ACTA ARITHMETICA
174.1 (2016)

La conjecture de Manin pour certaines surfaces de Châtelet

par

Kevin Destagnol (Paris)

Table des matières

1. Introduction. On définit la surface de Châtelet $S_{a,F}$ comme modèle minimal propre et lisse de variétés affines de $\mathbb{A}^3_{\mathbb{Q}}$ de la forme

$$X^2 - aY^2 = F(X,1)$$

2010 *Mathematics Subject Classification*: 11D45, 11N37, 11D57.
Key words and phrases: Manin's conjecture, Peyre's constant, Châtelet surfaces, number of representations as sum of two squares, descent method, torsors, counting rational points on algebraic varieties.
Received 28 September 2015; revised 6 January 2016.
Published online 10 June 2016.

DOI: 10.4064/aa8312-2-2016

où F est une forme binaire à coefficients entiers de degré 4, de discriminant non nul et a un entier qui n'est pas un carré. Ces surfaces introduites par Châtelet [10], [11] sont arithmétiquement très riches puisqu'elles correspondent à l'exemple historique donné en 1971 par Swinnerton-Dyer de variétés ne satisfaisant ni le principe de Hasse ni l'approximation faible. Elles sont également des désingularisations minimales de surfaces de del Pezzo de degré 4 de type de singularité $2\mathbf{A}_1$ conjuguées [7, remarque 2.3]. Les surfaces de del Pezzo ont été parmi les premières à être considérées dans le traitement de la conjecture de Manin ([3], [19], [23] ou encore [26] entre autres) puisque les plus simples dans la classification birationnelle d'Iskovskih [25].

L'objet de cet article est de décrire la répartition des points rationnels sur les surfaces de Châtelet dans les cas où $S_{a,F} := S$ avec F produit de deux formes linéaires F_1 et F_2 non proportionnelles par une forme quadratique F_3 irréductible sur $\mathbb{Q}[i]$ et $a = -1$. Tous les éléments quant à la géométrie de ces surfaces dont nous auront besoin ont été démontrés dans [15] et [16] et sont résumés dans [9] et [7] dans le cas où F est scindé. Ils s'adaptent au cas présent sans difficulté. En particulier, le système linéaire anticanonique $|\omega_S^{-1}|$ est sans point base, ce qui donne lieu à un morphisme $\psi : S \to \mathbb{P}^4$. On s'intéresse alors à la quantité

$$N(B) = \#\{x \in S(\mathbb{Q}) \mid (H_4 \circ \psi)(x) \leq B\},$$

où H_4 est une hauteur sur $\mathbb{P}^4(\mathbb{Q})$ qui sera définie en section 6.1. Le rang du groupe de Picard de S vaut ici 2 [9], si bien que la conjecture de Manin prend la forme

$$N(B) \sim c_S B \log(B)$$

pour une certaine constante $c_S > 0$. Peyre [30] dans un premier temps, puis Batyrev et Tschinkel [1] dans un cadre plus général, ont proposé une expression conjecturale de la constante c_S s'exprimant en termes d'une mesure de Tamagawa sur l'espace adélique associé à la surface S (voir aussi la formule empirique donnée par Peyre dans [31, formule 5.1]).

D'après [15] et [16], l'obstruction de Brauer–Manin est la seule obstruction au principe de Hasse et à l'approximation faible pour les surfaces de Châtelet et en particulier les surfaces considérées spécifiquement dans cet article ne satisfont pas nécessairement l'approximation faible mais satisfont le principe de Hasse. Il s'agit ici du troisième cas, après [7] et [8], pour lequel la conjecture de Manin dans sa forme forte conjecturée par Peyre dans [31, formule 5.1] est établie par des méthodes de descente sur des torseurs pour une classe de variétés ne satisfaisant pas l'approximation faible.

Les travaux de La Bretèche, Browning et Peyre [7] utilisant l'approche par les torseurs versels (introduits par Colliot-Thélène et Sansuc [12]–[14] et utilisés dans ce cadre pour la première fois par Salberger [34]) ont permis dans un premier temps d'établir la conjecture de Manin dans le cas de factorisations de type un produit de formes linéaires non proportionnelles [7], puis les travaux de La Bretèche et Browning ont fourni le cas d'un produit d'une forme linéaire et d'une forme cubique irréductible sur $\mathbb{Q}$ [6], et enfin les travaux de La Bretèche et Tenenbaum ceux d'une forme irréductible sur $\mathbb{Q}[i]$ de degré 4 ou d'un produit de deux formes quadratiques irréductibles sur $\mathbb{Q}[i]$ [8].

On achève dans cet article la preuve de la conjecture de Manin dans le cas des surfaces de Châtelet avec $a = -1$. Le théorème suivant améliore notamment la borne $N(B) \ll B \log(B)$ obtenue par Browning [9].

Théorème 1.1. *Lorsque $a = -1$ et $F = F_1F_2F_3$ avec F_1 et F_2 deux formes linéaires non proportionnelles et F_3 une forme quadratique irréductible sur $\mathbb{Q}[i]$, on a*

$$N(B) \underset{B\to\infty}{\sim} c_0 B \log(B),$$

où $c_0 = c_S$ est la constante conjecturée par Peyre.

Remarque. On peut se convaincre assez aisément que les méthodes développées ici permettraient de généraliser le résultat à tous les $a < 0$ mais au prix d'un certain nombre de complications techniques comme expliqué dans [8, Introduction]. Le cas $a > 0$ semble nécessiter une approche différente du fait du nombre infini d'unités du corps quadratique réel $\mathbb{Q}(\sqrt{a})$.

La méthode utilisée ici suit celle développée par La Bretèche, Browning et Peyre dans le cas précédemment cité. En particulier, la résolution de ce problème repose essentiellement sur l'estimation asymptotique de sommes du type

$$S(X) = \sum_{\mathbf{x}\in\mathbb{Z}^2\cap X\mathcal{R}} r(F_1(\mathbf{x}))r(F_2(\mathbf{x}))r(F_3(\mathbf{x})), \tag{1.1}$$

pour une région $\mathcal{R} \subset \mathbb{R}^2$ convenable et où $r(n)$ désigne le nombre de représentations d'un entier n comme somme de deux carrés. On rappelle qu'on a l'expression

$$r(n) = 4\sum_{d|n} \chi(d),$$

où χ désigne le caractère de Dirichlet non principal modulo 4. La méthode pour estimer ces sommes est inspirée de [5] où le même genre de sommes est étudiée mais pour la fonction τ nombre de diviseurs à la place de la fonction r. Pour la vérification de la conjecture de Peyre, on s'inspire ici de [8] et de [7]. Cependant, à la différence du cas traité dans [7], on établit que le traitement de la conjecture de Manin se fait au moyen d'un passage sur des torseurs distincts des torseurs versels dont on donne une description précise en section 7.

2. Estimations de sommes liées à la fonction r. Plus précisément, on considère $\mathbf{x} = (x_1, x_2)$, F_1 et F_2 deux formes linéaires binaires dans $\mathbb{Z}[x_1, x_2]$, F_3 une forme quadratique dans $\mathbb{Z}[x_1, x_2]$ et $\mathcal{R}$ est une région de $\mathbb{R}^2$ vérifiant les hypothèses suivantes que l'on notera **NH**:

(2.0)
- (i) Les formes F_1 et F_2 ne sont pas proportionnelles.
- (ii) La forme quadratique F_3 est irréductible sur $\mathbb{Q}[i]$.
- (iii) Pour tout $\mathbf{x} \in \mathcal{R}$ et pour tout $i \in \{1, 2, 3\}$, $F_i(\mathbf{x}) > 0$.
- (iv) La région $\mathcal{R}$ est convexe, bornée avec une frontière continûment différentiable.

On définit

$$X\mathcal{R} = \{X\mathbf{x} \mid \mathbf{x} \in \mathcal{R}\}$$

et on pose $F_1(\mathbf{x}) = a_1x_1+b_1x_2$, $F_2(\mathbf{x}) = a_2x_1+b_2x_2$ et $F_3(\mathbf{x}) = a_3x_1^2+b_3x_2^2+c_3x_1x_2$, avec a_i, b_i et c_3 entiers. Lorsque $J, L \in \mathbb{Z}[x_1, x_2]$ sont deux formes binaires homogènes, on note $\mathrm{disc}(J)$ le discriminant de $J(x, 1)$ et $\mathrm{Res}(J, L)$ le résultant de $J(x, 1)$ et de $L(x, 1)$. On considère alors

$$\Delta = \mathrm{disc}(F_3) = c_3^2-4a_3b_3 \neq 0, \quad \Delta_{12} = \mathrm{Res}(F_1, F_2) = a_1b_2-a_2b_1 \neq 0, \tag{2.1}$$

et

$$\Delta_{i3} = \mathrm{Res}(F_i, F_3) = a_3b_i^2 + b_3a_i^2 - c_3a_ib_i = F_3(-b_i, a_i) \neq 0$$

pour $i \in \{1, 2\}$ et, pour $\mathbf{d} = (d_1, d_2, d_3) \in \mathbb{N}^3$,

$$\Lambda(\mathbf{d}) = \{\mathbf{x} \in \mathbb{Z}^2 \mid d_i \mid F_i(\mathbf{x})\},$$

où l'on note systématiquement (sauf mention contraire) $d_i \mid F_i(\mathbf{x})$ pour $d_1 \mid F_1(\mathbf{x})$, $d_2 \mid F_2(\mathbf{x})$ et $d_3 \mid F_3(\mathbf{x})$. On introduit alors la quantité essentielle

$$\rho(\mathbf{d}) = \rho(\mathbf{d}, F_1, F_2, F_3) = \#(\Lambda(\mathbf{d}) \cap [0, d[^2)$$

où l'on note systématiquement $d = d_1d_2d_3$.

On pose également

$$L_\infty = L_\infty(F_1, F_2, F_3) = \max\{\|F_i\|\},$$

où $\|F_i\|$ désigne le plus grand coefficient en valeur absolue de la forme F_i,

$$r_\infty = r_\infty(\mathcal{R}) = \sup_{\mathbf{x}\in\mathcal{R}} \max\{|x_1|, |x_2|\}$$

et

$$r' = r'(F_1, F_2, F_3, \mathcal{R}) = \sup_{\mathbf{x}\in\mathcal{R}} \max\{|F_1(\mathbf{x})|, |F_2(\mathbf{x})|, \sqrt{|F_3(\mathbf{x})|}\}.$$

On note enfin

$$\mathcal{E} = \{n \in \mathbb{Z} \mid \exists \ell \in \mathbb{N},\, n \equiv 2^\ell \pmod{2^{\ell+2}}\}$$

ainsi que $\mathcal{E}_{2^n}$ sa projection modulo 2^n,

$$\mathcal{E}_{2^n} = \{k \in \mathbb{Z}/2^n\mathbb{Z} \mid \exists \ell \in \mathbb{N},\, k \equiv 2^\ell \pmod{2^{\min\{\ell+2,n\}}}\},$$

et

$$\eta = 1 - \frac{1 + \log\log 2}{\log 2} = 0.086071\ldots. \tag{2.2}$$

La borne $S(X) \ll X^2$ fournie par [2], où la quantité $S(X)$ a été définie en (1.1), est alors améliorée par le résultat suivant.

Théorème 2.1. *On suppose que les formes F_1, F_2 et F_3 et la région $\mathcal{R}$ vérifient les hypothèses* ***NH*** (2.0). *Soient $\varepsilon > 0$ et $X \geq 1$ tels que $r'X^{1-\varepsilon} \geq 1$. Alors*

$$S(X) = \pi^3 \mathrm{vol}(\mathcal{R}) X^2 \prod_p \sigma_p + O_\varepsilon\Big(\frac{L_\infty^\varepsilon (r_\infty r' + r_\infty^2) X^2}{(\log X)^{\eta-\varepsilon}}\Big),$$

où

$$\sigma_p = \Big(1 - \frac{\chi(p)}{p}\Big)^3 \sum_{\boldsymbol{\nu}\in\mathbb{N}^3} \frac{\chi(p)^{\nu_1+\nu_2+\nu_3}\rho(p^{\nu_1}, p^{\nu_2}, p^{\nu_3})}{p^{2(\nu_1+\nu_2+\nu_3)}}$$

lorsque p est impair et

$$\sigma_2 = 8 \lim_{n\to\infty} 2^{-2n} \#\{\mathbf{x} \in (\mathbb{Z}/2^n\mathbb{Z})^2 \mid F_i(\mathbf{x}) \in \mathcal{E}_{2^n}\}.$$

Le produit $\prod_{p>2} \sigma_p$ est bien absolument convergent.

On introduit alors l'ensemble

$$\mathfrak{D} = \{(\mathbf{d}, \mathbf{D}) \in \mathbb{N}^6 \mid d_i \mid D_i,\ 2 \nmid D_i\}$$

et pour $(\mathbf{d}, \mathbf{D}) \in \mathfrak{D}$, $X \geq 1$, on pose

$$\begin{aligned} S(X, \mathbf{d}, \mathbf{D}) &= S(X, \mathbf{d}, \mathbf{D}; \mathcal{R}, F_1, F_2, F_3) \\ &= \sum_{\mathbf{x}\in\Lambda(\mathbf{D})\cap X\mathcal{R}} r\Big(\frac{F_1(\mathbf{x})}{d_1}\Big) r\Big(\frac{F_2(\mathbf{x})}{d_2}\Big) r\Big(\frac{F_3(\mathbf{x})}{d_3}\Big). \end{aligned} \tag{2.3}$$

Cette somme est directement liée à un problème de comptage sur la variété affine de $\mathbb{A}^8$ d'équations

$$F_i(\mathbf{x}) = d_i(s_i^2 + t_i^2) \quad (i = 1, 2, 3), \tag{2.4}$$

où les (x_1, x_2) sont restreints à une certaine région.

On introduit ensuite les entiers ℓ_1, ℓ_2, ℓ_3 et les formes primitives F_1^*, F_2^* et F_3^* telles que

$$F_i = \ell_i F_i^*. \tag{2.5}$$

On considère alors

$$\mathbf{D}' = \Big(\frac{D_1}{(D_1, \ell_1)}, \frac{D_2}{(D_2, \ell_2)}, \frac{D_3}{(D_3, \ell_3)}\Big),$$

$$a(\mathbf{D}, \boldsymbol{\Delta}) = (D_1, \Delta_{12}\Delta_{13})(D_2, \Delta_{12}\Delta_{23})(D_3, \Delta(\Delta_{13}, \Delta_{23})) \tag{2.6}$$

avec $\mathbf{\Delta} = (\Delta, \Delta_{12}, \Delta_{13}, \Delta_{23})$ et

$$a'(\mathbf{D}, \mathbf{\Delta}) = a(\mathbf{D}', \mathbf{\Delta}') = (D'_1, \Delta'_{12}\Delta'_{13})(D'_2, \Delta'_{12}\Delta'_{23})(D'_3, \Delta'(\Delta'_{13}, \Delta'_{23})),$$

où

$$\mathbf{\Delta}' = (\Delta', \Delta'_{12}, \Delta'_{13}, \Delta'_{23}) = \left(\frac{\Delta}{\ell_3^2}, \frac{\Delta_{12}}{\ell_1\ell_2}, \frac{\Delta_{13}}{\ell_1^2\ell_3}, \frac{\Delta_{23}}{\ell_2^2\ell_3}\right).$$

On a alors le résultat suivant, crucial en vue de l'obtention de la conjecture de Manin.

Théorème 2.2. *Soient $\varepsilon > 0$ et $X \geq 1$ tels que $r'X^{1-\varepsilon} \geq 1$. Si les formes F_1, F_2 et F_3 et la région $\mathcal{R}$ vérifient les hypothèses* ***NH*** (2.0) *et $(\mathbf{d}, \mathbf{D}) \in \mathfrak{D}$, alors*

$$S(X, \mathbf{d}, \mathbf{D}) = \pi^3 \operatorname{vol}(\mathcal{R})X^2 \prod_p \sigma_p(\mathbf{d}, \mathbf{D}) + O_\varepsilon\left(\frac{L_\infty^\varepsilon D^\varepsilon (r_\infty r' + r_\infty^2) a'(\mathbf{d}, \mathbf{\Delta}) X^2}{(\log(X))^{\eta-\varepsilon}}\right),$$

où

$$\sigma_p(\mathbf{d}, \mathbf{D}) = \left(1 - \frac{\chi(p)}{p}\right)^3 \sum_{\boldsymbol{\nu} \in \mathbb{N}^3} \frac{\chi(p)^{\nu_1+\nu_2+\nu_3} \rho(p^{N_1}, p^{N_2}, p^{N_3})}{p^{2(N_1+N_2+N_3)}}$$

avec $N_i = \max\{\nu_p(D_i), \nu_i + \nu_p(d_i)\}$ lorsque $p > 2$ et

$$\sigma_2(\mathbf{d}, \mathbf{D}) = \sigma_2(\mathbf{d}) = 8 \lim_{n\to\infty} 2^{-2n} \#\{\mathbf{x} \in (\mathbb{Z}/2^n\mathbb{Z})^2 \mid F_i(\mathbf{x}) \in d_i \mathcal{E}_{2^n}\}. \tag{2.7}$$

De plus,

$$\prod_p \sigma_p(\mathbf{d}, \mathbf{D}) \ll L_\infty^\varepsilon D^\varepsilon a'(\mathbf{d}, \mathbf{\Delta}).$$

Remarque. Le même raisonnement que dans [5, section 6] permet, *mutatis mutandis*, de se ramener au Théorème 2.1 grâce à un changement de variables. Le fait que $\Lambda(\mathbf{D})$ ne soit pas un réseau (contrairement au cas de [7]) est pallié en le reliant à une réunion de réseaux de la même manière que dans [17]. Ainsi, on ne détaille pas ici la démonstration du Théorème 2.2.

Pour terminer cette section, dans l'optique de vérifier la conjecture de Peyre, il est bon de réinterpréter la constante obtenue dans le Théorème 2.2. On définit, pour $\boldsymbol{\lambda} \in \mathbb{N}^3$, $\boldsymbol{\mu} \in \mathbb{N}^3$ et p premier différent de 2,

$$N_{\boldsymbol{\lambda},\boldsymbol{\mu}}(p^n) = \#\{(\mathbf{x}, \mathbf{s}, \mathbf{t}) \in (\mathbb{Z}/p^n\mathbb{Z})^8 \mid F_i(\mathbf{x}) \equiv p^{\lambda_i}(s_i^2 + t_i^2) \pmod{p^n},\ p^{\mu_i} | F_i(\mathbf{x})\}$$

et

$$\omega_{\boldsymbol{\lambda},\boldsymbol{\mu}}(p) = \lim_{n\to\infty} p^{-5n-\lambda_1-\lambda_2-\lambda_3} N_{\boldsymbol{\lambda},\boldsymbol{\mu}}(p^n). \tag{2.8}$$

Ces quantités sont bien définies et correspondent aux densités p-adiques associées à la variété définie par (2.4). Pour le cas $p = 2$, on introduit

$$N_{\mathbf{d}}(2^n) = \#\{(\mathbf{x}, \mathbf{s}, \mathbf{t}) \in (\mathbb{Z}/2^n\mathbb{Z})^8 \mid F_i(\mathbf{x}) \equiv d_i(s_i^2 + t_i^2) \pmod{2^n}\}$$

et

$$\omega_{\mathbf{d}}(2) = \lim_{n\to\infty} 2^{-5n} N_{\mathbf{d}}(2^n). \tag{2.9}$$

Notant enfin $\omega_\infty(\mathcal{R})$ la densité archimédienne associée au problème de comptage (2.4), on obtient le résultat suivant, qui traduit le fait que le principe de Hasse est vérifié sur les torseurs décrits en section 7.

Théorème 2.3. *Supposons que les formes F_1, F_2 et F_3 et la région $\mathcal{R}$ vérifient les hypothèses* ***NH*** (2.0) *et que $(\mathbf{d},\mathbf{D}) \in \mathfrak{D}$. Pour tout nombre premier $p > 2$, on a $\omega_{\boldsymbol{\lambda},\boldsymbol{\mu}}(p) = \sigma_p(\mathbf{d},\mathbf{D})$ avec $\boldsymbol{\lambda} = (\nu_p(d_1),\nu_p(d_2),\nu_p(d_3))$ et $\boldsymbol{\mu} = (\nu_p(D_1),\nu_p(D_2),\nu_p(D_3))$, $\omega_{\mathbf{d}}(2) = \sigma_2(\mathbf{d})$ et $\omega_\infty(\mathcal{R}) = \pi^3 \operatorname{vol}(\mathcal{R})$.*

3. Propriétés des fonctions ρ. La fonction ρ a été abondamment étudiée, notamment dans [17], [27] et [28] ou [5]. Il résulte du théorème chinois que la fonction ρ est multiplicative dans le sens que si l'on se donne deux triplets $\mathbf{d}=(d_1,d_2,d_3)$ et $\mathbf{d}'=(d_1',d_2',d_3')$ tels que $(d_1d_2d_3, d_1'd_2'd_3')=1$, alors

$$\rho(d_1d_1', d_2d_2', d_3d_3') = \rho(\mathbf{d})\rho(\mathbf{d}').$$

Il suffit donc de l'étudier sur les triplets de nombres premiers. Le lemme immédiat suivant tiré de [5, lemme 1] permet de se ramener à ce cas.

Lemme 3.1. *Soient F_1, $F_2 \in \mathbb{Z}[x_1,x_2]$ des formes linéaires non proportionnelles et $F_3 \in \mathbb{Z}[x_1,x_2]$ une forme quadratique. Avec les notations de* (2.5), *pour $\mathbf{d} \in \mathbb{N}^3$, on a*

$$\frac{\rho(\mathbf{d},F_1,F_2,F_3)}{(d_1d_2d_3)^2} = \frac{\rho(\mathbf{d}',F_1^*,F_2^*,F_3^*)}{(d_1'd_2'd_3')^2},$$

où $\mathbf{d}' = (d_1/(d_1,\ell_1), d_2/(d_2,\ell_2), d_3/(d_3,\ell_3))$.

