignons au cas de la variété définie par $\Delta(a, b, c, d) + 4 = 0$. On a :

LEMME 2.4. — *Il existe une constante absolue C et des fermés homogènes V_j de $\mathbb{A}_{\mathbb{Z}}^4$ ($j = 1, 2$), de codimension j , tels que, pour tout p , on ait les propriétés suivantes :*

(i) *pour tout \mathbf{h} non nul de \mathbb{F}_p^4 , on a l'inégalité*

$$|S(\mathbf{h}; p)| \leq Cp^{\frac{5}{2}},$$

(ii) *pour tout \mathbf{h} hors de $V_j(\mathbb{F}_p)$, on a l'inégalité*

$$|S(\mathbf{h}; p)| \leq Cp^{\frac{3}{2} + \frac{j-1}{2}}.$$

Le point (i) est une conséquence de [Fo, prop. 1.2]. Toutefois, pour l'appliquer, il faut vérifier que le polynôme $\Delta(x, y, z, t) + 4$, comme polynôme de $\mathbb{C}[x, y, z, t]$, n'est divisible par aucun polynôme de degré 1. Ceci se montre directement.

Soit $P(x, y, z, t)$ un polynôme du premier degré divisant $\Delta(x, y, z, t) + 4$. Si le coefficient de x est non nul, on voit qu'il existe des nombres complexes α, β, γ et δ tels que le polynôme

$$\Delta(\alpha y + \beta z + \gamma t + \delta, y, z, t) + 4$$

soit formellement nul. Mais ceci est impossible, puisque le polynôme précédent, considéré comme polynôme de $\mathbb{C}[y, z, t]$ a pour terme constant 4. Le raisonnement est identique si le coefficient de y , de z ou de t dans le polynôme $P(x, y, z, t)$ est non nul. On peut donc appliquer la proposition 1.2 de [Fo].

Le point (ii) est une conséquence de [Fo, prop. 1.0]. \square

Nous utiliserons le lemme 2.4 sous la forme suivante (nous notons $\|\alpha\|$ la distance du réel α à l'entier le plus proche) :

PROPOSITION 2.5. — Soient q et r des entiers tels que q soit sans facteur carré et tels que $(q, r) = 1$. Soit $K(X; q, r^2)$ la somme

$$K(X; q, r^2) = \frac{1}{q^4 r^8} \sum_{\mathbf{h} \neq \mathbf{0} \pmod{qr^2}} \min \left(X, \left\| \frac{h_1}{qr^2} \right\|^{-1} \right) \min \left(X, \left\| \frac{h_2}{qr^2} \right\|^{-1} \right) \min \left(X, \left\| \frac{h_3}{qr^2} \right\|^{-1} \right) \min \left(X, \left\| \frac{h_4}{qr^2} \right\|^{-1} \right) |S(\mathbf{h}; q, r^2)|.$$

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

$$K(X; q, r^2) = O_\varepsilon \left(r^8 (q^{\frac{3}{2}} + q^{\frac{1}{2}} X^2 + q^{-\frac{3}{2}} X^4) (qrX)^\varepsilon \right).$$

Démonstration. — Notons que la dépendance en r de cette majoration est sans importance, puisque nous l'appliquerons avec r borné, et que, lorsque q est premier, la majoration de $K(X; q, 1)$ est une conséquence de [Fo, § II].

On écrit q sous la forme $q = p_1 \cdots p_s$. Le lemme 2.3, l'homogénéité des variétés V_1 et V_2 introduites dans le lemme 2.4, la majoration triviale $|S(\mathbf{h}; 1, r^2)| \leq r^8$ et les inclusions $\{\mathbf{0}\} \subset V_2 \subset V_1 \subset \mathbb{F}_p^4$ entraînent, pour tout \mathbf{h} modulo qr^2 , l'inégalité

$$|S(\mathbf{h}; q, r^2)| \leq C^s r^8 q^{\frac{3}{2}} \prod_{\substack{p|q \\ \mathbf{h}(\pmod{p}) \in V_1(\mathbb{F}_p)}} p^{\frac{1}{2}} \prod_{\substack{p|q \\ \mathbf{h}(\pmod{p}) \in V_2(\mathbb{F}_p)}} p^{\frac{1}{2}} \prod_{\substack{p|q \\ p|\mathbf{h}}} p^{\frac{1}{2}}.$$

Pour alléger l'écriture, on pose

$$\Xi(\alpha) = \min(X, \|\alpha\|^{-1}).$$

On décompose alors $K(X; q, r^2)$ sous la forme

$$(2.1) \quad K(X; q, r^2) \leq q^{-\frac{5}{2}} C^s (K_0(X; q, r^2) + K_1(X; q, r^2) + K_2(X; q, r^2) + K_3(X; q, r^2)),$$

avec

$$K_0(X; q, r^2) = \sum_{\mathbf{h} \pmod{qr^2}} \Xi\left(\frac{h_1}{qr^2}\right) \Xi\left(\frac{h_2}{qr^2}\right) \Xi\left(\frac{h_3}{qr^2}\right) \Xi\left(\frac{h_4}{qr^2}\right),$$

$$K_1(X; q, r^2) = \sum_{\mathbf{h} \pmod{qr^2}} \Xi\left(\frac{h_1}{qr^2}\right) \Xi\left(\frac{h_2}{qr^2}\right) \Xi\left(\frac{h_3}{qr^2}\right) \Xi\left(\frac{h_4}{qr^2}\right) \prod_{\substack{p|q \\ \mathbf{h}(\pmod{p}) \in V_1(\mathbb{F}_p)}} p^{\frac{1}{2}},$$

