SUR LE 3-RANG DES CORPS QUADRATIQUES DE DISCRIMINANT PREMIER OU PRESQUE PREMIER

K. BELABAS & E. FOUVRY

Table des matières

1. Introduction

L'objet principal de cet article est de parvenir au

Corollaire 1.1. *Il existe une infinité de nombres premiers $p \equiv 1$ modulo 4, tels que le groupe de classes d'idéaux de l'anneau des entiers de $\mathbb{Q}(\sqrt{p})$ ne possède aucun élément d'ordre 3. Plus précisément, il existe une constante $c_0 > 0$, telle que l'ensemble des $p \leqslant x$ vérifiant la propriété précédente soit de cardinal au moins égal à $c_0 x/\log x$ pour $x \geqslant 5$.*
La même propriété est vraie pour l'ensemble des $p \equiv 3$ modulo 4.

Rappelons qu'on conjecture l'existence d'une infinité de corps quadratiques réels $\mathbb{Q}(\sqrt{p})$ (p congru à 1 modulo 4) dont l'anneau des entiers est principal. On pense même que la proportion de tels premiers est d'environ 75,4% ([5, p. 58]). Cette conjecture, dite de Gauss-Hasse, a la réputation d'être d'une extrême difficulté : en introduisant $h(p)$, nombre de classes d'idéaux du corps $\mathbb{Q}(\sqrt{p})$, elle s'exprime comme le fait que l'équation $h(p) = 1$ a une infinité de solutions. Pour mémoire, rappelons que l'équation $h(-p) = 1$ a pour uniques solutions : $p = 2$, 3, 7, 11, 19, 43, 67 et 163. Notre résultat dit donc que, 3 ne divise pas $h(p)$, pour une proportion positive de p. Bien que le Corollaire 1.1 paraisse très timide dans la connaissance du nombre $h(p)$, c'est, à notre connaissance, le premier résultat inconditionnel allant dans la direction de cette conjecture.

Pour planter le décor des résultats et des techniques ayant trait à ce sujet, nous adopterons certaines conventions. On réservera la lettre p à un nombre premier et la lettre Δ à un *discriminant fondamental*, autrement dit Δ est un entier positif ou négatif, sans facteur carré impair et vérifiant les congruences $\Delta \equiv 1 \pmod 4$ ou $\Delta \equiv 8, 12 \pmod{16}$. Soit $X > 0$, on désignera alors par $\Delta^+(X)$ l'ensemble des discriminants fondamentaux compris strictement entre 0 et X et $\Delta^-(X)$ l'ensemble des discriminants strictement compris entre $-X$ et 0.

Soit $\mathrm{Cl}(\Delta)$ le groupe des classes d'idéaux de l'anneau des entiers de $\mathbb{Q}(\sqrt{\Delta})$. Soit $h_p^*(\Delta)$ le nombre d'éléments de $\mathrm{Cl}(\Delta)$ dont la puissance p-ième est un idéal principal. C'est une puissance de p et on pose $h_p^*(\Delta) = p^{r_p(\Delta)}$, l'entier $r_p(\Delta)$ est appelé *p-rang* de $\mathrm{Cl}(\Delta)$.

Le nombre $r_2(\Delta)$ a une description élémentaire essentiellement due à Gauss. On a $r_2(1) = 0$ (puisque $h(1) = 1$!) et, pour $\Delta \neq 1$

$$r_2(\Delta) = \omega(\Delta) - 1 \quad \text{ou} \quad \omega(\Delta) - 2, \tag{1}$$

($\omega(n)$ nombre de facteurs premiers de l'entier n), la deuxième éventualité a lieu uniquement lorsque $\Delta > 0$ et lorsque Δ a un diviseur premier congru à 3 modulo 4 (voir [16] Corollary 1 p. 457 et Note 20 p. 483, par exemple). Ainsi le Corollaire 1.1 implique qu'il existe une infinité de $\Delta > 0$ vérifiant $r_2(\Delta) = r_3(\Delta) = 0$. En fait, nous montrerons l'énoncé plus précis suivant

Corollaire 1.2. *Pour tout $k \geqslant 0$, il existe deux constantes $c'_k > 0$ et x_k, telles que pour $x \geqslant x_k$, on ait la minoration*

$$|\{\Delta, 0 < \Delta \leqslant X, r_2(\Delta) = k,\ r_3(\Delta) = 0\}| \geqslant c'_k \frac{x(\log\log x)^{k+1}}{\log x}.$$

Ce résultat est obtenu pour des Δ vérifiant le second cas de la formule (1), soit $\omega(\Delta) = k + 2$. Puisque, de façon classique, on sait que

$$|\{\Delta, 0 < \Delta \leqslant x, \omega(\Delta) \leqslant k + 2\}| \asymp \frac{x(\log\log x)^{k+1}}{\log x}$$

(k entier fixé, x tendant vers l'infini), on voit grâce à (1) que l'ordre asymptotique de la minoration du Corollaire 1.2 est correct.

Il n'existe pas de formule aussi simple et élégante que (1) pour les autres $r_p(\Delta)$. Même si on est moins exigeant, c'est-à-dire si on désire simplement connaître le comportement statistique de $r_p(\Delta)$ ou de $h_p^*(\Delta)$ (p fixé supérieur à 2), la situation reste vraiment pitoyable : absolument rien n'est connu pour un p général sauf pour $p = 3$ après le splendide travail de Davenport et Heilbronn ([9, 10]), qui est la clé de voûte de notre article et que nous présentons de la façon suivante :
Posons

$$\mathcal{H}(\Delta) = \frac{h_3^*(\Delta) - 1}{2}.$$

(C'est donc un entier, valant 0, 1, 4, 13,... On conjecture qu'il peut être arbitrairement grand sans connaître pour l'instant d'exemple supérieur à $\frac{3^6-1}{2} = 364$.) Pour mener de front le cas des Δ positifs et des Δ négatifs, nous posons

$$\alpha^+ = 1 \quad \text{et} \quad \alpha^- = 3. \tag{2}$$

Alors le comportement en moyenne de $\mathcal{H}(\Delta)$ est régi par les formules asymptotiques suivantes : lorsque X tend vers l'infini on a

$$\sum_{\Delta \in \Delta^{\pm}(X)} \mathcal{H}(\Delta) \sim \frac{\alpha^{\pm}}{6} \sum_{\Delta \in \Delta^{\pm}(X)} 1 \quad (\sim \alpha^{\pm} \frac{X}{2\pi^2}). \tag{3}$$

Signalons que, par exemple, on ne connaît pas d'équivalent à la somme

$$\sum_{\Delta \in \Delta^{\pm}(X)} \mathcal{H}^2(\Delta)$$

et que les formules (3) sont, pour l'instant, l'un des très rares cas où les très profondes conjectures heuristiques de Cohen-Lenstra ([5]), qui prévoient la structure en moyenne des groupes de classes des corps quadratiques, sont démontrées. Rappelons que ces conjectures prédisent, par exemple, que $r_p(\Delta)$ peut être arbitrairement grand et qu'il y a indépendance des comportements de $r_p(\Delta)$ et $r_{p'}(\Delta)$, pour des premiers p et p' distincts. Le Corollaire 1.2 s'inscrit donc dans cette dernière perspective.

La fonction $\mathcal{H}(\Delta)$ se répartit-elle harmonieusement suivant les progressions arithmétiques ? Cette question se pose naturellement après les travaux de Davenport et Heilbronn. Le cas particulier de la somme des $\mathcal{H}(\Delta)$ sur les $\Delta \equiv 0 \pmod{q}$ fut résolu de façon très satisfaisante par Belabas :

Théorème 1.3 ([1, Théorème 1.2])**.** *Soit $\varepsilon > 0$. Pour $X \to \infty$, on a les égalités*

$$\sum_{\substack{\Delta \in \Delta^{\pm}(X) \\ q|\Delta}} \mathcal{H}(\Delta) = \frac{\alpha^{\pm}}{2\pi^2} \frac{\nu(q)}{q} .X + O_{\varepsilon}\big(R_0(X, q, \varepsilon)\big),$$

uniformément pour q, entier sans facteur carré, inférieur à $X^{\frac{1}{15}-\varepsilon}$. Le coefficient $\alpha^{\pm}$ est défini en (2)*. On a désigné par $\nu(q)$ la fonction multiplicative telle que*

$$\nu(p) = \frac{p}{p+1},$$

et $R_0(X, q, \varepsilon)$ est la fonction

$$R_0(X, q, \varepsilon) = \frac{X}{q \log^2 X \log_2^{2-\varepsilon} X}.$$

Le symbole $\log_k$ désigne la fonction log itérée k fois. En choisissant $q = 1$ dans ce théorème, on précise les équivalences asymptotiques (3), mais ce n'est pas le meilleur terme d'erreur connu (voir [3]).

Le cas des autres progressions arithmétiques, par exemple de l'équivalence asymptotique

$$\sum_{\substack{\Delta \in \Delta^{\pm}(X) \\ \Delta \equiv 1 \pmod{q}}} \mathcal{H}(\Delta) \sim \frac{\nu'(q)}{q} \sum_{\Delta \in \Delta^{\pm}(X)} \mathcal{H}(\Delta), \ X \to \infty$$

uniformément pour $q \leqslant X^C$ sans facteur carré, où ν' fonction multiplicative et C constante positive n'a, à notre connaissance, fait l'objet d'aucune publication. Toutefois, les méthodes de [1], conduisent à l'existence d'une certaine constante $C > 0$ pour une fonction ν' explicite (on trouve $\nu'(p) = \frac{p^2}{p^2-1}$) — notons qu'il n'est nullement nécessaire d'appliquer des techniques de Fourier. Par contre, la recherche de bonnes valeurs de C — les plus grandes possibles — se démarque, sur plusieurs points, de la preuve du Théorème 1.3. Pour n'en citer qu'un, au §3.a.1 ci-dessous, on profitera d'une paramétrisation de la variété homogène d'équation $\Delta(a, b, c, d) \equiv 0$ modulo p. Un tel phénomène disparaît si l'équation devient $\Delta(a, b, c, d) \equiv 1$ modulo p. Nous n'abordons pas cette fort intéressante question dans notre travail.

En fait, lors de son application au crible, le Théorème 1.3 est utilisé sous la forme moins forte du

Corollaire 1.4. *Pour tout $\varepsilon > 0$ et X tendant vers l'infini, on a les égalités*

$$\sum_{q \leqslant X^{\frac{1}{15}-\varepsilon}} \mu^2(q) \Big| \sum_{\substack{\Delta \in \Delta^{\pm}(X) \\ q|\Delta}} \mathcal{H}(\Delta) - \frac{\alpha^{\pm}}{2\pi^2} \frac{\nu(q)}{q} .X \Big| = O_{\varepsilon}\Big(\frac{X}{\log X \log_2 X}\Big).$$

Pour parvenir au Corollaire 1.1, nous avons notablement amélioré les exposants apparaissant dans les Théorème 1.3 et Corollaire 1.4. La première idée nouvelle est d'étudier de façon plus poussée la quantité $N^*(\mathcal{B}_i; r, s)$ (voir §3 ou plutôt,

les sommes trigonométriques $S(\mathbf{h}; r, s)$ qui lui sont naturellement associées. On utilise de façon cruciale les propriétés géométriques de la variété sur laquelle la sommation est faite, c'est-à-dire le lieu où s'annule la fonction discriminant $\Delta(a, b, c, d)$ (voir Lemmes 3.1, 3.2, 3.4 et 3.5). On parvient ainsi au

Théorème 1.5. *L'énoncé du Théorème 1.3 reste vrai, si on remplace l'inégalité que doit vérifier q par l'inégalité $q \leqslant X^{\frac{3}{44}-\varepsilon}$.*

Le théorème précédent entraîne immédiatement que, dans le Corollaire 1.4, on peut remplacer l'exposant $\frac{1}{15}$ par $\frac{3}{44}$. L'amélioration de l'exposant n'est malheureusement pas à la mesure des innovations dans le traitement des sommes d'exponentielles $S(\mathbf{h}; r, s)$, évoquées ci-dessus. Ceci est, en partie, dû au fait qu'il faut s'assurer que les Δ en question sont bien fondamentaux. Toutefois cette approche est largement valorisée si on introduit une autre idée nouvelle par rapport à [1] : traiter *en moyenne* la contribution d'ensembles de points (a, b, c, d) de $\mathbb{Z}^4$ difficiles à appréhender mais de cardinal petit. Ces ensembles sont désignés par $\mathcal{D}(X, \rho, Q)$, $\mathcal{D}'(X, \rho)$ ou $\mathcal{D}^*_{m,\varepsilon}$ suivant les situations (voir §2 et §4). On parvient ainsi au

Théorème 1.6. *Pour tout $\varepsilon > 0$ et X tendant vers l'infini, on a les égalités*

$$\sum_{q \leqslant X^{\frac{2}{7}-\varepsilon}} \mu^2(q) \Big| \sum_{\substack{\Delta \in \Delta^{\pm}(X) \\ q \mid \Delta}} \mathcal{H}(\Delta) - \frac{\alpha^{\pm}}{2\pi^2} \frac{\nu(q)}{q} . X \Big| = O_{\varepsilon}\Big(\frac{X}{\log X \log_2 X}\Big).$$

Si q est restreint à parcourir l'ensemble des nombres premiers, on peut, dans les relations précédentes, remplacer l'exposant $\frac{2}{7}$ par $\frac{3}{10}$.

Une forme itérée de l'égalité (46) ci-dessous conduirait à une amélioration de la valeur de la quantité $R_0(X, q, \varepsilon)$ et des seconds membres des estimations du Corollaire 1.4 et du Théorème 1.6 : il est possible de gagner un facteur en $\log^{-A} X$ ($A > 0$). La forme que nous démontrerons ici est juste suffisante pour les applications au crible.

On étend la définition de la fonction $\mathcal{H}$ à tous les entiers n, en posant $\mathcal{H}(n) = 0$ si n n'est pas un discriminant fondamental. Appliquons les formules du crible linéaire à la suite $\mathcal{A}^{\pm}$ des entiers $\pm n$, compris entre 1 et X, affectés des poids $\mathcal{H}(\pm n)$. On obtient, par exemple, directement le corollaire suivant

Corollaire 1.7. *Pour tout $\varepsilon > 0$, il existe des constantes absolues c^+ et $c^- > 0$ telles qu'on ait, pour X tendant vers l'infini, les minorations*

$$\sum_{\substack{\Delta \in \Delta^{\pm}(X),\ r_3(\Delta) \geqslant 1 \\ p \mid \Delta \Longrightarrow p \geqslant X^{\frac{1}{7}-\varepsilon}}} \mathcal{H}(\Delta) \geqslant c^{\pm} \frac{X}{\log X}.$$

En combinant avec (1) et avec la relation $\mathcal{H}(\Delta) \leqslant h(\Delta) = O\big(\sqrt{|\Delta|}\log(2\,|\Delta|)\big)$, on peut donc affirmer que le système

$$\left\{ \begin{array}{l} r_2(\Delta) \leqslant 6 \\ r_3(\Delta) \geqslant 1 \end{array} \right. \tag{4}$$

a une infinité de solutions en discriminants fondamentaux, dont on peut au besoin imposer le signe. Le crible pondéré peut même ramener la constante 6 du système (4) à 3. Nous n'insisterons pas sur cette méthode (voir plus bas comment améliorer ces constantes en faisant appel au Théorème 1.8 ci-dessous), mais rappellerons simplement que dans ([1, Théorème 1.6]), l'auteur obtient la constante 8.

Mais l'énoncé du Théorème 1.6, à première vue, n'est pas suffisant pour fournir le Corollaire 1.1 par des méthodes de crible. L'étude de la preuve des Théorèmes 1.5 et 1.6 montre que le prix à payer, pour certifier que les Δ apparaissant dans les sommes sont sans facteur carré impair, est très lourd. Cette difficulté n'est pas sans rappeler celle que l'on rencontre si on cherche à compter dans un ensemble *raisonnable* (par exemple, l'ensemble $\{n^4+1, n \in \mathbb{N}\}$), le nombre d'éléments inférieurs à X, sans facteur carré, pour X tendant vers l'infini. En effet cribler par les p^2 pour p grand devient très délicat. Par contre, si on demande que les éventuels diviseurs p^2 soient supérieurs à un certain P^2 (P extrêmement grand mais fixé), le problème devient trivial par le principe d'inclusion-exclusion, et la formule asymptotique trouvée est une majoration très proche de la formule asymptotique escomptée pour le problème initial.

Ainsi, le théorème suivant est une transposition du Théorème 1.6 au cas des discriminants *n quasi-fondamentaux d'ordre P*, c'est-à-dire des entiers n, tels que si p^2 divise n, on a $p \geqslant P$ ou $p = 2$ et dans ce dernier cas on a $n \equiv 8$ ou 12 modulo 16. Nous montrerons le

Théorème 1.8. *Pour tout entier P, il existe une fonction $\mathcal{H}_P$ définie sur $\mathbb{Z}$ telle que i) Pour tout n, on a l'inégalité $\mathcal{H}(n) \leqslant \mathcal{H}_P(n)$,*

ii) Il existe $X_0(P)$ tel que, uniformément pour $X > X_0(P)$, on ait les deux inégalités

$$\sum_{0<\pm n\leqslant X} \mathcal{H}_P(n) \leqslant \big(1+O(P^{-1})\big) \sum_{\Delta\in\Delta^{\pm}(X)} \mathcal{H}(\Delta),$$

iii) Pour tout $\varepsilon > 0$, il existe $\eta = \eta(\varepsilon) > 0$ tel que, pour X tendant vers l'infini, on a

$$\sum_{q\leqslant X^{\frac{3}{8}-\varepsilon}} \mu^2(q) \Big| \sum_{\substack{0<\pm n\leqslant X \\ q|n}} \mathcal{H}_P(n) - \frac{\nu_P(q)}{q} \sum_{0<\pm n\leqslant X} \mathcal{H}_P(n) \Big| = O_{\varepsilon,P}\big(X^{1-\eta}\big)$$

où

$$\nu_P(q) = \nu(q) \prod_{\substack{p|q \\ p\geqslant P}} \frac{(p+1)(p^2+p-1)}{p^3}$$

L'exposant de répartition passe donc de $\frac{2}{7}$ à $\frac{3}{8}$, lorsqu'on crible $\mathcal{H}_P(n)$, dont la définition sera donnée au §4, plutôt que $\mathcal{H}(n)$. Cette valeur de $\frac{3}{8}$, obtenue sans intervention du grand crible, est remarquablement élevée et ce gain suffit pour prouver le Corollaire 1.1 (il suffisait d'avoir un exposant strictement supérieur à $\frac{1}{3}$, voir §7). Voyons maintenant comment améliorer le Corollaire 1.7 grâce au Théorème 1.8.
On appelle $\tilde{\mathcal{A}}$ la suite des entiers de $[1, X]$, affectés des coefficients $\mathcal{H}_P(n)$. Avec les notations du crible ([12, 13] par exemple), on a l'égalité de Buchstab, valable pour $z_1 \leqslant z$:

$$S(\mathcal{A}, z) = S(\mathcal{A}, z_1) - \sum_{z_1 \leqslant p < z} S(\mathcal{A}_p, p), \tag{5}$$

et par définition de $\tilde{\mathcal{A}}$, on a l'inégalité

$$S(\mathcal{A}, z) \geqslant S(\mathcal{A}, z_1) - \sum_{z_1 \leqslant p < z} S(\tilde{\mathcal{A}}_p, p). \tag{6}$$

Notons que, pour cette application, la notion de quasi-discriminant d'ordre 1 nous suffit. En effet, les quasi-discriminants d'ordre P sont utilisés uniquement pour évaluer $S(\tilde{\mathcal{A}}, z)$. Or la contrainte $(p|n \Longrightarrow p \geqslant z)$ implique évidemment $(p^2|n \Longrightarrow p \geqslant P)$ puisque P est fixé ! Ainsi, pour $z \geqslant P_0$, $S(\tilde{\mathcal{A}}, z)$ ne dépend pas de $P \leqslant P_0$ et l'on peut choisir $P = 1$.

Par définition des fonctions F et f du crible linéaire comme solutions des équations différentielles aux différences induites par l'égalité de Buchstab, on retrouve exactement la même minoration si on injecte à droite de (5) les majoration et minoration classiques du crible, en travaillant avec le Théorème 1.6. Par contre, on voit que l'inégalité (6) est strictement meilleure que (5), pour les applications, puisqu'on peut appliquer le Théorème 1.8, pour la majoration de $S(\tilde{\mathcal{A}}_p, p)$. La borne $\frac{1}{7}$ du Corollaire 1.7 est ainsi aisément franchie, la limite théorique, après itération de l'identité de Buchstab, étant, dans le Corollaire 1.7, la valeur $\frac{3}{16} - \varepsilon$ pour l'exposant.

Puisque dans ([12, p. 258]), on trouve la valeur $\Lambda_3 \geqslant \frac{11}{4}$ et qu'on a l'inégalité $\frac{3}{8}\Lambda_3 > 1$, on déduit que pour tout X assez grand, $\tilde{\mathcal{A}}$ contient des entiers ayant au plus trois facteurs premiers. Il serait intéressant — nous ne le faisons pas par manque de place — de pousser les arguments pour en déduire que $\mathcal{A}$ contient, lui-aussi, des entiers avec au plus trois facteurs premiers. On prouverait alors que le système

$$r_2(\Delta) \leqslant 2 \quad \text{et} \quad r_3(\Delta) \geqslant 1$$

a une infinité de solutions. Il faudrait alors comparer cette technique avec celle développée dans ([2, Chapitre 4]) qui étudie les valeurs pseudo-premières prises par le polynôme $y^2 - 4x^\ell$, pour x et y entiers et $\ell \geqslant 3$ un nombre premier fixé, afin d'exhiber des corps quadratiques de ℓ-rang au moins égal à 1, et de 2-rang contrôlé.