On a alors le résultat suivant.

Lemme 3.2. *Soient F_1, F_2 des formes linéaires primitives non proportionnelles et F_3 une forme quadratique primitive irréductible sur $\mathbb{Q}$.*

(a) *Pour tout nombre premier p, on a*

$$\rho(p^\nu,1,1) = \rho(1,p^\nu,1) = p^\nu.$$

(b) *Si $p \nmid 2\operatorname{disc}(F_3)$, alors*

$$\rho(1,1,p^\nu) = \varphi(p^\nu)\left(1+\left(\frac{\operatorname{disc}(F_3)}{p}\right)\right)\left\lceil\frac{\nu}{2}\right\rceil + p^{2(\nu-\lceil\nu/2\rceil)} \le (\nu+1)p^\nu.$$

De plus, si p est un facteur impair de $\operatorname{disc}(F_3)$, *on a*

$$\rho(1,1,p^\nu) \ll (\nu+1)p^{\nu+\min\{\lfloor\nu_p(\operatorname{disc}(F_3)/2)\rfloor,\lfloor\nu/2\rfloor\}}$$

et si $p=2$,

$$\rho(1,1,2^\nu) \ll (\nu+1)2^\nu.$$

(c) *Lorsque* $\max\{\nu_1,\nu_2\} \le \lceil \nu_3/2\rceil$ *et* p *impair, on a*
$$\rho(p^{\nu_1},p^{\nu_2},p^{\nu_3}) \ll (\nu_3+1)p^{2(\nu_1+\nu_2)+\nu_3}p^{\min\{\lfloor \nu_p(\mathrm{disc}(F_3)/2)\rfloor,\lfloor \nu_3/2\rfloor\}}.$$
De plus, lorsque $\max\{\nu_1,\nu_2\} = \nu_3 = 1$ *et* $p \nmid \Delta_{12}\Delta_{13}\Delta_{23}$, *on a*
$$\rho(p^{\nu_1},p^{\nu_2},p^{\nu_3}) \ll p^{2(\nu_1+\nu_2)}.$$
Enfin, lorsque $\max\{\nu_1,\nu_2\} \le \lceil \nu_3/2\rceil$, *on a*
$$\rho(2^{\nu_1},2^{\nu_2},2^{\nu_3}) \ll 2^{2(\nu_1+\nu_2)+\nu_3}.$$

(d) *Lorsque* $\lceil \nu_3/2\rceil \le \min\{\nu_1,\nu_2\}$ *et pour tout nombre premier* p, *on a*
$$\rho(p^{\nu_1},p^{\nu_2},p^{\nu_3}) \ll p^{\nu_1+\nu_2+2\nu_3+\min\{\nu_1,\nu_2,\nu_p(\Delta_{12})\}}.$$

(e) *Lorsque* $\nu_j \le \lceil \nu_3/2\rceil \le \nu_3 \le \nu_i$ *avec* $\{i,j\} = \{1,2\}$ *et pour tout nombre premier* p, *on a*
$$\rho(p^{\nu_1},p^{\nu_2},p^{\nu_3}) \ll \nu_3 p^{2\nu_j+\nu_i+\nu_3+\lfloor \nu_3/2\rfloor}(p^{\min\{\lceil \nu_3/2\rceil,\lceil \nu_p(\Delta_{i3})/2\rceil\}} + p^{r_p}),$$
où
$$r_p = \min\{\nu_i - \lceil \nu_3/2\rceil, \lceil \nu_p(\Delta_{i3})/2\rceil\} + \min\{\lceil \nu_3/2\rceil, \lceil \nu_p(\mathrm{disc}(F_3))/2\rceil\}.$$

(f) *Pour tout nombre premier* p, *on a*
$$\rho(p^{\nu_1},p^{\nu_2},p^{\nu_3}) \ll \min\{p^{2(\nu_2+\nu_3)+\nu_1}, p^{2(\nu_1+\nu_3)+\nu_2}, (\nu_3+1)p^{2(\nu_1+\nu_2)+3\nu_3/2}\}.$$

Démonstration. La preuve des points (a) à (e) se trouve dans [5, lemme 3]. Démontrons donc le point (f). En négligeant les deux conditions $p^{\nu_1} \mid F_1(\mathbf{x})$ et $p^{\nu_3} \mid F_3(\mathbf{x})$, on obtient les majorations
$$\rho(p^{\nu_1},p^{\nu_2},p^{\nu_3}) \le p^{2(\nu_1+\nu_3)}\rho(1,p^{\nu_2},1) = p^{2(\nu_1+\nu_3)+\nu_2}.$$
On obtient aussi la majoration
$$\rho(p^{\nu_1},p^{\nu_2},p^{\nu_3}) \le p^{2(\nu_2+\nu_3)+\nu_1}$$
en inversant les rôles de F_1 et F_2. En oubliant les deux conditions sur les formes linéaires, on obtient
$$\rho(p^{\nu_1},p^{\nu_2},p^{\nu_3}) \le p^{2(\nu_1+\nu_2)}\rho(1,1,p^{\nu_3})$$
et on conclut grâce au point (b). ∎

Suivant toujours [5, section 3], on peut déduire de ces deux lemmes que la fonction
$$f(\mathbf{d}) = \frac{\rho(\mathbf{d})}{d_1d_2d_3}$$
est proche, au sens de la convolution, de la fonction $R : \mathbf{d} \mapsto R(\mathbf{d}) = r_\Delta(d_3)$ avec

$$r_\Delta(\ell) = \sum_{k\mid\ell} \chi_\Delta(k) \tag{3.1}$$

où $\chi_\Delta(n) = \left(\frac{\Delta}{n}\right)$ est le symbole de Kronecker et Δ a été défini en (2.1). On note également h la fonction arithmétique satisfaisant

$$f(\mathbf{d}) = (h * R)(\mathbf{d}) = \sum_{\substack{\mathbf{k}\in\mathbb{N}^3 \\ k_i | d_i}} h\left(\frac{d_1}{k_1}, \frac{d_2}{k_2}, \frac{d_3}{k_3}\right) R(\mathbf{k}).$$

Lemme 3.3. *Soient F_1 et F_2 deux formes linéaires non proportionnelles et F_3 une forme quadratique irréductible sur $\mathbb{Q}$. Avec la notation* (3.1), *on a pour tout $A > 0$,*

$$\sum_{\mathbf{k}\in\mathbb{N}^3} \frac{|h(\mathbf{k})| \log(k_1k_2k_3)^A}{k_1k_2k_3} \ll L_\infty^\varepsilon.$$

En particulier,

$$\prod_{p>2} \sigma_p = L(1, \chi_\Delta\chi) \sum_{\mathbf{k}\in\mathbb{N}^3} \frac{h(\mathbf{k})\chi(k_1k_2k_3)}{k_1k_2k_3} \ll L_\infty^\varepsilon. \tag{3.2}$$

Démonstration. Il suffit de remarquer que la preuve [5, lemme 4] dans le cas $A = 1$ s'adapte immédiatement pour fournir le résultat. ∎

On définit également pour un polynôme $g \in \mathbb{Z}[X]$ la quantité

$$\rho_g(n) = \#\{x \in \mathbb{Z}/n\mathbb{Z} \mid g(x) \equiv 0 \pmod{n}\}.$$

Il s'agit d'une fonction multiplicative qu'il suffit donc d'étudier sur les puissances de nombres premiers. On aura besoin du résultat suivant (voir [6, lemme 1] par exemple).

Lemme 3.4. *Soient $g \in \mathbb{Z}[X]$ de degré $d \geq 2$ et p un nombre premier qui ne divise pas le contenu de g et tel que $p^\mu \,\|\, \mathrm{disc}(g)$. Alors, pour tout $\nu \geq 1$,*

$$\rho_g(p^\nu) \leq d \min\{p^{\mu/2}, p^{(1-1/d)\nu}, p^{\nu-1}\}.$$

4. Démonstration du Théorème 2.1

4.1. Extraction des valuations 2-adiques. On effectue ici un raisonnement préliminaire similaire à celui effectué dans [6, section 3] afin de pouvoir utiliser des décompositions semblables à celles de [24, section 3]. En utilisant les formules $r(2n) = r(n)$ et $r(n) = 0$ si $n \equiv 3 \pmod 4$, on obtient

$$S(X) = \sum_{k_0 \geq 0} \sum_{\substack{\mathbf{x}\in\mathbb{Z}^2\cap X\mathcal{R} \\ 2^{k_0} \| \mathbf{x}}} r(F_1(\mathbf{x}))r(F_2(\mathbf{x}))r(F_3(\mathbf{x})) = \sum_{k_0 \geq 0} S^*(2^{-k_0}X),$$

où

$$S^*(X) = \sum_{\substack{\mathbf{x}\in\mathbb{Z}^2\cap X\mathcal{R} \\ 2\nmid(x_1,x_2)}} r(F_1(\mathbf{x}))r(F_2(\mathbf{x}))r(F_3(\mathbf{x})).$$

En regroupant les termes selon la valuation 2-adique de $F_i(\mathbf{x})$, on a

$$S(X) = \sum_{k_0 \geq 0} \sum_{\mathbf{k} \in \mathbb{N}^3} S_{\mathbf{k}}(2^{-k_0} X),$$

avec $S_{\mathbf{k}}(X)$ la restriction de $S^*(X)$ aux $\mathbf{x}$ tels que

$$\nu_2(F_i(\mathbf{x})) = k_i, \quad 2^{-k_i} F_i(\mathbf{x}) \equiv 1 \pmod 4$$

et $2 \nmid \mathbf{x}$. On a clairement $2^{k_i} \leq F_i(\mathbf{x}) \leq (X')^{\deg(F_i)}$, donc $k_i \ll \log(X')$. On remarque également que $\min\{k_i, k_j\} \leq \nu_2(\Delta_{ij})$.

Lemme 4.1. *Lorsque*

$$\nu_2(F_i(\mathbf{x})) = k_i, \quad 2^{-k_i} F_i(\mathbf{x}) \equiv 1 \pmod 4$$

et $2 \nmid \mathbf{x}$*, il existe une matrice* $\mathbf{M} \in \mathcal{M}_2(\mathbb{Z})$ *inversible dans* $\mathbb{Q}$ *et* $\mathbf{x}' \in \mathbb{Z}^2$ *avec* $x_1' \equiv 1 \pmod 4$ *tels que* $\mathbf{x} = \mathbf{M}\mathbf{x}'$.

Démonstration. En raisonnant comme dans [6, section 3], on peut supposer sans perte de généralité que a_1 est impair. La première condition

$$2^{-k_1} F_1(\mathbf{x}) \equiv 1 \pmod 4 \tag{4.1}$$

équivaut alors à l'existence de $x_1' \equiv 1 \pmod 4$ tel que $x_1 = cx_2 + c' 2^{k_1} x_1'$ où $c' \in \{\pm 1\}$ tel que $c' \equiv a_1 \pmod 4$ et $c \in [0, 2^{k_1+2}[\cap \mathbb{Z}$ tel que

$$a_1 c \equiv -b_1 \pmod{2^{k_1+2}}.$$

Si $k_1 = 0$, on a alors automatiquement $2 \nmid \mathbf{x}$, et sinon, cette condition devient équivalente au fait que x_2 soit impair.

Intéressons-nous à présent à la deuxième condition

$$2^{-k_2} F_2(\mathbf{x}) \equiv 1 \equiv x_1' \pmod 4.$$

Si on suppose la première condition vérifiée, cette condition est équivalente à

$$F_2(cx_2 + c' 2^{k_1} x_1', x_2) \equiv 2^{k_2} x_1' \pmod{2^{k_2+2}}.$$

On considère alors $F_2'(X, Y) = F_2(cY + c' 2^{k_1} X, Y) = 2^{k_2'}(aX + bY)$ pour k_2', a et b trois entiers tels que $(2, a, b) = 1$. Si $k_2' > k_2$, alors les deux premières conditions n'ont pas de solution commune. Si $k_2' \leq k_2$ on pose

$$k_2'' = k_2 - k_2' \geq 0 \tag{4.2}$$

et $F_2''(X, Y) = 2^{-k_2'} F_2'(X, Y)$ de sorte que

$$F_2''(x_1', x_2) \equiv 2^{k_2''} x_1' \pmod{2^{k_2''+2}}.$$

On peut écrire $x_2 \equiv \alpha_2 x_1' \pmod{2^{k_2''+2}}$ pour un unique $\alpha_2 \in [0, 2^{k_2''+2}[\cap \mathbb{Z}$ pour obtenir

$$F_2''(1, \alpha_2) \equiv 2^{k_2''} \pmod{2^{k_2''+2}}. \tag{4.3}$$

Finalement, lorsque la première condition est vérifiée, la deuxième est vérifiée si, et seulement si, $k_2' \leq k_2$ et $x_2 = \alpha_2 x_1' + 2^{k_2''+2} x_2'$ pour α_2 solution de (4.3). De plus, si $k_1 \neq 0$, α_2 doit être choisi impair.

Posons $F_3'(X,Y)=F_3(cY+c'2^{k_1}X,Y)=2^{k_3'}(cX^2+dXY+eY^2)$ pour k_3', c, d et e quatre entiers tels que $(2,c,d,e)=1$ et $k_3''=k_3-k_3'$ lorsque $k_3'\leq k_3$. L'égalité

$$2^{-k_3}F_3(\mathbf{x})\equiv 1\equiv x_1'^2 \pmod 4$$

conduit alors de même à montrer que si la première condition est remplie, la troisième l'est si, et seulement si, $k_3'\leq k_3$ et s'il existe $\alpha_3\in[0,2^{k_3''+2}[\cap\mathbb{Z}$ solution de

$$F_3''(1,\alpha_3)\equiv 2^{k_3''} \pmod{2^{k_3''+2}} \tag{4.4}$$

tel que $x_2=\alpha_3x_1'+2^{k_3''+2}x_2''$, α_3 devant être choisi impair lorsque $k_1\neq 0$. Dans le cas où les trois conditions sont remplies simultanément, d'après ce qui précède, soit il n'existe pas de solution, soit il existe α_2 solution de (4.3) et α_3 solution de (4.4) tels que

$$x_2\equiv\alpha_2x_1' \pmod{2^{k_2''+2}} \quad \text{et} \quad x_2\equiv\alpha_3x_1' \pmod{2^{k_3''+2}}.$$

Donc

$$\alpha_2\equiv\alpha_3 \pmod{2^{\min\{k_2'',k_3''\}+2}}$$

et par conséquent x_2 est de la forme $x_2=\alpha x_1'+2^{\max(k_2'',k_3'')+2}x_2'$ avec $\alpha=\alpha_2$ si $k_2\geq k_3$ et $\alpha=\alpha_3$ si $k_3\geq k_2$ et pour un certain entier x_2'. On vient donc de montrer que si les conditions

$$\nu_2(F_i(\mathbf{x}))=k_i, \qquad 2^{-k_i}F_i(\mathbf{x})\equiv 1 \pmod 4$$

et $2\nmid\mathbf{x}$ admettent des solutions, ces dernières peuvent s'écrire $\mathbf{x}=\mathbf{M}\mathbf{x}'$ avec $x_1'\equiv 1 \pmod 4$ et

$$\begin{aligned}\mathbf{M}=\mathbf{M}_\alpha&=\begin{pmatrix} c'2^{k_1} & c\\ 0 & 1\end{pmatrix}\begin{pmatrix} 1 & 0\\ \alpha & 2^{\max\{k_2'',k_3''\}+2}\end{pmatrix}\\ &=\begin{pmatrix} c'2^{k_1}+c\alpha & c2^{\max\{k_2'',k_3''\}+2}\\ \alpha & 2^{\max\{k_2'',k_3''\}+2}\end{pmatrix},\end{aligned}$$

où $\alpha\in[0,2^{\max\{k_2'',k_3''\}+2}[\cap\mathbb{Z}$ vérifie

$$\begin{cases} F_2''(1,\alpha)\equiv 2^{k_2''} \pmod{2^{k_2''+2}},\\ F_3''(1,\alpha)\equiv 2^{k_3''} \pmod{2^{k_3''+2}},\\ \alpha\equiv 1 \pmod 2 \quad \text{lorsque } k_1\geq 1.\end{cases} \tag{4.5}$$

On remarque pour conclure que

$$|\det(\mathbf{M})|=2^{k_1+\max\{k_2'',k_3''\}+2}. \ \blacksquare$$

On majore alors

$$n(\mathbf{k})=n(k_1,k_2,k_3), \tag{4.6}$$

le nombre d'entiers α dans $[0,2^{\max\{k_2'',k_3''\}+2}[\cap\mathbb{Z}$ vérifiant (4.5).

Lemme 4.2. *On a $n(\mathbf{k}) \ll 1$ avec $n(\mathbf{k})$ défini en* (4.6) *et où la borne ne dépend que de la valuation 2-adique de $\Delta^* := \Delta_{12}\Delta_{13}\Delta_{23}\Delta$.*

Démonstration. On commence par traiter le cas où $k_1 \geq 1$, dans lequel on sait que α doit être impair. On a clairement

$$n(\mathbf{k}) \leq \# \left\{ x \in \mathbb{Z}/2^{k_1+\max\{k_2,k_3\}+2}\mathbb{Z} \;\middle|\; \begin{array}{l} x \equiv -b_1\overline{a_1} \pmod{2^{k_1}}, \\ F_2(x,1) \equiv 0 \pmod{2^{k_2}}, \\ F_3(x,1) \equiv 0 \pmod{2^{k_3}} \end{array} \right\},$$

où $\overline{a}_1$ désigne l'inverse multiplicatif de a_1 dans $\mathbb{Z}/2^{k_1}\mathbb{Z}$. Alors, si $k_1 \geq \max\{k_2,k_3\}$, on a

$$n(\mathbf{k}) \ll \frac{2^{k_1+\max\{k_2,k_3\}}}{2^{k_1}} = 2^{\max\{k_2,k_3\}}.$$

En utilisant le fait que $\min\{k_i,k_1\} \leq \nu_2(\Delta_{i1})$ pour $i \in \{2,3\}$, on en déduit

$$n(\mathbf{k}) \ll 2^{\nu_2(\Delta^*)} \ll 1.$$

Passons aux cas où $\max\{k_2,k_3\} > k_1$. On traite tout d'abord le cas $k_3 \geq k_2$. Par le Lemme 3.4,

$$n(\mathbf{k}) \ll \frac{2^{k_1+k_3}}{2^{k_3}}\rho_{F_3(x,1)}(2^{k_3}) \ll 2^{k_1}\rho_{F_3(x,1)}(2^{k_3}) \ll 2^{k_1+\nu_2(\Delta)/2} \ll 1.$$

Enfin, de la même manière, dans les cas où $k_2 \geq k_3$, on obtient

$$n(\mathbf{k}) \ll 2^{k_1}\rho_{F_2(x,1)}(2^{k_2}) \ll 2^{k_1} \ll 1.$$

Il reste à majorer $n(\mathbf{k})$ lorsque $k_1 = 0$. Dans ce cas, on procède de même que ci-dessus pour les α impairs, mais on doit ajouter tous les α pairs de $\left[0, 2^{\max\{k_2,k_3\}}\right[\cap \mathbb{Z}$ qui vérifient (4.5). Avec la notation (4.4), le nombre de ces α est majoré par celui des β tels que

$$F_3''(1,\beta) \equiv 0 \pmod{2^{k_3''}}.$$

Par le Lemme 3.4, cette quantité est majorée par $2^{\nu_2(\operatorname{disc}(F_3''))} \ll 1$, ce qui achève la preuve. ∎

On relie maintenant la quantité $n(\mathbf{k})$ et la constante σ_2 qui apparaît dans le Théorème 2.1.

Lemme 4.3. *On a*

$$\sigma_2 = 2\sum_{k_0 \geq 0} \frac{1}{2^{2k_0}} \sum_{k_1,k_2,k_3 \in \mathbb{N}^3} \frac{n(\mathbf{k})}{2^{k_1+\max\{k_2'',k_3''\}+2}},$$

où les entiers k_2'' et k_3'' se déduisent de k_2 et k_3 comme en (4.2) *et* (4.4).