$$K_2(X; q, r^2) = \sum_{\mathbf{h} \pmod{qr^2}} \Xi\left(\frac{h_1}{qr^2}\right) \Xi\left(\frac{h_2}{qr^2}\right) \Xi\left(\frac{h_3}{qr^2}\right) \Xi\left(\frac{h_4}{qr^2}\right) \prod_{\substack{p|q \\ \mathbf{h}(\pmod{p}) \in V_2(\mathbb{F}_p)}} p,$$

$$K_3(X; q, r^2) = \sum_{\mathbf{h} \neq \mathbf{0} \pmod{qr^2}} \Xi\left(\frac{h_1}{qr^2}\right) \Xi\left(\frac{h_2}{qr^2}\right) \Xi\left(\frac{h_3}{qr^2}\right) \Xi\left(\frac{h_4}{qr^2}\right) \prod_{\substack{p|q \\ p|\mathbf{h}}} p^{\frac{3}{2}}.$$

b.1) *Étude de $K_0(X; q, r^2)$.* — On a directement la majoration

$$(2.2) \quad K_0(X; q, r^2) \ll q^4 r^8 (\log qr)^4.$$

b.2) *Étude de $K_1(X; q, r^2)$.* — Cette étude est plus délicate. En sommant d'abord sur les diviseurs de q , on a

$$(2.3) \quad K_1(X; q, r^2) \leq \sum_{\delta|q} \delta^{\frac{1}{2}} \sum_{\substack{\mathbf{h} \bmod qr^2 \\ \forall p|\delta, \mathbf{h} \pmod p \in V_1(\mathbb{F}_p)}} \Xi\left(\frac{h_1}{qr^2}\right) \Xi\left(\frac{h_2}{qr^2}\right) \Xi\left(\frac{h_3}{qr^2}\right) \Xi\left(\frac{h_4}{qr^2}\right).$$

Appelons W_1 l'image de V_1 par l'application $(x_1, x_2, x_3, x_4) \mapsto (x_1, x_2, x_3)$. L'ensemble W_1 est une variété de dimension ≤ 3 . On note \widetilde{W}_1 le sous-ensemble de W_1 , constitué des (x_1, x_2, x_3) tels que, pour tout $x \in \mathbb{F}_p$, le point (x_1, x_2, x_3, x) appartient à $V_1(\mathbb{F}_p)$. Notons que $\widetilde{W}_1(\mathbb{F}_p)$ est une variété de dimension ≤ 2 . On décompose alors $K_1(X; q, r^2)$ en

$$K_1(X; q, r^2) \leq \sum_{\delta|q} \delta^{\frac{1}{2}} \sum_{\delta=\delta_1\delta_2} \sum_{\substack{(h_1, h_2, h_3) \bmod qr^2 \\ \forall p|\delta_1, (h_1, h_2, h_3) \in \widetilde{W}_1(\mathbb{F}_p) \\ \forall p|\delta_2, (h_1, h_2, h_3) \in W_1(\mathbb{F}_p) - \widetilde{W}_1(\mathbb{F}_p)}} \Xi\left(\frac{h_1}{qr^2}\right) \Xi\left(\frac{h_2}{qr^2}\right) \Xi\left(\frac{h_3}{qr^2}\right) \sum_{\substack{h_4 \bmod qr^2 \\ \forall p|\delta, (h_1, h_2, h_3, h_4) \in V_1(\mathbb{F}_p)}} \Xi\left(\frac{h_4}{qr^2}\right).$$

Pour évaluer la somme sur h_4 , on remarque que h_4 , modulo qr^2 , est de la forme

$$h_4 = \nu_4 + \lambda\delta_2$$

où $0 \leq \nu_4 < \delta_2$ et ne prend que $O(\delta_2^\varepsilon)$ et λ vérifiant $0 \leq \lambda < qr^2/\delta_2$. En effet, si $p \mid \delta_2$ et si (h_1, h_2, h_3) est fixé dans $W_1(\mathbb{F}_p) - \widetilde{W}_1(\mathbb{F}_p)$, il y a $O(1)$ choix pour h_4 modulo p pour que (h_1, h_2, h_3, h_4) appartienne à $V_1(\mathbb{F}_p)$. Lorsque $\lambda = 0$ ou $\lambda = qr^2/\delta_2 - 1$, on prend la majoration $\Xi \leq X$, sinon on somme la série harmonique en h_4 . On a donc

$$\sum_{\substack{h_4 \bmod qr^2 \\ \forall p|\delta, (h_1, h_2, h_3, h_4) \in V_1(\mathbb{F}_p)}} \Xi\left(\frac{h_4}{qr^2}\right) \ll r^2 \left(X + \frac{q}{\delta_2}\right) (qrX)^\varepsilon.$$

On oublie maintenant la condition $(h_1, h_2, h_3) \in W_1(\mathbb{F}_p) - \widetilde{W}_1(\mathbb{F}_p)$, et on itère le procédé; on a donc l'inégalité

$$K_1(X; q) \ll r^2 \sum_{\delta|q} \delta^{\frac{1}{2}} \sum_{\delta=\delta_1\delta_2} \left(X + \frac{q}{\delta_2}\right) (qrX)^\varepsilon \sum_{\substack{(h_1, h_2, h_3) \bmod qr^2 \\ \forall p|\delta_1, (h_1, h_2, h_3) \in \widetilde{W}_1(\mathbb{F}_p)}} \Xi\left(\frac{h_1}{qr^2}\right) \Xi\left(\frac{h_2}{qr^2}\right) \Xi\left(\frac{h_3}{qr^2}\right).$$