Par les formules (3), puisque $\alpha^- = 3\alpha^+$, on imagine que le 3-rang des corps quadratiques imaginaires a tendance à être plus grand que celui des corps quadratiques réels. Il est donc plus difficile de construire des $\Delta < 0$ avec un petit 3-rang, il n'est alors pas surprenant que le Corollaire 1.9 soit de moins bonne qualité que le Corollaire 1.1. On a

Corollaire 1.9. *Chacun des systèmes*

$$(I)\begin{cases} r_2(\Delta) &= 0 \\ r_3(\Delta) &\leqslant 1 \end{cases} \qquad (II)\begin{cases} r_2(\Delta) &\leqslant 3 \\ r_3(\Delta) &= 0 \end{cases}$$

a une infinité de solutions $\Delta < 0$. Plus précisément, il existe une constante absolue $c^- > 0$ telle que le nombre de solutions à chacun de ces systèmes, avec $\Delta \in \Delta^-(X)$ soit supérieur à $c^- X/\log X$, pour $X \to \infty$.

Remerciements Les auteurs remercient P. Michel pour de stimulantes discussions lors de l'élaboration de cet article. Le premier auteur remercie le Max-Planck-Institut für Mathematik (Bonn) pour son hospitalité.

2. La technique de Davenport-Heilbronn. Rappels et préparations techniques

L'objet de ce paragraphe est de citer clairement les résultats de Davenport-Heilbronn dont nous aurons ici besoin. Tous ces résultats sont évidemment les outils de base de [1].

Soit $\mathfrak{F}$ l'ensemble des formes cubiques binaires

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

à coefficients entiers. On définit $\mathfrak{F}^{\mathrm{irr}}_{\mathrm{prim}}$ comme étant le sous-ensemble de $\mathfrak{F}$ constitué des formes *primitives* (c'est-à-dire telles que $(a,b,c,d) = 1$) et *irréductibles* (c'est-à-dire telles que F ne soit pas de la forme $F = F_1F_2$ où F_1 et F_2 sont deux formes à coefficients entiers avec $\deg F_1 = 1$). Le discriminant de F est la quantité

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

Un élément M de $\mathrm{GL}(2,\mathbb{Z})$ définit un changement de variables. On dira que deux formes F et F' sont équivalentes s'il existe M de $\mathrm{GL}(2,\mathbb{Z})$ tel que $F' = F \circ M$. Soit Φ l'ensemble des classes de formes cubiques pour cette relation d'équivalence. Puisque le changement de variables conserve la primitivité et l'irréductibilité d'un élément de $\mathfrak{F}$, on peut considérer $\Phi^{\mathrm{irr}}_{\mathrm{prim}} \subset \Phi$, image de $\mathfrak{F}^{\mathrm{irr}}_{\mathrm{prim}}$ par la projection canonique. Rappelons aussi que les formes d'une même classe ont même discriminant.

Pour p nombre premier au moins égal à 3, on note V_p l'ensemble des classes F de $\Phi^{\mathrm{irr}}_{\mathrm{prim}}$ telles que p^2 ne divise pas $\Delta(F)$ et V_2 l'ensemble des classes F telles que $\Delta(F) \equiv 1 \pmod 4$ ou $\Delta(F) \equiv 8$ ou $12 \pmod{16}$. On pose aussi

$$V_q = \bigcap_{p|q} V_p, \qquad V = \bigcap_p V_p.$$

Donc V est l'ensemble des classes de formes de discriminant fondamental.

On définit U_p comme étant la réunion de V_p et de l'ensemble des classes F de $\Phi^{\text{irr}}_{\text{prim}}$ telles que, modulo p, F s'écrive $F = \lambda(\alpha x - \beta y)^3$ et $F(\beta, \alpha) \neq 0$ modulo p^2. Remarquons que la condition $F = \lambda(\alpha x - \beta y)^3$ implique que F n'appartient pas à V_p. On pose aussi

$$U = \bigcap_p U_p.$$

L'ensemble U ainsi construit est essentiellement l'ensemble des classes de formes cubiques dont le discriminant coïncide avec celui d'une extension cubique de $\mathbb{Q}$ (nous n'aurons pas besoin ici d'un énoncé précis de cette interprétation de U).

Soit $\mathcal{K}$ l'ensemble des extensions cubiques de $\mathbb{Q}$, $\mathcal{C}$ l'ensemble des classes d'isomorphismes de corps cubiques sur $\mathbb{Q}$. Rappelons que chaque classe d'équivalence contient soit un élément (le corps cubique en question est alors cyclique) soit trois éléments.

Le premier résultat nécessaire dans cette théorie est l'existence de la *bijection de Delone et Faddeev* (voir [11, §15]), qui associe ordres (non nécessairement maximaux) des corps cubiques et classes de formes cubiques (non nécessairement primitives), sans aucune conditions locales. Davenport et Heilbronn ont calculé son image quand on la restreint aux ordres maximaux et l'utilisent sous la forme suivante :

Lemme 2.1 ([9, 10])**.** *Il existe une application $K \longmapsto F_K$ de $\mathcal{K}$ dans $\mathfrak{F}^{irr}_{prim}$ telle que*

- *pour tout K, on a $\text{disc}(K) = \Delta(F_K)$;*
- *pour tout K, F_K appartient à U ;*
- *par passage au quotient, $K \longmapsto F_K$ est une bijection de $\mathcal{C}$ sur U.*

Le lien avec la fonction $\mathcal{H}(\Delta)$ se fait par une remarque d'algèbre (comptage de certains sous-groupes de $\text{Cl}(\Delta)$) et un peu de théorie du corps de classes couplée avec la bijection de Davenport-Heilbronn décrite dans le Lemme 2.1. On a donc, en se restreignant aux discriminants fondamentaux le

Lemme 2.2. *Soit Δ un discriminant fondamental. Il y a exactement $\mathcal{H}(\Delta)$ sous-groupes d'indice 3 dans $\text{Cl}(\Delta)$. Cet ensemble de sous-groupes d'indice 3 est en bijection avec les éléments de Φ^{irr}_{prim} de discriminant Δ.*

En fait, puisque Δ est fondamental, on peut tout aussi bien remplacer l'ensemble $\Phi^{\text{irr}}_{\text{prim}}$ par V dans le lemme précédent. On regroupe ces résultats sous la forme de la

Proposition 2.3. *Soient a et q deux entiers fixés. Soit $N_{a,q}(\xi, \eta; V)$ le nombre d'éléments de V dont le discriminant est strictement compris entre ξ et η, et est congru à a modulo q. On a, pour $X > 0$, les égalités*

$$\sum_{\substack{\Delta \in \Delta^+(X) \\ \Delta \equiv a \pmod{q}}} \mathcal{H}(\Delta) = N_{a,q}(0, X; V)$$

et

$$\sum_{\substack{\Delta\in\Delta^-(X)\\ \Delta\equiv a \pmod q}} \mathcal{H}(\Delta) = N_{a,q}(-X, 0; V).$$

Il faut maintenant calculer chacune des quantités $N_{a,q}$. À toute forme $F(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$ de $\mathfrak{F}$ on associe le point (a,b,c,d) de $\mathbb{R}^4$. L'idée est de se ramener à compter les points entiers d'un certain volume de $\mathbb{R}^4$, domaine fondamental pour l'action de $\mathrm{GL}(2,\mathbb{Z})$ sur $\mathbb{Z}^4$, identifié à $\mathfrak{F}$. En fait, pour se ramener au cas classique de la réduction des formes quadratiques, on introduit une relation d'équivalence plus stricte qu'auparavant sur $\mathfrak{F}$. À savoir, F et F' sont *proprement équivalentes* s'il existe M dans $\mathrm{SL}(2,\mathbb{Z})$ tel que $F' = F \circ M$. On note $\tilde{\Phi}$ et $\tilde{\Phi}^{\mathrm{irr}}_{\mathrm{prim}}$ l'ensemble des classes d'équivalences propres, par analogie avec les notations précédentes. On a dans l'idée qu'il y a deux fois plus de classes d'équivalence propres.

2.a. **Cas des formes de discriminant strictement positif.** À la forme cubique irréductible F on associe le covariant quadratique

$$H(x,y) = Ax^2 + Bxy + Cy^2,$$

avec

$$\begin{cases} A &= b^2 - 3ac \\ B &= bc - 9ad \\ C &= c^2 - 3bd \end{cases}$$

Ce covariant est le *hessien* de F, en fait $-4H(x,y) = \dfrac{\partial^2 F}{\partial x^2}\dfrac{\partial^2 F}{\partial y^2} - \Big(\dfrac{\partial^2 F}{\partial x \partial y}\Big)^2$. Il jouit de l'importante propriété

$$\mathrm{disc}(H) = -3\Delta(F)$$

et est ainsi strictement négatif. L'application $F \mapsto H$ commute à l'action de $\mathrm{GL}(2,\mathbb{Z})$, donc chaque classe de $\tilde{\Phi}$ a un représentant dans la région de l'espace défini par les inégalités

$$\begin{cases} \text{soit } -A < B \leqslant A < C \\ \text{soit } 0 \leqslant B \leqslant A = C. \end{cases}$$

À la différence du cas quadratique, $-\mathrm{Id}$ agit proprement sur $\mathfrak{F}^{\mathrm{irr}}$, ce qui nous permet d'imposer de surcroît $a > 0$. Dans ce cas, le représentant est unique, à moins que le covariant quadratique ne soit proportionnel à x^2+y^2 ou x^2+xy+y^2. Dans ce dernier cas, on a $O(1)$ représentants (en fait, au plus 3). Ces éventualités ont lieu lorsque $A = C$ et $B = 0$ ou lorsque $A = B = C$. Ceci nous amène à considérer le volume $\mathcal{V}$ défini par

$$\mathcal{V} = \{(a,b,c,d) \in \mathbb{R}^4; 1 \leqslant a,\ |B| \leqslant A \leqslant C\},$$

et pour X entier $\geqslant 1$, on appelle

$$\mathcal{V}(X) := \{(a,b,c,d) \in \mathcal{V}; 1 \leqslant \Delta(a,b,c,d) \leqslant X\}.$$

L'ensemble $\mathcal{V}(X)$ est une variété semi-algébrique, c'est-à-dire définie par un nombre fini d'équations ou d'inéquations algébriques. Cet ensemble est très biscornu, toutefois Davenport a calculé le nombre de points entiers contenus dans $\mathcal{V}(X)$:

Lemme 2.4 ([7, Lemmas 4, 5])**.** *Pour X tendant vers l'infini, on a l'égalité*

$$\operatorname{card} \mathcal{V}(X) \cap \mathbb{Z}^4 = \frac{\pi^2}{36} X + O(X^{\frac{15}{16}})$$

Pour le rendre plus agréable, nous allons ôter au volume $\mathcal{V}(X)$ un certain nombre de sous-ensembles que nous noterons par la lettre $\mathcal{D}$, comme *déchet*. Dans un premier temps, on constate que $\mathcal{V}(X)$ possède une pointe et, suivant en cela Davenport, nous jugeons préférable de l'étêter. On introduit un paramètre réel $\rho > 0$ et on pose, comme dans [1],

$$\mathcal{D}^{\text{pointe}}(X, \rho) = \{(a, b, c, d) \in \mathcal{V}(X), a \leqslant [X^{\frac{1}{4}-3\rho}]\},$$

$[\alpha]$ désignant la partie entière du réel α. On a aussi le

Lemme 2.5 ([7, Lemma 4])**.** *On a, pour X tendant vers l'infini, la relation*

$$\operatorname{card} \mathcal{D}^{pointe}(X, \rho) \cap \mathbb{Z}^4 = O(X^{1-\rho}).$$

On pose

$$\mathcal{X} = \mathcal{X}(X, \rho) = \mathcal{V}(X) - \mathcal{D}^{\text{pointe}}(X, \rho).$$

2.a.1. *Découpage de $\mathcal{X}(X, \rho)$.* Dans toute la suite, on appellera ξ un nombre tel que

$$1 - e^{-X} \leqslant \xi < 1.$$

L'introduction de ce réel ξ n'a rien d'important mais facilitera les notations des boites servant au découpage de $\mathcal{X}$. Soit Q un entier $\geqslant 1$, qui sera fixé par la suite suivant les situations. On considère le sous-ensemble maximal du réseau $\left(\xi Q\mathbb{Z}\right)^4$ inclus dans $\mathcal{X}$. Ce sous-ensemble, noté $\underline{\mathcal{X}}_Q$, est constitué de boites $\mathcal{B}_i$ ($i \in \mathcal{I}$) de côté ξQ. Par boite, nous entendons le produit d'intervalles (dans $\mathbb{R}^4$) de la forme

$$[k_1\xi Q, (k_1+1)\xi Q] \times [k_2\xi Q, (k_2+1)\xi Q] \times [k_3\xi Q, (k_3+1)\xi Q] \times [k_4\xi Q, (k_4+1)\xi Q],$$

avec k_1, k_2, k_3 et k_4 entiers. Pour ainsi dire, $\underline{\mathcal{X}}_Q$ est l'*amincissement* d'ordre Q de $\mathcal{X}$. Signalons que, pour X suffisamment grand, pour $Q \leqslant X^{10}$ et pour tous les k_i de valeurs absolues inférieures à X^{10}, chaque boite $\mathcal{B}_i$ contient exactement Q^4 points à coordonnées entières. C'est une conséquence du fait que ξ est extrêmement proche de 1.

De même, considérons le sous-ensemble minimal du réseau $\left(\xi Q\mathbb{Z}\right)^4$ contenant $\mathcal{X}$. C'est une réunion de boites $\mathcal{B}_j$, avec $j \in \mathcal{J}$, où $\mathcal{J}$ est un ensemble d'indices contenant $\mathcal{I}$. Nous appellerons cet ensemble de boites *épaississement* de $\mathcal{X}$ (terminologie introduite dans [1]), et on le note $\overline{\mathcal{X}}_Q$. En conclusion, nous avons l'encadrement

$$\bigcup_{i\in\mathcal{I}} \mathcal{B}_i = \underline{\mathcal{X}}_Q \subset \mathcal{X} \subset \overline{\mathcal{X}}_Q = \bigcup_{j\in\mathcal{J}} \mathcal{B}_j,$$

cet encadrement étant de meilleure qualité à mesure que Q décroît. Nous devons évaluer la perte qu'il engendre dans le dénombrement des points à coordonnées entières contenus dans $\mathcal{X}$. Pour faciliter l'écriture des résultats, nous notons maintenant les coordonnées de $\mathbb{R}^4$ par x_1, x_2, x_3 et x_4. On dit qu'une variété linéaire affine de dimension d (avec $1 \leqslant d \leqslant 3$) est *$Q$-régulière*, si elle a pour équations

$$x_{i_1} = k_1 \xi Q, \cdots, x_{i_{4-d}} = k_{4-d} \xi Q,$$

avec $1 \leqslant i_1 < \cdots < i_{4-d} \leqslant 4$, et les k_i sont des entiers. Ces variétés sont donc parallèles ou perpendiculaires aux axes de coordonnées et s'appuient sur le réseau $\big(\xi Q\mathbb{Z}\big)^4$.

Lemme 2.6. *Avec les conventions précédentes, on a, pour Q entier, la majoration*

$$\operatorname{card} \mathcal{J} - \operatorname{card} \mathcal{I} \ll \sum_{i=1}^{4} n_i,$$

où n_i est le nombre de variétés linéaires affines Q-régulières, de dimension i, qui coupent $\mathcal{X}$ ($n_4 = 1$ par définition). La constante contenue dans le symbole $\ll$ est absolue.

Preuve. Cela résulte de ce que tous les ensembles $\mathcal{X}_i$ et $\mathcal{X}_i^c$construits plus bas sont semi-algébriques, définis par un nombre borné d'inéquations polynomiales de degré borné et du fait suivant ([4, Prop 4.4.5], par exemple) : le nombre de composantes connexes d'un ensemble semi-algébrique réel est borné par un entier ne dépendant que des degrés et du nombre d'inéquations le définissant, ainsi que de la dimension de l'espace ambiant.
Considérons une boite $\mathcal{B}_j$ avec $j \in \mathcal{J}$ et $j \notin \mathcal{I}$. Nous construisons par récurrence trois suites décroissantes K_k, V_k et $\mathcal{X}_k$, $1 \leqslant i \leqslant k \leqslant 4$ telles que :

- $K_i \subset \cdots \subset K_4 = \mathcal{B}_j$, où K_k est une face de dimension k de K_4.
- $V_i \subset \cdots \subset V_4 = \mathbb{R}^4$, où V_k est une variété affine Q-régulière s'appuyant sur K_k (donc sur K_4).
- $\mathcal{X}_i \subset \cdots \subset \mathcal{X}_4 = \mathcal{X}$, oú $\mathcal{X}_k = \mathcal{X} \cap V_k$. On posera $\mathcal{X}_k^c = V_k - \mathcal{X}_k$, $\mathcal{X}^c = \mathcal{X}_4^c = \mathbb{R}^4 - \mathcal{X}$.

Supposons que K_k contienne un point de $\mathcal{X}_k$ et un point de $\mathcal{X}_k^c$ (c'est en particulier le cas pour $k = 4$). Trois éventualités apparaissent alors :

(i) le bord ∂K_k de K_k est inclus dans $\mathcal{X}_k$. Dans ce cas, on pose $i = k$ et la récurrence s'arrête là. Cependant, K_k contient dans son intérieur une composante connexe de $\mathcal{X}_k^c$, qui en possède $O(1)$. Il y a donc $O(1)$ boites répondant à cette disposition, pour chaque variété Q-régulière de dimension k rencontrant $\mathcal{X}$, soit au total $O(n_k)$.

(ii) le bord ∂K_k est inclus dans $\mathcal{X}_k^c$. Dans ce cas, K_k contient dans son intérieur une composante connexe de $\mathcal{X}$. De même que précédemment, on pose $i = k$ et l'on trouve $O(n_k)$ boites.

(iii) le bord ∂K_k contient des éléments de $\mathcal{X}_k$ et des éléments de $\mathcal{X}_k^c$. Dans ce cas, il existe au moins une face de dimension $k-1$ de K_k, notée K_{k-1}, intersection de K_k et d'une variété affine Q-régulière de dimension $k-1$, noté V_{k-1}, contenant à la fois des éléments de $\mathcal{X}_{k-1} = \mathcal{X}_k \cap V_{k-1}$ et des éléments de $\mathcal{X}_{k-1}^c = V_{k-1} - \mathcal{X}_{k-1}$. Nous sommes donc en mesure de poursuivre notre récurrence descendante sur la dimension des faces.

À la suite de cette construction, si K_4 n'est pas l'une des $O(n_4+n_3+n_2)$ boites correspondant aux cas (i) et (ii), nous avons construit une arête K_1 contenant un point de $\mathcal{X}$ et un point de $\mathcal{X}^c$. Plaçons nous donc dans ce dernier cas. L'intersection $\mathcal{X}_1$ de $\mathcal{X}$ avec la droite V_1 qui prolonge K_1 a $O(1)$ composantes connexes. Par hypothèse, K_1 se trouve à l'extrémité de l'une d'entre elles. Il y a donc au plus $O(n_1)$ arêtes K_1 possibles.

En regroupant les résultats de cette discussion, on conclut la preuve. □

Signalons que ce lemme est d'ailleurs valable pour tout semi-algébrique de $\mathbb{R}^N$ (en étendant la somme à droite jusqu'à $i = N$), la constante du symbole $\ll$ dépendant alors au plus de N, du nombre et du degré des inéquations polynomiales définissant l'ensemble semi-algébrique en question. La compacité assure simplement que les n_i sont finis.
Pour rendre effectif le Lemme 2.6, il faut calculer le nombre des variétés linéaires affines Q-régulières rencontrant $\mathcal{X}$. On a

Lemme 2.7. *Soit Q un entier $\geqslant 1$. Le nombre de variétés linéaires affines Q-régulières qui coupent $\mathcal{X}(X,\rho)$ est*

$$\sum_{i=1}^{4} n_i \ll Q^{-3} X^{\frac{3}{4}+3\rho} \log X + Q^{-1} X^{\frac{1}{4}+3\rho} + 1$$

Preuve. Il suffit d'appliquer le Corollaire 4.3 de [1] qui évalue la somme des volumes des projections de $\overline{\mathcal{X}}_Q$ sur les hyperplans de coordonnées. Cette somme de volumes est

$$\ll X^{\frac{3}{4}+3\rho} \log X + Q^2 X^{\frac{1}{4}+3\rho} + Q^3. \tag{7}$$

Ces projections sont des assemblages de cubes de dimension 3. Par division par Q^3, on a une majoration du nombre de cubes, qui portent chacun $O(1)$ variétés Q-régulières rencontrant $\mathcal{X}$. Comme elles sont manifestement toutes de ce type, on en déduit la formule souhaitée. □

Remarquons que deux boites $\mathcal{B}_j$ et $\mathcal{B}_{j'}$ distinctes, ne sont pas nécessairement disjointes. Mais si l'intersection de ces boites contient des points à coordonnées entières, c'est que ces deux boites ont un de leurs bords inclus dans l'un des hyperplans de coordonnées (voilà pourquoi nous avons travaillé avec le réseau $\left(\xi Q\mathbb{Z}\right)^4$ au lieu du réseau $\left(Q\mathbb{Z}\right)^4$ qui aurait semblé plus naturel). Appelons donc $\mathcal{D}^0(X,\rho)$ l'intersection de $\mathcal{X}$ avec la réunion des quatre hyperplans de coordonnées. L'expression (7) majore la somme des volumes des projections de $\overline{\mathcal{X}}_Q$ sur ces hyperplans de coordonnées. En choisissant $Q = 1$, on obtient

Lemme 2.8. *On a la majoration*

$$\operatorname{card} \mathcal{D}^0(X,\rho) \cap \mathbb{Z}^4 \ll X^{\frac{3}{4}+3\rho} \log X.$$

Un autre ensemble ennuyeux, appelé $\mathcal{D}^{=}(X)$, est constitué des $(a,b,c,d) \in \mathcal{V}(X)$ tels que $|B| = A$ ou $A = C$. Rappelons que si une classe de $\tilde{\Phi}$ a un représentant dans $\mathcal{D}^{=}(X)$, celui-ci n'est pas unique et que le nombre de tels représentants est alors en $O(1)$. Cet ensemble $\mathcal{D}^{=}(X)$ n'est pas très gros, puisqu'on a le

Lemme 2.9 ([7, Lemma 2])**.** *Pour X tendant vers l'infini, on a l'égalité*

$$\operatorname{card} \mathcal{D}^{=}(X) \cap \mathbb{Z}^4 = O\big(X^{\frac{3}{4}} \log X\big).$$

Il faut aussi supprimer l'ensemble des formes réductibles. On considère ainsi $\mathcal{D}^{\text{réd}}(X)$, ensemble des (a,b,c,d) de $\mathcal{V}(X)$ tels que la forme cubique associée soit réductible. Cet ensemble est lui-aussi petit puisqu'on a le

Lemme 2.10 ([7, Lemma 3])**.** *Pour X tendant vers l'infini, on a, pour tout $\varepsilon > 0$, l'égalité*

$$\operatorname{card} \mathcal{D}^{réd}(X) \cap \mathbb{Z}^4 = O\big(X^{\frac{3}{4}+\varepsilon}\big).$$

Remarquons que la condition $\Delta(a,b,c,d) \neq 0$ est ici primordiale, sinon l'ensemble $\mathcal{D}^{\text{réd}}(X) \cap \mathbb{Z}^4$ considéré ci-dessus est infini pour tout $X \geqslant 0$.