Démonstration. En partitionnant $(\mathbb{Z}/2^n\mathbb{Z})^2$ selon la valuation 2-adique de (x_1, x_2), on obtient l'égalité

$$\sigma_2 = \lim_{n\to\infty} \frac{8}{2^{2n}} \times \sum_{\substack{0\leq k_0\leq n\\ 0\leq k_1,k_2,k_3\leq n}} \#\{\mathbf{x}\in(\mathbb{Z}/2^{n-k_0}\mathbb{Z})^2 \mid 2\nmid \mathbf{x},\ F_i(\mathbf{x})\equiv 2^{k_i} \pmod{2^{m_{\mathbf{k},n,i}}}\},$$

où $m_{\mathbf{k},n,i} = \min\{k_i+2, n-k_0\}$ pour $i\in\{1,2,3\}$. On vérifie aisément grâce au Lemme 3.4 que la contribution des termes tels que pour au moins un des k_i $(1\leq i\leq 3)$ on ait $k_i+2 > n-k_0$ à la triple somme intérieure est négligeable. On peut donc s'intéresser uniquement aux triplets tels que $\max\{k_1,k_2,k_3\}\leq n-k_0-2$, ce qui revient à estimer

$$\sigma_2 = 8\lim_{n\to\infty} 2^{-2n} \times \sum_{\substack{0\leq k_0\leq n\\ 0\leq k_1,k_2,k_3\leq n-k_0-2}} \#\{\mathbf{x}\in(\mathbb{Z}/2^{n-k_0}\mathbb{Z})^2 \mid 2\nmid \mathbf{x},\ F_i(\mathbf{x})\equiv 2^{k_i} \pmod{2^{k_i+2}}\}.$$

On a vu en (4.1) qu'on pouvait supposer a_1 impair et que les conditions

$$\nu_2(F_i(\mathbf{x})) = k_i, \quad 2^{-k_i}F_i(\mathbf{x})\equiv 1 \pmod 4, \quad 2\nmid \mathbf{x}$$

impliquent l'existence de $x_1'\equiv 1 \pmod 4$ tel que

$$x_1\equiv cx_2 + c'2^{k_1}x_1' \pmod{2^{k_1+2}}$$

avec $c'\in\{\pm1\}$ et $c\equiv a_1 \pmod 4$. Par conséquent, x_1 est entièrement déterminé par la valeur de x_2 modulo 2^{k_1+2}. On sait ensuite que si on pose $x_2\equiv \alpha x_1' \pmod{2^{\max\{k_2'',k_3''\}+2}}$, alors α est une des $n(\mathbf{k})$ solutions de (4.5) dans $[0, 2^{\max\{k_2'',k_3''\}+2}[\,\cap\,\mathbb{Z}$. Posant $k=\max\{k_1,k_2'',k_3''\}$, on constate alors que les trois conditions de congruence ne dépendent que de la classe de $\mathbf{x}$ modulo 2^{k+2}. Autrement dit,

$$\sigma_2 = 8\lim_{n\to\infty} 2^{-2n} \sum_{\substack{0\leq k_0\leq n\\ 0\leq k_1,k_2,k_3\leq n-k_0-2}} 2^{2(n-k_0-k-2)} \times \#\{\mathbf{x}\in(\mathbb{Z}/2^{k+2}\mathbb{Z})^2 \mid 2\nmid \mathbf{x},\ F_i(\mathbf{x})\equiv 2^{k_i} \pmod{2^{k_i+2}}\},$$

soit

$$\sigma_2 = 2\sum_{k_0\geq 0}\frac{1}{2^{2k_0}} \sum_{k_1,k_2,k_3\geq 0}\frac{1}{2^{2k+2}} \times \#\{\mathbf{x}\in(\mathbb{Z}/2^{k+2}\mathbb{Z})^2 \mid 2\nmid \mathbf{x},\ F_i(\mathbf{x})\equiv 2^{k_i} \pmod{2^{k_i+2}}\}.$$

Dans le cas par exemple où $k=k_1$, cela fournit une contribution

$$2\sum_{k_0\geq 0}\frac{1}{2^{2k_0}}\sum_{0\leq k_2,k_3\leq k_1}\frac{1}{2^{2k_1+2}}2^{k_1-\max\{k_2'',k_3''\}}n(\mathbf{k}),$$

soit

$$2\sum_{k_0\geq 0}\frac{1}{2^{2k_0}}\sum_{0\leq k_2,k_3\leq k_1}\frac{n(\mathbf{k})}{2^{k_1+\max\{k_2'',k_3''\}+2}}.$$

On traite les deux autres cas de la même façon et en regroupant les trois contributions, on obtient finalement la formule

$$\sigma_2=2\sum_{k_0\geq 0}\frac{1}{2^{2k_0}}\sum_{k_1,k_2,k_3\geq 0}\frac{n(\mathbf{k})}{2^{k_1+\max\{k_2'',k_3''\}+2}}=\frac{2}{3}\sum_{k_1,k_2,k_3\geq 0}\frac{n(\mathbf{k})}{2^{k_1+\max\{k_2'',k_3''\}}}. \blacksquare$$

On écrit ensuite

$$\begin{aligned}S(X)=&\sum_{0\leq k_0}\sum_{0\leq\max(k_i)\leq\log\log X}S_{\mathbf{k}}(2^{-k_0}X)\\&+\sum_{k_0\geq 0}\sum_{\max(k_i)>\log\log X}S_{\mathbf{k}}(2^{-k_0}X).\end{aligned}\tag{4.7}$$

D'après ce qui précède,

$$S_{\mathbf{k}}(X)=\sum_{\alpha}S_{\mathbf{k},\alpha}(X)\tag{4.8}$$

où α parcourt les $n(\mathbf{k})$ solutions de (4.5) et où

$$S_{\mathbf{k},\alpha}(X)=\sum_{\substack{\mathbf{x}'\in\mathbb{Z}^2\cap X\mathcal{R}_{\mathbf{M}}\\ x_1'\equiv 1\,[4]}}r(F_1(\mathbf{M}\mathbf{x}'))r(F_2(\mathbf{M}\mathbf{x}'))r(F_3(\mathbf{M}\mathbf{x}')),\tag{4.9}$$

avec $\mathcal{R}_{\mathbf{M}}=\{\mathbf{x}'\in\mathbb{R}^2\mid\mathbf{M}\mathbf{x}'\in\mathcal{R}\}$. L'ensemble

$$\mathbf{M}\mathbb{Z}^2=\{\mathbf{M}\mathbf{x}'\mid\mathbf{x}'\in\mathbb{Z}^2\}$$

est un réseau de covolume $\det(\mathbf{M}\mathbb{Z}^2)=\det(\mathbf{M})$. On considère alors une base réduite $(\mathbf{e}_1,\mathbf{e}_2)$ de $\mathcal{R}_{\mathbf{M}}$, c'est-à-dire une base telle que $\mathbf{e}_1$ soit un vecteur non nul de norme minimale et $\mathbf{e}_2$ un vecteur de $\mathcal{R}_{\mathbf{M}}\smallsetminus\mathbf{e}_1\mathbb{Z}$ de norme minimale. Notant $\|\mathbf{x}\|=\max\{|x_1|,|x_2|\}$, on écrit alors tout $\mathbf{x}\in\mathbb{Z}^2\cap X\mathcal{R}$ sous la forme

$$\mathbf{x}=\mathbf{M}\mathbf{x}'=\lambda\mathbf{e}_1+\mu\mathbf{e}_2\tag{4.10}$$

pour deux entiers λ et μ. On pose alors

$$F_i'(\lambda,\mu)=F_i(\lambda\mathbf{e}_1+\mu\mathbf{e}_2),\qquad F_{\mathbf{M}}=F_1'F_2'F_3'.\tag{4.11}$$

On montre à présent que le second terme de (4.7) est un terme d'erreur acceptable dans l'optique du Théorème 2.1. Pour ce faire, on a besoin des deux lemmes suivants.

LEMME 4.4. *Pour tous $\varepsilon > 0$ et $X \geq 1$, on a $E \ll (\det(\mathbf{M})L_\infty)^\varepsilon$, où*

$$E = \prod_{4<p\leq X}\left(1+\frac{\rho^*_{F_{\mathbf{M}}}(p)\chi(p)}{p}\right)\prod_{i=1,2}\prod_{p\leq X}\left(1+\frac{d_i\chi(p)}{p}\right)$$

avec

$$\rho^*_{F_{\mathbf{M}}}(n) = \frac{1}{\varphi(n)}\#\left\{(x_1,x_2)\in(\mathbb{Z}/n\mathbb{Z})^2 \;\middle|\; \begin{array}{l} F_{\mathbf{M}}(x_1,x_2)\equiv 0 \pmod n, \\ (x_1,x_2,n)=1 \end{array}\right\},$$

$d_i \in \{0,1\}$ et $F_{\mathbf{M}}$ défini en (4.11).

Démonstration. On a

$$\prod_{i=1,2}\prod_{p\leq X}\left(1+\frac{d_i\chi(p)}{p}\right)\ll 1.$$

Notons $c(f)$ le contenu d'un polynôme f à coefficients entiers. Lorsque p divise $\delta := c(F_1')c(F_2')c(F_3')$, on a une contribution majorée par

$$\begin{aligned}\prod_{\substack{4<p\\ p\mid\delta}}\left(1+\frac{\rho^*_{F_{\mathbf{M}}}(p)\chi(p)}{p}\right) &= \prod_{\substack{4<p\\ p\mid\delta}}\left(1+\frac{(p+1)\chi(p)}{p}\right)\\ &\leq \prod_{p\mid\delta}\left(1+\frac{p+1}{p}\right)\leq 3^{\omega(\delta)}\ll\delta^\varepsilon\ll(\det(\mathbf{M})L_\infty)^\varepsilon.\end{aligned}$$

L'inégalité élémentaire $\rho^*_{F_1'F_2'F_3'}(p)\leq\rho^*_{F_1'}(p)+\rho^*_{F_2'}(p)+\rho^*_{F_3'}(p)$, valable pour tout nombre premier p, implique que les premiers p qui ne divisent pas δ contribuent pour

$$\prod_{\substack{4<p\leq X\\ p\nmid\delta}}\left(1+\frac{\rho^*_{F_{\mathbf{M}}}(p)\chi(p)}{p}\right)\ll\prod_{\substack{4<p\leq X\\ p\nmid\delta}}\left(1+\frac{(\rho^*_{F_1'}(p)+\rho^*_{F_2'}(p)+\rho^*_{F_3'}(p))\chi(p)}{p}\right).$$

On peut alors aisément majorer cette contribution par

$$\exp\left(\sum_{\substack{4<p\leq X\\ p\nmid\delta}}\frac{(\rho^*_{F_1'}(p)+\rho^*_{F_2'}(p)+\rho^*_{F_3'}(p))\chi(p)}{p}\right).$$

Or, d'une part pour $i\in\{1,2\}$,

$$\begin{aligned}\sum_{\substack{4<p\leq X\\ p\nmid\delta}}\frac{\rho^*_{F_i'}(p)\chi(p)}{p} &= \sum_{\substack{4<p\leq X\\ p\nmid\delta}}\frac{\chi(p)}{p}=\sum_{p\nmid\delta}\frac{\chi(p)}{p}+O(1)\\ &\leq\log\log(\det(\mathbf{M})L_\infty)+O(1).\end{aligned}$$

D'autre part,

$$\sum_{\substack{4<p\le X\\ p\nmid\delta}} \frac{\rho^*_{F_3'}(p)\chi(p)}{p} \ll \sum_{\substack{4<p\le X\\ p\nmid\delta}} \frac{\rho_{F_3'(x,1)}(p)\chi(p)}{p} + \log\log(\det(\mathbf{M})L_\infty) + O(1).$$

Pour pouvoir conclure, il nous reste donc à montrer que

$$\sum_{\substack{4<p\le X\\ p\nmid\delta}} \frac{\rho_{F_3'(x,1)}(p)\chi(p)}{p} \ll \log\log(\det(\mathbf{M})L_\infty) + O(1)$$

sous l'hypothèse que F_3 est irréductible sur $\mathbb{Q}[i]$. On voit tout de suite que

$$\rho_{F_3'(x,1)}(p) = 1 + \left(\frac{\operatorname{disc}(F_3'(x,1))}{p}\right)$$

où $\left(\frac{\cdot}{p}\right)$ désigne le symbole de Legendre modulo p. On décompose

$$\operatorname{disc}(F_3'(x,1)) = \varepsilon_3 u_3 v_3$$

où $\varepsilon_3 \in \{-1,1\}$, v_3 est un carré et u_3 est positif sans facteur carré. On a alors par multiplicativité

$$\rho_{F_3'(x,1)}(p) = 1 + \chi(p)^{(1-\varepsilon_3)/2}\left(\frac{u_3}{p}\right).$$

Comme la forme est irréductible sur $\mathbb{Q}[i]$, on a $u_3 \neq 1$ et on obtient donc un caractère de Dirichlet modulo u_3 non principal et distinct de χ, ce qui permet de conclure la preuve. ∎

Lemme 4.5. *Soit $\varepsilon > 0$. Lorsque $X \ge 1$ et $\mathbf{k} \in \mathbb{N}^3$, on a*

$$S_{\mathbf{k}}(X) \ll 2^{\varepsilon(k_1+\max\{k_2,k_3\})} L_\infty^\varepsilon \left(\frac{X^2}{2^{\max\{k_1,k_2,k_3\}}} + X^{1+\varepsilon}\right), \tag{4.12}$$

où $S_{\mathbf{k}}$ est définie en (4.8).

Démonstration. On reprend ici les notations (4.10). Un cas particulier du résultat de Davenport [18, lemme 5] permet d'obtenir les estimations

$$\lambda \ll \|\mathbf{x}\|/\|\mathbf{e}_1\|, \qquad \mu \ll \|\mathbf{x}\|/\|\mathbf{e}_2\|.$$

D'où, avec les notations (4.11),

$$S_{\mathbf{k},\alpha}(X) \ll \sum_{\substack{\lambda \ll X/\|\mathbf{e}_1\|\\ \mu \ll X/\|\mathbf{e}_2\|}} r(F_1'(\lambda,\mu))r(F_2'(\lambda,\mu))r(F_3'(\lambda,\mu)).$$

On introduit alors, en notant $r_0 = \frac{1}{4}r$, une fonction multiplicative r_1 définie de la manière suivante :

$$\forall p \text{ premier}, \forall \nu \ge 1, \qquad r_1(p^\nu) = \begin{cases} r_0(p) = 1 + \chi(p) & \text{si } \nu = 1,\\ (1+\nu)^3 & \text{sinon.}\end{cases}$$

Pour tous k, m et n entiers, on a ainsi

$$r_0(k)r_0(m)r_0(n) \leq r_1(kmn).$$

On en déduit la majoration

$$S_{\mathbf{k},\alpha}(X) \ll \sum_{\substack{\lambda \ll X/\|\mathbf{e}_1\| \\ \mu \ll X/\|\mathbf{e}_2\|}} r_1(F_{\mathbf{M}}(\lambda,\mu))$$

où $F_{\mathbf{M}}$ est un polynôme de $\mathbb{Z}[x_1,x_2]$ de degré 4 défini en (4.11). Alors

$$\|F_i'\| \leq (\deg(F_i')+1)\|\mathbf{M}\|^{\deg(F_i')} L_\infty$$

où $\|\mathbf{M}\|$ désigne le plus grand coefficient de la matrice en valeur absolue. Ici, à partir de l'expression de la matrice $\mathbf{M}$, on voit immédiatement que $\|\mathbf{M}\| \ll 2^{k_1+\max\{k_2,k_3\}}$. Donc

$$\|F_{\mathbf{M}}\| \ll 2^{4(k_1+\max\{k_2,k_3\})} L_\infty^3 \ll (2^{k_1+\max\{k_2,k_3\}} L_\infty)^4.$$

On déduit finalement de [4, corollaire 1] et du Lemme 4.4 que

$$S_{\mathbf{k},\alpha}(X) \ll 2^{\varepsilon(k_1+\max\{k_2,k_3\})} L_\infty^\varepsilon \left(\frac{X^2}{\|\mathbf{e}_1\| \cdot \|\mathbf{e}_2\|} + X^{1+\varepsilon} \right)$$

pour tout $\varepsilon > 0$. Or, on sait que pour tout réseau Γ de base réduite $(\mathbf{b}_1, \mathbf{b}_2)$,

$$\det(\Gamma) \leq \|\mathbf{b}_1\| \cdot \|\mathbf{b}_2\| \ll \det(\Gamma).$$

Donc, avec les notations (4.10),

$$\frac{1}{\|\mathbf{e}_1\| \cdot \|\mathbf{e}_2\|} \leq \frac{1}{\det(\mathbf{M})} \leq \frac{1}{2^{\max\{k_1,k_2,k_3\}}},$$

ce qui fournit finalement

$$S_{\mathbf{k},\alpha}(X) \ll 2^{\varepsilon(k_1+\max\{k_2,k_3\})} L_\infty^\varepsilon \left(\frac{X^2}{2^{\max\{k_1,k_2,k_3\}}} + X^{1+\varepsilon} \right).$$

On conclut la preuve grâce au Lemme 4.2. ■

On déduit de (4.8) et du Lemme 4.5 l'estimation

$$S_{\mathbf{k}}(2^{-k_0}X) \ll 2^{\varepsilon(k_1+\max\{k_2,k_3\})} L_\infty^\varepsilon \left(\frac{X^2}{2^{2k_0+\max\{k_1,k_2,k_3\}}} + \frac{X^{1+\varepsilon}}{2^{(1+\varepsilon)k_0}} \right).$$

On l'utilise pour estimer le deuxième terme de (4.7). Traitons par exemple le cas de la somme

$$S_1 := \sum_{0 \leq k_0} \sum_{k_2,k_3 \leq \log\log X} \sum_{k_1 > \log\log X} S_{\mathbf{k}}(2^{-k_0}X).$$

Quitte à prendre ε assez petit, par des majorations élémentaires on a

$$\begin{aligned}
S_1 &\ll \sum_{k_2,k_3\leq \log\log X}\ \sum_{k_1>\log\log X} 2^{\varepsilon(k_1+\max\{k_2,k_3\})} L_\infty^\varepsilon\left(\frac{X^2}{2^{\max\{k_1,k_2,k_3\}}}+X^{1+\varepsilon}\right)\\
&\ll L_\infty^\varepsilon(\log X)^\varepsilon \sum_{k_1>\log\log X} 2^{2\varepsilon k_1}\left(\frac{X^2}{2^{k_1}}+X^{1+\varepsilon}\right)\\
&\ll L_\infty^\varepsilon X^2(\log X)^{3\varepsilon\log(2)-\log(2)} \ll L_\infty^\varepsilon X^2(\log X)^{3\varepsilon\log 2-\eta}.
\end{aligned}$$

On traite de la même façon le terme d'erreur et les autres cas de sorte qu'avec les notations (4.9),

$$S(X)=\sum_{k_0\geq 0}\ \sum_{0\leq k_1,k_2,k_3\leq \log\log X} S_{\mathbf{k}}(2^{-k_0}X)+O\left(\frac{L_\infty^\varepsilon X^2}{(\log X)^{\eta-\varepsilon}}\right). \tag{4.13}$$

On pose alors $X'=r'X$, $Y=(r'X)^{1/2}/(\log X)^C$ pour une constante $C>0$ que l'on fixera plus tard et $F_{i,\mathbf{M}}(\mathbf{x}')=F_i(\mathbf{M}\mathbf{x}')$. Valables lorsque l'on a $0\leq m\leq (X')^2$ et $2^{-\nu_2(m)}m\equiv 1 \pmod 4$, les décompositions suivantes permettent de restreindre les intervalles dans lesquels varient les variables de façon acceptable :

(i) la décomposition $r(m)=4A_+(m)+4A_-(m)$ avec

$$A_+(m)=\sum_{\substack{d\mid m\\ d\leq \sqrt{X'}}}\chi(d),\qquad A_-(m)=\sum_{\substack{e\mid m\\ m>e\sqrt{X'}}}\chi(e),$$

appliquée à $F_{2,\mathbf{M}}(\mathbf{x}')$;

(ii) la décomposition $r(m)=4D_+(m)+4D_-(m)$ avec

$$D_+(m)=\sum_{\substack{d\mid m\\ d\leq X'}}\chi(d),\qquad D_-(m)=\sum_{\substack{e\mid m\\ m>eX'}}\chi(e),$$

appliquée à $F_{3,\mathbf{M}}(\mathbf{x}')$;

(iii) la décomposition $r(m)=4B_+(m)+4C(m)+4B_-(m)$, avec

$$B_+(m)=\sum_{\substack{d\mid m\\ d\leq Y}}\chi(d),\quad C(m)=\sum_{\substack{d\mid m\\ Y<d\leq X'/Y}}\chi(d),\quad B_-(m)=\sum_{\substack{e\mid m\\ m>eX'/Y}}\chi(e),$$

appliquée à $F_{1,\mathbf{M}}(\mathbf{x}')$.

On notera que, dans A_-, D_- et B_-, on a respectivement $e\leq\sqrt{X'}$, $e\leq X'$ et $e\leq Y$. On introduit alors les quantités

$$S_{\pm,\pm,\pm}(X;\mathbf{k},\alpha)=\sum_{\substack{\mathbf{x}'\in\mathbb{Z}^2\cap X\mathcal{R}_{\mathbf{M}}\\ x_1'\equiv 1\,[4]}} B_\pm(F_{1,\mathbf{M}}(\mathbf{x}'))A_\pm(F_{2,\mathbf{M}}(\mathbf{x}'))D_\pm(F_{3,\mathbf{M}}(\mathbf{x}')),$$

$$S_0(X;\mathbf{k},\alpha)=\sum_{\substack{\mathbf{x}'\in\mathbb{Z}^2\cap X\mathcal{R}_{\mathbf{M}}\\ x_1'\equiv 1\,[4]}} C(L_{1,\mathbf{M}}(\mathbf{x}'))r(F_{2,\mathbf{M}}(\mathbf{x}'))r(F_{3,\mathbf{M}}(\mathbf{x}')),$$

de sorte que

$$S_{\mathbf{k}}(X)=4^3\sum_{\alpha}\sum_{\pm,\pm,\pm}S_{\pm,\pm,\pm}(X;\mathbf{k},\alpha)+4\sum_{\alpha}S_0(X;\mathbf{k},\alpha). \tag{4.14}$$

4.2. Traitement de S_0. La contribution des sommes $S_0(X;\mathbf{k},\alpha)$ est

$$S_0(X)=\sum_{k_0\geq 0}\sum_{0\leq k_1,k_2,k_3\leq \log\log X}\sum_{\alpha}S_0(2^{-k_0}X;\mathbf{k},\alpha).$$

On montre dans cette section que la somme S_0 constitue un terme d'erreur convenable dans l'optique du Théorème 2.1.