Nous sommes ramenés au cas de l'inégalité (2.3), la variété V_1 étant remplacée par \widetilde{W}_1 et δ par δ_1 , d'où l'inégalité

$$K_1(X; q) \ll r^4 (qrX)^\varepsilon \sum_{\delta|q} \delta^{\frac{1}{2}} \sum_{\delta=\delta_1\delta_2} \left(X + \frac{q}{\delta_2}\right) \sum_{\substack{(h_1, h_2) \bmod qr^2 \\ \forall p|\delta_3, (h_1, h_2) \in \widetilde{W}_2(\mathbb{F}_p)}} \Xi\left(\frac{h_1}{qr^2}\right) \Xi\left(\frac{h_2}{qr^2}\right),$$

avec \widetilde{W}_2 variété de dimension ≤ 1 , soit encore

$$K_1(X; q) \ll r^8 (qrX)^\varepsilon \sum_{\delta|q} \delta^{\frac{1}{2}} \sum_{\delta=\delta_1\delta_2} \left(X + \frac{q}{\delta_2}\right) \sum_{\delta_1=\delta_3\delta_4} \left(X + \frac{q}{\delta_4}\right) \sum_{\delta_3=\delta_5\delta_6} \left(X + \frac{q}{\delta_6}\right) X,$$

puis en sommant sur les δ_i on obtient finalement

$$(2.4) \quad K_1(X, q) \ll r^8 \left(q^{\frac{1}{2}} X^4 + q^{\frac{7}{2}} X\right) (qrX)^\varepsilon.$$

b.3) Étude de $K_2(X; q)$. — L'étude est très proche de celle faite auparavant; toutefois la variété de départ V_1 est de dimension 2 (au lieu de 3), le facteur $\delta^{\frac{1}{2}}$ est remplacé par δ . On parvient alors à

$$(2.5) \quad K_2(X, q) \ll r^8 \left(qX^4 + q^3X^2\right) (qrX)^\varepsilon.$$

b.4) Étude de $K_3(X; q)$. — C'est pour cette somme uniquement qu'on utilise le fait que \mathbf{h} n'est pas nul modulo qr^2 . On majore $K_3(X; q)$ par

$$K_3(X; q) \leq \sum_{\substack{\delta|qr^2 \\ \delta \neq qr^2}} \delta^{\frac{3}{2}} \sum_{\substack{\mathbf{h} \neq 0 \bmod qr^2 \\ \delta|\mathbf{h}}} \Xi\left(\frac{h_1}{qr^2}\right) \Xi\left(\frac{h_2}{qr^2}\right) \Xi\left(\frac{h_3}{qr^2}\right) \Xi\left(\frac{h_4}{qr^2}\right).$$

On pose alors

$$(h_1, h_2, h_3, h_4) = \delta(n_1, n_2, n_3, n_4)$$

avec $0 \leq n_1, n_2, n_3, n_4 \leq qr^2/\delta$ et $\mathbf{n} \neq \mathbf{0}$; on obtient après sommation sur les n_i et en séparant suivant le nombre de n_i non nuls

$$(2.6) \quad K_3(X; q) \ll \sum_{\delta|qr^2} \delta^{\frac{3}{2}} ((qr^2\delta^{-1})^4 + X(qr^2\delta^{-1})^3 + X^2(qr^2\delta^{-1})^2 + X^3(qr^2\delta^{-1})) \log^4(qr),$$

soit encore

$$K_3(X; q) \ll r^8 (q^4 + q^3 X + q^2 X^2 + q^{\frac{3}{2}} X^3) (qX)^{\varepsilon}.$$

En regroupant (2.1), (2.2), (2.4), (2.5) et (2.6), on obtient l'inégalité

$$K(X; q) \ll r^8 (q^{\frac{3}{2}} + qX + q^{\frac{1}{2}} X^2 + q^{-1} X^3 + q^{-\frac{3}{2}} X^4) (qX)^{\varepsilon},$$

ce qui donne la proposition 2.4 en utilisant la relation $2\sqrt{AB} \leq A + B$ valable pour A et B positifs. \square

3. Formes cubiques

L'objet de ce paragraphe est de rappeler tout ce qu'il faut retenir du travail de Davenport et Heilbronn sur l'étude du 3-rang des corps quadratiques (cf. [DH1], [DH2]) et qui, bien entendu réapparaît dans [Be] et [BF], par exemple.

Soit $\mathcal{H}(\Delta)$ la fonction $\frac{1}{2}(3^{r_3(\Delta)} - 1)$; si n n'est pas un discriminant fondamental, on pose $\mathcal{H}(n) = 0$. Soit $\tilde{\mathcal{V}}$ le volume de \mathbb{R}^4 défini comme étant l'ensemble des quadruplets (a, b, c, d) vérifiant

$$a \geq 1 \quad \text{et} \quad \begin{cases} \text{soit} & -A < B \leq A < C, \\ \text{soit} & 0 \leq B \leq A = C, \end{cases}$$

où les fonctions A, B et C sont définies par les formules

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

(rappelons que la forme quadratique $Ax^2 + Bxy + Cy^2$ est la forme hessienne associée à $ax^3 + bx^2y + cxy^2 + dy^3$ et que son discriminant est $-3\Delta(a, b, c, d)$). On a la :

PROPOSITION 3.1. — *Pour tout discriminant fondamental $\Delta > 0$, on a l'égalité*

$$\mathcal{H}(\Delta) = \frac{1}{2} |\{(a, b, c, d) \in \tilde{\mathcal{V}}; ax^3 + bx^2y + cxy^2 + dy^3 \text{ irréductible} \\ \text{et } \Delta(a, b, c, d) = \Delta\}|.$$

Nous n'étudierons pas la répartition de la fonction \mathcal{H} dans les progressions arithmétiques (voir [NaHo, th. 1], pour le cas d'une progression fixée), mais celle d'une fonction majorant \mathcal{H} , ce qui nous permettra d'oublier quasiment la condition très ennuyeuse d'être un discriminant fondamental. Signalons que, pour tout entier n , on a de façon triviale l'inégalité

$$(3.1) \quad \mathcal{H}(n) \leq \frac{1}{2} g(n)$$

avec

$$g(n) = |\{(a, b, c, d) \in \mathcal{V}; \Delta(a, b, c, d) = n\}|$$

pour tout entier $n \geq 1$, où \mathcal{V} est un ensemble plus grand que $\tilde{\mathcal{V}}$:

$$\mathcal{V} = \{(a, b, c, d); a \geq 1, |B| \leq A \leq C\}.$$

L'inégalité est raffinée de la façon suivante. Soit P un entier fixé ≥ 3 ; on pose alors :

- $g_P(n) = 0$ si n n'est pas congru à 1, 5, 8, 9, 12 ou 13 modulo 16 ou si n est divisible par le carré d'un nombre premier impair inférieur à P ;
- $g_P(n) = g(n)$ dans le cas contraire.