On dénote par $\mathcal{D}^{\text{bord}}(X,\rho,Q)$ le complémentaire de l'amincissement $\underline{\mathcal{X}}_Q$ dans $\mathcal{X}$. On a donc l'inclusion

$$\mathcal{D}^{\text{bord}}(X,\rho,Q) \subset \bigcup_{j\in\mathcal{J}, j\notin\mathcal{I}} \mathcal{B}_j, \tag{8}$$

ce qui prouve que $\mathcal{D}^{\text{bord}}(X,\varepsilon,Q)$ n'est pas trop anarchique, puisqu'il est inclus dans

$$O\Big(Q^{-3} X^{\frac{3}{4}+3\rho} \log X + Q^{-1} X^{\frac{1}{4}+3\rho} + 1\Big)$$

boites ayant chacune Q^4 points entiers (Lemmes 2.6 et 2.7). On a donc la relation

$$\operatorname{card} \mathcal{D}^{\text{bord}}(X,\rho,Q) \cap \mathbb{Z}^4 \ll Q X^{\frac{3}{4}+3\rho} \log X + Q^3 X^{\frac{1}{4}+3\rho} + Q^4 =: E(X,\rho,Q). \tag{9}$$

Appelons donc $\mathcal{D}(X,\rho,Q)$ la réunion

$$\mathcal{D}(X,\rho,Q) = \mathcal{D}'(X,\rho) \cup \mathcal{D}^{\text{bord}}(X,\rho,Q),$$

où

$$\mathcal{D}'(X,\rho) := \mathcal{D}^{\text{pointe}}(X,\rho) \cup \mathcal{D}^0(X,\rho) \cup \mathcal{D}^{=}(X,\rho) \cup \mathcal{D}^{\text{réd}}(X,\rho).$$

On pose aussi

$$G(X,\rho,Q) = X^{1-\rho} + E(X,\rho,Q).$$

2.a.2. *Première évaluation de* $N_{0,q}(0,X,V)$. La notion de discriminant fondamental fait jouer un rôle particulier au nombre premier 2. Ceci nous amène à introduire de nouvelles notations dans le but de tenir compte de ce statut spécifique. Dans une première lecture, on pourra supposer que r et s sont impairs.

On dit que deux entiers r et s vérifient la condition (C.1) si

$$\text{(C.1)} \qquad \begin{cases} (r,s)=1 \\ v_p(rs)\leqslant 2 \quad (p\geqslant 3), \\ v_2(rs)=0,1, \text{ ou } 4. \end{cases}$$

Si r et s vérifient (C.1), pour toute boite $\mathcal{B}_i$ on note $N^*(\mathcal{B}_i;r,s)$ le nombre de points entiers (a,b,c,d) situés à l'intérieur de $\mathcal{B}_i$ tels que

- $(a,b,c,d,r)=1$,
- si 16 ne divise pas rs, rs divise $\Delta(a,b,c,d)$,
- si 16 divise rs, $\frac{rs}{16}$ divise $\Delta(a,b,c,d)$ et $\Delta(a,b,c,d)\in\{0,4\}$ modulo 16.

(Remarquons que $\Delta(F)\equiv(bc+ad)^2 \bmod 4$, donc $\Delta(F)$ modulo 4 ne peut prendre que les valeurs 0 ou 1 ; on a donc l'équivalence $\Delta(F)\in V_2 \iff \Delta(F)\notin\{0,4\}$ modulo 16.)

On désigne par $(C.2)_{r,s}$ l'ensemble de ces trois conditions sur (a,b,c,d). Enfin, on désigne par $H^*_{r,s}(X)$ le nombre de classes de formes cubiques $F=(a,b,c,d)$ irréductibles, primitives ou non, telles que (a,b,c,d) vérifie $(C.2)_{r,s}$ et telles que $1\leqslant\Delta(F)\leqslant X$. On définit finalement

$$\kappa(n)=\prod_{p\geqslant 3} p^{v_p(n)}.$$

En adoptant ces conventions et en regroupant les Lemmes 2.5, 2.8, 2.9 et 2.10 et la relation (9), on a la

Proposition 2.11. *Pour tout $\rho>0$, tout X et tout Q entiers supérieurs à 1, il existe un ensemble $\mathcal{D}=\mathcal{D}(X,\rho,Q)$, vérifiant*

$$\text{(10)} \qquad \operatorname{card}\mathcal{D}\cap\mathbb{Z}^4=O\big(G(X,\rho,Q)\big),$$

un ensemble d'hypercubes $\mathcal{B}_i$ ($i\in\mathcal{I}$) inclus dans $\mathbb{R}^4$, de côté de longueur égale à ξQ, tels que, pour tous les entiers r et s vérifiant (C.1)*, on ait l'égalité*

$$H^*_{r,s}(X)=\frac{1}{2}\sum_{i\in\mathcal{I}} N^*(\mathcal{B}_i;r,s)+O\Big(\sum_{\substack{(a,b,c,d)\in\mathcal{D}\\ \kappa(rs)\mid\Delta(a,b,c,d)}} 1\Big).$$

Rappelons que le facteur $\frac{1}{2}$ provient du fait qu'on s'intéresse à des classes modulo $\mathrm{SL}(2,\mathbb{Z})$. Nous aurons besoin de davantage de précision sur ces cubes $\mathcal{B}_i$:

Lemme 2.12. *Pour tout $\varepsilon>0$, on a l'égalité*

$$\sum_{i\in\mathcal{I}} N^*(\mathcal{B}_i;1,1)=\frac{\pi^2}{36}X+O\big(G(X,\rho,Q)\big),$$

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

$$\operatorname{card}\mathcal{I} \ll XQ^{-4}. \tag{11}$$

Preuve. Rappelons que la réunion des $\mathcal{B}_i$ ($i \in \mathcal{I}$) est l'amincissement d'ordre Q de $\mathcal{X}$ et que, hors des hyperplans de coordonnées, deux boites $\mathcal{B}_i$ distinctes n'ont pas en commun de points à coordonnées entières. On a donc l'encadrement

$$\begin{aligned}\sum_{i\in\mathcal{I}} N^*(\mathcal{B}_i;1,1) &\geqslant \operatorname{card}\mathcal{V}(X)\cap\mathbb{Z}^4 - \operatorname{card}\mathcal{D}(X,\rho,Q)\cap\mathbb{Z}^4\\ \sum_{i\in\mathcal{I}} N^*(\mathcal{B}_i;1,1) &\leqslant \operatorname{card}\mathcal{V}(X)\cap\mathbb{Z}^4 + O\big(\operatorname{card}\mathcal{D}^0(X,\rho)\cap\mathbb{Z}^4\big).\end{aligned}$$

Il reste à appliquer le Lemme 2.4 et la majoration (10) pour obtenir la première assertion. La majoration (11) est une conséquence directe du fait que

$$\operatorname{card}\mathcal{D}^0(X,\rho)\cap\mathbb{Z}^4 \leqslant \operatorname{card}\mathcal{V}(X)\cap\mathbb{Z}^4 = O(X)$$

et du fait que chaque $\mathcal{B}_i$ contient Q^4 entiers. Il est clair que pour $Q \gg X^{\frac{1}{4}}$, on peut avoir $\mathcal{I} = \emptyset$: la méthode de découpage n'a alors aucun intérêt. □

Le lien entre la fonction $N_{a,q}(0,X,V)$ de la Proposition 2.3 et la fonction $H^*_{r,s}(X)$ de la Proposition 2.11 se fait par le principe d'inclusion-exclusion sous la forme de l'égalité suivante et de ses variantes (voir §5 et §6), valable pour tout q sans facteur carré :

$$\begin{aligned}N_{0,q}(0,X,V) = &\sum_{(d,2q)=1}\mu(d)\sum_{\substack{\delta\mid q\\(\delta,2)=1}}\mu(\delta)H^*_{\delta q,d^2}(X)\\ &+\sum_{(2d,q)=1}\mu(2d)\sum_{\delta\mid q}\mu(\delta)H^*_{\delta q,16d^2}(X) + \sum_{(d,q)=1}\mu(d)\sum_{2\delta\mid q}\mu(2\delta)H^*_{8\delta q,d^2}(X).\end{aligned} \tag{12}$$

Dans cette expression, le premier terme détecte les éléments appartenant à l'intersection des V_p, pour p impair, les deux termes suivants s'occupant de l'appartenance à V_2, suivant que q est impair ou pair.

2.b. **Cas des discriminants négatifs.** La démarche est différente pour exhiber un représentant de chaque classe de Φ ou de $\tilde{\Phi}$. Le problème est de trouver un covariant quadratique adapté à cette situation. En effet le hessien ne remplit plus ce rôle, puisque c'est maintenant une forme quadratique indéfinie. Cette difficulté fut résolue par Mathews et Berwick ([15]) en associant à la forme $F = (a,b,c,d)$, la forme quadratique définie $Px^2+Qxy+Ry^2$ telle que

$$ax^3+bx^2y+cxy^2+dy^3 = (x-\theta y)(Px^2+Qxy+Ry^2),$$

avec θ, P, Q et R réels mais en général irrationnels. Cette forme quadratique se révèle être un covariant, à un scalaire multiplicatif près. Toute cette technique est exploitée dans ([8], [9] et [10]) et, bien sûr dans ([1] Théorèmes 3.5 et 3.11).

Dans notre cas, à l'arrivée, la situation est quasiment la même que pour les discriminants positifs. Maintenant le volume $\mathcal{V}(X)$ est

$$\mathcal{V}(X) = \Big\{(a,b,c,d);\ 1 \leqslant -\Delta(a,b,c,d) \leqslant X;\ d^2 - a^2 + ac - db \geqslant 0,$$
$$(a+b)(a+b+c) - ad \geqslant 0, \quad (a-b)(a-b+c) + ad \geqslant 0, \quad a \geqslant 1\Big\}.$$

La technique de découpage est la même que précédemment, la seule différence étant qu'à la fin le coefficient $\frac{\pi^2}{36}$, dans les Lemmes 2.4 et 2.12, doit être remplacé par $\frac{\pi^2}{12}$ ([8]).

3. Étude de $N^*(\mathcal{B}_i; r, s)$

Nous reprenons la démarche de Belabas ([1, §5]) mais en y incorporant de nouveaux ingrédients. Soit $\mathcal{B} = \mathcal{B}_i$ l'hypercube en question. On écrit donc

$$\mathcal{B} = [\alpha_1, \alpha_1 + \xi Q] \times [\alpha_2, \alpha_2 + \xi Q] \times [\alpha_3, \alpha_3 + \xi Q] \times [\alpha_4, \alpha_4 + \xi Q].$$

Puisque (r,s) vérifie (C.1), on décompose r et s de façon unique, en

$$r = r_1 r_2^2, \quad (r_1, r_2) = 1, \quad \mu^2(r_1) = 1,$$
$$s = s_1 s_2^2, \quad (s_1, s_2) = 1, \quad \mu^2(s_1) = 1,$$

et nous supposons dans un premier temps l'inégalité

$$Q \leqslant rs. \tag{13}$$

On développe en série de Fourier la fonction caractéristique de chacun des côtés. Si (13) est vérifiée, la fonction caractéristique χ du premier côté s'écrit

$$\chi(a) = \frac{1}{rs} \sum_{h_1 \pmod{rs}} \ \sum_{\alpha_1 \leqslant x_1 \leqslant \alpha_1 + \xi Q} e\Big(\frac{h_1(x_1 - a)}{rs}\Big),$$

avec $e(z) = \exp(2\pi i z)$. On voit alors que $N^*(\mathcal{B}; r, s)$ s'écrit comme

$$\frac{1}{(rs)^4} \sum_{\mathbf{h} \pmod{rs}} \ \sum_{\mathbf{x} \in \mathcal{B}} e\Big(\frac{\mathbf{h}\cdot\mathbf{x}}{rs}\Big) S(\mathbf{h}; r, s), \tag{14}$$

où on a posé $\mathbf{h} = (h_1, h_2, h_3, h_4)$, $\mathbf{x} = (x_1, x_2, x_3, x_4)$, le produit scalaire dans $\mathbb{R}^4$ étant noté par $\mathbf{h}\cdot\mathbf{x}$. Dans ce paragraphe, on réservera les lettres grasses aux vecteurs, et ceux-ci auront toujours quatre composantes. On a aussi posé

$$S(\mathbf{h}; r, s) = \sum e\Big(\frac{ah_1 + bh_2 + ch_3 + dh_4}{rs}\Big),$$

la somme étant faite sur les quadruplets (a,b,c,d) modulo rs satisfaisant $(C.2)_{r,s}$. Puisque r_1, r_2, s_1 et s_2 sont premiers entre eux deux à deux, on a l'égalité de multiplicativité

$$S(\mathbf{h}; r_1 r_2^2, s_1 s_2^2) = S(\mathbf{h}; r_1, 1) S(\mathbf{h}; r_2^2, 1) S(\mathbf{h}; 1, s_1), S(\mathbf{h}; 1, s_2^2),$$

conséquence du théorème chinois et de l'homogénéité des polynômes $\Delta(a,b,c,d)$ et $ah_1 + bh_2 + ch_3 + dh_4$. Toujours grâce à la multiplicativité, on est amené à étudier,

pour $p \geqslant 3$, $S(\mathbf{h}; 1, p^j)$ et $S(\mathbf{h}; p^j, 1)$ ($j = 1$ ou 2), et pour $p = 2$, $S(\mathbf{h}; 1, 2^j)$ et $S(\mathbf{h}; 2^j, 1)$ ($j = 1$ ou 4).

En se reportant au Lemme 4.6 de [1], lui-même hérité de ([10, Lemma 1]), les première et troisième égalités donnent la relation

$$S(\mathbf{0}; p^j, 1) = \nu_1(p^j).p^{4j},$$

avec

$$\nu_1(p) = \frac{(p+1)(p^2-1)}{p^4} \qquad \text{et} \qquad \nu_1(p^j) = 2\frac{(p^2-1)}{p^4} \quad (j > 1),$$

avec les mêmes conditions sur j que ci-dessus. En rajoutant les formes divisibles par p ($(a, b, c, d, p) = p$), on obtient

$$S(\mathbf{0}; 1, p^j) = \nu_2(p^j).p^{4j},$$

avec

$$\nu_2(p) = \frac{p^3+p^2-p}{p^4} \qquad \text{et} \qquad \nu_2(p^j) = \frac{2p^2-1}{p^4} \quad (j > 1).$$

Le terme principal de (14) est fourni par la contribution du terme où tous les h_i sont nuls ; il vaut donc (en étendant par multiplicativité la définition des fonctions ν_1 et ν_2)

$$\nu_1(r)\nu_2(s).N^*(\mathcal{B}; 1, 1). \tag{15}$$

Remarquons que $\nu_1(r)\nu_2(s)$ ainsi défini vérifie

$$\nu_1(r)\nu_2(s) = O(2^{\omega(rs)}(rs)^{-1}). \tag{16}$$

3.a. **Étude précise de $S(\mathbf{h}; p, 1)$.** Nous supposons que p est assez grand : $p \geqslant 5$. En utilisant l'invariance par multiplication par $\lambda \in \mathbb{F}_p^*$ on a l'égalité

$$S(\mathbf{h}; p, 1) = \frac{1}{p-1} \sum_{\lambda \in \mathbb{F}_p^*} \sum_{\substack{\mathbf{a} \in \mathbb{F}_p^4 \\ \mathbf{a} \neq 0, \Delta(\mathbf{a}) = 0}} e\big(\lambda \frac{\mathbf{a} \cdot \mathbf{h}}{p}\big).$$

En sommant sur λ, il apparaît des progressions géométriques, d'où l'égalité

$$S(\mathbf{h}; p, 1) = \frac{1}{p-1}\Big\{(p-1)\,|\{\mathbf{a}; \Delta(\mathbf{a}) = \mathbf{a}\cdot\mathbf{h} = 0 \pmod p,\ \mathbf{a} \neq 0 \pmod p\}| \\ - \quad |\{\mathbf{a}; \Delta(\mathbf{a}) = 0,\ \mathbf{a}\cdot\mathbf{h} \neq 0 \pmod p, \mathbf{a} \neq 0 \pmod p\}|\Big\}.$$

Soit encore

$$S(\mathbf{h}; p, 1) = \frac{1}{p-1}\big(p\nu(\mathbf{h}, p) - p^4\nu_1(p)\big), \tag{17}$$

où $\nu(\mathbf{h}, p)$ désigne le nombre de solutions de l'équation

$$\Delta(\mathbf{a}) = \mathbf{a}\cdot\mathbf{h} = 0 \pmod p, \quad \mathbf{a} \neq 0 \pmod p.$$

3.a.1. *Étude de* $\nu(\mathbf{h}, p)$. Tout d'abord, rappelons qu'on a trivialement

$$\nu(\mathbf{0}, p) = \nu_1(p)p^4 = p^3 + O(p^2).$$

Nous supposons dans la suite qu'on a $(\mathbf{h}, p) = 1$. Revenons maintenant à la signification de $\Delta(\mathbf{a}) = 0$ modulo p avec $\mathbf{a}$ non nul. Cette égalité signifie que la forme cubique F associée à $\mathbf{a} = (a_1, a_2, a_3, a_4)$

$$a_1x^3 + a_2x^2y + a_3xy^2 + a_4y^3$$

comporte, dans sa factorisation en facteurs linéaires sur $\overline{\mathbb{F}_p}$, un facteur double ou triple, ce facteur étant en fait à coefficients dans $\mathbb{F}_p$. Ceci équivaut donc au fait que F est de l'une ou l'autre des formes suivantes

(I) $$\alpha(x + \beta y)^2(x + \gamma y)$$

(II) $$\alpha y(x + \beta y)^2$$

(III) $$\alpha y^2(x + \beta y)$$

(IV) $$\alpha y^3.$$

Dans chacune de ces expressions, α, β et γ sont des éléments de $\mathbb{F}_p$, avec $\alpha \neq 0$. Les quatre cas s'excluent mutuellement et correspondent à la valeur du plus petit indice i tel que $a_i \neq 0$. Nous parvenons ainsi aux quatre paramétrisations

(I) $$\alpha(1, 2\beta + \gamma, \beta(2\gamma + \beta), \beta^2\gamma)$$

(II) $$\alpha(0, 1, 2\beta, \beta^2)$$

(III) $$\alpha(0, 0, 1, \beta)$$

(IV) $$\alpha(0, 0, 0, 1)$$

(α, β, γ) parcourant $\mathbb{F}_p^* \times \mathbb{F}_p \times \mathbb{F}_p$. Reportons chacune de ces paramétrisations dans l'équation $\mathbf{a} \cdot \mathbf{h} = 0$, et appelons $\nu_I(\mathbf{h}, p)$, $\nu_{II}(\mathbf{h}, p)$, $\nu_{III}(\mathbf{h}, p)$ et $\nu_{IV}(\mathbf{h}, p)$ le nombre de solutions trouvées dans chacun des cas. Il suffira d'appliquer l'égalité

$$\nu(\mathbf{h}, p) = \nu_{\mathrm{I}}(\mathbf{h}, p) + \nu_{\mathrm{II}}(\mathbf{h}, p) + \nu_{\mathrm{III}}(\mathbf{h}, p) + \nu_{\mathrm{IV}}(\mathbf{h}, p), \tag{18}$$

pour trouver la valeur de $\nu(\mathbf{h}, p)$.