Lemme 4.6. *Soient $\varepsilon>0$ et $X\geq 1$. Avec la notation* (2.2)*, on a*

$$S_0(X)\ll\frac{L_\infty^\varepsilon r_\infty r' X^2}{(\log X)^{\eta-\varepsilon}}.$$

Le reste de la section est consacrée à la démonstration de ce lemme. On s'inspire ici de la méthode utilisée dans [4, section 4]. On a clairement

$$S_0(X;\mathbf{k},\alpha)\ll\sum_{\substack{\mathbf{x}'\in\mathbb{Z}^2\cap X\mathcal{R}_{\mathbf{M}}\\ x_1'\equiv 1\,[4]}}|C(F_{1,\mathbf{M}}(\mathbf{x}'))|r(F_{2,\mathbf{M}}(\mathbf{x}'))r(F_{3,\mathbf{M}}(\mathbf{x}')).$$

On pose alors

$$\begin{aligned} E&=\{m\in\mathbb{Z}\mid \exists d\,|\,m,\ Y<d\leq X/Y\},\\ E_{k_0}&=\{m\in\mathbb{Z}\mid \exists\mathbf{x}\in 2^{-k_0}X\mathcal{R},\ F_1(\mathbf{x})=m\},\\ \mathcal{B}_{k_0}&=E\cap E_{k_0},\end{aligned}$$

de sorte que

$$S_0(2^{-k_0}X;\mathbf{k},\alpha)\ll\sum_{m\in\mathcal{B}_{k_0}}S_{0,m}(2^{-k_0}X)|C(m)|$$

où

$$S_{0,m}(X)=\sum_{\substack{\mathbf{x}\in\mathbb{Z}^2\cap X\mathcal{R}\\ F_1(\mathbf{x})=m}}r(F_2(\mathbf{x}))r(F_3(\mathbf{x})).$$

On en déduit donc que

$$S_0(X)\ll(\log\log X)^3\sum_{k_0\geq 0}\sum_{m\in\mathcal{B}_{k_0}}S_{0,m}(2^{-k_0}X)|C(m)|.$$

D'après [4, lemme 6], on a, lorsque $2^{k_0} \leq \sqrt{X}$,

$$\sum_{m \in \mathcal{B}_{k_0}} |C(m)| \ll \frac{r' 2^{-k_0} X (\log\log X')^{9/4}}{(\log X')^{\eta}}.$$

On en déduit, pour tout $X \geq 1$, la majoration

$$S_0(X) \ll \frac{r' X (\log\log X')^{21/4}}{(\log X')^{\eta}} \sum_{k_0 \geq 0} 2^{-k_0} \max_{m \in \mathbb{N}} |S_{0,m}(2^{-k_0} X)| + X. \tag{4.15}$$

On montre alors le lemme suivant qui permet de conclure que la contribution de S_0 donne un terme d'erreur convenable.

LEMME 4.7. *Il existe une constante absolue $c > 0$ telle que*

$$S_{0,m}(X) \ll L_\infty^{\varepsilon} r_\infty X (\log\log X')^{c}.$$

Démonstration. On adapte ici la démonstration de [4, lemme 5]. Supposons que $a_1 \neq 0$. Alors

$$x_1 = \frac{m - b_1 x_2}{a_1}$$

et par conséquent

$$F_2(\mathbf{x}) = \frac{A_2 m + B_2 n}{a_1} = F_2'(m,n)$$

avec $A_2 = a_2$, $B_2 = a_1 b_2 - a_2 b_1$ et $n = x_2$. Donc

$$F_3(\mathbf{x}) = \frac{A_3 m^2 + B_3 n^2 + C_3 mn}{a_1^2} = F_3'(m,n)$$

avec $A_3 = a_3$, $B_3 = a_3 b_1^2 + b_3 a_1^2 - c_3 b_1 a_1$ et $C_3 = c_3 a_1 - 2 a_3 b_1$. On peut remarquer que $B_2 B_3 \neq 0$. On pose alors

$$B_2' = \frac{B_2}{\gcd(A_2 m, B_2)}, \qquad B_3' = \frac{B_3}{\gcd(A_3 m^2, B_3, C_3 m)},$$

$$A_2'(m) = \frac{A_2 m}{\gcd(A_2 m, B_2)}, \qquad A_3'(m) = \frac{A_3 m^2}{\gcd(A_3 m^2, B_3, C_3 m)},$$

$$C_3'(m) = \frac{C_3 m}{\gcd(A_3 m^2, B_3, C_3 m)}.$$

On introduit enfin $h := 2 \times 3 \times a_1 B_2 B_3 \varDelta^*$ avec la notation du Lemme 4.2 et la fonction multiplicative r_2 définie pour p premier et ν entier naturel par

$$r_2(p^\nu) = \begin{cases} (\nu+1)^2 & \text{si } p \mid h \text{ ou } \nu \geq 2, \\ r_0(p^\nu) = 1 + \chi(p) & \text{sinon,} \end{cases}$$

de sorte que

$$S_{0,m}(X) \leq 16 \tau(h)^2 \sum_{n \leq R_\infty X} r_2(G_m(n)) \ll L_\infty^{\varepsilon} \sum_{n \leq R_\infty X} r_2(G_m(n)),$$

où

$$G_m(n) = (A_2'(m) + B_2'n)(A_3'(m) + B_3'n^2 + C_3'(m)n).$$

On rappelle qu'un nombre premier est dit *fixe* par un polynôme P à coefficients entiers si $P(n) \equiv 0 \pmod p$ pour tout entier n. Le polynôme G_m étant irréductible et primitif de degré 3, seuls $p = 2$ et $p = 3$ peuvent être des premiers fixes. Deux applications successives éventuelles du lemme 5 couplées à la remarque 8 de [2] montrent qu'il existe $a \in \{0, 1\}$, $b \in \{0, 1, 2\}$ et $0 \leq \mu \leq 4$ tels que

$$G_{m,2}(x) = \frac{G_m(3^a \times 2^b x + k)}{3^a \times 2^\mu}$$

soit sans premier fixe pour un certain entier $k \leq 10$. On déduit finalement la majoration

$$S_{0,m}(X) \ll L_\infty^\varepsilon \sum_{n \ll r_\infty X} r_2(G_{m,2}(n)).$$

Pour $r_\infty X \gg L_\infty^\varepsilon (X')^\varepsilon$ et $\varepsilon \in]0, 1[$, une application de [2, théorème 2] permet d'obtenir l'estimation

$$S_{0,m}(X) \ll L_\infty^\varepsilon r_\infty X \prod_{p \ll r_\infty X} \left(\left(1 - \frac{\rho_{G_{m,2}}(p)}{p}\right) \sum_{\nu \geq 0} \frac{r_2(p^\nu)\rho_{G_{m,2}}(p^\nu)}{p^\nu} \right).$$

En utilisant le Lemme 3.4, on obtient

$$\begin{aligned} \sum_{\nu \geq 1} \frac{r_2(p^\nu)\rho_{G_{m,2}}(p^\nu)}{p^\nu} &\leq \frac{6}{p} + \frac{27}{p} + 3 \sum_{\nu \geq 3} \frac{(\nu+1)^2}{p^{\nu/3}} \\ &\leq \frac{6}{p} + \frac{27}{p} + \frac{1167}{p} = \frac{1200}{p}. \end{aligned} \tag{4.16}$$

On déduit de tout cela que les nombres premiers p qui divisent le discriminant de $G_{m,2}$ ont une contribution à $S_{0,m}(X)$

$$\ll L_\infty^\varepsilon r_\infty X \prod_{p | \mathrm{disc}(G_{m,2})} \left(1 + \frac{1200}{p}\right).$$

Une étude attentive du passage de F_m à $G_{m,2}$ ainsi que [2, lemme 1] montrent que $\mathrm{disc}(G_{m,2}) \ll L_\infty^{19} m^6$. On en déduit donc

$$L_\infty^\varepsilon r_\infty X \prod_{p | \mathrm{disc}(G_{m,2})} \left(1 + \frac{1200}{p}\right) \ll L_\infty^\varepsilon r_\infty X (\log\log X')^{1200},$$

puisqu'il est nécessaire que $m \leq X'$ pour que $S_{0,m}(X)$ soit non nulle.

On traite maintenant la contribution des p qui ne divisent pas le discriminant. Pour ces nombres premiers, on a une meilleure majoration de

$\rho_{G_{m,2}}(p^\nu) \ll 1$, qui donne de la même façon qu'en (4.16) les majorations

$$\sum_{\nu\geq 2}\frac{r_2(p^\nu)\rho_{G_{m,2}}(p^\nu)}{p^\nu} \ll \sum_{\nu\geq 2}\frac{(\nu+1)^2}{p^\nu} \ll \frac{1}{p^2}.$$

Cela permet de négliger tous les exposants $\nu \geq 2$. On en déduit donc

$$\begin{aligned}S_{0,m}(X) \ll{}& L_\infty^\varepsilon r_\infty X(\log\log X')^{1200}\\ &\times \prod_{\substack{p\ll r_\infty X\\ p\nmid \mathrm{disc}(G_{m,2})}}\Big(1-\frac{\rho_{G_{m,2}}(p)}{p}\Big)\Big(1+\frac{r_2(p)\rho_{G_{m,2}}(p)}{p}\Big),\end{aligned}$$

soit

$$\begin{aligned}S_{0,m}(X) &\ll L_\infty^\varepsilon r_\infty X(\log\log X')^{1200}\prod_{\substack{p\ll r_\infty X\\ p\nmid \mathrm{disc}(G_{m,2})}}\Big(1+\frac{(r_2(p)-1)\rho_{G_{m,2}}(p)}{p}\Big)\\ &\ll L_\infty^\varepsilon r_\infty X(\log\log X')^{1200}\prod_{p\ll r_\infty X}\Big(1+\frac{\chi(p)\rho_{G_{m,2}}(p)}{p}\Big)\\ &\ll L_\infty^\varepsilon r_\infty X(\log\log X')^{1200+O(1)}.\end{aligned}$$

On raisonne ici comme lors de la preuve du Lemme 4.4 et on utilise le fait que $\rho_{G_{m,2}}(p) = \rho_{G_m}(p)$ pour tout $p \geq 5$ et le fait que G_m est irréductible sur $\mathbb{Q}[i]$. Dans le cas contraire, lorsque $n \leq L_\infty^\varepsilon(X')^\varepsilon$, on a

$$r_2(G_{m,2}(n)) \ll G_{m,2}(n)^\varepsilon \ll L_\infty^\varepsilon(X')^\varepsilon \ll L_\infty^\varepsilon r_\infty^\varepsilon X^\varepsilon.$$

La dernière majoration découle de l'inégalité $r' \leq 2L_\infty r_\infty$. D'où

$$S_{0,m}(X) \ll L_\infty^\varepsilon r_\infty X^\varepsilon \ll L_\infty^\varepsilon r_\infty X(\log\log X')^{O(1)}$$

pour ε assez petit. ∎

Pour conclure, on tire finalement de (4.15) et du Lemme 4.7 la majoration

$$\begin{aligned}S_0(X) &\ll \frac{L_\infty^\varepsilon r_\infty r' X^2(\log\log X')^{21/4+c_0}}{(\log X')^\eta}\sum_{k_0\geq 0}2^{-2k_0}\\ &\ll \frac{L_\infty^\varepsilon r_\infty r' X^2(\log\log X')^{21/4+c_0}}{(\log X')^\eta},\end{aligned}$$

ce qui fournit

$$S_0(X) \ll \frac{L_\infty^\varepsilon r_\infty r' X^2}{(\log X')^{\eta-\varepsilon}}.$$

Puisque l'hypothèse $r'X^{1-\varepsilon} \geq 1$ garantit que $\log X' \gg \log X$, cette estimation est convenable pour obtenir le Lemme 4.6. Ceci achève le traitement de S_0.

4.3. Traitement des $S_{\pm,\pm,\pm}$ et fin de la preuve du Théorème 2.1. On traite ici le cas de $S_{-,-,-}(X;\mathbf{k},\alpha)$ qui est le plus délicat, les autres cas se traitant de manière similaire. On utilise dans la suite les notations $V_1 = Y$, $V_2 = \sqrt{X'}$, $V_3 = X'$ et on pose

$$\mathcal{R}^{-,-,-,}_{\mathbf{M},4,\mathbf{d}} = \left\{ \mathbf{x}' \in \mathbb{Z}^2 \cap \mathcal{R}_{\mathbf{M}} \;\middle|\; \begin{array}{l} F_1(\mathbf{M}\mathbf{x}') > r'd_1Y^{-1}, \\ F_2(\mathbf{M}\mathbf{x}') > (r')^{1/2}d_2X^{-1/2}, \\ F_3(\mathbf{M}\mathbf{x}') > r'd_3/X, \\ x'_1 \equiv 1\ [4] \end{array} \right\}.$$

On a

$$S_{-,-,-}(X;\mathbf{k},\alpha) = \sum_{\substack{\mathbf{d}\in\mathbb{N}^3 \\ d_i\le V_i}} \chi(d_1d_2d_3)\#(\Lambda_{\mathbf{M}}(\mathbf{d}) \cap X\mathcal{R}^{-,-,-,}_{\mathbf{M},4,\mathbf{d}}),$$

où $\Lambda_{\mathbf{M}}(\mathbf{d}) = \Lambda(\mathbf{d}, F_{1,\mathbf{M}}, F_{2,\mathbf{M}}, F_{3,\mathbf{M}})$. On applique alors le lemme de géométrie des nombres suivant qui est dû à Daniel [17, lemme 3.2] et La Bretèche et Browning [5, lemme 5].

Lemme 4.8. *Soient $\varepsilon > 0$, F_1, F_2 et F_3 des formes vérifiant les hypothèses **NH** (2.0), $X \ge 1$, V_1, V_2, $V_3 \ge 2$ et $V = V_1V_2V_3$. Alors il existe une constante absolue $A > 0$ telle que*

$$\sum_{\substack{\mathbf{d}\in\mathbb{N}^3 \\ d_i\le V_i}} \left| \#\left(\Lambda(\mathbf{d}) \cap X\mathcal{R}_{4,\mathbf{d}}\right) - \mathrm{vol}(\mathcal{R}_{\mathbf{d}})X^2\frac{\rho(\mathbf{d})}{4(d_1d_2d_3)^2} \right| \ll L_\infty^{\varepsilon}(r_\infty X\sqrt{V} + V)(\log V)^A,$$

avec $\mathcal{R}_{\mathbf{d}} \subset \mathcal{R}$ une région de frontière continûment différentiable dépendant de $\mathbf{d}$ et où $X\mathcal{R}_{4,\mathbf{d}} = \{\mathbf{x} \in \mathbb{Z}^2 \cap X\mathcal{R}_{\mathbf{d}} \mid x_1 \equiv 1 \pmod 4\}$.

Démonstration. Le lemme se démontre pour des formes primitives et on passe aux formes vérifiant **NH** (2.0) comme dans [5]. Les éléments de la preuve sont dans l'article [17] de Daniel ainsi que dans [27], [28] et [2]. Il faut simplement préciser en plus la dépendance par rapport aux formes et noter que la dépendance de la région par rapport à l'indice de sommation ne change absolument rien dans la preuve. ∎

On obtient ici l'égalité

$$\begin{aligned} S_{-,-,-}(X;\mathbf{k},\alpha) &= \sum_{\substack{\mathbf{d}\in\mathbb{N}^3 \\ d_i\le V_i}} \chi(d_1d_2d_3)\frac{X^2}{2^{k_1+\max\{k''_2,k'_3\}+2}}\frac{\mathrm{vol}(\mathcal{R}^{-,-,-}_{\mathbf{d}})}{4}\frac{\rho(\mathbf{d})}{(d_1d_2d_3)^2} \\ &\quad + O\big(2^{\varepsilon(k_1+k_2+k_3)}L_\infty^{\varepsilon}(r_\infty X\sqrt{V} + V)(\log V)^A\big) \end{aligned} \tag{4.17}$$

où

$$\mathcal{R}_{\mathbf{d}}^{-,-,-} = \left\{ \mathbf{x} \in \mathcal{R} \;\middle|\; F_1(\mathbf{x}) > \frac{r' d_1}{Y},\ F_2(\mathbf{x}) > \frac{(r')^{1/2} d_2}{X^{1/2}},\ F_3(\mathbf{x}) > \frac{r' d_3}{X} \right\}.$$

Posant

$$T = 2^{\varepsilon(k_1+k_2+k_3)} L_\infty^\varepsilon (r_\infty X \sqrt{V} + V)(\log V)^A,$$

un calcul élémentaire fournit alors immédiatement

$$T \ll 2^{\varepsilon(k_1+k_2+k_3)} L_\infty^\varepsilon X^2 \left(\frac{r_\infty r'}{(\log X)^{C/2-A}} + \frac{(r')^2}{(\log X)^{C-A}} \right).$$

Si $r' \le r_\infty (\log X)^{A+1}$, l'estimation précédente avec $C = 2A + 8$ donne

$$\begin{aligned} T &\ll 2^{\varepsilon(k_1+k_2+k_3)} L_\infty^\varepsilon X^2 \left(\frac{r_\infty r'}{(\log X)^4} + \frac{r' r_\infty}{(\log X)^7} \right) \\ &\ll 2^{\varepsilon(k_1+k_2+k_3)} L_\infty^\varepsilon X^2 \frac{r_\infty r'}{(\log X)^4}. \end{aligned}$$

On remarque alors en utilisant [2, théorème 1] que

$$\begin{aligned} T \ll S_{-,-,-}(X; \mathbf{k}, \alpha) &\ll \sum_{x_i \le r_\infty X} \tau(F_{1,\mathbf{M}}(\mathbf{x})) \tau(F_{2,\mathbf{M}}(\mathbf{x})) \tau(F_{3,\mathbf{M}}(\mathbf{x})) \\ &\ll \sum_{x_i \le r_\infty X} \tau_0(F_{1,\mathbf{M}}(\mathbf{x}) F_{2,\mathbf{M}}(\mathbf{x}) F_{3,\mathbf{M}}(\mathbf{x})) \\ &\ll 2^{\varepsilon(k_1+k_2+k_3)} L_\infty^\varepsilon r_\infty^2 X^2 (\log X)^3, \end{aligned}$$

où l'on a introduit la fonction multiplicative

$$\tau_0(p^\nu) = \begin{cases} 2 = \tau(p^\nu) & \text{si } \nu = 1, \\ (\nu+1)^3 & \text{sinon.} \end{cases}$$

Cela permet d'obtenir, si $r' \ge r_\infty (\log X)^{A+1}$, la majoration

$$\begin{aligned} T &\ll 2^{\varepsilon(k_1+k_2+k_3)} L_\infty^\varepsilon r_\infty r' X^2 (\log X)^{3-A-1} \\ &\ll 2^{\varepsilon(k_1+k_2+k_3)} L_\infty^\varepsilon r_\infty r' X^2 (\log X)^{2-A}, \end{aligned}$$

ce qui implique que dans ce cas également

$$T \ll 2^{\varepsilon(k_1+k_2+k_3)} L_\infty^\varepsilon X^2 \frac{r_\infty r'}{(\log X)^4}.$$

Pour conclure le traitement du terme d'erreur, il ne reste plus qu'à remplacer X par $2^{-k_0} X$ puis à sommer pour obtenir une contribution

$$\ll L_\infty^\varepsilon r_\infty r' \sum_{k_0 \ge 0} \frac{2^{-2k_0} X^2}{(\log(2^{-k_0} X))^4} \sum_{k_1, k_2, k_3 \le \log\log X} 2^{\varepsilon(k_1+k_2+k_3)} n(\mathbf{k}).$$

En utilisant le Lemme 4.2, on obtient

$$\ll L_\infty^\varepsilon r_\infty r' X^2 \frac{(\log X)^{3\varepsilon \log 2}}{(\log X)^4} \ll L_\infty^\varepsilon r_\infty r' \frac{X^2}{\log X}$$

pour $\varepsilon \leq 1/\log 2$. Ceci est satisfaisant dans l'optique du Théorème 2.1.