On pose enfin

$$(3.2) \quad \mathcal{H}_P(n) = \frac{1}{2} g_P(n).$$

On a donc, pour tout $P \geq 2$, et tout $n > 0$, l'inégalité

$$(3.3) \quad \mathcal{H}(n) \leq \mathcal{H}_P(n).$$

Cette inégalité est d'autant meilleure que P est grand puisque le support de la fonction \mathcal{H}_P épouse de mieux en mieux la fonction caractéristique de l'ensemble des discriminants fondamentaux.

4. Théorèmes d'équirépartition

Pour utiliser les formules de crible, nous contrôlerons le terme d'erreur par la

PROPOSITION 4.1. — *Pour tout $\varepsilon > 0$ et tout $P \geq 3$, on a la majoration*

$$(4.1) \quad \sum_{q \leq X^{\frac{1}{3}-\varepsilon}} \mu^2(q) \left| \sum_{\substack{n \leq X \\ q|n}} g_P(n+4) - \frac{\nu_P(q)}{q} \sum_{n \leq X} g(n) \right| = O_{\varepsilon, P}(X \log^{-2} X),$$

avec

$$\nu_P(q) = \prod_{p|q} \frac{\rho(p, 4)}{p^3} \prod_{\substack{p \leq P \\ p \nmid q/(2, q)}} \left(1 - \xi(p) \frac{(2, q, p)^4}{\rho((2, q, p), 4)} \right),$$

où les fonctions ρ et ξ sont définis lors des lemmes 2.1 et 2.2.

a) Réduction de la preuve de la proposition.

Pour prouver la proposition 4.1, il suffit de montrer la même relation mais pour la fonction $g_P(n, Y)$, avec $Y = X^{\frac{1}{4}-3\eta}$ et $\eta > 0$ très petit, à savoir

$$(4.2) \quad \sum_{q \leq X^{\frac{1}{3}-\varepsilon}} \mu^2(q) \left| \sum_{\substack{n \leq X \\ q|n}} g_P(n+4, Y) - \frac{\nu_P(q)}{q} \sum_{n \leq X} g(n, Y) \right| = O_{\varepsilon, P}(X \log^{-2} X),$$

où $g_P(n, Y)$ et $g(n, Y)$ sont définis comme $g_P(n)$ et $g(n)$ à la différence près que la condition $a \geq 1$ est remplacée par $a \geq Y$, dans la définition de \mathcal{V} . En effet, on sait (cf. [Da, Lemma 4]) qu'on a la majoration

$$|\mathcal{E}| := \left| \{(a, b, c, d) \in \mathcal{V}, 1 \leq \Delta(a, b, c, d) \leq X, a \leq X^{\frac{1}{4}-3\eta}\} \right| = O(X^{1-\eta}).$$

Le remplacement de $g_P(n)$ et de $g(n)$ par $g_P(n, Y)$ et $g(n, Y)$ introduit dans la partie gauche de (4.1) une erreur en

$$O\left(\sum_{(a, b, c, d) \in \mathcal{E}} \tau(\Delta(a, b, c, d) + 4) \right) = O(X^{1-\eta/2}),$$

ce qui est acceptable. La lettre τ désigne la fonction nombre de diviseurs.

Enfin, par le principe d'inclusion-exclusion, pour parvenir à (4.2), il suffit de vérifier, pour tout r , sans facteur carré, ayant tous ses facteurs premiers inférieurs à P , qu'on a la relation

$$(4.3) \quad \sum_{\substack{q \leq X^{\frac{1}{3}-\varepsilon} \\ (q,r)=1 \text{ ou } 2}} \mu^2(q) \left| \sum_{\substack{n \leq X, q|n \\ n+4 \in \mathcal{C}(r^2)}} g(n+4, Y) - \prod_{\substack{p|q \\ p \equiv 1 \pmod{2, q, r}}} \frac{\rho(p, 4)}{p^4} \prod_{p|r} \xi(p) \sum_{n \leq X} g(n, Y) \right| = O_{\varepsilon, r}(X \log^{-2} X),$$

où, en désignant par r' le plus grand entier impair divisant r , on a posé

$$\mathcal{C}(r^2) = \left\{ n; r'^2 \mid n \text{ et } n \equiv 0, 4 \pmod{\left(\frac{r}{r'}\right)^4} \right\}.$$

On voit que le cas où r est pair est plus compliqué à écrire que le cas où r est impair. Cette difficulté supplémentaire, uniquement confinée à un problème de notations, nous incite à nous restreindre à prouver (4.3) dans le cas où r est impair. Nous nous restreignons donc au cas où r est impair.

b) Découpage.