3.a.2. *Étude de* $\nu_I(\mathbf{h}, p)$. Puisque α est non nul, il suffira de multiplier par $(p-1)$, le nombre de solutions à l'équation aux inconnues β et γ

$$(h_1 + 2\beta h_2 + \beta^2 h_3) + \gamma(h_2 + 2\beta h_3 + \beta^2 h_4) = 0. \tag{19}$$

- Si les deux polynômes en β, $(h_1 + 2\beta h_2 + \beta^2 h_3)$ et $(h_2 + 2\beta h_3 + \beta^2 h_4)$, n'ont pas de zéro commun, (19) a $p + O(1)$ solutions en couples (β, γ).
- Dans les autres cas, (19) a $O(p)$ solutions (nous pourrions être beaucoup plus précis, c'est inutile ici).

Les deux polynômes $(h_1+2\beta h_2+\beta^2 h_3)$ et $(h_2+2\beta h_3+\beta^2 h_4)$ ont un zéro commun dans $\overline{\mathbb{F}_p}$ si et seulement si leur résultant est nul. Un calcul facile montre que ce résultant vaut

$$\Delta^*(\mathbf{h}) := -\Delta(h_1, 3h_2, 3h_3, h_4)/27.$$

En conclusion, nous avons montré que

$$\nu_{\mathrm{I}}(\mathbf{h}, p) = p^2 + O(p) \quad \text{si } \Delta^*(\mathbf{h}) \neq 0 \pmod p$$

et

$$\nu_{\mathrm{I}}(\mathbf{h}, p) = O(p^2) \quad \text{si } \Delta^*(\mathbf{h}) = 0 \pmod p.$$

3.a.3. *Étude de ν_{II}, ν_{III} et ν_{IV}.* Un calcul facile montre que $\nu_{\mathrm{II}}(\mathbf{h}, p) = O(p)$ ou $O(p^2)$ suivant que $(h_2, h_3, h_4) \neq (0,0,0)$ ou $= (0,0,0)$ modulo p. De même, on a $\nu_{\mathrm{III}}(\mathbf{h}, p) = O(p)$ ou $O(p^2)$ suivant que $(h_3, h_4) \neq (0,0)$ ou $= (0,0)$ modulo p. Enfin, on a trivialement, $\nu_{\mathrm{IV}}(\mathbf{h}, p) = O(p)$.

Enfin, remarquons que si les deux dernières coordonnées de $\mathbf{h}$ sont nulles, on a $\Delta^*(\mathbf{h}) = 0$ modulo p. Il est alors facile de regrouper, grâce à (17) et (3.6), les différents résultats sous la forme du

Lemme 3.1. *La somme $S(\mathbf{h}; p, 1)$ vérifie la relation*

$$S(\mathbf{h}; p, 1) = O\big((\mathbf{h}, p)(\Delta^*(\mathbf{h}), p)p\big).$$

3.b. **Étude précise de $S(\mathbf{h}; 1, p)$.** On utilise l'égalité triviale

$$S(\mathbf{h}; 1, p) = S(\mathbf{h}; p, 1) + 1.$$

Le Lemme 3.1 entraîne alors le

Lemme 3.2. *La somme $S(\mathbf{h}; 1, p)$ vérifie la relation*

$$S(\mathbf{h}; 1, p) = O\big((\mathbf{h}, p)(\Delta^*(\mathbf{h}), p)p\big).$$

Les Lemmes 3.1 et 3.2 constituent donc une amélioration de ([1, Proposition 5.3]) qui donnait, pour les sommes en question, une majoration en $O\big((\mathbf{h}, p)\ p^2\big)$. Enfin, on peut interpréter notre étude de ces sommes comme un cas très particulier d'un résultat général de Katz et Laumon ([14, Introduction]) qui affirme que, pour $\mathbf{h}$ hors d'un fermé de Zariski, la somme trigonométrique

$$S(\mathbf{h}, \mathcal{V}) = \sum_{\mathbf{a} \in \mathcal{V}} e(\frac{\mathbf{a} \cdot \mathbf{h}}{p}),$$

où $\mathcal{V}$ est une variété de dimension k satisfaisant des hypothèses raisonnables, vérifie la relation $S(\mathbf{h}, \mathcal{V}) = O(p^{\frac{k}{2}})$. Dans notre cas, la structure particulière de $\mathcal{V}$ définie par $\Delta(a,b,c,d) = 0$, conduit à une définition explicite et agréable de ce fermé de Zariski comme lieu où $\Delta^*(\mathbf{h}) = 0$, ainsi qu'à un meilleur exposant que ce que l'on peut espérer en général.

3.c. **Étude précise de $S(\mathbf{h};p^2,1)$.** Dans un premier temps, nous supposons que $(\mathbf{h},p)=1$. La somme en question est donc

$$S(\mathbf{h};p^2,1)=\sum_{\substack{\Delta(\mathbf{a})=0 \pmod{p^2}\\(\mathbf{a},p)=1}} e\Big(\frac{\mathbf{a}\cdot\mathbf{h}}{p^2}\Big).$$

On écrit le vecteur $\mathbf{a}$ sous la forme

$$\mathbf{a}=\mathbf{a}^{(0)}+p\mathbf{a}^{(1)},$$

où chacun des vecteurs $\mathbf{a}^{(0)}$ et $\mathbf{a}^{(1)}$ a ses composantes comprises entre 0 et $p-1$. Par la formule de Taylor, on a

$$\Delta(\mathbf{a})=\Delta(\mathbf{a}^{(0)})+p(\mathrm{grad}_{\mathbf{a}^{(0)}}\Delta)\cdot\mathbf{a}^{(1)} \pmod{p^2}.$$

Si $\mathbf{a}^{(0)}$ est tel que $\Delta(\mathbf{a}^{(0)})=0$ modulo p, on appelle $H(\mathbf{a}^{(0)})$ l'ensemble des $\mathbf{x}$ de $\mathbb{F}_p^4$ tels que

$$(\mathrm{grad}_{\mathbf{a}^{(0)}}\Delta)\cdot\mathbf{x}=-\Delta(\mathbf{a}^{(0)})/p \pmod{p}.$$

Avec ces conventions, on voit que

$$S(\mathbf{h};p^2,1)=\sum_{\substack{\Delta(\mathbf{a}^{(0)})=0 \pmod{p}\\(\mathbf{a}^{(0)},p)=1}} e\Big(\frac{\mathbf{a}^{(0)}\cdot\mathbf{h}}{p^2}\Big)\sum_{\mathbf{a}^{(1)}\in H(\mathbf{a}^{(0)})} e\Big(\frac{\mathbf{a}^{(1)}\cdot\mathbf{h}}{p}\Big). \tag{20}$$

On constate que la seconde somme est nulle lorsque

- le vecteur $\mathrm{grad}_{\mathbf{a}^{(0)}}\Delta$ est nul modulo p : l'ensemble $H(\mathbf{a}^{(0)})$ est, suivant les cas, vide ou égal à $\mathbb{F}_p^4$,
- les vecteurs $\mathbf{h}$ et $\mathrm{grad}_{\mathbf{a}^{(0)}}\Delta$ ne sont pas colinéaires dans $\mathbb{F}_p^4$.

Ces remarques transforment la définition de $S(\mathbf{h};p^2,1)$ en

$$S(\mathbf{h};p^2,1)=\sum_{\mathbf{a} \pmod{p^2}} e\Big(\frac{\mathbf{a}\cdot\mathbf{h}}{p^2}\Big),$$

la somme étant faite sur les $\mathbf{a}$ tels que

$$\Delta(\mathbf{a})=0 \pmod{p^2},\ \mathrm{grad}_{\mathbf{a}}\Delta\neq 0 \pmod{p}, \mathrm{grad}_{\mathbf{a}}\Delta \parallel \mathbf{h} \pmod{p}, \tag{21}$$

le symbole $\parallel$ signifiant que les vecteurs sont parallèles. Nous utiliserons la formule suivante que l'on vérifie par calcul et qui donne la valeur du gradient du discriminant, en un point où celui-ci s'annule :

Lemme 3.3. *Soit* $\mathbf{a}$ *un vecteur de* $\big(\mathbb{Z}/p^2\mathbb{Z}\big)^4$ *auquel est associée la forme cubique*

$$\alpha(a_1x+a_2y)^2(b_1x+b_2y).$$

On a alors

$$\mathrm{grad}_{\mathbf{a}}\Delta=4\alpha(a_1b_2-b_1a_2)^3(a_2^3,-a_1a_2^2,a_1^2a_2,-a_1^3).$$

Bien qu'il soit possible, ici comme au §3.a, de raisonner avec un espace projectif sur l'anneau considéré (respectivement $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/p^2\mathbb{Z}$), nous avons préféré séparer les **a** apparaissant dans (21) en quatre sous–ensembles disjoints. Par analogie à ce qui a été fait au §3.a.1, on sépare donc les cas suivant la valeur du plus petit indice i tel que $a_i \neq 0$ modulo p. La situation est un peu plus délicate, puisqu'il s'agit de congruences modulo p^2 (remarquons que les formes cubiques ne doivent pas être totalement ramifiées modulo p, sinon le gradient est nul).

Développons ce raisonnement lorsque $i = 1$. Soit donc $F(x, y) = a_1x^3 + a_2x^2y + a_3xy^2 + a_4y^3$ une forme cubique modulo p^2, avec $(a_1, p) = 1$ et $\Delta(F) \equiv 0$ modulo p^2, avec toujours p nombre premier $\geqslant 5$. Puisque $\Delta(F) \equiv 0$ modulo p, $F(x, y)$ modulo p s'écrit

$$F(x, y) = u(x + vy)^2(x + wy)$$

avec $(u, p) = (v - w, p) = 1$. Le changement de variables $X = x + vy,\ Y = y$, qui correspond à l'action d'une matrice de $\mathrm{GL}(2, \mathbb{Z})$, permet d'écrire F comme

$$F(x, y) = G(X, Y) = uX^2\big(X + (w - v)Y\big) \pmod p.$$

Ainsi modulo p^2, $G(X, Y)$ s'écrit, pour certains k_1, k_2, k_3 et k_4 modulo p, comme

$$G(X, Y) = (u + k_1p)\big(X^3 + (w - v + k_2p)X^2Y + k_3pXY^2 + k_4pY^3\big).$$

Puisqu'on a $\Delta(F) \equiv \Delta(G) \equiv 0$ modulo p^2, on voit, par la formule explicite du discriminant en fonction des coefficients, qu'on a obligatoirement $k_4 \equiv 0$ modulo p. On peut alors écrire, modulo p^2, l'égalité

$$G(X, Y) = (u + k_1p)\Big(X + \frac{k_3p}{2(w - v)}Y\Big)^2\Big(X + \big(w - v - p(\frac{k_3}{w - v} - k_2)\big)Y\Big).$$

En revenant aux variables x et y, nous sommes donc parvenus à l'écriture (unique) de $F(x, y)$ modulo p^2 comme

$$\text{(I)} \qquad \alpha(x + \beta y)^2(x + \gamma y), \quad (\alpha, p) = (\beta - \gamma, p) = 1.$$

En raisonnant de même pour les valeurs $i = 2$, 3 et 4, on parvient aux trois autres cas

$$\text{(II)} \qquad \alpha(p\alpha_1x + y)(x + \beta y)^2, \quad (\alpha, p) = 1;$$

$$\text{(III)} \qquad \alpha(p\alpha_1x + y)^2(x + \beta y), \quad (\alpha, p) = 1;$$

$$\text{(IV)} \qquad \alpha(p\alpha_1x + y)^2(p\alpha_2x + y), \quad (\alpha, p) = 1.$$

Dans chacune de ces expressions (I), (II), (III) et (IV), α, β et γ parcourent l'ensemble des classes modulo p^2, α_1 et α_2 l'ensemble des classes modulo p. Ceci étant fixé, on voit que, suivant les cas, le gradient au point **a** est parallèle dans $\mathbb{F}_p^4$ au vecteur

$$\text{(I)} \qquad (\beta^3, -\beta^2, \beta, -1);$$

$$\text{(II)} \qquad (\beta^3, -\beta^2, \beta, -1);$$

$$\text{(III)} \qquad (1, 0, 0, 0);$$

Dans le cas (IV), le gradient est nul modulo p. Ainsi, si $\mathbf{h}$ modulo p n'est pas parallèle à l'une des formes (I), (II) ou (III), la somme $S(\mathbf{h};p^2,1)$ est nulle. Ceci nous autorise à supposer que $\mathbf{h}$ est de la forme

$$\mathbf{h} = \lambda(v^3, -uv^2, u^2v, -u^3) + p\mathbf{h}', \tag{22}$$

avec $(u,v) \in \mathbf{F}_p^2$, $(u,v) \neq (0,0)$, $\lambda \in \mathbb{F}_p^*$, $\mathbf{h}' = (h_1', h_2', h_3', h_4') \in \mathbb{F}_p^4$. Dans cette écriture, il n'y a pas unicité de λ, u et v. Notons $S_I(\mathbf{h};p^2,1)$ la contribution à $S(\mathbf{h};p^2,1)$ des $\mathbf{a}$ de la forme (I). Puisque cette famille est stable par multiplication par α modulo p^2 tel que $(\alpha,p)=1$, on a, par sommation de progressions géométriques, l'égalité

$$S_I(\mathbf{h};p^2,1) = \frac{1}{p^2-p} \sum_{\substack{\alpha \bmod p^2 \\ (\alpha,p)=1}} \sum_{\substack{(I) \\ \Delta(\mathbf{a})=0 \pmod{p^2} \\ \operatorname{grad}_{\mathbf{a}} \Delta \| \mathbf{h} \pmod p}} e\big(\alpha \frac{\mathbf{a}\cdot\mathbf{h}}{p^2}\big),$$

qui donne encore

(23)

$$\begin{aligned} S_{\mathrm{I}}(\mathbf{h}\,;p^2,1) = \\ p^2 \left|\left\{\mathbf{a} \text{ de la forme (I) avec } \alpha=1, \operatorname{grad}_{\mathbf{a}}\Delta \parallel \mathbf{h} \pmod p, \mathbf{a}\cdot\mathbf{h} \equiv 0 \pmod{p^2}\right\}\right| \\ -p \left|\left\{\mathbf{a} \text{ de la forme (I) avec } \alpha=1, \operatorname{grad}_{\mathbf{a}}\Delta \parallel \mathbf{h} \pmod p, \mathbf{a}\cdot\mathbf{h} \equiv 0 \pmod{p}\right\}\right|. \end{aligned}$$

Pour que les équations précédentes aient des solutions, il faut que dans l'écriture (22) de $\mathbf{h}$, on ait $u \neq 0$ modulo p. Ceci étant admis, on peut supposer que dans l'écriture de $\mathbf{h}$ on a $u=1$ et dans ce cas, on est ramené à ne considérer que les $\mathbf{a}$ de la forme (I), avec $\alpha=1$, $\beta=v$ et $\gamma \neq v$ modulo p.

Pour expliciter (23), on étudie maintenant la relation

$$\mathbf{a}\cdot\mathbf{h} = 0 \quad \text{modulo } p \text{ ou } p^2.$$

Avec les notations précédentes, on est ramené, après simplification par p, à l'équation

$$\mathbf{a}\cdot\mathbf{h}' = 0 \quad \text{modulo 1 ou } p,$$

suivant les cas. Soit encore à compter le nombre de (β,γ) modulo p^2, vérifiant $\beta = v$ modulo p, $\gamma \neq v$ modulo p, tels que

$$(h_1' + 2\beta h_2' + \beta^2 h_3') + \gamma(h_2' + 2\beta h_3' + \beta^2 h_4') = 0 \quad \text{modulo 1 ou } p. \tag{24}$$

Si on considère cette équation modulo 1, elle a évidemment $p^3 + O(p^2)$ solutions.

Regardons maintenant (24) modulo p : on introduit le vecteur $\Upsilon(\mathbf{h})$, de $\mathbb{F}_p^2$, défini par

$$\Upsilon(\mathbf{h}) = (u^2h_1' + 2uvh_2' + v^2h_3', u^2h_2' + 2uvh_3' + v^2h_4') := (\Upsilon_1(\mathbf{h}), \Upsilon_2(\mathbf{h})),$$

cette définition dépend évidemment du choix de (u,v) dans l'écriture (22), mais ceci est sans importance pour les applications. On a facilement

- si $\Upsilon(\mathbf{h}) = (0,0)$, cette équation a $p^3 + O(p^2)$ solutions,
- si $\Upsilon_2(\mathbf{h}) = 0$ et $\Upsilon_1(\mathbf{h}) \neq 0$, (24) n'a aucune solution,

- dans les autres cas, c'est–à–dire $\Upsilon_2(\mathbf{h}) \neq 0$, (24) a $p^2 + O(p)$ solutions.

En se retournant vers (23), nous avons donc montré que si $\mathbf{h}$ modulo p n'est pas de la forme $(\beta^3, -\beta^2, \beta, -1)$ modulo p, la somme $S_{\mathrm{I}}(\mathbf{h}; p^2, 1)$ est nulle. Si $\mathbf{h}$ est de la forme précédente, $S_{\mathrm{I}}(\mathbf{h}; p^2, 1)$ vaut $p^5 + O(p^4)$ si $\Upsilon(\mathbf{h}) = (0, 0)$ et $O(p^4)$ si $\Upsilon(\mathbf{h}) \neq (0, 0)$.

L'étude de $S_{\mathrm{II}}(\mathbf{h}; p^2, 1)$ est plus aisée puisque nous ne sommes guère exigeants. Une démarche identique montre qu'on a nécessairement $\beta \equiv v$ modulo p, si on veut que $\mathbf{h}$, décomposé par (22) avec $u = 1$, soit parallèle au gradient (voir (II)). De façon triviale, on voit que pour le triplet $(\alpha, \beta, \alpha_1)$ on a effectivement $O(p^4)$ choix, et ceci sert de majoration pour S_{II}. Finalement, l'étude de S_{III} est identique à celle de S_{I}, à condition de n'envisager que des $\mathbf{h}$ qui, dans l'écriture (22), sont tels que $v = 1$ et $u = 0$.

Pour tenir compte de ces différentes situations, on définit $\Xi(\mathbf{h}, p)$ par les formules suivantes :

- Si $\mathbf{h}$ modulo p n'est pas de la forme
$$\mathbf{h} = \lambda(v^3, -uv^2, u^2v, -u^3) + p\mathbf{h}',$$
avec $(u, v) \in \mathbf{F}_p^2$, $\lambda \in \mathbb{F}_p^*$, $\mathbf{h}' = (h_1', h_2', h_3', h_4') \in \mathbb{F}_p^4$, on pose $\Xi(\mathbf{h}, p) = 1$,
- Si $\mathbf{h}$ est de la forme précédente, on pose
$$\Xi(\mathbf{h}, p) = (\Upsilon_1(\mathbf{h}), \Upsilon_2(\mathbf{h}), p),$$
avec $\big(\Upsilon_1(\mathbf{h}), \Upsilon_2(\mathbf{h})\big)$ défini ci–dessus. Il est facile de vérifier, pour tout a premier à p, la relation
$$\Xi(a\mathbf{h}, p) = \Xi(\mathbf{h}, p).$$

La majoration universelle
$$\big|S(\mathbf{h}; p^2, 1)\big| \leqslant \big|S(\mathbf{0}; p^2, 1)\big| \leqslant \nu_1(p^2).p^8 = O(p^6).$$
nous permet de traiter le cas $(\mathbf{h}, p) = p$, qui implique d'ailleurs $\Xi(\mathbf{h}, p) = p$. On regroupe ces différents résultats en le

Lemme 3.4. *La somme $S(\mathbf{h}; p^2, 1)$ vérifie la relation*
$$S(\mathbf{h}; p^2, 1) = O\big((\mathbf{h}, p) \cdot \Xi(\mathbf{h}, p).p^4\big).$$

3.d. **Étude précise de $S(\mathbf{h}; 1, p^2)$.** On utilise la majoration triviale
$$\big|S(\mathbf{h}; 1, p^2) - S(\mathbf{h}; p^2, 1)\big| \leqslant \big|\big\{\mathbf{a} \pmod{p^2}; (\mathbf{a}, p) = p\big\}\big| = p^4,$$
le Lemme 3.4 entraîne alors le

Lemme 3.5. *La somme $S(\mathbf{h}; 1, p^2)$ vérifie la relation*
$$S(\mathbf{h}; 1, p^2) = O\big((\mathbf{h}, p) \cdot \Xi(\mathbf{h}, p).p^4\big).$$

Les Lemmes 3.4 et 3.5 améliorent ainsi la Proposition 5.3 de [1], où on trouve pour $S(\mathbf{h}; p^2, 1)$ et $S(\mathbf{h}; 1, p^2)$ une majoration en $O((\mathbf{h}, p)p^5)$.

3.e. **Formule finale pour $N^*(\mathcal{B}_i;r,s)$.** Par les formules (14) et (15), on obtient

$$N^*(\mathcal{B}_i;r,s)=\nu_1(r)\nu_2(s)N^*(\mathcal{B}_i;1,1) + \frac{1}{(rs)^4}\sum_{\substack{\mathbf{h}\ (\mathrm{mod}\ rs)\\ \mathbf{h}\neq\mathbf{0}}}\sigma_1(h_1)\sigma_2(h_2)\sigma_3(h_3)\sigma_4(h_4)S(\mathbf{h};r,s), \tag{25}$$

avec (r,s) vérifiant (C.1) et

$$\sigma_i(h_i)=\sum_{\alpha_i\leqslant x_i\leqslant\alpha_i+\xi Q} e\Big(\frac{h_ix_i}{rs}\Big).$$

Signalons d'emblée la majoration

$$\sigma_i(h_i)=O\big(\min(Q,\Big\|\frac{h_i}{rs}\Big\|^{-1})\big), \tag{26}$$

où $\|x\|$ désigne la distance du réel x à l'entier le plus proche. On décompose toujours r et s comme au début du §3 et on définit par multiplicativité

$$\Xi(\mathbf{h},r_2s_2)=\prod_{\substack{p\mid r_2s_2\\ p>3}}\Xi(\mathbf{h},p).$$

Par la multiplicativité de la somme S et par application des Lemmes Lemme 3.1, Lemme 3.2, Lemme 3.4 et Lemme 3.5, on a la majoration

$$S(\mathbf{h};r,s)=O\Big((\mathbf{h},r_1s_1)(\mathbf{h},r_2s_2)(\Delta^*(\mathbf{h}),r_1s_1)\Xi(\mathbf{h},r_2s_2)r_1s_1(r_2s_2)^4C^{\omega(rs)}\Big), \tag{27}$$

pour une certaine constante absolue C.