On passe maintenant à l'étude du terme principal de (4.17). On exploite pour ce faire les deux lemmes élémentaires suivants sur les séries de Dirichlet associées à des convolutions pour étudier

$$\mathcal{S}(V_1,V_2,V_3) = \sum_{d_i \leq V_i} \chi(d_1d_2d_3) \frac{\rho(d_1,d_2,d_3)}{(d_1d_2d_3)^2}. \tag{4.18}$$

Lemme 4.9. *Soient $A>0$, g, w deux fonctions arithmétiques et C, C', C'' trois constantes telles que*

$$\sum_{d=1}^{\infty} \frac{|w(d)|(\log 2d)^A}{d} \leq C'' \quad \textit{et} \quad \sum_{d \leq x} \frac{g(d)}{d} = C + O\Big(\frac{C'}{(\log 2x)^A}\Big).$$

Alors

$$\sum_{n \leq x} \frac{(g*w)(n)}{n} = C \sum_{d=1}^{\infty} \frac{w(d)}{d} + O\Big(\frac{C''(C+C')}{(\log 2x)^A}\Big).$$

Démonstration. La preuve se trouve dans [6, lemme 5]. ■

Lemme 4.10. *Soient g, w deux fonctions arithmétiques et C, C', C'' trois constantes telles que*

$$\sum_{d=1}^{\infty} \frac{|w(d)| \log 2d}{d} \leq C'' \quad \textit{et} \quad \sum_{d \leq x} \frac{g(d)}{d} = C \log x + O(C').$$

Alors

$$\sum_{n \leq x} \frac{(g*w)(n)}{n} = C(\log x) \sum_{d=1}^{\infty} \frac{w(d)}{d} + O(C''(C+C')).$$

Démonstration. La preuve est très similaire à celle du lemme précédent et nous ne la rédigeons pas ici. ■

Lemme 4.11. *Si on note $V_m = \min\{V_i\}$, pour tout $A>0$, on a*

$$\mathcal{S}(V_1,V_2,V_3) = \Big(\frac{\pi}{4}\Big)^3 \prod_{p>2} \sigma_p + O\Big(\frac{L_\infty^\varepsilon}{(\log V_m)^A}\Big).$$

Démonstration. On utilise les notations du Lemme 3.3 pour écrire

$$\mathcal{S}(V_1,V_2,V_3) = \sum_{d_i \leq V_i} \chi(d_1d_2d_3) \frac{(h*R)(d_1,d_2,d_3)}{d_1d_2d_3},$$

où

$$\chi(d_1d_2d_3)(h*R)(d_1,d_2,d_3) = \sum_{e_i|d_i}\chi\Big(\frac{d_1}{e_1}\frac{d_2}{e_2}\frac{d_3}{e_3}\Big)h\Big(\frac{d_1}{e_1},\frac{d_2}{e_2},\frac{d_3}{e_3}\Big)\chi(e_1e_2e_3)r_\Delta(e_3).$$

Supposons que $V_3\geq V_2\geq V_1$. On commence alors par sommer sur d_3 et e_3 si bien qu'on doit estimer la somme suivante :

$$\sum_{d_3\leq V_3}\sum_{e_3|d_3}\frac{\chi(d_3/e_3)h(d_1/e_1,d_2/e_2,d_3/e_3)\chi(e_3)r_\Delta(e_3)}{d_3}.$$

Le Lemme 4.9 avec $g=\chi r_\Delta=\chi*(\chi\chi_\Delta)$ et $w=\chi h$ où h est vue simplement comme fonction de sa troisième variable fournit alors que cette somme est égale à

$$\frac{\pi}{4}L(1,\chi\chi_\Delta)\sum_{k_3\geq 1}\frac{\chi(k_3)h(d_1/e_1,d_2/e_2,k_3)}{k_3} + O\Big(\frac{1}{(\log V_3)^A}\sum_{k_3\geq 1}\frac{|h(d_1/e_1,d_2/e_2,k_3)|(\log 2k_3)^A}{k_3}\Big),$$

où l'on a utilisé le fait que $L(1,\chi)=\pi/4$. On somme alors désormais sur d_2 et e_2. Par une nouvelle application du Lemme 4.9 avec toujours $w=\chi h$ où h est vue comme fonction de la deuxième variable uniquement cette fois et avec $g=\chi$, le terme principal ci-dessus devient

$$\Big(\frac{\pi}{4}\Big)^2L(1,\chi\chi_\Delta)\sum_{k_2,k_3\geq 1}\frac{\chi(k_2k_3)h(d_1/e_1,k_2,k_3)}{k_2k_3} + O\Big(\frac{1}{(\log V_2)^A}\sum_{k_2,k_3\geq 1}\frac{|h(d_1/e_1,k_2,k_3)|(\log 2k_2)^A}{k_2k_3}\Big).$$

Pour traiter le terme d'erreur de la sommation sur d_3 et e_3, on utilise le Lemme 4.10 avec $g=1$ et $w=|h|$ vue comme fonction de sa deuxième variable pour obtenir une contribution

$$O\Big(\frac{\log V_2}{(\log V_3)^A}\sum_{k_2,k_3\geq 1}\frac{|h(d_1/e_1,k_2,k_3)|(\log 2k_3)^A(\log 2k_2)^A}{k_2k_3}\Big).$$

On effectue alors la même manipulation sur la somme sur d_1 et e_1. Le Lemme 3.3 permet d'obtenir que les quantités de la forme

$$\sum_{k_1,k_2,k_3\geq 1}\frac{|h(k_1,k_2,k_3)|(\log 2k_3)^A(\log 2k_2)^A(\log 2k_1)^A}{k_1k_2k_3}$$

ont une contribution

$$\ll \sum_{k_1,k_2,k_3\geq 1} \frac{|h(k_1,k_2,k_3)|(\log 2k_1k_2k_3)^{3A}}{k_1k_2k_3} \ll L_\infty^\varepsilon.$$

Cela permet de conclure la preuve grâce à l'expression (3.2) obtenue dans le Lemme 3.3. ∎

On est alors en mesure de terminer la démonstration du Théorème 2.1. Il ne reste plus qu'à introduire le terme $\mathrm{vol}(\mathcal{R}_{\mathbf{d}}^{-,-,-})$ dans (4.17). Pour ce faire, on pose

$$\mathcal{S}'(X;\mathcal{R}) = \sum_{d_i\leq V_i} \frac{\chi(d_1d_2d_2)\rho(\mathbf{d})\mathrm{vol}(\mathcal{R}_{\mathbf{d}}^{-,-,-})}{(d_1d_2d_3)^2}. \tag{4.19}$$

On s'inspire alors de [8, section 7.3] et on écrit

$$\mathrm{vol}(\mathcal{R}_{\mathbf{d}}^{-,-,-}) = \iint_{\mathcal{R}} \mathbf{1}_{\mathcal{R}_{\mathbf{d}}^{-,-,-}}(\mathbf{x})\, d\mathbf{x}.$$

En réinjectant dans (4.19) et en intervertissant les sommations, on aboutit à

$$\mathcal{S}'(X;\mathcal{R}) = \iint_{\mathcal{R}} \sum_{\substack{d_1\leq \min\{Y,F_1(\mathbf{x})r'^{-1}Y\}\\ d_2\leq\min\{\sqrt{X'},F_2(\mathbf{x})r'^{-1/2}\sqrt{X}\}\\ d_3\leq\min\{X',F_3(\mathbf{x})r'^{-1}X\}}} \frac{\chi(d_1d_2d_2)\rho(\mathbf{d})}{(d_1d_2d_3)^2}\, d\mathbf{x}.$$

Le Lemme 4.11 permet d'obtenir l'estimation

$$\mathcal{S}'(X;\mathcal{R}) = \left(\frac{\pi}{4}\right)^3 \mathrm{vol}(\mathcal{R}) \prod_{p>2}\sigma_p + O(L_\infty^\varepsilon I(X))$$

avec

$$\begin{aligned} I(X) &= I(X;F_1,F_2,Q)\\ &= \iint_{\mathcal{R}} \frac{1}{\log(\min\{F_1(\mathbf{x})r'^{-1}Y, F_2(\mathbf{x})r'^{-1/2}\sqrt{X}, F_3(\mathbf{x})r'^{-1}X\})}\, d\mathbf{x}. \end{aligned}$$

On établit alors l'estimation

$$I(X) \ll_\varepsilon \frac{r_\infty^2 L_\infty^\varepsilon}{(\log X)^\eta}. \tag{4.20}$$

Lorsque $L_\infty > (\log X)^{1/\varepsilon}$, le Lemme 3.3 puis le changement de variables $\mathbf{x} = r_\infty\mathbf{z}$ permettent d'obtenir les majorations

$$\mathcal{S}'(X;\mathcal{R}) \ll L_\infty^\varepsilon \iint_{\mathcal{R}} d\mathbf{x} \ll r_\infty^2 L_\infty^\varepsilon \iint_{||\mathbf{z}||\leq 1} d\mathbf{z} \ll r_\infty^2 L_\infty^\varepsilon.$$

Ces dernières sont alors suffisantes pour établir (4.20). Dans le cas où on a $L_\infty \leq (\log X)^{1/\varepsilon}$, on peut majorer $I(X)$ par la somme des $I_i(X)$ pour $1 \leq i \leq 3$ avec

$$\begin{aligned}
I_1(X) &= \iint_{\mathcal{R}} \frac{1}{\log(F_1(\mathbf{x})r'^{-1}Y+2)}\, d\mathbf{x},\\
I_2(X) &= \iint_{\mathbf{x}\in\mathcal{R}} \frac{1}{\log(F_2(\mathbf{x})r'^{-1/2}X+2)}\, d\mathbf{x},\\
I_3(X) &= \iint_{\mathbf{x}\in\mathcal{R}} \frac{1}{\log(F_3(\mathbf{x})r'^{-1}X+2)}\, d\mathbf{x}.
\end{aligned}$$

Traitons par exemple le cas du dernier terme ci-dessus. En effectuant un changement de variables $\mathbf{x} = r_\infty \mathbf{z}$, on a

$$I_3(X) \leq r_\infty^2 \iint_{\|\mathbf{z}\|\leq 1} \frac{1}{\log(F_3(\mathbf{z})r_\infty^2 r'^{-1}X+2)}\, d\mathbf{z}.$$

On peut alors constater qu'un changement de variables $\mathbf{u} = E\mathbf{z}$ (voir [5, section 6]) fait apparaître l'inverse de $\det(E)$, et ainsi on peut intégrer plutôt sur la forme J définie par $J(\mathbf{z}) = F_3(E\mathbf{z})$ (voir [8]) et obtenir par exemple

$$\begin{aligned}
I_3(X) &\leq \frac{r_\infty^2}{\sqrt{\log(r_\infty^2 r'^{-1}X)}} \iint_{\|\mathbf{z}\|\leq 1} \frac{1}{\sqrt{|\log(J(\mathbf{z})+2)|}}\, d\mathbf{z}\\
&\ll \frac{r_\infty^2}{\sqrt{\log(r_\infty^2 r'^{-1}X)}}.
\end{aligned}$$

Mais les inégalités $r'/(2L_\infty) \leq r_\infty \leq 2L_\infty r'$ démontrées en [5, section 5] ainsi que l'hypothèse $r'X^{1-\varepsilon} \geq 1$ fournissent la majoration

$$\frac{1}{\log(r_\infty^2 r'^{-1}X)} \leq \frac{1}{\log\left(\frac{X^\varepsilon}{4(\log X)^{2/\varepsilon}}\right)},$$

qui permet de conclure également dans ce cas à la majoration (4.20). On traite de manière tout à fait analogue les autres cas, ce qui permet d'obtenir

$$\begin{aligned}
S_{-,-,-}(X;\mathbf{k},\alpha) = {}& \frac{X^2}{2^{k_1+\max\{k_2'',k_3''\}+2}}\left(\frac{\pi}{4}\right)^3 \frac{\operatorname{vol}(\mathcal{R})}{4}\prod_{p>2}\sigma_p\\
&+ O_\varepsilon\left(L_\infty^\varepsilon r_\infty^2 \frac{X^2}{(\log X)^\eta}\right).
\end{aligned} \tag{4.21}$$

En combinant (4.13), (4.14), le Lemme 4.6, (4.21) et le Lemme 4.3, on conclut à l'estimation

$$S(X) = \sum_{k_0 \geq 0} \sum_{\mathbf{k} \in \mathbb{N}^3} \Bigg(\frac{2^{-2k_0+9} X^2 n(\mathbf{k})}{2^{k_1 + \max\{k_2'', k_3''\}+2}} \Big(\frac{\pi}{4} \Big)^3 \frac{\mathrm{vol}(\mathcal{R})}{4} \prod_{p>2} \sigma_p \\ + O_\varepsilon \Big(L_\infty^\varepsilon (r_\infty r' + r_\infty^2) \frac{2^{-2k_0} X^2}{(\log X)^{\eta - \varepsilon}} \Big) \Bigg)$$

qui permet d'achever la preuve du Théorème 2.1.

5. Démonstration du Théorème 2.3 : interprétation de la constante. Pour $A \in \mathbb{Z}$, $\alpha \in \mathbb{N}$ et p^n une puissance d'un nombre premier, on pose

$$S_\alpha(A; p^n) = \#\{(x, y) \in (\mathbb{Z}/p^n\mathbb{Z})^2 \mid p^\alpha (x^2 + y^2) \equiv A \pmod{p^n}\}.$$

Si $\alpha \leq n$, on a clairement

$$S_\alpha(A; p^n) = p^{2\alpha} S_0(A/p^\alpha; p^{n-\alpha})$$

lorsque $\alpha \leq \nu_p(A)$, et $S_\alpha(A; p^n) = 0$ sinon. Il suffit donc de traiter le cas $\alpha = 0$, ce que fournit le lemme suivant issu de [4, section 2].

Lemme 5.1. *Lorsque* $p \equiv 1 \pmod 4$, *on a*

$$S_0(A; p^n) = \begin{cases} p^n + np^n(1 - 1/p) & \text{si } \nu_p(A) \geq n, \\ (1 + \nu_p(A)) p^n (1 - 1/p) & \text{sinon.} \end{cases}$$

Lorsque $p \equiv 3 \pmod 4$, *on a*

$$S_0(A; p^n) = \begin{cases} p^{2[n/2]} & \text{si } \nu_p(A) \geq n, \\ p^n(1 + 1/p) & \text{si } \nu_p(A) < n \text{ et } 2 \mid \nu_p(A), \\ 0 & \text{sinon.} \end{cases}$$

et pour $p = 2$, *on a*

$$S_0(A; 2^n) = \begin{cases} 2^n & \text{si } \nu_2(A) \geq n - 1, \\ 2^{n+1} & \text{si } \nu_p(A) < n - 1 \text{ et } 2^{-\nu_2(A)} A \equiv 1 \pmod 4), \\ 0 & \text{sinon.} \end{cases}$$

5.1. Le cas $p \equiv 1 \pmod 4$**.** On raisonne de manière similaire à [5, section 4] à différence qu'on utilise le Lemme 5.1. On pose

$$M_\nu(p^n) = \#\{\mathbf{x} \in (\mathbb{Z}/p^n\mathbb{Z})^2 \mid \nu_p(F_i(\mathbf{x})) = \nu_i\},$$
$$M_\nu'(p^n) = \#\{\mathbf{x} \in (\mathbb{Z}/p^n\mathbb{Z})^2 \mid \nu_p(F_i(\mathbf{x})) \geq \nu_i\}.$$

Lorsque $n \geq \nu_1 + \nu_2 + \nu_3$, on a clairement

$$\begin{aligned} M'_\nu(p^n) &= p^{2n-2\nu_1-2\nu_2-2\nu_3}\rho(p^{\nu_1}, p^{\nu_2}, p^{\nu_3}), \\ M_\nu(p^n) &= \sum_{\mathbf{e}\in\{0,1\}^3} (-1)^{e_1+e_2+e_3} M'_{\nu+\mathbf{e}}(p^n). \end{aligned} \tag{5.1}$$

Avec la notation (2.8) et posant $m_j = \max\{\lambda_j, \mu_j\}$, on a alors

$$\begin{aligned} N_{\lambda,\mu}(p^n) = p^{3n+\lambda_1+\lambda_2+\lambda_3}\left(1-\frac{1}{p}\right)^3 & \\ \times \sum_{m_j\leq\nu_j<n} M_\nu(p^n) \prod_{1\leq j\leq 3}(1+\nu_j-\lambda_j) + O(n^4p^{4n}). \end{aligned}$$

En utilisant l'identité (5.1), en divisant par $p^{5n+\lambda_1+\lambda_2+\lambda_3}$ et en faisant tendre n vers l'infini, on obtient

$$\begin{aligned} \omega_{\lambda,\mu}(p) = \left(1-\frac{1}{p}\right)^3 \sum_{m_j\leq\nu_j}\sum_{\mathbf{e}\in\{0,1\}^3}(-1)^{e_1+e_2+e_3}\frac{\rho(p^{\nu_1+e_1}, p^{\nu_2+e_2}, p^{\nu_3+e_3})}{p^{2(\nu_1+e_1+\nu_2+e_2+\nu_3+e_3)}} & \\ \times \prod_{1\leq j\leq 3}(1+\nu_j-\lambda_j). \end{aligned}$$

On effectue alors les changements de variables $n_j = \nu_j + e_j - \lambda_j$ pour obtenir

$$\begin{aligned} \omega_{\lambda,\mu}(p) = \left(1-\frac{1}{p}\right)^3 \sum_{m_j-\lambda_j\leq n_j}\frac{\rho(p^{n_1+\lambda_1}, p^{n_2+\lambda_2}, p^{n_3+\lambda_3})}{p^{2(n_1+\lambda_1+n_2+\lambda_2+n_3+\lambda_3)}} & \\ \times \sum_{0\leq e_j\leq\min\{1,\lambda_j+n_j-m_j\}}(-1)^{e_1+e_2+e_3}\prod_{1\leq j\leq 3}(1+n_j-e_j). \end{aligned}$$

Or,

$$\sum_{0\leq e\leq\min\{1,\lambda+n-m\}}(-1)^e(1+n-e) = \begin{cases} 1 & \text{si } \lambda+n-m\geq 1, \\ 1+m-\lambda & \text{si } \lambda+n-m=0, \end{cases}$$

et $(1+m-\lambda) = \#\mathbb{Z}\cap[0, m-\lambda]$. Donc

$$\begin{aligned} \prod_{i=1}^3 \#\mathbb{Z}\cap[0, m_i-\lambda_i] \times \frac{\rho(p^{m_1}, p^{m_2}, p^{m_3})}{p^{2(m_1+m_2+m_3)}} & \\ = \sum_{n_i\leq m_i-\lambda_i}\frac{\rho(p^{\max\{m_1,\lambda_1+n_1\}}, p^{\max\{m_2,\lambda_2+n_2\}}, p^{\max\{m_3,\lambda_3+n_3\}})}{p^{2(\max\{m_1,\lambda_1+n_1\}+\max\{m_2,\lambda_2+n_2\}+\max\{m_3,\lambda_3+n_3\})}} \end{aligned}$$

et finalement

$$\omega_{\lambda,\mu}(p) = \left(1-\frac{1}{p}\right)^3 \sum_{n_i\geq 0}\frac{\rho(p^{\max\{m_1,\lambda_1+n_1\}}, p^{\max\{m_2,\lambda_2+n_2\}}, p^{\max\{m_3,\lambda_3+n_3\}})}{p^{2(\max\{m_1,\lambda_1+n_1\}+\max\{m_2,\lambda_2+n_2\}+\max\{m_3,\lambda_3+n_3\})}}.$$

On a donc bien obtenu l'identité $\omega_{\boldsymbol{\lambda},\boldsymbol{\mu}}(p) = \sigma_p(\mathbf{d},\mathbf{D})$ pour tout nombre premier $p \equiv 1 \pmod 4$.

5.2. Le cas $p \equiv 3 \pmod 4$. Avec les mêmes notations que lors de la section précédente, lorsque $p \equiv 3 \pmod 4$, on aboutit de la même manière à

$$N_{\lambda,\mu}(p^n) = p^{5n+\lambda_1+\lambda_2+\lambda_3}\left(1+\frac{1}{p}\right)^3 \times \sum_{\substack{m_i \le \nu_i \\ 2 \mid \nu_i - \lambda_i}} \sum_{\mathbf{e}\in\{0,1\}^3} (-1)^{e_1+e_2+e_3} \frac{\rho(p^{\nu_1+e_1}, p^{\nu_2+e_2}, p^{\nu_3+e_3})}{p^{2(\nu_1+e_1+\nu_2+e_2+\nu_3+e_3)}} + O(n^4 p^{4n}).$$

Passant à la limite et effectuant le même changement de variables que dans le cas précédent, on obtient

$$\omega_{\lambda,\mu}(p) = \left(1+\frac{1}{p}\right)^3 \sum_{n_i \ge m_i - \lambda_i} \frac{\rho(p^{n_1+\lambda_1}, p^{n_2+\lambda_2}, p^{n_3+\lambda_3})}{p^{2(n_1+\lambda_1+n_2+\lambda_2+n_3+\lambda_3)}} \times \sum_{\substack{0 \le e_i \le \min\{1, \lambda_i+n_i-m_i\} \\ e_i \equiv n_i\,[2]}} (-1)^{e_1+e_2+e_3}.$$

Or,

$$\sum_{\substack{0 \le e \le \min\{1,\lambda+n-m\} \\ e \equiv n\,[2]}} (-1)^e = \begin{cases} (-1)^n & \text{si } \lambda+n-m \ge 1, \\ 1 & \text{si } \lambda+n-m = 0 \text{ et } 2 \mid m-\lambda, \\ 0 & \text{si } \lambda+n-m = 0 \text{ et } 2 \nmid m-\lambda. \end{cases}$$

On conclut alors comme lors de la section précédente à l'égalité souhaitée $\omega_{\boldsymbol{\lambda},\boldsymbol{\mu}}(p) = \sigma_p(\mathbf{d},\mathbf{D})$ pour tout nombre premier $p \equiv 3 \pmod 4$.

5.3. Le cas $p = 2$. Le Lemme 5.1 fournit immédiatement la relation

$$\omega_{\mathbf{d}}(2) = \lim_{n\to\infty} 2^{-2n+3} \#\{\mathbf{x} \in (\mathbb{Z}/2^n\mathbb{Z})^2 \mid F_i(\mathbf{x}) \in d_i \mathcal{E}_{2^n}\} = \sigma_2(\mathbf{d}),$$

où $\sigma_2(\mathbf{d})$ est définie en (2.7) et $\omega_{\mathbf{d}}(2)$ en (2.9).

5.4. Le cas de la densité archimédienne. Enfin, pour terminer le traitement de la constante, il reste à regarder la densité archimédienne. On remarque pour commencer que

$$\omega_{\mathcal{R}}(\infty) = 2^6 \omega_{\mathcal{R}}^+(\infty)$$

où $\omega_{\mathcal{R}}^+(\infty)$ est défini de la même façon que $\omega_{\mathcal{R}}(\infty)$ avec les conditions supplémentaires $s_i, t_i > 0$ pour tout $1 \le i \le 3$. On utilise la forme de Leray en paramétrant par les t_i. La forme de Leray est par conséquent ici donnée par

$$(-2^3 t_1 t_2 t_3)^{-1}\, ds_1\, ds_2\, ds_3\, dx_1\, dx_2.$$

En effet, la variété est définie comme le lieu des zéros des polynômes

$$f_i(\mathbf{x},\mathbf{s},\mathbf{t}) = \frac{F_i(\mathbf{x})}{d_i} - (s_i^2 + t_i^2) \qquad (1 \le i \le 3)$$

et on a

$$\det \begin{pmatrix} \frac{\partial f_1}{\partial t_1} & \frac{\partial f_2}{\partial t_1} & \frac{\partial f_3}{\partial t_1} \\ \frac{\partial f_1}{\partial t_2} & \frac{\partial f_2}{\partial t_2} & \frac{\partial f_3}{\partial t_2} \\ \frac{\partial f_1}{\partial t_3} & \frac{\partial f_2}{\partial t_3} & \frac{\partial f_3}{\partial t_3} \end{pmatrix} = \det \begin{pmatrix} -2t_1 & 0 & 0 \\ 0 & -2t_2 & 0 \\ 0 & 0 & -2t_3 \end{pmatrix} = -2^3 t_1 t_2 t_3.$$

On utilise ici le fait que

$$\int_0^{\sqrt{A}} \frac{ds}{\sqrt{A - s^2}} = \frac{\pi}{2}. \tag{5.2}$$

En substituant $t_i = \sqrt{d_i^{-1} F_i(\mathbf{x}) - s_i^2}$, on obtient finalement

$$\omega_{\mathcal{R}}^{+}(\infty) = 2^{-3} \int_{\mathcal{R}} \Bigg(\prod_{1 \le i \le 3} \int_0^{\sqrt{d_i^{-1} F_i(\mathbf{x})}} \frac{ds_i}{\sqrt{d_i^{-1} F_i(\mathbf{x}) - s_i^2}} \Bigg) dx_1\, dx_2,$$

soit

$$\omega_{\mathcal{R}}(\infty) = \pi^3 \operatorname{vol}(\mathcal{R}).$$

Cela achève la preuve du Théorème 2.3.