Soit \mathcal{W} le volume défini par

$$\mathcal{W} = \{ (a, b, c, d); a \geq Y, 1 \leq \Delta(a, b, c, d) \leq X, |B| \leq A \leq C \}.$$

Puisque r est impair, la preuve de (4.3) revient à montrer la relation

$$(4.4) \quad \sum_{\substack{q \leq X^{\frac{1}{3}-\varepsilon} \\ (q,r)=1}} \mu^2(q) \left| \sum_{\substack{M \in \mathcal{W} \\ \Delta(M)+4 \equiv 0 \pmod{q} \\ \Delta(M) \equiv 0 \pmod{r^2}}} 1 - \prod_{p|q} \frac{\rho(p, 4)}{p^4} \prod_{p|r} \xi(p) \sum_{M \in \mathcal{W}} 1 \right| = O_{\varepsilon, r}(X \log^{-2} X),$$

où M symbolise le point (a, b, c, d) . La technique de [BF, prop. 2.11] affirme que pour tout $Q \geq 1$ il existe un ensemble de $O(XQ^{-4})$ hypercubes disjoints, notés \mathcal{B}_i (avec i appartenant à un certain ensemble d'indices \mathcal{I}), de côtés de longueur Q , parallèles aux axes de coordonnées, dont la réunion est incluse dans \mathcal{W} et tels qu'on ait pour $\mathcal{D} := \mathcal{W} - \bigcup_{i \in \mathcal{I}} \mathcal{B}_i$ la majoration

$$(4.5) \quad |\mathcal{D} \cap \mathbb{Z}^4| = O(X^{1-\eta} + QX^{\frac{3}{4}+3\eta} \log X + Q^3 X^{\frac{1}{4}+3\eta} + Q^4).$$

On pose alors

$$Q = X^{\frac{1}{4}-5\eta};$$

ainsi par (4.5), le cardinal des points M de \mathcal{W} n'appartenant à aucun des \mathcal{B}_i est en $O(X^{1-\eta})$, c'est-à-dire négligeable, nous déduisons donc

$$\sum_{\substack{q \leq X^{\frac{1}{3}-\varepsilon} \\ (q,r)=1}} \mu^2(q) \left| \sum_{\substack{M \in \mathcal{D} \\ \Delta(M)+4 \equiv 0 \pmod{q} \\ \Delta(M) \equiv 0 \pmod{r^2}}} 1 - \prod_{p|q} \frac{\rho(p,4)}{p^4} \prod_{p|r} \xi(p) \sum_{M \in \mathcal{D}} 1 \right| = O_{\varepsilon,r}(X(\log X)^{-2}),$$

puisque la somme est, après interversion de sommations, majorée en

$$O\left(\sum_{M \in \mathcal{D}} \tau(\Delta(M) + 4)\right).$$

C'est ici que nous avons utilisé l'effet de moyenne sur q . Pour montrer la relation (4.4) et par conséquent la proposition 4.1, il suffit de montrer que, pour tout $i \in \mathcal{I}$, pour tout $q \leq X^{\frac{1}{3}-\varepsilon}$, premier avec r , on a la relation

$$(4.6) \quad \sum_{\substack{M \in \mathcal{B}_i \\ \Delta(M)+4 \equiv 0 \pmod{q} \\ \Delta(M) \equiv 0 \pmod{r^2}}} 1 = \prod_{p|q} \frac{\rho(p,4)}{p^4} \prod_{p|r} \xi(p) \sum_{M \in \mathcal{B}_i} 1 + O_{\varepsilon,r}(q^{-1}Q^4 \log^{-3} X).$$

c) Preuve de (4.6).

Supposons que $\mathcal{B}_i = \mathcal{B} = [x_1; x_1 + Q] \times \cdots \times [x_4; x_4 + Q]$ et, dans un premier temps qu'on a l'inégalité

$$(4.7) \quad Q \leq qr^2.$$

On développe en série de Fourier la fonction caractéristique de l'intervalle $[x_i; x_i + Q]$. La partie gauche de (4.6) devient donc

$$\frac{1}{q^4 r^8} \sum_{(h_1, h_2, h_3, h_4) \pmod{qr^2}} \sum_{(x_1, x_2, x_3, x_4) \in \mathcal{B}} \exp\left(2\pi i \frac{h_1 x_1 + h_2 x_2 + h_3 x_3 + h_4 x_4}{qr^2}\right) S(\mathbf{h}; q, r^2),$$

où la fonction $S(\mathbf{h}; q, r^2)$ est définie au lemme 2.3. Le terme $\mathbf{h} = (0, 0, 0, 0)$ donne le terme principal à droite de (4.6). La contribution des autres \mathbf{h}

est un terme d'erreur noté $E(Q; q, r^2)$. En sommant les progressions géométriques sur les x_i , on a l'inégalité

$$|E(Q; q, r^2)| \ll \frac{1}{q^4 r^8} \sum_{\mathbf{h} \neq \mathbf{0} \pmod{qr^2}} \min\left(Q, \left\| \frac{h_1}{qr^2} \right\|^{-1}\right) \min\left(Q, \left\| \frac{h_2}{qr^2} \right\|^{-1}\right) \min\left(Q, \left\| \frac{h_3}{qr^2} \right\|^{-1}\right) \min\left(Q, \left\| \frac{h_4}{qr^2} \right\|^{-1}\right) |S(\mathbf{h}; q, r^2)|,$$

et cette quantité est exactement la quantité $K(Q; q, r^2)$ traitée dans la proposition 2.5. On a donc

$$E(Q; q, r^2) \ll_{\varepsilon} \left(q^{\frac{3}{2}} + q^{\frac{1}{2}} Q^2 + q^{-\frac{3}{2}} Q^4 \right) X^{\varepsilon}$$

et la formule (4.6) est démontrée pourvu que $\varepsilon = 10\eta$.