Le second terme à droite de (25) est noté T, c'est un terme d'erreur que nous allons majorer en utilisant (27). Soient δ_1, D_1, δ_2 et D_2 quatre entiers tels que

$$\delta_1|D_1|r_1s_1 \quad\text{et}\quad \delta_2|D_2|r_2s_2. \tag{28}$$

Notons $\Lambda(\delta_1,D_1;\delta_2,D_2)$ la somme

$$\Lambda(\delta_1,D_1;\delta_2,D_2)=\sum_{\substack{\mathbf{h}\ \mathrm{mod}\ rs\\ \mathbf{h}\neq0}}|\sigma_1(h_1)|\,|\sigma_2(h_2)|\,|\sigma_3(h_3)|\,|\sigma_4(h_4)|\,,$$

la variable de sommation $\mathbf{h}$ vérifiant en plus les conditions de sommation

$$(\mathbf{h},r_1s_1)=\delta_1,\ (\mathbf{h},r_2s_2)=\delta_2,\ (\Delta^*(\mathbf{h}),r_1s_1)=D_1,\ \Xi(\mathbf{h},r_2s_2)=D_2.$$

Avec ces notations, on voit que T vérifie la relation

$$T\ll\frac{(rs)^\varepsilon}{(r_1s_1)^3(r_2s_2)^4}\sum_{\delta_1}\sum_{\delta_2}\sum_{D_1}\sum_{D_2}\delta_1\delta_2D_1D_2\Lambda(\delta_1,D_1;\delta_2,D_2), \tag{29}$$

avec δ_1, δ_2, D_1 et D_2 vérifiant (28).

Pour $0\leqslant i\leqslant 3$, on note $\Lambda^{(i)}(\delta_1,D_1;\delta_2,D_2)$ les contributions à $\Lambda(\delta_1,D_1;\delta_2,D_2)$ des $\mathbf{h}$ ayant exactement i composantes nulles modulo rs. Les quantités $T^{(i)}$, se

définissent de façon analogue à partir de T. Ces quantités $T^{(i)}$ et $\Lambda^{(i)}$ vérifient une inégalité analogue à (29).

3.e.1. *Étude de* $\Lambda(\delta_1, D_1; \delta_2, D_2)$. Il est naturel de faire le changement de variables $\mathbf{h} = \delta_1\delta_2\mathbf{k}$. Le vecteur $\mathbf{k}$ vérifie alors les relations

$$(\Delta^*(\mathbf{k}), \frac{r_1 s_1}{\delta_1}) = \frac{D_1}{\delta_1}, \quad \Xi(\mathbf{k}, \frac{r_2 s_2}{\delta_2}) = \frac{D_2}{\delta_2},$$

et ses quatre composantes parcourent les classes modulo $K := \frac{rs}{\delta_1\delta_2}$. Nous gardons aussi la condition $\mathbf{k} \neq 0$ modulo K et la condition de coprimalité $(\mathbf{k}, \frac{r_1 s_1}{\delta_1}\frac{r_2 s_2}{\delta_2}) = 1$.

Nous éclatons la sommation sur $\mathbf{k}$ en imposant la valeur des facteurs communs à k_1, k_2, $\frac{D_1}{\delta_1}$ et $\frac{D_2}{\delta_2}$. Soit d_1 un diviseur de $\frac{D_1}{\delta_1}$ et d_2 un diviseur de $\frac{D_2}{\delta_2}$. Notons qu'il y a $O\big((rs)^\varepsilon\big)$ couples (d_1, d_2). Appelons $\Lambda_{d_1,d_2}(\delta_1, D_1; \delta_2, D_2)$ la somme définie par les mêmes conditions que $\Lambda(\delta_1, D_1; \delta_2, D_2)$, à la différence près que le vecteur $\mathbf{k} = (k_1, k_2, k_3, k_4) = (\delta_1\delta_2)^{-1}\mathbf{h}$ vérifie les propriétés suivantes

- $(k_1, k_2, \frac{D_1}{\delta_1}) = d_1$,
- $(k_1, k_2, \frac{D_2}{\delta_2}) = d_2$.

Ceci étant posé, on voit que, pour $i = 1$ ou 2, k_i est de la forme $k_i = d_1 d_2 n_i$ avec $0 \leqslant n_i \leqslant K/(d_1 d_2)$. Étudions maintenant les congruences que doit vérifier k_3 modulo d_2 et $\frac{D_2}{d_2\delta_2}$:

- Si $p|d_2$, $\mathbf{k}$ doit être de la forme $\lambda(v^3, -uv^2, u^2v, -u^3)$. On a donc $v = 0$ modulo p et $u \neq 0$ modulo p (sinon on aurait $p|(\mathbf{k}, \frac{r_2 s_2}{\delta_2})$ ce qui est interdit), donc $p|k_3$. Or on doit avoir aussi $p|\Upsilon_1(\mathbf{k})$ donc $p|k_1'$. En conclusion, on a les relations $d_2^2|k_1$ et $d_2|k_3$ (on a décomposé $\mathbf{k}$ modulo p comme on l'a fait en (22) pour $\mathbf{h}$).
- Si p divise $\frac{D_2}{d_2\delta_2}$. Le fait que $\mathbf{k}$ mod p soit de la forme $\lambda(v^3, -uv^2, u^2v, -u^3)$ entraîne que, lorsque k_1 et k_2 sont connus modulo p, on a $v \neq 0$ modulo p et qu'il y a $O(1)$ possibilités pour k_3 et k_4 modulo p. Puis, l'équation $p|\Upsilon_1(\mathbf{k})$ entraîne que k_3' modulo p ne peut prendre qu'une valeur lorsque u et v ont leurs valeurs fixées modulo p.

Terminons par les congruences que k_4 doit vérifier modulo d_1, $\frac{D_1}{d_1\delta_1}$, d_2 et $\frac{D_2}{d_2\delta_2}$.

- Si $p|d_1$, le polynôme $\Delta^*(k_1, k_2, k_3, k_4)$, considéré comme polynôme en k_4 modulo p, est formellement nul. Ceci n'entraîne donc aucune contrainte pour k_4 modulo p, lorsque $k_1 = k_2 = 0$, modulo p.
- Si $p|\frac{D_1}{d_1\delta_1}$ et par conséquent p ne divise pas (k_1, k_2), le polynôme précédent n'est pas formellement nul. Lorsque k_1, k_2 et k_3 sont fixés, il y a au plus 2 valeurs pour k_4 modulo p telles que $\Delta^*(\mathbf{k}) = 0$ modulo p.
- Si $p|d_2$ l'équation $\Upsilon_2(\mathbf{k}) = 0$ entraîne $p|k_2'$, ce qui signifie que $d_2^2|k_2$. En se reportant à ce qui précède, nous avions montré que $d_2^2|k_1$ et que $d_2|k_3$.
- Si $p|\frac{D_2}{d_2\delta_2}$ et ne divise donc pas d_2, en poursuivant le raisonnement fait pour k_3 dans ce cas, on voit que $v \neq 0$ modulo p, que k_4 modulo p est connu

dès que k_1 et k_2 le sont. Enfin l'équation $p|\Upsilon_2(\mathbf{k})$ entraîne la connaissance de k_4' modulo p.

Nous retiendrons de la discussion précédente les renseignements suivants, qui nous seront utiles pour l'étude de $\Lambda_{d_1,d_2}(\delta_1, D_1; \delta_2, D_2)$:

- La condition $(k_1, k_2, \frac{D_1}{\delta_1}) = d_1$ n'entraîne aucune contrainte particulière pour k_3 et k_4 modulo d_1.
- Lorsque k_1, k_2 et k_3 sont fixés modulo $\frac{D_1}{d_1\delta_1}$, il y a au plus $O((r_1s_1)^\varepsilon)$ solutions pour k_4 modulo $\frac{D_1}{d_1\delta_1}$ à l'équation $\Delta^*(\mathbf{k}) = 0$.
- On a en fait les relations plus précises $d_2^2|k_1$, $d_2^2|k_2$ et $d_2|k_3$.
- Si k_1 et k_2 sont fixés modulo $(\frac{D_2}{d_2\delta_2})^2$, les nombres k_3 et k_4 appartiennent à $O\big((r_2s_2)^\varepsilon\big)$ classes de congruences modulo $(\frac{D_2}{d_2\delta_2})^2$.

3.e.2. *Étude de* $\Lambda^{(0)}(\delta_1, D_1; \delta_2, D_2)$. Nous allons majorer $\Lambda^{(0)}_{d_1,d_2}(\delta_1, D_1; \delta_2, D_2)$ en sommant d'abord sur k_4. D'après l'étude précédente, on voit que, lorsque k_1, k_2 et k_3 sont fixés, il existe $O\big((rs)^\varepsilon\big)$ entiers ν tels que

$$1 \leqslant \nu \leqslant L_4 := \frac{D_1}{d_1\delta_1}\Big(\frac{D_2}{d_2\delta_2}\Big)^2, \quad \text{et } k_4 \text{ est de la forme } k_4 = \nu + \ell L_4,$$

avec $0 \leqslant \ell \leqslant KL_4^{-1}$. Lorsque k_4 est associé à la valeur $\ell = 0$, on applique la majoration

$$\sigma_4(\delta_1\delta_2k_4) \ll Q.$$

Lorsque $\ell \geqslant 1$, on a la majoration

$$\sigma_4(\delta_1\delta_2k_4) \ll \frac{rs}{\delta_1\delta_2L_4}.\frac{1}{\ell}$$

(voir (26)) car on peut toujours se restreindre au cas où $1 \leqslant \delta_1\delta_2k_4 \leqslant \frac{rs}{2}$. Ceci conduit à l'inégalité

$$\sum_{h_4} |\sigma_4(h_4)| \ll \Big(Q + \frac{rsd_1d_2^2\delta_2}{D_1D_2^2}\Big).(rs)^\varepsilon. \tag{30}$$

Pour sommer sur k_3, on remarque que, lorsque k_1 et k_2 sont fixés, il existe des entiers ν tels que

$$1 \leqslant \nu \leqslant L_3 := \frac{D_2^2}{d_2\delta_2^2} \quad \text{et } k_3 \text{ est de la forme } k_3 = \nu + \ell L_3$$

avec $0 \leqslant \ell \leqslant KL_3^{-1}$. Le nombre des ν est en $O\big((rs)^\varepsilon\big)$. En différenciant, comme précédemment, les cas $\ell = 0$ et $\ell \neq 0$ on parvient à

$$\sum_{h_3} |\sigma_3(h_3)| \ll \Big(Q + \frac{rsd_2\delta_2}{\delta_1D_2^2}\Big).(rs)^\varepsilon. \tag{31}$$

Il reste à sommer sur k_1 et k_2. Nous ne conservons que la propriété que chacun de ces entiers est divisible par $d_1 d_2^2$, d'où la majoration

$$\sum_{h_2} |\sigma_2(h_2)| \ll \frac{rs}{\delta_1\delta_2 d_1 d_2^2}.(rs)^\varepsilon, \tag{32}$$

et une majoration identique pour la somme sur h_1. En regroupant (30), (3.19) et (3.20), nous sommes parvenus à

$$\Lambda^{(0)}_{d_1,d_2}(\delta_1, D_1; \delta_2, D_2) \ll \Big(\frac{rs}{\delta_1\delta_2 d_1 d_2^2}\Big)^2 \Big(Q + \frac{rs d_2\delta_2}{\delta_1 D_2^2}\Big)\Big(Q + \frac{rs d_1 d_2^2 \delta_2}{D_1 D_2^2}\Big).(rs)^\varepsilon$$

ce qui conduit, après sommation sur $d_1 | \frac{D_1}{\delta_1}$ et $d_2 | \frac{D_2}{\delta_2}$, à la majoration suivante :

$$\Lambda^{(0)}(\delta_1, D_1; \delta_2, D_2) \ll \Big(\frac{rs}{\delta_1\delta_2}\Big)^2 \Big(Q + \frac{rs\delta_2}{\delta_1 D_2^2}\Big)\Big(Q + \frac{rs\delta_2}{D_1 D_2^2}\Big).(rs)^\varepsilon.$$

En reportant dans l'analogue de (29) pour $T^{(0)}$, on obtient, après sommation sur les δ_1, δ_2, D_1 et D_2, la majoration

$$T^{(0)} \ll \vartheta(rs, Q)(rs)^\varepsilon. \tag{33}$$

avec

$$\vartheta(rs, Q) = r_1 s_1 (r_2 s_2)^4 + r_1 s_1 (r_2 s_2)^2 Q + r_2 s_2 Q^2,$$

où nous avons décomposé $r = r_1 r_2^2$, $s = s_1 s_2^2$ comme au début du §3.

3.e.3. *Étude de* $\Lambda^{(1)}(\delta_1, D_1; \delta_2, D_2)$. On étudie donc la contribution des $\mathbf{h}$ avec une seule coordonnée nulle. Imaginons que $h_3 = 0$. On utilise la majoration triviale $\sigma_3(0) \ll Q \ll \Big(Q + \frac{rs d_2\delta_2}{\delta_1 D_2^2}\Big).(rs)^\varepsilon$. On reconnaît alors (31), les calculs précédents donnent donc

$$T^{(1)} \ll \vartheta(rs, Q)(rs)^\varepsilon. \tag{34}$$

Le cas où h_4 est nul est conduit de même. Par contre si h_1 ou h_2 est nul, on utilise la relation d'échange de variables $\Delta(a, b, c, d) = \Delta(d, c, b, a)$, pour se ramener au cas précédent.

3.e.4. *Étude de* $\Lambda^{(2)}(\delta_1, D_1; \delta_2, D_2)$. Le cas où nous aurions $h_3 = h_4 = 0$ se traite en utilisant $\sigma_3(0)$, $\sigma_4(0) \ll Q$ et en se ramenant aux inégalités (30) et (3.19). Par contre on ne peut pas, par échange de variables, se ramener à ce cas, lorsque par exemple on a $h_2 = h_3 = 0$. Nous faisons alors une étude directe assez simple. On a d'après la définition, la majoration

$$\Lambda^{(2)}(\delta_1, D_1; \delta_2, D_2) \ll Q^2 \sum_{\substack{\delta_1\delta_2 | h_1 \\ 1 \leqslant h_1 \leqslant rs}} \frac{rs}{h_1} \sum_{\substack{\delta_1\delta_2 | h_4 \\ 1 \leqslant h_4 \leqslant rs}} \frac{rs}{h_4} \ll Q^2 \frac{(rs)^{2+\varepsilon}}{\delta_1^2\delta_2^2},$$

en reportant cette majoration dans l'analogue de (29) pour $T^{(2)}$, on a finalement

$$T^{(2)} \ll (r_2 s_2 Q^2)(rs)^\varepsilon \tag{35}$$

3.e.5. *Étude de* $\Lambda^{(3)}(\delta_1, D_1; \delta_2, D_2)$. Dans cette situation, nous utilisons la majoration

$$\Lambda^{(3)}(\delta_1, D_1; \delta_2, D_2) \ll Q^3 \sum_{\substack{\delta_1\delta_2|h_1 \\ 1\leqslant h_1\leqslant rs}} \frac{rs}{h_1} \ll Q^3 \frac{(rs)^{1+\varepsilon}}{\delta_1\delta_2},$$

qui fournit la majoration

$$T^{(3)} \ll \frac{Q^3}{r_1s_1r_2s_2}.(rs)^{\varepsilon} \ll r_2s_2Q^2.(rs)^{\varepsilon}, \tag{36}$$

puisqu'on a supposé (13). En regroupant les relations (33),. . .,(36), on a finalement

$$T \ll \vartheta(rs, Q)(rs)^{\varepsilon} \tag{37}$$

Finalement, les formules (25) et (37) donnent l'expression

$$N^*(\mathcal{B}; r, s) = \nu_1(r)\nu_2(s)N^*(\mathcal{B}; 1, 1) + O\big(\vartheta(rs, Q)(rs)^{\varepsilon}\big). \tag{38}$$

valable pour $1 \leqslant Q \leqslant rs$, r et s vérifiant (C.1), avec $\vartheta(rs, Q)$ défini en (33).

Signalons que, le résultat de ([1, p. 929]), transposé dans nos notations, conduit à la valeur moins forte $\vartheta(rs, Q) = (r_1s_1)^2(r_2s_2)^5$ (toujours pour $Q \leqslant rs = r_1s_1(r_2s_2)^2$) et que (38) reste vraie si $\mathcal{B}$ est le produit de 4 intervalles de longueurs inférieures à Q. Par contre, lorsque $\mathcal{B}$ est une boite avec $Q = rs$, cette boite contient un représentant et un seul des classes modulo rs dans $\mathbb{Z}^4$. Il n'y a donc pas lieu de faire un développement en série de Fourier (14).

Dans le cas où (13) n'est pas vérifié, on décompose $\mathcal{B}$ en $O\big((Q(rs)^{-1} + 1)^4\big)$ cubes de côté rs ou de *cubes incomplets* (produit de 4 intervalles de longueurs inférieures à ξrs, situés sur les bords du découpage de $\mathcal{B}$). On applique alors (38) à chacun des cubes incomplets et ceux-ci sont au nombre de $O\big((Q(rs)^{-1} + 1)^3\big)$. En posant

$$\begin{cases} \vartheta^*(rs, Q) &= \vartheta(rs, \min(rs, Q)) \quad \text{si } rs \neq Q \\ \vartheta^*(rs, rs) &= 0 \end{cases}$$

on peut énoncer la

Proposition 3.6. *Soient r et s vérifiant* (C.1)*. Pour tout cube $\mathcal{B}$ de côté ξQ, on a l'égalité*

$$N^*(\mathcal{B}; r, s) = \nu_1(r)\nu_2(s)N^*(\mathcal{B}; 1, 1) + O\Big(\vartheta^*(rs, Q)(Q(rs)^{-1} + 1)^3(rs)^{\varepsilon}\Big).$$

En regroupant la Proposition 2.11, le Lemme 2.12, la Proposition 3.6 et (16), on peut énoncer la

Proposition 3.7. *Pour tout $\varepsilon > 0$, tout ρ, tout $Q \geqslant 1$, tous entiers r et s vérifiant* (C.1)*, on a l'égalité*

$$H^*_{r,s}(X) = \nu_1(r)\nu_2(s)\frac{\pi^2}{72}X + O\Big(\sum_{\substack{(a,b,c,d)\in\mathcal{D}\\ \kappa(rs)|\Delta(a,b,c,d)}} 1\Big) + O\Big(\vartheta^*(rs,Q)Q^{-4}X(Q(rs)^{-1}+1)^3(rs)^{\varepsilon} + (rs)^{-1+\varepsilon}G(X,\rho,Q)\Big) \tag{39}$$

Une égalité similaire a lieu pour les discriminants négatifs à condition de remplacer 72 *par* 24*.*

Rappelons que $\mathcal{D}$ est constitué de la réunion de $\mathcal{D}^{\mathrm{bord}}(X,\rho,Q)$ et d'autres sous-ensembles qui contiennent $O(X^{1-\rho}+X^{\frac{3}{4}+\varepsilon})$ points entiers (voir la définition de $\mathcal{D}(X,\rho,Q)$, après (9)). L'ensemble $\mathcal{D}^{\mathrm{bord}}(X,\rho,Q)$ n'est pas trop alambiqué, puisqu'il est inclus dans les boites $\mathcal{B}_j$ avec $j \in \mathcal{J}$ et $j \notin \mathcal{I}$. Ces boites sont au nombre de $O(Q^{-4}E\big(X,\rho,Q)\big)$ (voir (8)), pour lesquelles la Proposition 3.6 s'applique. Nous pouvons énoncer la

Proposition 3.8. *Pour tout $X \geqslant 1$, tout $\varepsilon > 0$, tout $\rho > 0$, tout $Q \geqslant 1$, il existe un ensemble $\mathcal{D}' = \mathcal{D}'(X,\rho)$ de cardinal $O(X^{1-\rho}+X^{\frac{3}{4}+\varepsilon})$ tel qu'on ait, pour tout r et s vérifiant* (C.1)*, l'égalité*

$$H^*_{r,s}(X) = \nu_1(r)\nu_2(s)\frac{\pi^2}{72}X + O\Big(\sum_{\substack{(a,b,c,d)\in\mathcal{D}'\\ \kappa(rs)|\Delta(a,b,c,d)}} 1\Big). \tag{40}$$

$$+\quad O\Big(\vartheta^*(rs,Q)Q^{-4}(X+E(X,\rho,Q))(Q(rs)^{-1}+1)^3(rs)^{\varepsilon}+(rs)^{-1+\varepsilon}G(X,\rho,Q)\Big)$$

Une égalité similaire a lieu pour les discriminants négatifs à condition de remplacer 72 *par* 24*.*

Si on majore trivialement le premier terme d'erreur par $O(\operatorname{card}\mathcal{D}')$, on a déjà un renseignement intéressant mais uniquement pour les petites valeurs de rs.