6. Démonstration du Théorème 1.1

6.1. Passage aux torseurs et reformulation du problème de comptage. On note Z^m l'ensemble des vecteurs de $\mathbb{Z}^m$ premiers entre eux dans leur ensemble. On introduit également la norme de $\mathbb{R}^5$ suivante :

$$\|\mathbf{x}\| = \max\{|x_0|, |x_1|, |x_2|, \delta^{-1}|x_3|, \delta^{-1}|x_4|\}, \tag{6.1}$$

où

$$\delta = \sqrt{(|a_1| + |b_1|)(|a_2| + |b_2|)(|a_3| + |b_3| + |c_3|)}. \tag{6.2}$$

On introduit la hauteur exponentielle sur $\mathbb{P}^4(\mathbb{Q})$, associée à la norme définie en (6.1), définie par

$$H_4 : \mathbb{P}^4(\mathbb{Q}) \to \mathbb{R}_*^+, \qquad [x_0 : x_1 : x_2 : x_3 : x_4] \mapsto \|(x_0, x_1, x_2, x_3, x_4)\|,$$

avec $[x_0 : x_1 : x_2 : x_3 : x_4]$ choisi de telle sorte que les x_i soient des entiers premiers entre eux. On introduit aussi $\mathcal{T}_{\mathrm{spl}} \subset \mathbb{A}_{\mathbb{Q}}^5 = \operatorname{Spec}(\mathbb{Q}[y,z,t,u,v])$ le sous-schéma défini par l'équation

$$y^2 + z^2 = t^2 F_1(u,v) F_2(u,v) F_3(u,v) \tag{6.3}$$

avec les conditions $(y,z,t)\neq 0$ et $(u,v)\neq 0$. Il s'agit d'un $\mathbb{G}_{\mathrm{m}}^2$-torseur pour S [7, définition 4.1]. On pose

$$\mathcal{D}=\{d\in\mathbb{N}\mid p\,|\,d\Rightarrow p\equiv 1 \pmod 4\}.$$

Lorsque $d_0\in\mathcal{D}$, tous les diviseurs de d_0 sont aussi dans $\mathcal{D}$. On introduit ensuite

$$r(n;m)=\#\{(a,b)\in\mathbb{Z}^2\mid n=a^2+b^2,\ (m,a,b)=1\}.$$

Alors clairement $r(n;1)=r(n)$ et $r(y^2n;y)=0$ si $y\notin\mathcal{D}$.

Utilisant une inversion de Möbius pour traiter la condition de coprimalité, on aboutit, pour $y\in\mathcal{D}$, à la formule

$$r(y^2n;y)=\sum_{k|y}\mu(k)r\Big(\frac{y^2n}{k^2}\Big). \tag{6.4}$$

Enfin, considérant l'ensemble

$$\varSigma:=\{\boldsymbol{\varepsilon}\in\{-1,+1\}^3\mid \varepsilon_1\varepsilon_2\varepsilon_3=1,\ \varepsilon_1=1\} \tag{6.5}$$

et pour $\boldsymbol{\varepsilon}\in\varSigma$ et $T\geq 1$ la région

$$R^{\boldsymbol{\varepsilon}}(T)=\{(u,v)\in\mathbb{R}^2\mid |u|,|v|\leq\sqrt{T},\ \varepsilon_iF_i(u,v)>0\},$$

on en déduit le lemme suivant.

Lemme 6.1. *On a $N(B)=N_1(B)+O(B)$ où*

$$N_1(B)=\sum_{k\in\mathcal{D}}\mu(k)\sum_{\substack{\ell\leq B/k\\ \ell\in\mathcal{D}}}\sum_{\boldsymbol{\varepsilon}\in\varSigma}\sum_{(u,v)\in Z^2\cap R^{\boldsymbol{\varepsilon}}(B/k\ell)} r\big(\ell^2F_1^+(u,v)F_2^+(u,v)F_3^+(u,v)\big),$$

où l'on note $F_i^+=\varepsilon_iF_i$.

Démonstration. Le lemme 2 de [9] nous garantit que $N(B)=\frac14T(B)$ avec

$$T(B)=\#\left\{(y,z,t;u,v)\in Z^3\times Z^2\ \middle|\ \begin{array}{l}\|(v^2t,uvt,u^2t,y,z))\|\leq B,\\ y^2+z^2=t^2F(u,v)\end{array}\right\}.$$

Puisque pour un $(y,z,t;u,v)$ compté, on a

$$\|(v^2t,uvt,u^2t,y,z))\|=\max\{u^2,v^2\}|t|,$$

on en déduit, par symétrie sur le signe de t, que

$$N(B)=\tfrac12\#\{(y,z,t;u,v)\in(Z^3\times Z^2)\cap\mathcal{T}_{\mathrm{spl}}\mid 0<\max\{u^2,v^2\}t\leq B\}.$$

Un raisonnement élémentaire montre que la contribution des (u,v) tels que $F_1(u,v)F_2(u,v)F_3(u,v)=0$ est $O(1)$, ce qui permet d'écrire $N(B)=N_1(B)+O(B)$ avec

$$N_1(B)=\frac12\sum_{\substack{t\leq B\\ t\in\mathcal{D}}}\sum_{\substack{\varepsilon_i\in\{-1,+1\}\\ \varepsilon_1\varepsilon_2\varepsilon_3=1}}\sum_{(u,v)\in Z^2\cap R^{\boldsymbol{\varepsilon}}(B/t)} r\big(t^2F_1(u,v)F_2(u,v)F_3(u,v);t\big).$$

En posant $k\ell = t$, la formule (6.4) fournit que $N_1(B)$ est égal à

$$\frac{1}{2}\sum_{k\in\mathcal{D}}\mu(k)\sum_{\substack{\ell\le B/k\\ \ell\in\mathcal{D}}}\sum_{\substack{\varepsilon_i\in\{-1,+1\}\\ \varepsilon_1\varepsilon_2\varepsilon_3=1}}\sum_{(u,v)\in Z^2\cap R^{\boldsymbol{\varepsilon}}(B/k\ell)} r\big(\ell^2F_1^+(u,v)F_2^+(u,v)F_3^+(u,v)\big).$$

On en déduit alors immédiatement la formule de l'énoncé du lemme avec $\varepsilon_1 = 1$. Le passage à la somme sur $\boldsymbol{\varepsilon} \in \Sigma$ sera utile en section 7 puisque l'ensemble Σ sera utilisé pour décrire certaines classes d'isomorphie de torseurs. ■

Dans la suite, on notera pour éviter d'alourdir les notations

$$\omega(\gcd(a_0,\dots,a_n)) = \omega(a_0,\dots,a_n).$$

L'idée est maintenant de passer d'un problème de comptage sur $\mathcal{T}_{\mathrm{spl}}$ à un problème de comptage sur des variétés affines de $\mathbb{A}^8$ de la forme (2.4), autrement dit d'exprimer le problème de comptage sur certains torseurs qui seront explicités en section 7. On introduit pour ce faire, lorsque $\mathbf{d} = (d_1,d_2,d_3)$, $d = d_1d_2d_3$, $\mathbf{n} = (n_1,n_2,n_3)$ et $\mathbf{d}' = (d_1',d_2',d_3')$, les notations

$$c(d,\mathbf{n}) = 3^{\omega(d,n_1,n_2,n_3)}\prod_{\substack{\{i,j,k\}=\{1,2,3\}\\ i<j}} 2^{\omega(d,n_i,n_j)-\omega(d,n_i,n_j,n_k)},$$

$$c'(\mathbf{d},\mathbf{d}',\mathbf{n}) = c(d,\mathbf{n})2^{\omega(d_1'd_2',n_1/d_1,n_2/d_2)}.$$

On a alors le lemme suivant où l'on rappelle que l'on note $r_0 = r/4$.

Lemme 6.2. *Soient n_0, n_1, n_2 et n_3 quatre entiers supérieurs ou égaux à 1 avec $n_0\in\mathcal{D}$. Alors*

$$r_0(n_0n_1n_2n_3) = \sum_{\substack{\mathbf{d},\mathbf{d}'\in\mathcal{D}^3\\ d_1d_2d_3\mid n_0,\ d_id_j'd_k'\mid n_i}}\sum_{m_i\mid C(n_i)}\frac{\mu(d_1d_2d_3)\mu(d_1'd_2')\mu(d_3')}{c'(\mathbf{d},\mathbf{d}',\mathbf{n})}$$
$$\times r_0\Big(\frac{n_0}{d_1d_2d_3}\Big)r_0\Big(\frac{n_1}{d_1d_2'd_3'm_1}\Big)r_0\Big(\frac{n_2}{d_2d_1'd_3'm_2}\Big)r_0\Big(\frac{n_3}{d_3d_1'd_2'm_3}\Big),$$

où (i,j,k) parcourt l'ensemble des permutations de $\{1,2,3\}$ et où

$$C(n_i) = \prod_{\substack{p\equiv 3\ (\mathrm{mod}\ 4)\\ \nu_p(n_i)\equiv 1\ (\mathrm{mod}\ 2)\\ \nu_p(n_1n_2n_3)\equiv 0\ (\mathrm{mod}\ 2)}} p \qquad (1\le i\le 3). \tag{6.6}$$

Démonstration. Utilisant la formule d'éclatement pour deux entiers (voir par exemple [5, lemme 10]), on obtient

$$r_0(n_0n_1n_2n_3) = \sum_{d\mid(n_1n_2n_3,n_0)}\mu(d)r_0\Big(\frac{n_0}{d}\Big)r_0\Big(\frac{n_1n_2n_3}{d}\Big).$$

Dans la somme, les entiers d sont sans facteur carré et dans $\mathcal{D}$ lorsque $n_0 \in \mathcal{D}$. On compte alors le nombre de décompositions $d = d_1d_2d_3$ avec $d_1 \,|\, n_1$, $d_2 \,|\, n_2$ et $d_3 \,|\, n_3$. Notant

$$N(d, \mathbf{n}) = \#\{(d_1, d_2, d_3) \in \mathbb{N}^3 \mid d_i \,|\, n_i \text{ et } d = d_1d_2d_3\}$$

le nombre de telles décompositions, on a $c(d, \mathbf{n}) = N(d, \mathbf{n})$ lorsque d est sans facteur carré. En effet, $c(\,\cdot\,, \mathbf{n})$ et $N(\,\cdot\,, \mathbf{n})$ sont deux fonctions multiplicatives. Il suffit donc de montrer qu'elles coïncident sur les nombres premiers. Soit alors p un nombre premier. Si $p \,|\, n_1n_2n_3$, on a clairement

$$N(p, \mathbf{n}) = \#\{i \mid p \,|\, n_i\} = c(p, \mathbf{n}).$$

Cela permet bien de conclure à l'égalité souhaitée. Par conséquent,

$$r_0(n_0n_1n_2n_3) = \sum_{\substack{d_1d_2d_3|n_0 \\ d_1|n_1,\, d_2|n_2,\, d_3|n_3}} \frac{\mu(d_1d_2d_3)}{c(d, \mathbf{n})} r_0\Big(\frac{n_0}{d_1d_2d_3}\Big) r_0\Big(\frac{n_1}{d_1}\frac{n_2}{d_2}\frac{n_3}{d_3}\Big).$$

Posant

$$n_i^{(1)} = \prod_{p\equiv 1 \,(\mathrm{mod}\, 4)} p^{\nu_p(n_i)}, \qquad n_i^{(3)} = \prod_{p\equiv 3 \,(\mathrm{mod}\, 4)} p^{\nu_p(n_i)},$$

on a par multiplicativité,

$$r_0\Big(\frac{n_1}{d_1}\frac{n_2}{d_2}\frac{n_3}{d_3}\Big) = r_0\Big(\frac{n_1^{(1)}}{d_1}\frac{n_2^{(1)}}{d_2}\frac{n_3^{(1)}}{d_3}\Big) r_0(n_1^{(3)}n_2^{(3)}n_3^{(3)}). \tag{6.7}$$

On utilise alors la formule d'éclatement pour trois entiers donnée par [7, lemme 9] pour le premier terme du membre de droite de (6.7):

$$r_0\Big(\frac{n_1^{(1)}}{d_1}\frac{n_2^{(1)}}{d_2}\frac{n_3^{(1)}}{d_3}\Big) = \sum_{\substack{d_i'd_j'|n_k/d_k \\ d_i'\in\mathcal{D}}} \frac{\mu(d_1')\mu(d_2'd_3')}{2^{\omega(d_2',n_2/d_2)+\omega(d_3',n_3/d_3)}} \times r_0\Big(\frac{n_1^{(1)}}{d_1d_2'd_3'}\Big) r_0\Big(\frac{n_2^{(1)}}{d_2d_1'd_3'}\Big) r_0\Big(\frac{n_3^{(1)}}{d_3d_1'd_2'}\Big).$$

Concernant le deuxième terme du membre de droite de (6.7), en remarquant que r_0 ne prend que les valeurs 0 ou 1 sur des entiers n'ayant que des facteurs premiers congrus à 3 modulo 4, on a les égalités

$$\begin{aligned} r_0(n_1^{(3)}n_2^{(3)}n_3^{(3)}) &= r_0\Big(\frac{n_1^{(3)}}{C(n_1)}\Big) r_0\Big(\frac{n_2^{(3)}}{C(n_2)}\Big) r_0\Big(\frac{n_3^{(3)}}{C(n_3)}\Big) \\ &= \sum_{m_i|C(n_i)} r_0\Big(\frac{n_1^{(3)}}{m_1}\Big) r_0\Big(\frac{n_2^{(3)}}{m_2}\Big) r_0\Big(\frac{n_3^{(3)}}{m_3}\Big). \end{aligned}$$

La seconde égalité découle du fait que pour tout m_i divisant strictement $C(n_i)$,

$$r_0\left(\frac{n_1^{(3)}}{m_1}\right)r_0\left(\frac{n_2^{(3)}}{m_2}\right)r_0\left(\frac{n_3^{(3)}}{m_3}\right)=0.$$

En regroupant les facteurs par multiplicativité, on obtient bien la formule souhaitée. ∎

On note dans la suite

$$F_{i,e}=eF_i^+=e\varepsilon_iF_i,\qquad F_{3,e}=e^2F_3^+=e^2\varepsilon_3F_3,$$

pour tout entier naturel e. On introduit également

$$\Delta_{ij}^{(1)}=\prod_{\substack{p\mid\Delta_{ij}\\ p\equiv 1\ (\mathrm{mod}\ 4)}}p,\qquad \Delta_{ij}^{(3)}=\prod_{\substack{p\mid\Delta_{ij}\\ p\equiv 3\ (\mathrm{mod}\ 4)}}p\qquad (1\le i<j\le 3) \tag{6.8}$$

et l'ensemble

$$M=\left\{\mathbf{m}\in\mathbb{N}^3\ \middle|\ \begin{array}{l} m_i\mid[\Delta_{ij}^{(3)},\Delta_{ik}^{(3)}],\ (m_i,m_j)\mid\Delta_{ij}^{(3)}\\ \mu^2(m_i)=1,\ \sqrt{m_1m_2m_3}\in\mathbb{N}\end{array},\ \{i,j,k\}=\{1,2,3\}\right\}. \tag{6.9}$$

Posant $\mathcal{R}=R^{\boldsymbol{\varepsilon}}(1)$ et pour $d\in\mathbb{N}$ fixé,

$$f_d(n)=\sum_{sk=n}\mu(k)r(ds^2), \tag{6.10}$$

on déduit alors des Lemmes 6.1 et 6.2 le lemme suivant.

Lemme 6.3. *Avec les notations* (2.3) *et* (6.5), *on a*

$$\begin{aligned}N_1(B)=\frac{1}{2^6}&\sum_{\substack{e\ge1\\ d\in\mathcal{D}}}\mu(e)\mu(d)\sum_{\substack{n\le N\\ n\in\mathcal{D}}}f_d(n)\sum_{\boldsymbol{\varepsilon}\in\Sigma}\sum_{\substack{k_4k_1k_1'\mid\gcd(\Delta_{23},d)\\ k_4k_2k_2'\mid\gcd(\Delta_{13},d)\\ k_4k_3k_3'\mid\gcd(\Delta_{12},d)}}\sum_{\substack{k_4k_4'\mid\gcd(\Delta_{12},\Delta_{13},\Delta_{23},d)\\ k_5k_5'\mid\Delta_{12}}}\\ &\times\frac{\mu(k_1')\mu(k_2')\mu(k_3')\mu(k_4')\mu(k_5')}{3^{\omega(k_4)}2^{\omega(k_5)+\omega(k_1)+\omega(k_2)+\omega(k_3)}}\sum_{\substack{\mathbf{d},\mathbf{d}'\in\mathcal{D}^3\\ d=d_1d_2d_3,d_i'\mid\Delta_{jk}\\ k_5k_5'\mid d_1'd_2'}}\sum_{\mathbf{m}\in M}\mu(d_1'd_2')\mu(d_3')S\left(\sqrt{\frac{B}{de^2n}},\mathbf{e},\mathbf{E}\right),\end{aligned}$$

où $N=\delta B/(d^{5/4}e)$ *et*

$$S(e^{-1}\sqrt{T},\mathbf{e},\mathbf{E})=S(e^{-1}\sqrt{T},\mathbf{e},\mathbf{E};\mathcal{R},F_{1,e},F_{2,e},F_{3,e})$$

pour $T\ge1$ *et avec*

$$\begin{aligned}&e_1=d_1d_2'd_3'm_1,\quad e_2=d_2d_1'd_3'm_2,\quad e_3=d_3d_1'd_2'm_3,\\ &E_1=[e_1,k_4k_2k_2',k_4k_3k_3',k_4k_4',d_1k_5k_5'],\\ &E_2=[e_2,k_4k_1k_1',k_4k_3k_3',k_4k_4',d_2k_5k_5'],\\ &E_3=[e_3,k_4k_1k_1',k_4k_2k_2',k_4k_4'].\end{aligned} \tag{6.11}$$

Démonstration. Pour (u,v) premiers entre eux, on a

$$\gcd(F_i(u,v),F_j(u,v))\,|\,\varDelta_{ij}\qquad(1\leq i<j\leq 3).\tag{6.12}$$

Or, grâce au Lemme 6.2, on obtient pour $r(\ell^2F_1^+(u,v)F_2^+(u,v)F_3^+(u,v))$ l'expression suivante :

$$\frac{1}{2^6}\sum_{\substack{\mathbf{d},\mathbf{d}'\in\mathcal{D}^3\\ d_1d_2d_3|\ell^2,\, d_id'_jd'_k|F_i(u,v)}}\ \sum_{\substack{\mathbf{m}\in M\\ m_i|F_i(u,v)}}\frac{\mu(d_1d_2d_3)\mu(d'_1d'_2)\mu(d'_3)}{c'(\mathbf{d},\mathbf{d}',F_1^+(u,v),F_2^+(u,v),F_3^+(u,v))}$$
$$\times\, r\Big(\frac{\ell^2}{d_1d_2d_3}\Big)r\Big(\frac{F_1^+(u,v)}{e_1}\Big)r\Big(\frac{F_2^+(u,v)}{e_2}\Big)r\Big(\frac{F_3^+(u,v)}{e_3}\Big).$$

En effet, par (6.12), un triplet $\mathbf{m}$ tel que $m_i\,|\,C(F_i(u,v))$ pour tout $1\leq i\leq 3$ avec la notation (6.6) est dans M. Par ailleurs, pour un triplet $\mathbf{m}\in M$ tel que $m_i\,|\,F_i(u,v)$ pour tout $1\leq i\leq 3$ mais $m_j\nmid C(F_j(u,v))$ pour un certain j, on a

$$r\Big(\frac{F_1^+(u,v)}{d_1d'_2d'_3m_1}\Big)r\Big(\frac{F_2^+(u,v)}{d_2d'_1d'_3m_2}\Big)r\Big(\frac{F_3^+(u,v)}{d_3d'_1d'_2m_3}\Big)=0.$$