Enfin, dans le cas où l'inégalité (4.7) n'est pas vérifiée, c'est-à-dire lorsque $qr^2 < Q$ est satisfaite, on voit que \mathcal{B}_i est la réunion disjointe d'un certain nombre d'hypercubes $\mathcal{B}_{i,j}$ dont les côtés sont tous de longueur qr^2 et de $O((Qq^{-1}r^{-2})^3)$ parallélépipèdes rectangles $\mathcal{C}_{i,k}$ dont tous les côtés sont de longueur $\leq qr^2$ et un au moins de longueur $< qr^2$. On s'intéresse alors à prouver un analogue de (4.6), pour chaque $\mathcal{B}_{i,j}$ et chaque $\mathcal{C}_{i,k}$. Le cas des $\mathcal{B}_{i,j}$ est trivial, puisqu'on a un système complet de résidus modulo qr^2 , l'analogue de (4.6) est alors vrai sans terme d'erreur. Le cas des $\mathcal{C}_{i,k}$ est plus délicat, mais est très proche du cas où (4.7) est vérifiée; nous ne faisons donc que l'esquisser. En développant en série de Fourier la fonction caractéristique de chaque $\mathcal{C}_{i,k}$, et en appliquant les lemmes 2.3 et 2.4 (i), on voit que le nombre de M à l'intérieur de $\mathcal{C}_{i,k}$ tels que $\Delta(M) + 4 \equiv 0$ modulo q et $\Delta(M) \equiv 0$ modulo r^2 , vérifie une égalité analogue à (4.6), mais avec un terme d'erreur en $O_{\varepsilon,r}(q^{\frac{5}{2}+\varepsilon})$. En sommant sur j et k , on obtient donc la formule (4.6) avec un terme d'erreur $\ll_{\varepsilon,r} q^{\frac{5}{2}+\varepsilon} (Q/q)^3 \ll q^{-1} Q^4 \log^{-3} X$. \square

5. Preuve du théorème

Soit \mathcal{A} l'ensemble $\mathcal{A} = \{a; 1 \leq a \leq X\}$, chaque a étant affecté du poids positif ou nul $w(a)$ tel que

$$w(a) = \begin{cases} \mathcal{H}(a+4) & \text{si } a+4 = \Delta, \text{ discriminant fondamental,} \\ 0 & \text{dans le cas contraire.} \end{cases}$$

Soit P un réel grand, mais fixé. On note aussi $\tilde{\mathcal{A}}$ l'ensemble

$$\tilde{\mathcal{A}} = \{a; 1 \leq a \leq X\},$$

chaque a étant maintenant affecté du poids positif ou nul $\mathcal{H}_P(a + 4)$, où la fonction $\mathcal{H}_P(a)$ est définie en (3.2). Soit z un réel et \mathcal{P} l'ensemble des nombres premiers. Avec les notations classiques du crible, on note

$$S(\mathcal{A}; \mathcal{P}, z) = \sum_{\substack{a \leq X \\ p|a \Rightarrow p \geq z}} w(a), \quad S(\tilde{\mathcal{A}}; \mathcal{P}, z) = \sum_{\substack{a \leq X \\ p|a \Rightarrow p \geq z}} \mathcal{H}_P(a + 4).$$

La démonstration s'inspire de celle présentée dans [BF, § VII]. Soit $C(X, u)$ la fonction définie par l'égalité

$$\left| \left\{ 5 \leq \Delta \leq X; p \mid \Delta \Rightarrow p \geq X^{\frac{1}{u}}, \mu^2(\Delta + 4) = 1, r_3(\Delta + 4) = 0 \right\} \right| = C(X, u) \frac{X}{\log X},$$

où u est une constante vérifiant $2 < u < 3$. Signalons que les Δ comptés dans le cardinal précédent ont au plus 2 facteurs premiers. Puisque le poids $w(a)$ vaut 0 ou prend des valeurs au moins égales à 1, on a l'inégalité

$$(5.1) \quad S(\mathcal{A}; \mathcal{P}, X^{\frac{1}{u}}) \geq -C(X, u) \frac{X}{\log X} + \left| \left\{ 5 \leq \Delta \leq X; p \mid \Delta \Rightarrow p \geq X^{\frac{1}{u}}, \mu^2(\Delta + 4) = 1 \right\} \right|.$$

On reconnaît à droite de (5.1) le cardinal des entiers $n < X$, congrus à 1 modulo 4, dont tous les facteurs premiers sont distincts et supérieurs à $X^{\frac{1}{u}}$, tels que $n + 4$ soit sans facteur carré. Ce cardinal est évalué par le lemme suivant :

LEMME 5.1. — Soit $2 < u < 3$. On a, pour $X \rightarrow \infty$, l'égalité

$$\left| \left\{ n \leq X; n \equiv 1 \pmod{4}, \mu^2(n + 4) = 1, p \mid n \Rightarrow p \geq X^{\frac{1}{u}} \right\} \right| = \left(\frac{1}{2} + o(1) \right) \cdot \Gamma \cdot (1 + \log(u - 1)) \frac{X}{\log X},$$

où $\Gamma = \prod_{p>2} \left(1 - \frac{1}{p(p-1)} \right)$.

Preuve. — Soit $S(X, u)$ le cardinal étudié. On écrit d'abord l'égalité

$$(5.2) \quad S(X, u) = \sum_d \mu(d) \sum_{\substack{n \leq X \\ d^2 \mid n+4}} 1,$$

la variable n vérifiant de plus les conditions

$$n \equiv 1 \pmod{4} \quad \text{et} \quad p \mid n \Rightarrow p \geq X^{\frac{1}{u}}.$$

La deuxième somme est nulle si d est pair. Sinon les n considérés sont, à une erreur négligeable près, soit les nombres premiers $\leq X$, vérifiant une certaine congruence modulo $4d^2$, soit les produits $\leq X$ de deux nombres premiers $\geq X^{\frac{1}{u}}$, vérifiant la même congruence. Le théorème des nombres premiers dans les progressions arithmétiques dit que la somme des cardinaux de ces deux ensembles est, en adoptant les notations de la théorie des nombres premiers, égale à

$$\begin{aligned} \frac{1}{2\varphi(d^2)} \left(\pi(X) + \sum_{X^{\frac{1}{u}} < p < X^{\frac{1}{2}}} \pi\left(\frac{X}{p}\right) \right) + O(X(\log X)^{-\frac{5}{2}}) \\ = \frac{1}{2\varphi(d^2)} (1 + \log(u-1)) \text{li } X + O(X(\log X)^{-\frac{5}{2}}). \end{aligned}$$