4. Théorèmes de type Brun-Titchmarsh

La Proposition 3.8 souffre d'être sans intérêt lorsque r_2s_2 (voir la décomposition de l'entier r donnée lors de l'énoncé de (C.1)) est grand. Pour cribler et ainsi accéder à des discriminants fondamentaux, il nous faut donc d'autres idées. Les énoncés des Propositions 4.1 et 4.4 ne sont pas sans rappeler leurs équivalents pour la répartition des nombres premiers dans les progressions arithmétiques de raisons trop grandes pour être abordées par les méthodes actuelles d'analyse complexe.

4.a. **Un résultat individuel.** Nous montrerons la

Proposition 4.1. *Soit q et n deux entiers sans facteur carré, 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 V_q est*

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

Cet énoncé est de la même veine que le Lemme 6.4 de [1] (lui-même hérité de [10]) mais il est plus général (l'entier n n'est plus nécessairement premier) et plus précis, puisque la Proposition 3.8 remplace avantageusement la Proposition 5.5 de [1].

4.a.1. *Lemmes préparatoires.* Comme dans [10] et dans [1], on commence par compter le nombre de classes de formes cubiques, dont le hessien est réductible (signalons qu'un tel hessien est improprement équivalent à une forme quadratique du type $My(kx+\ell y)$, avec $0\leqslant l<k$ et $(k,\ell)=1$). Soit τ la fonction nombre de diviseurs. On a

Lemme 4.2. *Soit $B(k,M)$ le nombre de classes de formes cubiques dont le hessien est équivalent à $My(kx+\ell y)$ avec $0\leqslant\ell<k$ et $(k,\ell)=1$. On a alors l'inégalité*

$$B(k,M)\leqslant 2k\tau(M).$$

De plus, si n sans facteur carré divise k et vérifie $(n,M)=1$, on a l'inégalité plus précise

$$B(k,M)\leqslant 6^{\omega(n)}k\tau(M)/n.$$

Preuve. On se reporte à la démonstration de ([10, Lemma 8]). Si $F=ax^3+bx^2y+cxy^2+dy^3$, on voit que F est déterminée par les valeurs de a, k, ℓ et M. On a aussi les congruences

$$3a\ell^2\equiv 0\ (\mathrm{mod}\ k^2)\quad\text{et}\quad 9a^2\ell^3\pm Mk^4\equiv 0\ (\mathrm{mod}\ 9ak^3).$$

Si $k=1$, alors $\ell=0$ et la deuxième congruence prouve que que a divise M, soit $\tau(M)$ choix possibles.

Si $k\neq 1$, on pose $s=3ak^{-2}$ ($\in\mathbb{N}$), d'où $s^2\ell^3\pm M\equiv 0$ modulo $3sk$, soit $s|M$. On a donc $\tau(M)$ choix possibles pour s, donc pour a. On a donc au plus k choix pour ℓ et le $\pm$ donne le facteur 2. D'où la première partie du Lemme 4.2.

Maintenant si $p|k$, avec $(p,M)=1$, alors p ne divise pas s et la congruence $s^2\ell^3\pm M\equiv 0$ modulo p a au plus 6 solutions en ℓ, donc au plus $6^{\omega(n)}kn^{-1}$ solutions en ℓ dans $[0,k[$. □

Nous en déduisons le

Lemme 4.3. *Soit n un entier sans facteur carré. Le nombre de classes de formes cubiques de discriminant D avec $|D| \leqslant X$ telles que n^2 divise D et telles que le hessien soit réductible est*

$$\ll 12^{\omega(n)} \frac{X}{n^2}.$$

Preuve. Puisque le hessien est réductible, il est de la forme (à équivalence près) $My(kx + \ell y)$ avec $0 \leqslant \ell < k$ et $(k, \ell) = 1$. On a aussi la relation $D = -3M^2k^2$, donc $n|Mk$. On décompose n sous la forme $n = uv$, où $v|M$, $u|k$, et $(u, Mv^{-1}) = 1$. D'après le Lemme 4.2, le cardinal étudié est majoré par

$$\sum_{uv=n} \sum_{\substack{k'M' \leqslant \sqrt{3X}/n \\ (u,vM')=1}} B(uk', vM') \ll \sum_{uv=n} 6^{\omega(u)} \sum_{M'} \tau(vM') \sum_{k' \leqslant \sqrt{3X}/(nM')} k' \ll 12^{\omega(n)} \frac{X}{n^2}.$$

□

4.a.2. *Preuve de la Proposition 4.1.* Considérons d'abord les classes de formes cubiques de discriminant D et de hessien réductible. Or ce hessien est de discriminant $-3D$ et doit être un carré. Donc D est de la forme $-3\alpha^2$, avec $\alpha \in \mathbb{N}$ et $q|D$. Mais D appartient à V_ℓ pour tout ℓ premier divisant q. Ceci n'est possible que si $q = 1$ ou $q = 3$. Que cet ensemble de formes cubiques soit vide ou non, le Lemme 4.3 donne la majoration $O_\varepsilon\Big(\frac{X^{1+\varepsilon}}{qn^2}\Big)$.

Passons aux formes cubiques de discriminant D, de hessien irréductible. Ce hessien est de la forme MH_1, avec $M \in \mathbb{Z}^*$, H_1 forme quadratique primitive, de discriminant $f^2\Delta$ avec Δ discriminant fondamental. On a donc la relation

$$-3D = f^2M^2\Delta.$$

Par ([10, Lemma 10]), il y a $O(\tau(M)3^{\omega(f)}h_3^*(\Delta))$ classes de formes cubiques dont le hessien est dans la classe de MH_1. La nature de la majoration recherchée nous permet de supposer que n et q sont premiers à 6, donc que n divise fM. L'hypothèse $D \in V_q$ implique alors $q|\Delta$. Le nombre $\mathcal{A}$ de classes recherché est ainsi

$$\mathcal{A} \ll \sum_{\substack{f,M \\ n|fM}} \tau(M)3^{\omega(f)} \sum_{\substack{|\Delta| \leqslant \frac{X}{3f^2M^2} \\ q|\Delta}} h_3^*(\Delta) \ll X^\varepsilon \sum_{\substack{u \\ n|u}} \sum_{|\Delta| \leqslant \frac{X}{3u^2} q|\Delta} \mathcal{H}(\Delta) + \frac{X^{1+\varepsilon}}{n^2q}. \tag{41}$$

La Proposition 2.3 et la formule (12) donnent la majoration

$$\sum_{\substack{|\Delta| \leqslant Y \\ q|\Delta}} \mathcal{H}(\Delta) \leqslant H_{q,1}^*(Y) + H_{q,1}^*(-Y),$$

(la notation $H_{q,1}^*(-Y)$ signifie qu'on dénombre des classes de formes cubiques de discriminant compris entre $-Y$ et 0). En majorant trivialement le dernier terme

à droite de l'égalité de la Proposition 3.8 par $O(\operatorname{card}\mathcal{D}') = O(Y^{1-\rho}+Y^{\frac34+\varepsilon})$ on parvient à la relation

$$\sum_{\substack{|\Delta|\leqslant Y\\ q|\Delta}}\mathcal{H}(\Delta)\ll\frac{Y}{q}+\vartheta^*(q,Q)\frac{Y+E(Y,\rho,Q)}{Q^4}\Big(\frac{Q}{q}+1\Big)^3Y^{\varepsilon}$$
$$+\frac{G(Y,\rho,Q)}{q}Y^{\varepsilon}+Y^{1-\rho}+Y^{\frac34+\varepsilon}.$$

On choisit alors

$$Q=q^{\frac23},\quad Y^{\rho}=Y^{\frac{1}{16}}q^{\frac{1}{12}}.$$

Puisque q est sans facteur carré, on a $\vartheta^*(q,Q)\ll q^{\frac53}$, d'où la majoration

$$\sum_{\substack{|\Delta|\leqslant Y\\ q|\Delta}}\mathcal{H}(\Delta)\ll\Big(\frac{Y}{q}+\frac{Y^{\frac{15}{16}}}{q^{\frac{1}{12}}}+q^{\frac54}Y^{\frac{7}{16}}+q^{\frac53}\Big)Y^{\varepsilon}. \tag{42}$$

La majoration précédente est de mauvaise qualité pour q grand par rapport à Y. Il vaut mieux dans ce cas recourir à la majoration suivante, conséquence de (3)

$$\sum_{\substack{|\Delta|\leqslant Y\\ q|\Delta}}\mathcal{H}(\Delta)\ll Y. \tag{43}$$

On reporte (42) dans (41), avec $Y=\frac{X}{3u^2}$ et on somme sur les $u\leqslant q^{-\frac{10}{9}}\sqrt{X}$ divisibles par n. Pour les u restants, on utilise la majoration (43), d'où

$$\mathcal{A}\ll X^{\varepsilon}\Big(\frac{X}{n^2q}+\frac{X^{\frac{15}{16}}}{n^{\frac{15}{8}}q^{\frac{1}{12}}}+\frac{q^{\frac{10}{9}}X^{\frac12}}{n}\Big).$$

4.b. **Un résultat en moyenne.** Le but de la Proposition 4.4 est de notablement améliorer cette inégalité, mais *en moyenne*. Nous introduisons la notation suivante, valable pour tout entier l, tout entier m et $\varepsilon>0$ très petit :

$$Q_{m,\varepsilon}=\max\Big(\Big[\big(\frac{X}{m^2}\big)^{\frac14}X^{-\varepsilon}\Big],1\Big),\quad \mathcal{D}^*_{m,\varepsilon}=\mathcal{D}(\frac{X}{m^2},\varepsilon,Q_{m,\varepsilon}),$$

où $\mathcal{D}(X,\rho,Q)$ est défini après (8). On a

Proposition 4.4. *Soit q sans facteur carré, n un entier premier avec q. 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 V_q est*

$$\ll\Big(\frac{X}{n^2q}+\frac{q^{\frac23}X^{\frac12}}{n}\Big)X^{5\varepsilon}+\sum_{l\leqslant\sqrt{X}/(nq^{2/3})}\ \sum_{\substack{(a,b,c,d)\in\mathcal{D}^*_{ln,\varepsilon}\\ \kappa(q)|\Delta(a,b,c,d)}}1.$$

Preuve. On suit la démonstration de la Proposition 4.1. On part de l'inégalité (41) mais on utilise la Proposition 3.7 (au lieu de la Proposition 3.8). En posant $u = ln$ et en donnant à X et à Q respectivement les valeurs $\pm X/(l^2n^2)$ et $Q_{ln,\varepsilon}$, on a

$$H^*_{q,1}\Big(\frac{X}{l^2n^2}\Big) \ll \nu_1(q)\frac{X}{l^2n^2} + \vartheta^*(q,Q_{ln,\varepsilon})X^{5\varepsilon}\Big(1+\frac{X^{\frac14}}{(ln)^{\frac12}q}\Big)^3 + \frac{X}{l^2n^2q}q^{\varepsilon} + \sum_{\substack{(a,b,c,d)\in\mathcal{D}^*_{ln,\varepsilon}\\ \kappa(q)|\Delta(a,b,c,d)}} 1,$$

ce qui donne

$$H^*_{q,1}\Big(\frac{X}{l^2n^2}\Big) \ll \frac{X^{1+5\varepsilon}}{ql^2n^2} + \vartheta^*(q,Q_{ln,\varepsilon})X^{5\varepsilon} + \sum_{\substack{(a,b,c,d)\in\mathcal{D}^*_{ln,\varepsilon}\\ \kappa(q)|\Delta(a,b,c,d)}} 1. \tag{44}$$

Rappelons qu'on a trivialement, pour q sans facteur carré, la relation

$$\vartheta^*(q,Q_{ln,\varepsilon}) \ll q^2. \tag{45}$$

Au lieu de la majoration (44), on peut aussi utiliser (43). Posons donc $L_1 = n^{-1}q^{-2}X^{\frac12}$ et $L_2 = n^{-1}q^{-\frac23}X^{\frac12}$. Pour $1 \leqslant l \leqslant L_1$, on utilise (45) ; pour $L_1 < l \leqslant L_2$, on a $\vartheta^*(q,Q_{ln,\varepsilon}) \ll qQ_{ln,\varepsilon}$. Enfin pour $l \geqslant L_2$, on utilise (43). Le calcul donne

$$\mathcal{A} \ll \Big(\frac{X}{n^2q} + \frac{X^{\frac12}}{n} + \frac{q^{\frac23}X^{\frac12}}{n}\Big)X^{5\varepsilon} + \sum_{l\leqslant L_2}\sum_{\substack{(a,b,c,d)\in\mathcal{D}^*_{ln,\varepsilon}\\ \kappa(q)|\Delta(a,b,c,d)}} 1,$$

d'où la Proposition 4.4. □

5. Démonstration des Théorèmes 1.5 et 1.6

Nous suivons les notations de [1, §6] : soient q et r deux entiers premiers entre eux, avec q sans facteur carré et r impair et soit R un multiple de q sans facteur carré. On pose alors $f(R,q,r,X)$ le nombre de classes de formes cubiques $ax^3+bx^2y+cxy^2+dy^3$, de discriminant compris entre 0 et X telles que

- la forme $F = (a,b,c,d)$ est irréductible,
- q divise $\Delta(a,b,c,d)$,
- $\Delta(a,b,c,d) \in V_R$,
- pour tout premier $p|r$, on a $\Delta(a,b,c,d) \equiv 0 \pmod{p^2}$.

On note aussi $P_Y = \prod_{p\leqslant Y} p$. On a donc l'égalité

$$N_{0,q}(0,X;V) = f(P_\infty,q,1,X).$$

Par le principe d'inclusion-exclusion, en posant

$$Y = \frac{\log X}{\log_3 X}, \quad Z = X^{\varepsilon},$$

on a l'égalité

$$\begin{aligned} N_{0,q}(0,X;V) &= f(qP_Y,q,1,X) - \sum_{\substack{Y<p\leqslant Z\\(p,q)=1}} f(qP_Y,q,p,X) \\ &\quad + O\Big(\sum_{\substack{Y<p_1<p_2\leqslant Z\\(p_1p_2,q)=1}} f(qP_Y,q,p_1p_2,X)\Big) \\ &\quad + O\Big(\sum_{\substack{p>Z\\(p,q)=1}} f(qP_Y,q,p,X)\Big), \\ &=: A_1 - A_2 + O(A_3) + O(A_4), \end{aligned} \tag{46}$$

par définition.

5.a. **Preuve d'une forme moins forte du Théorème 1.5.** Nous allons, dans un premier temps, montrer l'exactitude du Théorème 1.5, mais sous la contrainte plus forte $q \leqslant X^{\frac{1}{16}-\varepsilon}$. Ce premier pas présente plusieurs avantages : d'abord celui de rendre cet exposé complet, d'introduire la méthode dans un cadre plus simple, enfin, de clarifier le bas de la page 929 de [1], qui permettait de parvenir à $q \leqslant X^{\frac{1}{15}-\varepsilon}$.

5.a.1. *Étude de A_4.* Nous appliquons la Proposition 4.1 : on a

$$A_4 \leqslant \sum_{p>Z} \left|\left\{F\in\Phi;\Delta(F)\leqslant X, F\in V_q, \Delta(F)\equiv 0 \pmod{qp^2}\right\}\right|,$$

d'où

$$A_4 \ll X^{\frac{\varepsilon}{2}} \sum_{p>Z}\left(\frac{X}{p^2q} + \frac{X^{\frac{15}{16}}}{p^{\frac{15}{8}}q^{\frac{1}{12}}} + \frac{q^{\frac{10}{9}}X^{\frac{1}{2}}}{p}\right) \ll \frac{X}{q}X^{-\frac{\varepsilon}{2}}, \tag{47}$$

en sommant sur p, dès que $q \leqslant X^{\frac{3}{44}-\varepsilon}$.

5.a.2. *Une formule exacte pour $f(R,q,r,X)$.* Nous appliquons là-aussi le principe d'inclusion-exclusion en séparant le cas des pairs et des impairs, sous la forme

$$\begin{aligned} f(R,q,r,X) = &\sum_{\substack{d|R\\(d,2q)=1}} \mu(d) \sum_{\substack{\delta|q\\(2,\delta)=1}} \mu(\delta) H^*_{\delta q, d^2r^2}(X) \\ &+ \sum_{\substack{2d|R\\(2d,q)=1}} \mu(2d) \sum_{\delta|q} \mu(\delta) H^*_{\delta q, 16d^2r^2}(X) \\ &+ \sum_{\substack{d|R\\(d,2q)=1}} \mu(d) \sum_{2\delta|q} \mu(2\delta) H^*_{8\delta q, d^2r^2}(X) \end{aligned} \tag{48}$$

Pour faciliter l'exposé, on suppose que R (donc q) est impair (le cas où q est pair est analogue et se traite en tenant compte des trois termes à droite de (48)). On

fait appel à la Proposition 3.8 pour calculer $H^*_{q\delta,d^2r^2}$. Ainsi le coefficient du terme principal est

$$\Big(\sum_{\delta|q}\mu(\delta)\nu_1(q\delta)\Big)\Big(\sum_{\substack{(d,q)=1\\ d|R}}\mu(d)\nu_2(d^2r^2)\Big)$$

$$= \nu_1(q)\nu_2(r^2)\Big(\sum_{\delta|q}\mu(\delta)\frac{\nu_1(\delta^2)}{\nu_1(\delta)}\Big)\prod_{\substack{p|R\\(p,q)=1}}\big(1-\nu_2(p^2)\big),$$

$$= \frac{\nu(q)}{q}\nu_2(r^2)\prod_{p|R}\big(1-\frac{1}{p^2}\big)^2, \tag{49}$$

où la fonction ν est celle du Théorème 1.3.

La formule (48) comporte $\tau(R)$ termes et on a toujours $d|Rq^{-1}$. On choisit $Q=\delta qd^2r^2$. Le terme en ϑ^* dans (40) est alors nul. La Proposition 3.8, pour r_1, r_2, s_1 et s_2 valant respectivement $\frac{q}{\delta}$, δd, 1 et r, engendre donc pour terme d'erreur dans (48), un terme qui est

$$\ll \sum_{\substack{d|R\\(d,q)=1}}\sum_{\delta|q}\Big\{\frac{G(X,\rho,\delta qd^2r^2)}{\delta qd^2r^2}X^{\varepsilon}+X^{1-\rho}+X^{\frac34+\varepsilon}\Big\}. \tag{50}$$

Donnons à ρ la valeur $\frac{1}{16}$. Le terme d'erreur (50) a l'écriture explicite suivante

$$\ll \sum_{\substack{d|R\\(d,q)=1}}\sum_{\delta|q}\Big\{\frac{\delta qd^2r^2X^{\frac{15}{16}}+\delta^3q^3d^6r^6X^{\frac{7}{16}}+\delta^4q^4d^8r^8}{\delta qd^2r^2}X^{\varepsilon}+X^{\frac{15}{16}}\Big\}. \tag{51}$$

En sommant sur δ et sur d, puis en regroupant avec (49), nous parvenons à la

Proposition 5.1. *Pour tout $\varepsilon>0$, tout q sans facteur carré, tout R multiple de q, tout r impair, premier à R, on a l'égalité*

$$f(R,q,r,X)=\frac{\nu(q)}{q}\nu_2(r^2)\prod_{p|R}\Big(1-\frac{1}{p^2}\Big)^2\frac{\pi^2X}{72}+O\Big((X^{\frac{15}{16}}+r^4R^4X^{\frac{7}{16}}+r^6R^6)(RX)^{\varepsilon}\Big).$$

5.a.3. *Étude de A_1.* En donnant à r et R les valeurs 1 et $qP_Y\ll qX^{\frac{\varepsilon}{10}}$, la Proposition 5.1 donne l'égalité

$$A_1=\frac{\nu(q)}{q}\prod_{\substack{p\leqslant Y\\ \text{ou } p|q}}\big(1-\frac{1}{p^2}\big)^2\frac{\pi^2X}{72}+O\Big((X^{\frac{15}{16}}+q^4X^{\frac{7}{16}}+q^6)X^{\varepsilon}\Big). \tag{52}$$

5.a.4. *Étude de A_2.* Nous appliquons là-aussi la Proposition 5.1 avec $R=qP_Y$ et une sommation sur $r=p$ compris entre Y et Z et ne divisant pas q. Puisque

l'intervalle de variation de p est petit, le terme d'erreur est identique à celui de (52), quitte à modifier la puissance X^{ε}. Par contre le terme principal est

$$\frac{\nu(q)}{q}\frac{\pi^2 X}{72}\prod_{\substack{p\leqslant Y\\ \text{ou } p|q}}\big(1-\frac{1}{p^2}\big)^2\sum_{\substack{Y<p\leqslant Z\\(p,q)=1}}\nu_2(p^2).$$

Grâce à la formule (52), on voit que le terme principal de A_1-A_2 est

$$\frac{\nu(q)}{q}\frac{\pi^2 X}{72}\prod_{\substack{p\leqslant Y\\ \text{ou } p|q}}\big(1-\frac{1}{p^2}\big)^2\Big(1-\sum_{\substack{Y<p\leqslant Z\\(p,q)=1}}\nu_2(p^2)\Big).$$

On écrit alors l'égalité

$$\prod_{\substack{Y<p\leqslant Z\\(p,q)=1}}\big(1-\nu_2(p^2)\big)=1-\sum_{\substack{Y<p\leqslant Z\\(p,q)=1}}\nu_2(p^2)+O\big(Y^{-2}(\log Y)^{-2}\big),$$

pour parvenir finalement à la relation

$$A_1-A_2=\frac{\nu(q)}{q}\frac{\pi^2 X}{72}\Big(\frac{36}{\pi^4}+O\big(Y^{-2}(\log Y)^{-2}\big)\Big)+O\Big((X^{\frac{15}{16}}+q^4X^{\frac{7}{16}}+q^6)X^{10\varepsilon}\Big).$$

5.a.5. *Étude de A_3.* Pour sommer la formule apparaissant dans (46), nous appliquons la Proposition 5.1, avec $r=p_1p_2$, R étant le produit qP_Y. Le terme d'erreur est le même que dans (5.a.4) à condition d'augmenter le coefficient de ε. En utilisant le fait que

$$\sum_{Y\leqslant p_1<p_2\leqslant Z}\nu_2(p_1^2p_2^2)\ll Y^{-2}(\log Y)^{-2},$$

on a la relation

$$A_3\ll Xq^{-1}Y^{-2}(\log Y)^{-2}+(X^{\frac{15}{16}}+q^4X^{\frac{7}{16}}+q^6)X^{20\varepsilon}. \tag{53}$$

En regroupant (46), (47), (5.a.4) et (53), on a l'égalité

$$\begin{aligned}\sum_{\substack{\Delta\in\Delta^+(X)\\ q|\Delta}}1&=N_{0,q}(0,X;V)\\&=\frac{\nu(q)}{q}\frac{X}{2\pi^2}+O\Big(\frac{X\log_3^2X}{q\log^2X\log_2^2X}\Big)+O\big(X^{\frac{15}{16}}+q^4X^{\frac{7}{16}}+q^6)X^{20\varepsilon}\big)\\&=\frac{\nu(q)}{q}\frac{X}{2\pi^2}+O\Big(\frac{X\log_3^2X}{q\log^2X\log_2^2X}\Big),\end{aligned}$$

pourvu que $q\leqslant X^{\frac{1}{16}-30\varepsilon}$. La preuve de la forme moins forte du Théorème 1.5 est ainsi complète.