L'entier $d=d_1d_2d_3$ divise ℓ, donc est nécessairement dans $\mathcal{D}$. On écrit alors $\ell=ds$ et grâce au Lemme 6.1 on obtient

$$N_1(B)=\frac{1}{2^6}\sum_{\substack{dk\leq B\\ k,d\in\mathcal{D}}}\mu(d)\mu(k)\sum_{\substack{s\leq B/(dk)\\ s\in\mathcal{D}}}r(ds^2)$$
$$\times\sum_{\substack{\mathbf{d},\mathbf{d}'\in\mathcal{D}^3\\ d=d_1d_2d_3}}\ \sum_{\mathbf{m}\in M}\mu(d'_1d'_2)\mu(d'_3)\mathcal{S}_{\mathbf{d},\mathbf{d}',\mathbf{m}}\Big(\frac{B}{dsk}\Big),$$

où, pour $T\geq 1$, on a posé

$$\mathcal{S}_{\mathbf{d},\mathbf{d}',\mathbf{m}}(T)=\sum_{\boldsymbol{\varepsilon}\in\varSigma}\ \sum_{\substack{(u,v)\in Z^2\cap R^{\boldsymbol{\varepsilon}}(T)\\ e_1|F_1(u,v),\, e_2|F_2(u,v),\\ e_3|F_3(u,v)}}\frac{r\big(\frac{F_1^+(u,v)}{e_1}\big)r\big(\frac{F_2^+(u,v)}{e_2}\big)r\big(\frac{F_3^+(u,v)}{e_3}\big)}{c'(\mathbf{d},\mathbf{d}',F_1^+(u,v),F_2^+(u,v),F_3^+(u,v))}.$$

Avec la notation (6.10) et grâce à (6.12), on aboutit à la formule

$$N_1(B)=\frac{1}{2^6}\sum_{\substack{dn\leq B\\ dn\in\mathcal{D}}}\mu(d)f_d(n)\sum_{\substack{\mathbf{d},\mathbf{d}'\in\mathcal{D}^3\\ d=d_1d_2d_3,\, d'_j|\varDelta_{ik}}}\ \sum_{\mathbf{m}\in M}\mu(d'_1d'_2)\mu(d'_3)\mathcal{S}_{\mathbf{d},\mathbf{d}',\mathbf{m}}\Big(\frac{B}{dn}\Big).$$

Alors, en utilisant à nouveau (6.12), on obtient

$$\mathcal{S}_{\mathbf{d},\mathbf{d}',\mathbf{m}}(T) = \sum_{\boldsymbol{\varepsilon}\in\Sigma} \sum_{\substack{k_1k_4\,|\,\gcd(\Delta_{23},d)\\ k_2k_4\,|\,\gcd(\Delta_{13},d)\\ k_3k_4\,|\,\gcd(\Delta_{12},d)}} \sum_{\substack{k_4\,|\,\gcd(\Delta_{12},\Delta_{13},\Delta_{23},d)\\ k_5\,|\,\gcd(\Delta_{12},d'_1d'_2)}} \frac{1}{3^{\omega(k_4)}2^{\omega(k_5)+\omega(k_1)+\omega(k_2)+\omega(k_3)}} \times \sum_{\substack{(u,v)\in Z^2\cap R^{\boldsymbol{\varepsilon}}(T)\\ e_1|F_1(u,v),e_2|F_2(u,v)\\ e_3|F_3(u,v)}} r\left(\frac{F_1^+(u,v)}{e_1}\right) r\left(\frac{F_2^+(u,v)}{e_2}\right) r\left(\frac{F_3^+(u,v)}{e_3}\right),$$

où la somme intérieure porte sur les couples (u,v) tels que

$$\begin{cases} k_1 = \gcd(d, F_2(u,v), F_3(u,v))/\gcd(d, F_1(u,v), F_2(u,v), F_3(u,v)),\\ k_2 = \gcd(d, F_1(u,v), F_3(u,v))/\gcd(d, F_1(u,v), F_2(u,v), F_3(u,v)),\\ k_3 = \gcd(d, F_1(u,v), F_2(u,v))/\gcd(d, F_1(u,v), F_2(u,v), F_3(u,v)),\\ k_4 = \gcd(d, F_1(u,v), F_2(u,v), F_3(u,v)),\\ k_5 = \gcd(d'_1d'_2, F_1(u,v)/d_1, F_2(u,v)/d_2). \end{cases} \tag{6.13}$$

Plusieurs inversions de Möbius successives fournissent alors

$$\mathcal{S}_{\mathbf{d},\mathbf{d}',\mathbf{m}}(T) = \sum_{\boldsymbol{\varepsilon}\in\Sigma} \sum_{\substack{k_4k_1k'_1|\gcd(\Delta_{23},d)\\ k_4k_2k'_2|\gcd(\Delta_{13},d)\\ k_4k_3k'_3|\gcd(\Delta_{12},d)}} \sum_{\substack{k_4k'_4|\gcd(\Delta_{12},\Delta_{13},\Delta_{23},d)\\ k_5k'_5|\gcd(\Delta_{12},d'_1d'_2)}} \frac{\mu(k'_1)\mu(k'_2)\mu(k'_3)\mu(k'_4)\mu(k'_5)}{3^{\omega(k_4)}2^{\omega(k_5)+\omega(k_1)+\omega(k_2)+\omega(k_3)}} \times \sum_{\substack{(u,v)\in Z^2\cap R^{\boldsymbol{\varepsilon}}(T)\\ e_1|F_1(u,v),e_2|F_2(u,v)\\ e_3|F_3(u,v)}} r\left(\frac{F_1^+(u,v)}{e_1}\right) r\left(\frac{F_2^+(u,v)}{e_2}\right) r\left(\frac{F_3^+(u,v)}{e_3}\right),$$

où la somme intérieure porte désormais sur les couples (u,v) tels que

$$\begin{cases} k_4k_1k'_1 \mid \gcd(d, F_2(u,v), F_3(u,v)),\\ k_4k_2k'_2 \mid \gcd(d, F_1(u,v), F_3(u,v)),\\ k_4k_3k'_3 \mid \gcd(d, F_1(u,v), F_2(u,v)),\\ k_4k'_4 \mid \gcd(d, F_1(u,v), F_2(u,v), F_3(u,v)),\\ k_5k'_5 \mid \gcd(d'_1d'_2, F_1(u,v)/d_1, F_2(u,v)/d_2). \end{cases} \tag{6.14}$$

On a $(\mathbf{e},\mathbf{E})\in\mathfrak{D}$ et on peut alors réécrire cette somme sous la forme

$$
\begin{aligned}
(6.15)\qquad & \mathcal{S}_{\mathbf{d},\mathbf{d}',\mathbf{m}}(T)\\
&=\sum_{\boldsymbol{\varepsilon}\in\Sigma}\sum_{\substack{k_4k_1k_1'|\gcd(\Delta_{23},d)\\ k_4k_2k_2'|\gcd(\Delta_{13},d)\\ k_4k_3k_3'|\gcd(\Delta_{12},d)}}\ \sum_{\substack{k_4k_4'|\gcd(\Delta_{12},\Delta_{13},\Delta_{23},d)\\ k_5k_5'|\gcd(\Delta_{12},d_1'd_2')}}\frac{\mu(k_1')\mu(k_2')\mu(k_3')\mu(k_4')\mu(k_5')}{3^{\omega(k_4)}2^{\omega(k_5)+\omega(k_1)+\omega(k_2)+\omega(k_3)}}\\
&\qquad\times\sum_{(u,v)\in Z^2\cap\sqrt{T}\mathcal{R}^{\boldsymbol{\varepsilon}}(1)\cap\Lambda(\mathbf{E})} r\Big(\frac{F_1^+(u,v)}{e_1}\Big)r\Big(\frac{F_2^+(u,v)}{e_2}\Big)r\Big(\frac{F_3^+(u,v)}{e_3}\Big).
\end{aligned}
$$

Reste encore à supprimer la condition de coprimalité sur les couples (u,v) au moyen d'une dernière inversion de Möbius. Avec la notation (2.3), la somme intérieure de (6.15) est alors égale à

$$\sum_{e=1}^{\infty}\mu(e)S(e^{-1}\sqrt{T},\mathbf{e},\mathbf{E}).$$

On obtient ainsi le lemme avec $N=B/(de^2)$. Mais on peut remarquer que $S(\sqrt{B/(de^2n)},\mathbf{e},\mathbf{E})$ est nulle si l'on n'a pas

$$d_1\le(|a_1|+|b_1|)\sqrt{\frac{B}{dn}},\quad d_2\le(|a_2|+|b_2|)\sqrt{\frac{B}{dn}},\quad d_3\le(|a_3|+|b_3|+|c_3|)\frac{B}{dn}.$$

En effet, on a par exemple

$$F_{1,e}(u,v)\le(|a_1|+|b_1|)e\max\{|u|,|v|\}\le(|a_1|+|b_1|)\sqrt{\frac{B}{dn}}$$

dans la région considérée. Avec la notation (6.2), on a donc en réalité

$$d^{3/4}n^{1/2}\le\delta B^{1/2}.\tag{6.16}$$

Mais pour que $S(\sqrt{B/(de^2n)},\mathbf{e},\mathbf{E})$ soit non nulle, il faut aussi imposer $de^2n\le B$ et par conséquent, $d^{1/2}en^{1/2}\le B^{1/2}$, ce qui, combiné avec (6.16), implique

$$d^{5/4}en\le\delta B$$

et démontre bien le lemme énoncé. ∎

6.2. Fin de la preuve du Théorème 1.1. On obtient alors le théorème suivant.

THÉORÈME 6.1. *Lorsque $B\to\infty$, on a*

$$N(B)=c_0B\log(B)(1+o(1))$$

avec

$$c_0 = \frac{\pi^2}{2^4} \sum_{e=1}^{\infty} \frac{\mu(e)}{e^2} \sum_{d \in \mathcal{D}} \frac{\mu(d) r_0(d) \varphi^\dagger(d)}{d}$$
$$\times \sum_{\boldsymbol{\varepsilon} \in \Sigma} \mathrm{vol}(\mathcal{R}) \sum_{\substack{\mathbf{d}, \mathbf{d}' \in \mathcal{D}^3 \\ d = d_1 d_2 d_3,\, d_i' \mid \Delta_{jk}}} \sum_{\mathbf{m} \in M} \mu(d_1' d_2') \mu(d_3')$$
$$\times \sum_{\substack{k_4 k_1 k_1' \mid \gcd(\Delta_{23}, d) \\ k_4 k_2 k_2' \mid \gcd(\Delta_{13}, d) \\ k_4 k_3 k_3' \mid \gcd(\Delta_{12}, d)}} \sum_{\substack{k_4 k_4' \mid \gcd(\Delta_{12}, \Delta_{13}, \Delta_{23}, d) \\ k_5 k_5' \mid \gcd(\Delta_{12}, d_1' d_2')}} \frac{\mu(k_1')\mu(k_2')\mu(k_3')\mu(k_4')\mu(k_5')}{3^{\omega(k_4)} 2^{\omega(k_5) + \omega(k_1) + \omega(k_2) + \omega(k_3)}} \sigma^{\boldsymbol{\varepsilon}}(\mathbf{e}, \mathbf{E}, e)$$

avec

$$\sigma^{\boldsymbol{\varepsilon}}(\mathbf{e}, \mathbf{E}, e) := \prod_p \sigma_p^{\boldsymbol{\varepsilon}}(\mathbf{e}, \mathbf{E}, e), \tag{6.17}$$

où

$$\sigma_p^{\boldsymbol{\varepsilon}}(\mathbf{e}, \mathbf{E}, e) = \left(1 - \frac{\chi(p)}{p}\right)^3 \sum_{\boldsymbol{\nu} \in \mathbb{N}^3} \frac{\chi(p)^{\nu_1 + \nu_2 + \nu_3} \rho\left(p^{N_1}, p^{N_2}, p^{N_3}\right)}{p^{2(N_1 + N_2 + N_3)}},$$

$N_i = \max\{\nu_p(E_i), \nu_i + \nu_p(e_i)\}$ *et*

$$\sigma_2^{\boldsymbol{\varepsilon}}(\mathbf{e}, e) = 8 \lim_{n \to \infty} 2^{-2n} \#\{\mathbf{x} \in (\mathbb{Z}/2^n\mathbb{Z})^2 \mid e^{\deg(F_i)} F_i(\mathbf{x}) \in \varepsilon_i m_i \mathcal{E}_{2^n}\}.$$

La fin de cette section est consacrée à la preuve de ce théorème. Il permet de démontrer le Théorème 1.1 modulo le fait que la constante c_0 soit bien la constante conjecturée par Peyre, ce qui fera l'objet de la section suivante. On utilise évidemment le Théorème 2.2 pour estimer la somme

$$S(\sqrt{T}, \mathbf{e}, \mathbf{E}) = S(\sqrt{T}, \mathbf{e}, \mathbf{E}; \mathcal{R}, F_{1,e}, F_{2,e}, F_{3,e})$$

et obtenir le lemme suivant.

Lemme 6.4. *Soit $\varepsilon > 0$ tel que $r'(\sqrt{T})^{1-\varepsilon} \geq 1$. Alors, avec les notations du Théorème* 6.1,

$$S(\sqrt{T}, \mathbf{e}, \mathbf{E}) = \pi^3 \,\mathrm{vol}(\mathcal{R}) T \prod_p \sigma_p^{\boldsymbol{\varepsilon}}(\mathbf{e}, \mathbf{E}, e) + O_{\varepsilon, F_{i,e}}\left(\frac{T}{(\log T)^{\eta - \varepsilon}}\right).$$

De plus,

$$\sigma^{\boldsymbol{\varepsilon}}(\mathbf{e}, \mathbf{E}, e) \ll (de)^{\varepsilon} a'(\mathbf{E}, \boldsymbol{\Delta}),$$

uniformément en tous les paramètres $\mathbf{d}$, $\mathbf{d}'$, $\mathbf{m}$, $\mathbf{k}$, $\mathbf{k}'$, ε_i, e, $\mathbf{e}$, $\mathbf{E}$ *et* d.

On raisonne alors comme dans [5, preuve du lemme 9] afin d'obtenir une majoration uniforme de $S(\sqrt{T}, \mathbf{e}, \mathbf{E})$, mis à part qu'on utilise une majoration différente pour la quantité $\det(G_f(\mathcal{A}))$ qui y apparaît. On remarque ici qu'il faut bien faire attention au fait qu'on travaille avec les formes $F_{i,e}$ et qu'on a notamment une dépendance des coefficients en la variable e. On a ainsi le lemme suivant.

LEMME 6.5. *Pour $T \geq 1$ et $(\mathbf{e}, \mathbf{E}) \in \mathfrak{D}$, on a*

$$S(\sqrt{T}, \mathbf{e}, \mathbf{E}) \ll c(F_1)c(F_2)c(F_3)(\Delta^*)^3(deL_\infty)^\varepsilon \gcd(d,e)a'(\mathbf{E}, \boldsymbol{\Delta}) \times \left(r_\infty(\mathcal{R})^2 \frac{T}{d} + r_\infty(\mathcal{R})^{1+\varepsilon} T^{1/2+\varepsilon} \right),$$

où $c(P)$ est le contenu d'un polynôme à coefficients entiers.

Démonstration. On raisonne ici comme dans [5, section 6]. Avec les notations (2.5), on pose

$$E_i'' = \frac{E_i}{\gcd(E_i', b)\gcd(E_i, e\ell_i)}, \qquad E_3'' = \frac{E_3}{\gcd(E_3', b^2)\gcd(E_3, e^2\ell_3)}.$$

Des calculs élémentaires garantissent

$$E'' = E_1''E_2''E_3'' \geq \frac{E}{\gcd(E_1, be\ell_1)\gcd(E_2, be\ell_2)\gcd(E_3, b^2e^2\ell_3)}.$$

Mais revenant à la définition de $E_1/\gcd(E_1, be\ell_1)$, avec la notation du Lemme 4.2 on obtient

$$\frac{E_1}{\gcd(E_1, be\ell_1)} \geq \frac{1}{\Delta^*} \frac{d_1}{\gcd(d_1, be\ell_1)}.$$

En procédant de la même façon avec les indices 2 et 3, on aboutit finalement à

$$E'' \geq \frac{1}{(\Delta^*)^3} \frac{d}{\gcd(d_1, be\ell_1)\gcd(d_2, be\ell_2)\gcd(d_3, b^2e^2\ell_3)}.$$

Alors

$$E'' \geq \frac{1}{c(F_1)c(F_2)c(F_3)(\Delta^*)^3} \frac{d}{\gcd(d_1, be)\gcd(d_2, be)\gcd(d_3, b^2e^2)}.$$

Puisque $d = d_1d_2d_3$ est sans facteur carré, d_3 l'est aussi et donc

$$E'' \geq \frac{1}{c(F_1)c(F_2)c(F_3)(\Delta^*)^3} \frac{d}{\gcd(d_1, be)\gcd(d_2, be)\gcd(d_3, be)}.$$

Pour finir, on utilise le fait que

$$\gcd(d_1, be)\gcd(d_2, be)\gcd(d_3, be) = \gcd(d_1d_2d_3, be) = \gcd(d, be).$$

pour conclure à l'inégalité

$$E'' \geq \frac{1}{c(F_1)c(F_2)c(F_3)(\Delta^*)^3} \frac{d}{\gcd(d, be)}.$$

Cela permet de finir la démonstration du lemme exactement comme dans [5, lemme 9]. ∎

On a ensuite besoin de quelques résultats issus de [6, lemme 14] concernant la fonction f_d définie en (6.10) pour $d \in \mathcal{D}$. Si $d \in \mathcal{D}$ est sans facteur carré, alors, pour $x \geq 2$, on a

$$\sum_{\substack{n \leq x \\ n \in \mathcal{D}}} \frac{f_d(n)}{n} = \frac{4 r_0(d) \varphi^\dagger(d)}{\pi} \big(\log x + O(\log^3(2 + \omega(d))) \big), \tag{6.18}$$

où

$$\varphi^\dagger(d) = \prod_{p \mid d} \left(1 + \frac{1}{p}\right)^{-1}.$$

Pour $\varepsilon > 0$ et $0 < \theta \leq 1$, on déduit de ces résultats la majoration

$$\sum_{\substack{n \leq x \\ n \in \mathcal{D}}} \frac{|f_d(n)|}{n^\theta} \leq x^{1-\theta} \sum_{\substack{n \leq x \\ n \in \mathcal{D}}} \frac{|f_d(n)|}{n} \ll d^\varepsilon x^{1-\theta} \log x. \tag{6.19}$$

On en déduit à présent la conjecture de Manin pour les surfaces de Châtelet considérées. On utilise la formule asymptotique obtenue grâce au Théorème 2.2 de $S(\sqrt{T}, \mathbf{e}, \mathbf{E})$ dans l'expression de $N_1(B)$ que l'on a obtenue dans le Lemme 6.4. Pour pallier la non uniformité de cette estimation, on pose

$$\mathcal{U}(B) = \mathcal{U}^{\boldsymbol{\varepsilon}}_{\mathbf{e},\mathbf{E},e}(B) = \sum_{\substack{n \leq N \\ n \in \mathcal{D}}} f_d(n) S\left(\sqrt{\frac{B}{de^2 n}}, \mathbf{e}, \mathbf{E}\right),$$

avec N défini lors du Lemme 6.3, de telle sorte que

$$N_1(B) = \frac{1}{2^6} \sum_{e \geq 1} \sum_{d \in \mathcal{D}} \mu(e)\mu(d) \sum_{\boldsymbol{\varepsilon} \in \Sigma} \sum_{\substack{\mathbf{d}, \mathbf{d}' \in \mathcal{D}^3 \\ d = d_1 d_2 d_3,\, d_i' \mid \Delta_{jk}}} \sum_{\mathbf{m} \in M} \mu(d_1' d_2') \mu(d_3')$$
$$\times \sum_{\substack{k_4 k_1 k_1' \mid \gcd(\Delta_{23}, d) \\ k_4 k_2 k_2' \mid \gcd(\Delta_{13}, d) \\ k_4 k_3 k_3' \mid \gcd(\Delta_{12}, d)}} \sum_{\substack{k_4 k_4' \mid \gcd(\Delta_{12}, \Delta_{13}, \Delta_{23}, d) \\ k_5 k_5' \mid \gcd(\Delta_{12}, d_1' d_2')}} \frac{\mu(k_1')\mu(k_2')\mu(k_3')\mu(k_4')\mu(k_5')}{3^{\omega(k_4)} 2^{\omega(k_5) + \omega(k_1) + \omega(k_2) + \omega(k_3)}} \mathcal{U}(B).$$

Avec la notation (6.17), on introduit alors la quantité $E^{\boldsymbol{\varepsilon}}(B; \mathbf{e}, \mathbf{E}, e)$ comme étant donnée par

$$\frac{1}{B \log B} \left| \mathcal{U}(B) - 4\pi^2 \operatorname{vol}(\mathcal{R}) \sigma^{\boldsymbol{\varepsilon}}(\mathbf{e}, \mathbf{E}, e) r_0(d) \varphi^\dagger(d) \frac{B \log B}{de^2} \right|.$$

Les résultats (6.18) et (6.19) impliquent que

$$E^{\boldsymbol{\varepsilon}}(B; \mathbf{e}, \mathbf{E}, e) \xrightarrow[B \to \infty]{} 0,$$

à $\mathbf{e}$, $\mathbf{E}$, $\mathbf{d}$, $\mathbf{d}'$, $\mathbf{m}$, $\mathbf{k}$, $\mathbf{k}'$, d et e fixés. Pour conclure, on souhaite appliquer un théorème de convergence dominée et il suffit donc de montrer la majoration

$$\sum_{\substack{e\geq 1\\ d\in\mathcal{D}}}\sum_{\boldsymbol{\varepsilon}\in\Sigma}\sum_{\substack{\mathbf{d},\mathbf{d}'\in\mathcal{D}^3\\ d=d_1d_2d_3,\, d_i'|\Delta_{jk}}}\sum_{\mathbf{m}\in M}\sum_{\substack{k_4k_1k_1'|\gcd(\Delta_{23},d)\\ k_4k_2k_2'|\gcd(\Delta_{13},d)\\ k_4k_3k_3'|\gcd(\Delta_{12},d)}}$$
$$\times\sum_{\substack{k_4k_4'|\gcd(\Delta_{12},\Delta_{13},\Delta_{23},d)\\ k_5k_5'|\gcd(\Delta_{12},d_1'd_2')}} E^{\boldsymbol{\varepsilon}}(B;\mathbf{e},\mathbf{E},e)\ll 1.$$

Pour ce faire, on a besoin du lemme suivant.