On reporte, pour d petit ($d \leq \log^{\frac{5}{4}} X$), cette expression dans (5.2); on somme alors sur d . Pour les grandes valeurs de d , on utilise la majoration triviale $O(Xd^{-2})$. \square

La formule (5.1) donne donc la minoration

$$(5.3) \quad S(\mathcal{A}; \mathcal{P}, X^{\frac{1}{u}}) \geq \left(\frac{1}{2} + o(1)\right) \cdot \Gamma \cdot (1 + \log(u-1)) \frac{X}{\log X} - C(X, u) \frac{X}{\log X}.$$

On majore la partie gauche de (5.3) en écrivant, grâce à (3.3), l'inégalité

$$(5.4) \quad S(\mathcal{A}; \mathcal{P}, X^{\frac{1}{u}}) \leq S(\tilde{\mathcal{A}}; \mathcal{P}, X^{\frac{1}{u}}).$$

Pour appliquer les formules du crible on écrit, pour q sans facteur carré, l'égalité

$$\sum_{\substack{n \leq X \\ q \mid n}} g_P(n+4) = \frac{\omega(q)}{q} \prod_{2 \leq p \leq P} (1 - \xi(p)) \left(\sum_{n \leq X} g(n) \right) + r(X, q)$$

avec

$$\omega(q) = \prod_{2 \mid q} \frac{8}{15} \prod_{\substack{2 < p \leq P \\ p \mid q}} (1 - \xi(p))^{-1} \prod_{p \mid q} \frac{\rho(p, 4)}{p^3},$$

le terme d'erreur $r(X, q)$ étant contrôlé, en moyenne sur $q \leq X^{\frac{1}{3}-\varepsilon}$, par la proposition 4.1. La fonction ω vérifie les conditions du crible linéaire,

on a donc la majoration suivante, pour tout $\eta > 0$ et $X \geq X(u, \eta, P)$

$$(5.5) \quad S(\tilde{\mathcal{A}}; \mathcal{P}, X^{\frac{1}{u}}) \leq \frac{1}{2} V(X^{\frac{1}{u}}) \cdot \prod_{2 < p \leq P} (1 - \xi(p)) \left(\sum_{n \leq X} g(n) \right) (F(\frac{1}{3}u) + \eta).$$

Dans cette expression, le coefficient $\frac{1}{2}$ provenant de (3.2), la fonction $F(s)$ est l'habituelle fonction du crible : elle vaut $2e^\gamma/s$ pour $s < 3$. Enfin, le produit eulérien $V(X^{\frac{1}{u}})$ est défini par

$$V(X^{\frac{1}{u}}) = \frac{2}{3} \prod_{2 < p \leq P} \left(1 - \frac{\rho(p, 4)}{p^4} (1 - \xi(p))^{-1} \right) \prod_{P < p < X^{\frac{1}{u}}} \left(1 - \frac{\rho(p, 4)}{p^4} \right).$$

Puisque $1 - \xi(p) = (1 - 1/p^2)^2$, l'expression de $V(X^{\frac{1}{u}})$ prend la forme plus agréable

$$\begin{aligned} V(X^{\frac{1}{u}}) &= \frac{2}{3} \prod_{2 < p \leq P} \left(1 - \frac{p}{p^2 - 1} \right) \prod_{P < p < X^{\frac{1}{u}}} \left(1 - \frac{p^2 - 1}{p^3} \right) \\ &= \frac{2}{3} \prod_{2 < p < X^{\frac{1}{u}}} \left(1 - \frac{1}{p} \right) \prod_{2 < p \leq P} \frac{p(p^2 - p - 1)}{(p - 1)(p^2 - 1)} \prod_{P < p < X^{\frac{1}{u}}} \frac{p^3 - p^2 + 1}{p^2(p - 1)}. \end{aligned}$$

Il est maintenant aisé de faire apparaître la constante Γ . Par la formule de Mertens, on voit qu'il existe une constante c_P , qui tend vers 1 lorsque $P \rightarrow \infty$, telle que pour $X \rightarrow \infty$, on ait

$$(5.6) \quad V(X^{\frac{1}{u}}) \sim c_P \cdot \Gamma \cdot \frac{\pi^2}{6} \cdot \frac{e^{-\gamma u}}{\log X}.$$

En reportant (5.6) dans (5.5) et (5.4), on a finalement l'inégalité

$$S(\mathcal{A}; \mathcal{P}, X^{\frac{1}{u}}) \leq (3 + \eta) \cdot \frac{6}{\pi^2} \cdot \Gamma \cdot c'_P \cdot \frac{1}{\log X} \left(\sum_{n \leq X} g(n) \right),$$

valable, pour tout $P \geq 3$, pour une certaine constante c'_P (qui tend vers 1 quand $P \rightarrow \infty$), pour tout $\eta > 0$, pourvu que $X > X(u, \eta, P)$. Or $\sum_{n \leq X} g(n)$ est le nombre de points M , à coordonnées entières, situés à l'intérieur de \mathcal{V} , vérifiant $\Delta(M) \leq X$ et on sait que ce nombre de points est équivalent à $\frac{1}{36} \pi^2 X$ (cf. [Da, Lemmas 4, 5]). On a donc, en prenant P suffisamment grand, l'inégalité suivante

$$(5.7) \quad S(\mathcal{A}; \mathcal{P}, X^{\frac{1}{u}}) \leq \left(\frac{1}{2} + \eta \right) \cdot \Gamma \cdot \frac{X}{\log X},$$