5.b. **Preuve du Théorème 1.5.** Nous pouvons donc supposer que l'entier q sans facteur carré vérifie

$$X^{\frac{1}{16}-\varepsilon} \leqslant q \leqslant X^{\frac{3}{44}-\varepsilon}. \tag{54}$$

Nous donnons à Y et à Z les mêmes valeurs que précédemment, mais nous donnons à Q une valeur plus faible et à ρ une valeur plus grande :

$$Q = [\delta q^{\gamma} d^2 r^2], \quad \rho = \frac{3}{44},$$

et γ sera un réel que l'on prendra arbitrairement proche, de $\frac{2}{3}$, mais supérieur à ce nombre.
Avec ces conventions, (47) reste valable, par contre le terme d'erreur (50) doit être modifié en

$$\ll X^{\frac{\varepsilon}{2}} \sum_{\substack{d|R\\(d,q)=1}} \sum_{\delta|q} \Big\{ \frac{\vartheta^*(\delta q d^2 r^2, Q) X}{Q^4} + \frac{G(X, \frac{3}{44}, Q)}{\delta q d^2 r^2} + X^{\frac{41}{44}} \Big\}, \tag{55}$$

puisque, par application de la Proposition 3.8, la fonction ϑ^* est maintenant non nulle. Rendons explicite le terme d'erreur en revenant aux définitions des fonctions ϑ^* et G, on trouve qu'il est

$$\ll X^{\frac{\varepsilon}{2}} \sum_{\substack{d|R\\(d,q)=1}} \sum_{\delta|q} \Big\{ X \Big(\frac{1}{\delta q^{4\gamma-1} d^4 r^4} + \frac{1}{\delta^2 q^{3\gamma-1} d^4 r^4} + \frac{1}{\delta q^{2\gamma} d^3 r^3} \Big)$$
$$+ \quad \Big(\frac{X^{\frac{21}{22}}}{q^{1-\gamma}} + \delta^2 q^{3\gamma-1} d^4 r^4 X^{\frac{5}{11}} + \delta^3 q^{4\gamma-1} d^6 r^6 \Big) + X^{\frac{41}{44}} \Big\}.$$

En sommant maintenant sur $\delta|q$ et sur $d|Rq^{-1}$, on a une version modifiée de la Proposition 5.1, à savoir

Proposition 5.2. *On a l'égalité suivante, pour tout $\varepsilon > 0$, pour tout $\gamma > 0$, tout q sans facteur carré, tout R multiple de q, tout r impair, premier à R :*

$$f(R,q,r,X) = \frac{\nu(q)}{q} \nu_2(r^2) \prod_{p|R} \Big(1 - \frac{1}{p^2}\Big)^2 \frac{\pi^2 X}{72}$$
$$+ \quad O\Bigg(\Big(\frac{X}{q^{3\gamma-1} r^4} + \frac{X}{q^{2\gamma} r^3} + \frac{X^{\frac{21}{22}}}{q^{1-\gamma}} + \frac{r^4 R^4 X^{\frac{5}{11}}}{q^{3-3\gamma}} + \frac{r^6 R^6}{q^{4-4\gamma}} + X^{\frac{41}{44}} \Big) (RX)^{\varepsilon} \Bigg).$$

La démarche est alors la même pour obtenir une formule pour $A_1 - A_2$ et une majoration pour A_3 à la différence près que le terme d'erreur doit être modifié

pour tenir compte de la Proposition 5.2. Pour être plus précis, on arrive à l'égalité

$$\sum_{\substack{\Delta\in\Delta^+(X)\\ q|\Delta}} 1 = \frac{\nu(q)}{q}\frac{X}{2\pi^2} + O\Big(\frac{X\log_3^2 X}{q\log^2 X\log_2^2 X}\Big) + O\Big(\big(\frac{X}{q^{3\gamma-1}} + \frac{X}{q^{2\gamma}} + \frac{X^{\frac{21}{22}}}{q^{1-\gamma}} + q^{3\gamma+1}X^{\frac{5}{11}} + q^{4\gamma+2} + X^{\frac{41}{44}}\big)X^{10\varepsilon}\Big),$$

d'où le Théorème 1.5, en raison de l'hypothèse (54) et en prenant γ de la forme $\gamma = \frac{2}{3} + 100\varepsilon$.

5.c. **Preuve d'une forme moins forte du Théorème 1.6.** Dans un premier temps, nous démontrons le Théorème 1.6, avec l'exposant $\frac{1}{5}$ au lieu de $\frac{2}{7}$. Du point de vue combinatoire notre démarche est la même qu'aux §5.a et §5.b pour décomposer $N_{0,q}(0, X; V)$ (formule (46)). Mais nous utilisons les Propositions 3.7 et 4.4 au lieu des Propositions 3.8 et 4.1. Pour ε très petit, on fixe les notations suivantes : γ est une constante positive que l'on fixera par la suite ; on pose

$$\rho = \varepsilon, \quad Q' \leqslant q < 2Q', \quad Q = [Q'^{\gamma}],$$

et on impose l'inégalité

$$Q < X^{\frac{1}{4}-10\varepsilon}. \tag{56}$$

Avec ces conventions, on a, par la Proposition 3.7, l'égalité

$$H^*_{\delta q,d^2r^2}(X) = \nu_1(\delta q)\nu_2(d^2r^2)\frac{\pi^2 X}{72} + O\Big(\vartheta^*(\delta q d^2r^2, q^\gamma)\frac{X}{q^{4\gamma}}\big(\frac{q^\gamma}{\delta q d^2r^2}+1\big)^3\Big) + O\big(\frac{X^{1-\varepsilon}}{\delta q d^2r^2}\big) + O\Big(\sum_{\substack{(a,b,c,d)\in\mathcal{D}\\ \kappa(q)|\Delta(a,b,c,d)}} 1\Big), \tag{57}$$

où $\mathcal{D} = \mathcal{D}(X, \varepsilon, Q)$ est un sous-ensemble de points de $\mathbb{Z}^4$ vérifiant

$$0 < \Delta(a,b,c,d) \ll X \quad \text{et} \quad \operatorname{card}\mathcal{D} = O\big(G(X,\varepsilon,Q)\big) = O(X^{1-\varepsilon}).$$

(Insistons sur le fait que $\mathcal{D}$ est indépendant de q dans l'intervalle $[Q', 2Q']$.) La formule (57) se transforme en

$$H^*_{\delta q,d^2r^2}(X) = \nu_1(\delta q)\nu_2(d^2r^2)\frac{\pi^2 X}{72} + O\Big(X^{1+\varepsilon}\big(\frac{1}{d^2r^2q^{2+\gamma}} + \frac{1}{\delta^2d^4r^4q^2} + \frac{1}{\delta^2d^5r^5q^{3-\gamma}} + \frac{\delta^3d^4r^4}{q^{4\gamma-1}} + \frac{\delta d^2r^2}{q^{3\gamma-1}} + \frac{\delta dr}{q^{2\gamma}}\big)\Big) + O\big(\frac{X^{1-\varepsilon}}{\delta q d^2r^2}\big) + O\Big(\sum_{\substack{(a,b,c,d)\in\mathcal{D}\\ \kappa(q)|\Delta(a,b,c,d)}} 1\Big). \tag{58}$$

En sommant sur $\delta|q$ et $d|Rq^{-1}$ on arrive à la

Proposition 5.3. *Pour tout $\varepsilon > 0$, pour tout $\gamma > 0$, tout q sans facteur carré, tout R multiple de q, tout r impair, premier à R et tout Q vérifiant* (56)*, on a l'égalité*

$$f(R,q,r,X) = \frac{\nu(q)}{q}\nu_2(r^2)\prod_{p|R}\big(1-\frac{1}{p^2}\big)^2\cdot\frac{\pi^2 X}{72}$$
$$+\quad O\bigg(X\Big(\frac{1}{r^2q^{2+\gamma}}+\frac{1}{r^4q^2}+\frac{1}{r^5q^{3-\gamma}}+\frac{r^4R^4}{q^{4\gamma}}+\frac{r^2R^2}{q^{3\gamma}}+\frac{rR}{q^{2\gamma}}\Big)(RX)^{\varepsilon}\bigg)$$
$$+\quad O\big(\frac{X^{1-\frac{\varepsilon}{2}}}{qr^2}R^{\varepsilon}\big)+O\bigg(\Big(\sum_{\substack{(a,b,c,d)\in\mathcal{D}\\ \kappa(q)|\Delta(a,b,c,d)}}1\Big)(RX)^{\varepsilon}\bigg).$$

En donnant à Y et à Z les mêmes valeurs que précédemment, on parvient à l'égalité

$$A_1-A_2+O(A_3)=\frac{\nu(q)}{q}\frac{X}{2\pi^2}+O\Big(\frac{X\log_3^2 X}{q\log^2 X\log_2^2 X}\Big)$$
$$+\quad O\bigg(X\Big(\frac{1}{q^2}+\frac{1}{q^{3-\gamma}}+\frac{1}{q^{4\gamma-4}}+\frac{1}{q^{3\gamma-2}}+\frac{1}{q^{2\gamma-1}}\Big)X^{\varepsilon}\bigg)$$
$$+\quad O\big(\frac{X^{1-\frac{\varepsilon}{2}}}{q}\big)+O\bigg(\Big(\sum_{\substack{(a,b,c,d)\in\mathcal{D}\\ \kappa(q)|\Delta(a,b,c,d)}}1\Big)X^{\frac{\varepsilon}{2}}\bigg), \tag{59}$$

où les A_i sont définis dans (46).

5.c.1. *Majoration en moyenne de A_4.* Il reste à majorer A_4 par la Proposition 4.4. On a la relation

$$A_4 \leqslant \sum_{p>Z}\big|\big\{F\in\Phi;\Delta(F)\leqslant X, F\in V_q,\Delta(F)\equiv 0\ (\mathrm{mod}\ qp^2)\big\}\big|,$$

d'où

$$A_4 \ll X^{\frac{\varepsilon}{2}}\sum_{p>Z}\Big(\frac{X}{p^2q}+\frac{q^{\frac{2}{3}}X^{\frac{1}{2}}}{p}+\sum_{l\leqslant\sqrt{X}/(pq^{2/3})}\ \sum_{\substack{(a,b,c,d)\in\mathcal{D}^*_{lp,\varepsilon}\\ \kappa(q)|\Delta(a,b,c,d)}}1\Big), \tag{60}$$

où $\mathcal{D}^*_{lp,\varepsilon}$ est un certain ensemble d'entiers (a,b,c,d), indépendant de q, de cardinal $Xl^{-2}p^{-2}X^{-2\varepsilon}$, sur lequel, on a $0<\Delta(a,b,c,d)\ll X$. La formule (60) devient ainsi

$$A_4 \ll \frac{X^{1-\frac{\varepsilon}{2}}}{q}+q^{\frac{2}{3}}X^{\frac{1}{2}+\varepsilon}+X^{\varepsilon}\sum_{p>Z}\ \sum_{l\leqslant\sqrt{X}/(pq^{2/3})}\ \sum_{\substack{(a,b,c,d)\in\mathcal{D}^*_{lp,\varepsilon}\\ \kappa(q)|\Delta(a,b,c,d)}}1, \tag{61}$$

En regroupant avec (59), nous obtenons la formule suivante

$$\sum_{\substack{\Delta\in\Delta^+(X)\\ q|\Delta}} 1=\frac{\nu(q)}{q}\frac{X}{2\pi^2}+O\Big(\frac{X\log_3^2 X}{q\log^2 X\log_2^2 X}\Big)+O(X^\varepsilon R_1(q,X))+O(X^\varepsilon R_2(q,X))$$

avec

$$R_1(q,X)=q^{\frac{2}{3}}X^{\frac{1}{2}}+X\Big(\frac{1}{q^2}+\frac{1}{q^{3-\gamma}}+\frac{1}{q^{4\gamma-4}}+\frac{1}{q^{3\gamma-2}}+\frac{1}{q^{2\gamma-1}}\Big)$$

et

$$R_2(q,X)=\sum_{\substack{(a,b,c,d)\in\mathcal{D}\\ \kappa(q)|\Delta(a,b,c,d)}} 1+\sum_{p>Z}\sum_{l\leqslant\sqrt{X}/(pq^{2/3})}\sum_{\substack{(a,b,c,d)\in\mathcal{D}^*_{lp,\varepsilon}\\ \kappa(q)|\Delta(a,b,c,d)}} 1.$$

On voit que le terme $R_1(q,X)$ est en $O(\frac{X^{1-\frac{\varepsilon}{2}}}{q})$ si on prend $X^{\frac{1}{15}}\leqslant Q'\leqslant X^{\frac{1}{5}-\varepsilon}$, il faut alors prendre γ très légèrement supérieur à $\frac{5}{4}$. Enfin par une interversion de sommations, et en constatant que (a,b,c,d) étant fixé, il y a $O(X^{\frac{\varepsilon}{2}})$ entiers q tels que $\mu^2(q)=1$ et $\kappa(q)$ divise $\Delta(a,b,c,d)$, on arrive finalement à la relation

$$\sum_{Q'\leqslant q\leqslant 2Q'} R_2(q,X)=O(X^{1-\frac{\varepsilon}{2}}).$$

On en déduit alors par sommation sur les Q' de la forme $Q'=2^k$, le Théorème 1.6, mais avec l'exposant $\frac{1}{5}-\varepsilon$ au lieu de $\frac{2}{7}-\varepsilon$.

5.d. **Preuve du Théorème 1.6.** Voyons comment atteindre l'exposant $\frac{2}{7}$. L'idée est de faire subir un traitement spécial aux grands diviseurs δ de q qui, lors de la sommation (58) pour l'obtention de la Proposition 5.3, ont une contribution démesurée. On a le

Lemme 5.4. *Soit $\mathcal{E}(X,q,\varepsilon)$, l'ensemble des points (a,b,c,d) de $\mathcal{V}(X)$ défini par*

$$\mathcal{E}(X,q,\varepsilon)=\bigcup_{\delta\geqslant q^{\frac{1}{2}+\varepsilon};\ \delta|q}\{(a,b,c,d)\in\mathcal{V}(X);\delta^2|\Delta(a,b,c,d)\}.$$

On a alors l'égalité

$$|\mathcal{E}(X,q,\varepsilon)|=O\big(X^{1-\frac{\varepsilon}{2}}q^{-1}+X^{\frac{1}{2}+\varepsilon}\big).$$

Preuve. On utilise la Proposition 4.1. On remarque que chaque $\Delta(a,b,c,d)$ appartient à V_1, d'où la relation

$$|\mathcal{E}(X,q,\varepsilon)|\ll\sum_{\delta>q^{\frac{1}{2}+\varepsilon};\ \delta|q} X^\varepsilon\Big(\frac{X}{\delta^2}+\frac{X^{\frac{15}{16}}}{\delta^{\frac{15}{8}}}+\frac{X^{\frac{1}{2}}}{\delta}\Big)=O\big(X^{1-\frac{\varepsilon}{2}}q^{-1}+X^{\frac{1}{2}+\varepsilon}\big).$$

□

Soit $\tilde{f}(R,q,r,X)$ le nombre de points (a,b,c,d) comptés dans $f(R,q,r,X)$ mais n'appartenant pas à $\mathcal{E}(X,q,\varepsilon)$. Grâce au Lemme 5.4, on a l'encadrement

$$f(R,q,r,X) - O\big(X^{1-\frac{\varepsilon}{2}}q^{-1}\big) \leqslant \tilde{f}(R,q,r,X) \leqslant f(R,q,r,X),$$

pourvu que $q < X^{\frac{1}{2}-\varepsilon}$. La formule (46) devient alors

$$N_{0,q}(0,X;V) = \tilde{f}(qP_Y,q,1,X) - \sum_{Y<p\leqslant Z} \tilde{f}(qP_Y,q,p,X) + O\big(A_3+A_4+X^{1-\frac{\varepsilon}{2}}q^{-1}\big).$$

Nous disposons aussi d'une formule exacte pour $\tilde{f}(R,q,r,X)$, qui remplace (48), à savoir

$$\begin{aligned}\tilde{f}(R,q,r,X) = &\sum_{\substack{d|R\\(d,2q)=1}} \mu(d) \sum_{\substack{\delta|q,\delta<q^{1/2+\varepsilon}\\(2,\delta)=1}} \mu(\delta) H^*_{\delta q,d^2r^2}(X)\\ &+ \sum_{\substack{2d|R\\(2d,q)=1}} \mu(2d) \sum_{\delta|q,\delta<q^{1/2+\varepsilon}} \mu(\delta) H^*_{\delta q,16d^2r^2}(X)\\ &+ \sum_{\substack{d|R\\(d,2q)=1}} \mu(d) \sum_{2\delta|q,\delta<q^{1/2+\varepsilon}} \mu(2\delta) H^*_{8\delta q,d^2r^2}(X).\end{aligned}$$

Comme lors de la preuve de la Proposition 5.3, on fait appel à la Proposition 3.7, mais ici le coefficient du terme principal est

$$\Big(\sum_{\delta<q^{\frac{1}{2}+\varepsilon};\ \delta|q} \mu(\delta)\nu_1(q\delta)\Big)\Big(\sum_{\substack{(d,q)=1\\d|R}} \mu(d)\nu_2(d^2r^2)\Big),$$

qui diffère donc du terme principal

$$\frac{\nu(q)}{q}\nu_2(r^2)\prod_{p|R}\big(1-\frac{1}{p^2}\big)^2, \tag{62}$$

(qu'on obtiendrait, si on supprimait la condition $\delta < q^{\frac{1}{2}+\varepsilon}$, voir (49)), d'au plus de la quantité

$$\begin{aligned}\Big(\sum_{\substack{\delta\geqslant q^{\frac{1}{2}+\varepsilon}\\\delta|q}} \nu_1(q\delta)\Big)\Big(\sum_{\substack{(d,q)=1\\d|R}} \nu_2(d^2r^2)\Big) &= O\Big(\nu_2(r^2)\nu_1(q)\sum_{\substack{\delta\geqslant q^{\frac{1}{2}+\varepsilon}\\\delta|q}} \frac{\nu_1(q\delta)}{\nu_1(q)}\Big)\\ &= O\Big(\nu_2(r^2)\nu_1(q)\sum_{\substack{\delta\geqslant q^{\frac{1}{2}+\varepsilon}\\\delta|q}} \delta^{-1-\frac{\varepsilon}{3}}\Big)\end{aligned}$$

soit encore

$$O\big(\nu_2(r^2)\nu_1(q)q^{-\frac{1}{2}-\frac{\varepsilon}{2}}\big). \tag{63}$$

Le calcul du terme d'erreur est identique à celui de la Proposition 5.3, à la différence près qu'on doit sommer

$$\ll X^{1+\varepsilon} \sum_{\substack{d|R\\(d,q)=1}} \sum_{\substack{\delta\leqslant q^{\frac12+\varepsilon}\\ \delta|q}} \Big(\frac{1}{d^2r^2q^{2+\gamma}}+\frac{1}{\delta^2d^4r^4q^2}+\frac{1}{\delta^2d^5r^5q^{3-\gamma}}+\frac{\delta^3d^4r^4}{q^{4\gamma-1}}+\frac{\delta d^2r^2}{q^{3\gamma-1}}+\frac{\delta dr}{q^{2\gamma}}\Big)$$
$$+ O\big(\frac{X^{1-\varepsilon}}{\delta q d^2r^2}\big) + O\Big(\sum_{\substack{(a,b,c,d)\in\mathcal{D}\\ \kappa(q)|\Delta(a,b,c,d)}} 1\Big)$$

et c'est ici qu'on gagne puisque la somme sur δ est beaucoup plus courte. En incorporant (63), on voit que la Proposition 5.3 est modifiée en la

Proposition 5.5. *On a l'égalité suivante, pour tout $\varepsilon>0$, pour tout $\gamma>0$, tout q sans facteur carré, tout R multiple de q, tout r impair, premier à R et tout Q vérifiant* (56) *:*

$$\tilde f(R,q,r,X) = \frac{\nu(q)}{q}\nu_2(r^2)\prod_{p|R}\big(1-\frac{1}{p^2}\big)^2\frac{\pi^2X}{72}$$
$$+O\bigg(X\Big(\frac{1}{r^2q^{2+\gamma}}+\frac{1}{r^4q^2}+\frac{1}{r^5q^{3-\gamma}}+\frac{r^4R^4}{q^{4\gamma+\frac32}}+\frac{r^2R^2}{q^{3\gamma+\frac12}}+\frac{rR}{q^{2\gamma+\frac12}}\Big)(RX)^{\varepsilon}\bigg)$$
$$+O\big(\frac{X^{1-\frac{\varepsilon}{2}}}{qr^2}R^{\varepsilon}\big)+O\bigg(\Big(\sum_{\substack{(a,b,c,d)\in\mathcal{D}\\ \kappa(q)|\Delta(a,b,c,d)}}1\Big)(RX)^{\frac{\varepsilon}{10}}\bigg).$$

La démonstration se poursuit comme dans la preuve du Théorème 1.6 affaibli, mais en prenant ici γ légèrement supérieur à $\frac78$.