valable pour tout $\eta > 0$, pourvu que $X > X(u, \eta)$. En confrontant (5.3) et (5.7), on a finalement la minoration

$$(5.8) \quad \left| \left\{ 5 \leq \Delta \leq X; p \mid \Delta \Rightarrow p \geq X^{\frac{1}{u}}, \right. \right. \\ \left. \left. \mu^2(\Delta + 4) = 1, r_3(\Delta + 4) = 0 \right\} \right| \\ \geq \left(\frac{1}{2} - \eta \right) \cdot \Gamma \cdot \log(u - 1) \cdot \frac{X}{\log X},$$

pour tout $\eta > 0$, pourvu que X soit suffisamment grand. Les Δ apparaissant à gauche de (5.8) ont au plus deux facteurs premiers. Pour se restreindre aux Δ avec $r_2(\Delta) = 0$, nous utilisons le critère suivant, dû essentiellement à Gauss, mais dont la forme donnée ici se trouve dans [He, P. VII.12, Th. 4] :

CRITÈRE 5.2. — Soient Δ un discriminant fondamental et $\omega(|\Delta|)$ son nombre de facteurs premiers. Le 2-rang $r_2(\Delta)$ vaut

$$\omega(|\Delta|) - 1 \quad \text{ou} \quad \omega(|\Delta|) - 2,$$

la deuxième éventualité ayant lieu si et seulement si Δ est positif et a au moins un diviseur premier congru à 3 modulo 4. En particulier, les seuls Δ , positifs et impairs, tels que $h(\Delta)$ soit lui aussi impair, sont, soit les nombres premiers congrus à 1 modulo 4, soit les produits de deux nombres premiers distincts, congrus à 3 modulo 4.

Pour terminer la preuve du théorème, il suffit, grâce à ce critère, de faire disparaître, à gauche de (5.8), les Δ ayant exactement deux facteurs premiers p_1 et p_2 , tous deux congrus à 1 modulo 4, supérieurs à $X^{\frac{1}{u}}$, vérifiant $\mu^2(p_1 p_2 + 4) = 1$. Par une démonstration identique à celle du lemme 5.1, on a l'équivalence asymptotique

$$\left| \left\{ n \leq X; n = p_1 p_2, \mu^2(n + 4) = 1, \right. \right. \\ \left. \left. X^{\frac{1}{u}} \leq p_1 < p_2, p_1 \equiv p_2 \equiv 1 \pmod{4} \right\} \right| \\ \sim \frac{\Gamma}{4} \cdot \log(u - 1) \cdot \frac{X}{\log X}.$$

Par soustraction à (5.8), on obtient la minoration suivante, valable pour tout $2 < u < 3$, tout $\eta > 0$ et tout $X > X(u, \eta)$

$$\left| \left\{ 5 \leq \Delta \leq X; p \mid \Delta \Rightarrow p \geq X^{\frac{1}{u}}, \right. \right. \\ \left. \left. r_2(\Delta) = 0, \mu^2(\Delta + 4) = 1, r_3(\Delta + 4) = 0 \right\} \right| \\ \geq \left(\frac{1}{4} - \eta \right) \cdot \Gamma \cdot \log(u - 1) \cdot \frac{X}{\log X}.$$

Ceci termine la preuve du théorème. \square

Puisque u peut être pris arbitrairement proche de 2, on est tout proche de montrer qu'il y a une infinité de p tels que $p \equiv 1$ modulo 4, $p + 4$ soit sans facteur carré et tels que $r_3(p + 4) = 0$. Ceci a été signalé dans l'introduction.

BIBLIOGRAPHIE

- [Be] BELABAS (K.). — *Crible et 3-rang des corps quadratiques*, Annales Inst. Fourier, t. **46**, 1996, p. 909–949.
- [BF] BELABAS (K.), FOUVRY (E.). — *Sur le 3-rang des corps quadratiques de discriminant premier ou presque premier*, à paraître dans Duke Math. J.
- [CL] COHEN (H.), LENSTRA (H.W.). — *Heuristics on class groups of number fields*, Number Theory, Noordwijkerhout 1983 Proceedings, Lecture Note Math., Springer-Verlag, t. **1068**, 1984, p. 33–62.
- [DF] DANIEL (S.), FOUVRY (E.). — *On real quadratic fields with odd class number*, Math. Annalen, t. **313**, 1999, p. 371–384.
- [Da] DAVENPORT (H.). — *On the class number of binary cubic forms, I*, J. London Math. Soc., t. **27**, 1951, p. 183–192; erratum, ibid., t. **27**, 1951, p. 512.
- [DH1] DAVENPORT (H.), HEILBRONN (H.). — *On the density of discriminants of cubic fields*, Bull. London Math. Soc., t. **1**, 1969, p. 345–348.
- [DH2] DAVENPORT (H.), HEILBRONN (H.). — *On the density of discriminants of cubic fields, II*, Proc. Roy. Soc. London A., t. **322**, 1971, p. 405–420.
- [Fo] FOUVRY (E.). — *Consequences of a result of N. Katz and G. Laumon concerning trigonometric sums*. — Preprint.
- [He] HERZ (C.S.). — *Construction of class fields*, in Seminar on Complex Multiplication, Lecture Notes in Mathematics, Springer Verlag, t. **21**, 1966.
- [KaLa] KATZ (N.), LAUMON (G.). — *Transformation de Fourier et majoration de sommes exponentielles*, Publ. Math. I.H.E.S., t. **62**, 1985, p. 145–202; corrigendum, t. **69**, p. 233.
- [NaHo] NAKAGAWA (J.), HORIE (K.). — *Elliptic curves with no torsion points*, Proc. Amer. Math. Soc., t. **104**, 1988, p. 20–25.