Enfin, lorsque q est premier, la somme sur les $\delta|q$, inférieurs à $q^{\frac12+\varepsilon}$ se réduit à un seul terme. On peut prendre γ légèrement supérieur à $\frac23$, mais la majoration de A_4, plus précisément le terme $q^{\frac23}X^{\frac12}$ de (61), amène à supposer $q\leqslant X^{\frac{3}{10}-\varepsilon}$.

6. Les discriminants quasi-fondamentaux

Dans ce paragraphe, nous nous intéressons à un décompte de formes cubiques, non nécessairement primitives. Pour ce faire, nous introduisons les ensembles $\tilde V_p$, dont la définition est identique à celle des ensembles V_p du §2, à la différence près que la primitivité des formes est omise. Plus précisément, pour $p\geqslant 3$, on désigne par $\tilde V_p$ l'ensemble des classes F de Φ^{irr} telles que p^2 ne divise pas $\Delta(F)$ et $\tilde V_2$ est l'ensemble des classes F de Φ^{irr} telles que $\Delta(F)\equiv 1 \pmod 4$ ou $\Delta(F)\equiv 8$ ou $12 \pmod{16}$. Comme leurs homologues V_p, les ensembles $\tilde V_p$ vérifient l'égalité

$$V=\bigcap_p \tilde V_p$$

(en effet, si p divise chaque coefficient de F, alors p^4 divise $\Delta(F)$). En fait nous travaillerons à partir de l'inclusion évidente, valable pour tout $P > 2$,

$$V \subset \bigcap_{p<P} \tilde{V}_p,$$

inclusion qui est naturellement de meilleure qualité à mesure que P croît. On voit que le discriminant de toute forme cubique participant à la partie droite de (6) est un discriminant fondamental d'ordre P, notion définie dans l'introduction. L'inclusion (6) se traduit par une inégalité entre les quantités définies lors de la Proposition 2.3 :

$$N_{a,q}(0, X; V) \leqslant N_{a,q}(0, X; \bigcap_{p<P} \tilde{V}_p).$$

On a la variante suivante de (12),

$$\begin{aligned} (64)\quad N_{0,q}(0, X; \bigcap_{p<P} \tilde{V}_p) &= \sum_{(d,2q)=1} \mu(d) \sum_{\substack{\delta|q \\ (\delta,2)=1}} \mu(\delta) H^*_{1,\delta q d^2}(X) \\ &+ \sum_{(2d,q)=1} \mu(2d) \sum_{\delta|q} \mu(\delta) H^*_{1,16\delta q d^2}(X) + \sum_{(d,q)=1} \mu(d) \sum_{2\delta|q} \mu(2\delta) H^*_{1,8\delta q d^2}(X); \end{aligned}$$

où les variables de sommation d et δ vérifient

$$p|\delta d \Longrightarrow p < P.$$

Signalons que (64) n'a que $O_P(1)$ termes. Nous allons uniquement utiliser la Proposition 3.7 avec les valeurs

$$r = 1, \quad s = \delta q d^2, \quad \rho = \varepsilon, \quad Q = X^{\frac{1}{4}-10\varepsilon},$$

mais aucun résultat de type Brun-Titchmarsh découlant de la fastidieuse étude des sommes trigonométriques modulo p^2 (voir §3). Avec ce choix de paramètres, on a les relations

$$G(X, \rho, Q) = O(X^{1-\varepsilon})$$

et

$$\vartheta^*(\delta q d^2, Q) \ll_P (q + \min(q, Q)) \min(q, Q) \ll q \min(q, Q).$$

Grâce à (39), le premier terme à droite de (64) s'écrit

$$\begin{aligned} &\nu_2(q) \frac{\pi^2 X}{72} \prod_{\substack{p<P \\ (p,2q)=1}} \Big(1 - \nu_2(p^2)\Big) \prod_{\substack{p|q \\ 2<p<P}} \Big(1 - \frac{\nu_2(p^2)}{\nu_2(p)}\Big) \\ &\quad + O_P\Big(q \min(q, X^{\frac{1}{4}})(\frac{X^{\frac{1}{4}}}{q} + 1)^3 X^{50\varepsilon}\Big) + O_P\big(\frac{X^{1-\varepsilon}}{q}\big) + O_P\Big(\sum_{\substack{(a,b,c,d)\in\mathcal{D} \\ \kappa(q)|\Delta(a,b,c,d)}} 1\Big). \end{aligned}$$

Les deux autres termes ont des expressions du même type mais tenant compte de la parité de q et du rôle du nombre premier 2. En regroupant ces trois termes principaux, on voit alors que le terme principal de (64) s'écrit

$$\frac{\pi^2 X}{72}\prod_{p|q}\frac{p^2+p-1}{p^3}\cdot\prod_{\substack{p<P\\(p,q)=1}}\Big(1-\frac{2p^2-1}{p^4}\Big)\cdot\prod_{\substack{p<P\\p|q}}\Big(1-\frac{2p^2-1}{p(p^2+p-1)}\Big),$$

soit encore

$$\frac{\nu(q)}{q}\cdot\prod_{\substack{p|q\\p\geqslant P}}\frac{(p+1)(p^2+p-1)}{p^3}\cdot\prod_{p<P}\Big(1-\frac{1}{p^2}\Big)^2\cdot\frac{\pi^2 X}{72}.$$

En utilisant la fonction multiplicative $\nu_P(q)$ définie au §1, on voit que ce terme principal est aussi

$$\frac{\nu_P(q)}{q}\prod_{p\geqslant P}\Big(1-\frac{1}{p^2}\Big)^{-2}\cdot\frac{X}{2\pi^2},$$

et nous sommes donc parvenus à l'égalité

$$N_{0,q}(0,X;\bigcap_{p<P}\tilde{V}_p)=\frac{\nu_P(q)}{q}\prod_{p\geqslant P}\Big(1-\frac{1}{p^2}\Big)^{-2}\cdot\frac{X}{2\pi^2}$$

$$+O_P\Big(q\min(q,X^{\frac14})(\frac{X^{\frac14}}{q}+1)^3X^{50\varepsilon}\Big)+O_P\big(\frac{X^{1-\varepsilon}}{q}\big)+O_P\Big(\sum_{\substack{(a,b,c,d)\in\mathcal{D}\\\kappa(q)|\Delta(a,b,c,d)}}1\Big).$$

Pour prouver le Théorème 1.8, on prend pour $\mathcal{H}_P(n)$ la fonction qui compte le nombre de classes de formes cubiques, de discriminant n, appartenant à $\bigcap_{p<P}\tilde{V}_p$ et on a directement l'égalité

$$N_{a,q}(0,X;\bigcap_{p<P}\tilde{V}_p)=\sum_{\substack{1\leqslant n\leqslant X\\n\equiv a\pmod q}}\mathcal{H}_P(n).$$

L'assertion *i)* est alors triviale. Pour l'assertion *ii)*, on confronte (6) avec $q=1$ et la relation (3) (rappelons que l'ensemble $\mathcal{D}$ est de cardinal $O(X^{1-\varepsilon})$). Pour obtenir les assertions *iii)* du même théorème, on somme sur $q\leqslant D$ le terme d'erreur à droite de (6), dont la contribution est

$$\ll X^{1-\frac{\varepsilon}{2}}+\sum_{q\leqslant D}q\min(q,X^{\frac14})\big(\frac{X^{\frac14}}{q}+1\big)^3+\sum_{(a,b,c,d)\in\mathcal{D}}\sum_{\substack{q\\\kappa(q)|\Delta(a,b,c,d)}}1$$

$$\ll X^{1-\frac{\varepsilon}{2}}+D^2X^{\frac14+\varepsilon}+\operatorname{card}\mathcal{D}X^{\frac{\varepsilon}{2}}\ll X^{1-\frac{\varepsilon}{2}}$$

pourvu que $D\leqslant X^{\frac38-30\varepsilon}$.

Le cas des discriminants négatifs est absolument identique.

7. Démonstration des Corollaires 1.1, 1.2 et 1.9

Nous travaillerons avec les notations suivantes :
Soit $\mathcal{A}^+$ la suite des entiers a compris entre 1 et X, affectés du poids $\mathcal{H}(a)$ (rappelons que l'on a posé $\mathcal{H}(a) = 0$ si a n'est pas un discriminant fondamental). On fixe un (grand) entier P, et l'on pose $\tilde{\mathcal{A}}^+$ la suite des entiers a compris entre 1 et X affectés des poids $\mathcal{H}_P(a)$.
Les quantités $\mathcal{A}^-$ et $\tilde{\mathcal{A}}^-$ sont définies par analogie mais concernent les entiers a compris entre $-X$ et -1. Le Théorème 1.8 nous incite à travailler avec les formules d'approximation

$$\left|\tilde{\mathcal{A}}_q^{\pm}\right| = \frac{\nu_P(q)}{q}\mathbb{X}_P^{\pm} + r(\tilde{\mathcal{A}}^{\pm}, q),$$

où on pose, pour q sans facteur carré,

$$\left|\tilde{\mathcal{A}}_q^{\pm}\right| = \sum_{\substack{1\leqslant \pm n\leqslant X\\ q|n}} \mathcal{H}_P(n), \quad \text{et} \quad \mathbb{X}_P^{\pm} = \sum_{1\leqslant \pm n\leqslant X} \mathcal{H}_P(n),$$

en imitant les formules du crible. Le Théorème 1.8 et la relation (3) donnent, pour $X > X_0(P)$, les encadrements

$$(1-o(1))\frac{X}{2\pi^2} \leqslant \mathbb{X}_P^{+} \leqslant (1+o(1))(1+O(P^{-1}))\frac{X}{2\pi^2} \tag{65}$$

et

$$(1-o(1))\frac{3X}{2\pi^2} \leqslant \mathbb{X}_P^{-} \leqslant (1+o(1))(1+O(P^{-1}))\frac{3X}{2\pi^2}. \tag{66}$$

On vérifie que la fonction $\nu_P(p)$ satisfait bien les hypothèses du crible linéaire (condition (3) de [13] avec $\kappa = 1$). On voit que les formules du crible de Rosser, dans la forme qu'en a donnée Iwaniec ([13, Theorem 1]), produisent pour la fonction

$$S(\tilde{\mathcal{A}}^{\pm}, z) := \sum_{\substack{1\leqslant \pm n\leqslant X\\ p|n\Longrightarrow p\geqslant z}} \mathcal{H}_P(n),$$

la majoration

$$S(\tilde{\mathcal{A}}^{\pm}, z) \leqslant \prod_{p<z}\big(1-\frac{\nu_P(p)}{p}\big)\big\{F(\frac{\log D}{\log z})+o(1)\big\}\mathbb{X}_P^{\pm} + \sum_{q\leqslant D}\mu^2(q)\left|r(\tilde{\mathcal{A}}^{\pm}, q)\right|, \tag{67}$$

où $o(1)$ est un terme d'erreur qui tend vers 0 dans notre application, et F est l'habituelle fonction du crible en dimension 1. Le Théorème nous incite à prendre $D = X^{\frac{3}{8}-\varepsilon}$, puisqu'on a la majoration

$$\sum_{q\leqslant D}\mu^2(q)\left|r(\tilde{\mathcal{A}}^{\pm}, q)\right| = o_P(\frac{X}{\log X}), \tag{68}$$

et le produit eulérien de (67) vaut

$$\prod_{p<z}\big(1-\frac{\nu_P(p)}{p}\big)=\frac{\pi^2}{6}.\frac{e^{-\gamma}}{\log z}(1+O(P^{-1}))\big(1+O(\frac{1}{\log z})\big), \tag{69}$$

où γ est la constante d'Euler. En posant $z=X^{\frac{1}{u}}$ (u constante >1) et en regroupant (65),...,(7.5), on a l'inégalité

$$S(\tilde{\mathcal{A}}^{\pm},z)\leqslant\alpha^{\pm}\frac{u}{12e^{\gamma}}F(\frac{3u}{8})\frac{X}{\log X}(1+\eta),$$

pour tout $\eta>0$, $P>P_0(\eta)$ et $X>X_0(\eta,P)$. Bien entendu, sous les mêmes conditions, on a l'inégalité,

$$S(\mathcal{A}^{\pm},z)\leqslant\alpha^{\pm}\frac{u}{12e^{\gamma}}F(\frac{3u}{8})\frac{X}{\log X}(1+\eta), \tag{70}$$

puisque trivialement, on a $S(\mathcal{A}^{\pm},z)\leqslant S(\tilde{\mathcal{A}}^{\pm},z)$. On conçoit pourquoi il est avantageux de travailler avec la suite $\tilde{\mathcal{A}}^{\pm}$, puisque son exposant de répartition est $\frac{3}{8}-\varepsilon$ au lieu de $\frac{2}{7}-\varepsilon$.

7.a. **Démonstration du Corollaire 1.1.** Soit $\delta>0$ très petit et soit $u>1$ une constante telle que, pour une suite de X tendant vers l'infini, on ait l'inégalité

$$\Big|\Big\{\Delta\in\Delta^{+}(X);\quad p|\Delta\Longrightarrow p\geqslant X^{\frac{1}{u}},r_3(\Delta)=0\Big\}\Big|\leqslant\delta.\frac{X}{\log X}. \tag{71}$$

Puisque, hors de l'ensemble de la ligne précédente, tout Δ compté dans $S(\mathcal{A}^{+},X^{\frac{1}{u}})$ vérifie $\mathcal{H}(\Delta)\geqslant 1$, l'inégalité (70) entraîne l'encadrement

$$\begin{aligned}\Big|\Big\{\Delta\in\Delta^{+}(X);\quad p|\Delta\Longrightarrow p\geqslant X^{\frac{1}{u}}\Big\}\Big|-\delta.\frac{X}{\log X}&\\ \leqslant S(\mathcal{A}^{+},X^{\frac{1}{u}})\leqslant\frac{u}{12e^{\gamma}}F(3u/8)\frac{X}{\log X}(1+\eta).&\end{aligned} \tag{72}$$

À la gauche de cette inégalité apparaît, à un terme négligeable près, le nombre des entiers $<X$, congrus à 1 modulo 4, dont tous les facteurs premiers sont supérieurs à $X^{\frac{1}{u}}$, cardinal que l'on sait être équivalent à

$$\frac{1}{2}uw(u)\frac{X}{\log X}\ (X\to\infty),$$

avec $w(u)$ fonction de Buchstab ([17, Théorème 3, p. 406]). On sait aussi que

$$w(u)=\frac{F(u)+f(u)}{2e^{\gamma}},$$

avec F et f fonctions du crible linéaire. Finalement, la relation (72) montre que u vérifie l'inégalité

$$3(F(u)+f(u))\leqslant F(\frac{3u}{8})+\eta+\delta.\frac{12e^{\gamma}}{u},$$

pour tout $\eta > 0$, soit encore

$$3(F(u) + f(u)) \leqslant F(\frac{3u}{8}) + \delta.\frac{12e^{\gamma}}{u}. \tag{73}$$

Signalons que si u vérifie (71), il en est de même pour tout u' tel que $1 < u' \leqslant u$. Pour $s \leqslant 3$ on a $F(s) = 2e^{\gamma}s^{-1}$ et pour $s \leqslant 2$, on a $f(s) = 0$, donc (73) n'a aucune solution en $u > 1$, par choix de δ très petit, d'où le Corollaire 1.1, dans le cas des nombres premiers congrus à 1 modulo 4.

Le cas des p congrus à 3 modulo 4, nécessite un traitement un peu différent puisque p n'est pas un discriminant fondamental, par contre $4p$ en est un, et on a l'égalité $\mathbb{Q}(\sqrt{p}) = \mathbb{Q}(\sqrt{4p})$. Il faut donc cribler par les premiers impairs la suite des entiers a congrus à 12 modulo 16, compris entre 1 et X, affectés du poids $\mathcal{H}(a)$. La technique est la même que précédemment à la différence près que l'on doit utiliser la relation :

Pour tout $\varepsilon > 0$, il existe $\eta = \eta(\varepsilon) > 0$, tel que pour $X > X_0(P)$ tendant vers l'infini, on a

$$\sum_{\substack{q \leqslant X^{\frac{3}{8}-\varepsilon} \\ q \text{ impair}}} \mu^2(q) \Big| \sum_{\substack{0<n\leqslant X \\ n\equiv 12 \mod 16,\ q|n}} \mathcal{H}_P(n) - \frac{\nu_P(q)}{q} \sum_{\substack{0<n\leqslant X \\ n\equiv 12 \mod 16}} \mathcal{H}_P(n) \Big| = O_{\varepsilon,P}\big(X^{1-\eta}\big),$$

qui n'est qu'une variante de la première relation du Théorème 1.8 *iii)*.

7.b. **Démonstration du Corollaire 1.2.** Pour le Corollaire 1.2, il suffit de modifier la preuve précédente pour affirmer que, uniformément sur l'ensemble des $k+1$-uplets $(p'_1, \cdots, p'_{k+1})$ vérifiant

$$p'_1 \equiv 3 \pmod 4, \quad p'_2 \equiv \cdots \equiv p'_{k+1} \equiv 1 \pmod 4$$

et

$$p'_1 < p'_2 < \cdots < p'_{k+1} \leqslant \exp(\sqrt{\log x}),$$

on a la minoration

$$\left| \left\{ p \leqslant \frac{X}{p'_1 \cdots p'_{k+1}} \ ; \ p \equiv 3 \pmod 4, r_3(pp'_1 \cdots p'_{k+1}) = 0 \right\} \right| \gg \frac{X}{p'_1 \cdots p'_{k+1} \log X}.$$

On somme alors sur les p'_i vérifiant les conditions précédentes et on applique (1) qui affirme qu'on a $r_2(pp'_1 \cdots p'_{k+1}) = k$. Reprendre les techniques précédentes en introduisant cette minuscule condition de congruence modulo $p'_1 \cdots p'_{k+1}$ ne pose pas de difficulté majeure (il faudra conserver tout au long des calculs, la condition $\Delta \equiv 0 \pmod{p'_1 \cdots p'_{k+1}}$).

7.c. **Preuve du Corollaire 1.9, système II..** La démarche est la même : on part de (70), mais maintenant avec $\alpha^- = 3$. L'inégalité (73) devient dans ce cas

$$F(u) + f(u) \leqslant F(\frac{3u}{8}) + \delta.\frac{4e^{\gamma}}{u}, \tag{74}$$

et cette inégalité entraîne $u < 4.8$ pour δ suffisamment petit. En effet, des tables des fonctions F et f donnent $F(4.8) + f(4.8) = 1.999\ldots$ et on a facilement

$F(\frac{3.4,8}{8}) = \frac{16.e^\gamma}{3.4,8} = 1,978\ldots$ Par (1), on a donc prouvé le Corollaire 1.9, système II.

7.d. **Preuve du Corollaire 1.9, système I.** On a toujours $\alpha^- = 3$, mais on considère maintenant, pour δ positif très petit, $u > 1$ tel qu'on ait l'inégalité

$$\left|\left\{\Delta \in \Delta^-(X); \quad p|\Delta \Longrightarrow p \geqslant X^{\frac{1}{u}}, r_3(\Delta) \leqslant 1\right\}\right| \leqslant \delta \frac{X}{\log X},$$

pour une suite de X tendant vers l'infini. Maintenant, hors de l'ensemble ci-dessus, on a $\mathcal{H}(\Delta) \geqslant 4$, et l'inégalité (74) est modifiée par l'intrusion à gauche d'un facteur 4, soit

$$4(F(u) + f(u)) \leqslant F(\frac{3u}{8}) + \delta.\frac{4e^\gamma}{u},$$

inéquation qui n'a aucune solution en $u > 1$, pourvu que δ soit très petit.

Références

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

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

[3] K. Belabas, On the mean 3-rank of quadratic fields, *Compositio Mathematica* **118** (1999), pp. 1–9.

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

[5] H. Cohen & H. W. Lenstra, Jr., Heuristics on class groups of number fields, in *Number theory, Noordwijkerhout 1983* (Berlin), Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 33–62.

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

[7] 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.

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

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

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

[11] B. N. Delone & D. K. Faddeev, *The theory of irrationalities of the third degree*, Translations of Mathematical Monographs, vol. 10, American Mathematical Society, 1964.

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

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

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

[15] 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.

[16] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, second ed., Springer-Verlag, Berlin, 1990.

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

Karim Belabas
Max-Planck-Institut für Mathematik
Gottfried-Clarenstrasse, 26.
D-53225 Bonn

Étienne Fouvry
Mathématique-Bâtiment 425
Université de Paris-Sud
F-91405 Orsay Cedex

Email : {Karim.Belabas,Etienne.Fouvry}@math.u-psud.fr