Lemme 6.6. *Pour tout $\varepsilon>0$, on a $|\sigma^{\boldsymbol{\varepsilon}}(\mathbf{e},\mathbf{E},e)|\ll d^{-1/6+\varepsilon}e^{\varepsilon}$.*

Démonstration. On procède en majorant chaque facteur eulérien dans la définition de $\sigma^{\boldsymbol{\varepsilon}}(\mathbf{e},\mathbf{E},e)$ en (6.17). Pour $p=2$, on peut majorer $\sigma_2^{\boldsymbol{\varepsilon}}(\mathbf{e},\mathbf{E},e)$ par 8. Pour les p impairs, on utilise la majoration donnée par le point (f) du Lemme 3.2. On a alors

$$|\sigma_p^{\boldsymbol{\varepsilon}}(\mathbf{e},\mathbf{E},e)|\ll\sum_{\boldsymbol{\nu}\in\mathbb{N}^3}(N_3+1)\frac{1}{p^{N_1/3+N_2/3+N_3/6}},$$

où les $N_i=\max\{\nu_p(E_i),\nu_i+\nu_p(e_i)\}$ ont été définis dans le Lemme 6.4. On tire alors parti du fait que d soit sans facteur carré. On note $d=d_1d_2d_3$ et $\delta_i=\nu_p(d_i)$ de sorte que l'on peut supposer $\delta_1+\delta_2+\delta_3=1$ lorsque $p\,|\,d$. De plus, par définition de E_i et N_i, on voit que $N_i\geq\nu_i+\delta_i$ et donc

$$\prod_{p|d}|\sigma_p^{\boldsymbol{\varepsilon}}(\mathbf{e},\mathbf{E},e)|\ll\prod_{p|d}p^{-(\delta_1+\delta_2+\delta_3)/6}\prod_{p|d}\sum_{\boldsymbol{\nu}\in\mathbb{N}^3}(N_3+1)\frac{1}{p^{\nu_1/3+\nu_2/3+\nu_3/6}}.$$

Alors

$$\prod_{p|d}p^{-(\delta_1+\delta_2+\delta_3)/6}=\prod_{p|d}p^{-1/6}=d^{-1/6}$$

puisque d est sans facteur carré. D'autre part,

$$\prod_{p|d}\sum_{\boldsymbol{\nu}\in\mathbb{N}^3}(N_3+1)\frac{1}{p^{\nu_1/3+\nu_2/3+\nu_3/6}}\ll d^{\varepsilon}\prod_{p|d}(1+\nu_p(d))\ll d^{\varepsilon}$$

et finalement

$$\prod_{p|d}|\sigma_p^{\boldsymbol{\varepsilon}}(\mathbf{e},\mathbf{E},e)|\ll d^{-1/6+\varepsilon}.\ \blacksquare$$

En raisonnant alors comme dans [6, section 7] et en utilisant le Lemme 6.5, on obtient

$$E^{\boldsymbol{\varepsilon}}(B;\mathbf{e},\mathbf{E},e)\ll(de)^{\varepsilon}\gcd(d,e)a'(\mathbf{E},\boldsymbol{\Delta})\left(\frac{1}{d^2e^2}+\frac{1}{d^{9/8}e^{3/2}}+\frac{1}{d^{5/4}e^2}\right),$$

soit

$$E^{\boldsymbol{\varepsilon}}(B;\mathbf{e},\mathbf{E},e)\ll(de)^{\varepsilon}\gcd(d,e)a'(\mathbf{E},\boldsymbol{\Delta})\frac{1}{d^{9/8}e^{3/2}}.$$

Ensuite, puisque $a'(\mathbf{E},\boldsymbol{\Delta})$ concerne les formes primitives, on n'a en réalité pas de dépendance en e et par définition de cette quantité en (2.6),

$$a'(\mathbf{E},\boldsymbol{\Delta}) \ll 1,$$

où la constante est indépendante des paramètres de sommation. Enfin, le fait que

$$\sum_{e=1}^{\infty}\sum_{d\in\mathcal{D}}(de)^{\varepsilon}\gcd(d,e)\frac{1}{d^{9/8}e^{3/2}} \ll 1$$

pour ε assez petit nous autorise à appliquer le théorème de convergence dominée pour obtenir le Théorème 6.1.

7. La constante de Peyre. Pour conclure la démonstration du Théorème 1.1, il reste à montrer que la constante c_0 obtenue dans le Théorème 6.1 est en accord avec la conjecture de Peyre [31, formule 5.1], puisqu'on peut montrer que les surfaces de Châtelet sont des variétés "presque de Fano" au sens de [31, définition 3.1]. On note c_S la constante conjecturée par Peyre. Suivant [30] et [34], on a

$$c_S = \alpha(S)\beta(S)\omega_H(S(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}(S)}),$$

où

$$\beta(S) = \#H^1(\mathrm{Gal}(\overline{\mathbb{Q}},\mathbb{Q}),\mathrm{Pic}(\overline{S})) = \mathrm{Coker}(\mathrm{Br}(\mathbb{Q})\to\mathrm{Br}(S)),$$

$\alpha(S)$ est le volume d'un certain polytope dans le dual du cône effectif et $\omega_H(S(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}(S)})$ est un nombre de Tamagawa.

7.1. Les facteurs $\alpha(S)$ et $\beta(S)$. Pour commencer, il est nécessaire de rappeler quelques éléments relatifs à la géométrie de S tirés de [15] et [16]. On considère $K=\mathbb{Q}(\sqrt{\Delta})$ le corps de décomposition de F ainsi que le corps biquadratique $L=\mathbb{Q}(\sqrt{\Delta},i)$. Si l'on note $\mathcal{G}=\mathrm{Gal}(L/\mathbb{Q})$, clairement $\mathcal{G}\cong(\mathbb{Z}/2\mathbb{Z})^2$ est engendré par la conjugaison complexe σ et par τ, la conjugaison dans K. Enfin, pour toute extension k de $\mathbb{Q}$, on notera $S_k = S\times_{\mathbb{Q}}\mathrm{Spec}(k)$.

Sur $\overline{\mathbb{Q}}$, on écrit $F_3(u,v)=(a_3'u+b_3'v)(a_4'u+b_4'v)$ avec a_3', a_4', b_3' et b_4' dans K tels que $\tau(a_3')=a_4'$ et $\tau(b_3')=b_4'$. En particulier, si l'on définit

$$\Delta_{34} = a_3'b_4' - a_4'b_3' \neq 0, \tag{7.1}$$

on a $\tau(\Delta_{34})=-\Delta_{34}$. Sur L, la surface S_L admet 10 diviseurs exceptionnels qui sont des courbes d'auto-intersection négative. Huit d'entre elles sont d'auto-intersection -1 et sont données pour $i\in\{1,2\}$ par

$$D_i^+:\quad u=-b_i/a_i,\quad x+iy=0;\qquad D_i^-:\quad u=-b_i/a_i,\quad x-iy=0,$$

et pour $i\in\{3,4\}$ par

$$D_i^+:\quad u=-b_i'/a_i',\quad x+iy=0;\qquad D_i^-:\quad u=-b_i'/a_i',\quad x-iy=0,$$

tandis que les deux dernières sont d'auto-intersection -2 et sont données par

$$E^+ : \quad t=0, \quad x+iy=0; \qquad E^- : \quad t=0, \quad x-iy=0.$$

On a également

$$\begin{aligned}\mathrm{Pic}(S_L) &= \langle [E^\pm],[D_i^\pm] \mid i\in\{1,2,3,4\}\rangle \\ &= \langle [E^+],[D_1^+],[D_2^+],[D_3^+],[D_4^+],[D_1^-]\rangle \cong \mathbb{Z}^6\end{aligned}$$

avec les relations

$$[D_i^+]+[D_i^-]=[D_j^+]+[D_j^-] \tag{7.2}$$

pour $i,j\in\{1,2,3,4\}$ et

$$[E^+]+[D_i^+]+[D_j^+]=[E^-]+[D_\ell^-]+[D_m^-] \tag{7.3}$$

pour $\{i,j,\ell,m\}=\{1,2,3,4\}$ et on rappelle que la formule d'adjonction fournit la relation

$$\omega_S^{-1}=2E^+ + \sum_{i=1}^4 D_i^+ = 2E^- + \sum_{i=1}^4 D_i^-. \tag{7.4}$$

Or, $\mathrm{Pic}(S_{\overline{\mathbb{Q}}})\cong \mathrm{Pic}(S_L)$ et $\mathrm{Pic}(S)=(\mathrm{Pic}(S_L))^{\mathcal{G}}$ puisque $S(\mathbb{Q})\neq\emptyset$. Décrivons alors l'action de $\mathcal{G}$ sur le groupe de Picard géométrique. On a

$$\sigma(E^+)=E^-, \qquad \sigma(D_i^+)=D_i^-$$

pour tout $i\in\{1,2,3,4\}$ lorsque $\Delta>0$, tandis que

$$\sigma(E^+)=E^-, \quad \forall i\in\{1,2\}\ \sigma(D_i^+)=D_i^-, \quad \sigma(D_3^+)=D_4^-, \quad \sigma(D_3^-)=D_4^+$$

si $\Delta<0$ et dans tous les cas

$$\tau(D_3^+)=D_4^+, \quad \tau(D_3^-)=D_4^-,$$

les autres éléments étant fixés. On en déduit les lemmes suivants.

Lemme 7.1. *On a* $\mathrm{Pic}(S)=\langle[\omega_S^{-1}],[D_1^+]+[D_1^-]\rangle$.

Démonstration. Soit $D=a[D_1^+]+b[D_2^+]+c[D_3^+]+d[D_4^+]+e[E^+]+f[D_1^-]$ un élément de $\mathrm{Pic}(S_{\overline{\mathbb{Q}}})$. On a que $D\in\mathrm{Pic}(S)$ si, et seulement si, $\sigma(D)=\tau(D)=D$, soit si, et seulement si,

$$\begin{aligned}D=(b+c+d-e)([D_1^+]+[D_1^-])+f[D_1^+]+(a-e)[D_1^-]\\ +(e-b)[D_2^+]+(e-c)[D_3^+]+(e-d)[D_4^+]+e[E^+]\end{aligned}$$

et $D=a[D_1^+]+b[D_2^+]+d[D_3^+]+c[D_4^+]+e[E^+]+f[D_1^-]$ (ce qui implique notamment $c=d$). Comme $[D_1^+]+[D_1^-]\in\mathrm{Pic}(S)$, on en déduit que $D\in\mathrm{Pic}(S)$ si, et seulement si,

$$\begin{aligned}\sigma\bigl(D-(b+c+d-e)([D_1^+]+[D_1^-])\bigr)&=\tau\bigl(D-(b+c+d-e)([D_1^+]+[D_1^-])\bigr)\\ &=D-(b+c+d-e)([D_1^+]+[D_1^-]).\end{aligned}$$

Cela équivaut à $e = 2b = 2c = 2d$ et $a = b + f$ si bien que

$$D - (b+c+d-e)([D_1^+] + [D_1^-]) = (a-2b)([D_1^+] + [D_1^-]) + b[\omega_S^{-1}]$$

et

$$D - (b+c+d-e)([D_1^+] + [D_1^-]) \in \mathbb{Z}([D_1^+] + [D_1^-]) \oplus \mathbb{Z}\omega_S^{-1}. \blacksquare$$

Lemme 7.2. *On a $\alpha(S) = 1/2$.*

Démonstration. Posons $e_1 = \omega_S^{-1}$ et $e_2 = [D_1^+] + [D_1^-]$. On sait que dans ce cas, le cône effectif $\Lambda_{\text{eff}}(S)$ est engendré par les sommes d'éléments d'orbites des courbes d'auto-intersections négatives. Par conséquent,

$$\begin{aligned}\Lambda_{\text{eff}}(S) &= \langle [E^+] + [E^-], [D_1^+] + [D_1^-], [D_3^+] + [D_4^+] + [D_3^-] + [D_4^-] \rangle \\ &= \langle [E^+] + [E^-], [D_1^+] + [D_1^-] \rangle.\end{aligned}$$

On utilise alors la définition suivante de la constante $\alpha(S)$ donnée dans [30] :

$$\alpha(S) = \text{Vol}\{x \in \Lambda_{\text{eff}}(S)^\vee \mid \langle \omega_S^{-1}, x\rangle = 1\},$$

où la mesure sur l'hyperplan

$$\mathcal{H} = \{x \in \text{Pic}(S)^\vee \otimes_{\mathbb{Z}} \mathbb{R} \mid \langle \omega_S^{-1}, x\rangle = 1\}$$

est définie dans [30]. Le cône $\Lambda_{\text{eff}}(S)$ est engendré par $e_1 - 2e_2$ et e_2, si bien que la constante $\alpha(S)$ est donnée par le volume de la région

$$\{(x,y) \in \mathbb{R}^2 \mid x = 1,\ y > 0,\ x - 2y > 0\}.$$

Autrement dit, on obtient la longueur du segment $[0, 1/2]$, soit $\alpha(S) = 1/2$. $\blacksquare$

On aurait également pu montrer que le groupe de Galois $G = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ ne fixe aucune (-1)-courbe et que le cardinal du groupe de Weyl associé au type de singularité $2\mathbf{A}_1$ où les deux singularités sont conjuguées est égal à 2. La table 2 de [20] ainsi que [21] nous permettait alors d'en conclure que $\alpha(S) = 1/2$.

Pour calculer $\beta(S)$, on utilise [36, proposition 7.1.2], qui fournit $\beta(S) = 2$ dans le cas considéré dans cet article.

7.2. Torseurs versels. D'après [32, proposition 8.3] ou [19, proposition 2.1], l'ensemble des classes d'isomorphisme de torseurs versels au-dessus de S possédant au moins un point rationnel est fini, ce qui permet d'exhiber une partition finie de l'ensemble des points rationnels de S, indexée par toute famille de représentants de ces classes d'isomorphisme. En contraste avec [7], il est plus délicat dans le cas de cet article de déterminer explicitement un tel système de représentants.

On considère l'ensemble

$$\mathcal{B} = \left\{ \boldsymbol{\beta} \in \mathbb{Z}^2 \times \mathbb{Z}[\Delta]^2 \;\middle|\; \begin{array}{l} \tau(\beta_3) = \beta_4,\ \exists(\beta_3', n) \in \mathbb{Z}^2 \text{ tels que } \beta_3\beta_4 = \beta_3' n \\ \text{avec } \sqrt{\beta_1\beta_2\beta_3'} \in \mathbb{Z} \text{ et } n \in N_{\mathbb{Q}[i]/\mathbb{Q}}(\mathbb{Z}[i]) \end{array} \right\}$$

ainsi que le sous-ensemble $\mathcal{B}_M^\Sigma$ des $\boldsymbol{\beta}\in\mathcal{B}$ pour lesquels il existe $(\boldsymbol{\varepsilon},\mathbf{m})$ dans $\Sigma\times M$ tels que

$$\beta_1=\varepsilon_1 m_1,\qquad \beta_2=\varepsilon_2 m_2,\qquad \beta_3'=\varepsilon_3 m_3.$$

Notons que l'ensemble $\mathcal{B}_M^\Sigma$ est infini. Pour $\boldsymbol{\beta}\in\mathcal{B}$, on note $\mathcal{T}_{\boldsymbol{\beta}}$ le sous-ensemble constructible de $\mathbf{A}^{10}_{\mathbb{Q}}=\operatorname{Spec}(\mathbb{Q}[X_i,Y_i\mid 0\leq i\leq 4])$ défini par les deux équations quadratiques

$$\phi_1^{\boldsymbol{\beta}}=\phi_2^{\boldsymbol{\beta}}=0$$

invariantes sous le groupe de Galois $\mathcal{G}$ avec

$$\begin{aligned}\phi_1^{\boldsymbol{\beta}}&=a_2\beta_1(X_1^2+Y_1^2)-a_1\beta_2(X_2^2+Y_2^2)\\&\quad-\frac{\Delta_{12}}{\Delta_{34}}\Big(a_4\beta_3\big(X_3^2+Y_3^2+\Delta(X_4^2+Y_4^2)+2\sqrt{\Delta}(X_3X_4+Y_3Y_4)\big)\\&\quad+a_3\beta_4\big(X_3^2+Y_3^2+\Delta(X_4^2+Y_4^2)-2\sqrt{\Delta}(X_3X_4+Y_3Y_4)\big)\Big),\\ \phi_2^{\boldsymbol{\beta}}&=b_2\beta_1(X_1^2+Y_1^2)-b_1\beta_2(X_2^2+Y_2^2)\\&\quad-\frac{\Delta_{12}}{\Delta_{34}}\Big(b_4\beta_3\big(X_3^2+Y_3^2+\Delta(X_4^2+Y_4^2)+2\sqrt{\Delta}(X_3X_4+Y_3Y_4)\big)\\&\quad+b_3\beta_4\big(X_3^2+Y_3^2+\Delta(X_4^2+Y_4^2)-2\sqrt{\Delta}(X_3X_4+Y_3Y_4)\big)\Big),\end{aligned}$$

et les conditions

$$\begin{aligned}\forall i\neq j\in[\![0,2]\!]^2,&\quad ((X_i,Y_i),(X_j,Y_j))\neq((0,0),(0,0)),\\ \forall i\in[\![0,2]\!],&\quad ((X_i,Y_i),(X_3,Y_3,X_4,Y_4))\neq((0,0),(0,0,0,0)).\end{aligned}$$

Définissons à présent un morphisme $\pi_{\boldsymbol{\beta}}:\mathcal{T}_{\boldsymbol{\beta}}\to S$. Pour ce faire, comme dans [7, section 4], il suffit de définir un morphisme $\hat{\pi_{\boldsymbol{\beta}}}:\mathcal{T}_{\boldsymbol{\beta}}\to\mathcal{T}_{\mathrm{spl}}$. Considérons alors une extension finie k de $\mathbb{Q}$ et $((x_i,y_i))_{0\leq i\leq 4}$ dans $\mathcal{T}_{\boldsymbol{\beta}}(k)$. Il existe alors un couple $(u,v)\in k^2\setminus\{(0,0)\}$ tel que

$$\begin{aligned}u&=\frac{1}{\Delta_{12}}\big(b_2\beta_1(x_1^2+y_1^2)-b_1\beta_2(x_2^2+y_2^2)\big)\\&=\frac{1}{\Delta_{34}}\Big(a_4\beta_3\big(x_3^2+y_3^2+\Delta(x_4^2+y_4^2)+2\sqrt{\Delta}(x_3x_4+y_3y_4)\big)\\&\qquad+a_3\beta_4\big(x_3^2+y_3^2+\Delta(x_4^2+y_4^2)-2\sqrt{\Delta}(x_3x_4+y_3y_4)\big)\Big)\end{aligned}$$

et

$$\begin{aligned}v&=\frac{1}{\Delta_{12}}\big(a_2\beta_1(x_1^2+y_1^2)-a_1\beta_2(x_2^2+y_2^2)\big)\\&=\frac{1}{\Delta_{34}}\Big(b_4\beta_3\big(x_3^2+y_3^2+\Delta(x_4^2+y_4^2)+2\sqrt{\Delta}(x_3x_4+y_3y_4)\big)\\&\qquad+b_3\beta_4\big(x_3^2+y_3^2+\Delta(x_4^2+y_4^2)-2\sqrt{\Delta}(x_3x_4+y_3y_4)\big)\Big)\end{aligned}$$

tels que

$$F_1(u,v) = \beta_1(x_1^2+y_1^2), \qquad F_2(u,v) = \beta_2(x_2^2+y_2^2),$$
$$F_3(u,v) = \beta_3\beta_4[(x_3^2-y_3^2-\Delta(x_4^2-y_4^2))^2+(x_3y_3-\Delta y_3y_4)^2].$$

On remarque en particulier que la quantité $F_3(u,v)/(\beta_3\beta_4)$ est bien une somme de deux carrés, mais une somme de deux carrés particulière puisqu'il s'agit d'une norme de L sur $\mathbb{Q}$. On note alors $\alpha_{\boldsymbol{\beta}}$ la racine carrée positive de $\beta_1\beta_2\beta_3'$ et $n = z_{\boldsymbol{\beta}}\overline{z_{\boldsymbol{\beta}}}$ et on considère

$$\begin{cases} x+iy = z_{\boldsymbol{\beta}}\alpha_{\boldsymbol{\beta}}(z_0)^2\displaystyle\prod_{j=1}^4 z_j, \\ x-iy = \overline{z_{\boldsymbol{\beta}}}\alpha_{\boldsymbol{\beta}}(\overline{z_0})^2\displaystyle\prod_{j=1}^4 \overline{z_j}, \\ t = z_0\overline{z_0}, \end{cases}$$

où l'on a posé $z_j = x_j + iy_j$ pour $j \in \{0,1,2\}$ et

$$z_3 = (x_3^2-y_3^2-\Delta(x_4^2-y_4^2)) + i(x_3y_3-\Delta y_3y_4).$$

Alors $x^2+y^2 = t^2F(u,v)$ et $(x,y,t,u,v) \in \mathcal{T}_{\mathrm{spl}}(k)$, ce qui permet de définir $\pi_{\boldsymbol{\beta}}$.

Lemme 7.3. *Pour tout $\boldsymbol{\beta} \in \mathcal{B}$, la variété $\mathcal{T}_{\boldsymbol{\beta}}$ équipée du morphisme $\pi_{\boldsymbol{\beta}}$ et de l'action naturelle de T_{NS} définie de la même façon que dans* [7, section 4] *est un torseur versel pour S et*

$$S(\mathbb{Q}) = \bigsqcup_{\boldsymbol{\beta}\in\mathcal{B}_M^{\Sigma}} \pi_{\boldsymbol{\beta}}(\mathcal{T}_{\boldsymbol{\beta}}(\mathbb{Q})).$$

Démonstration. On utilisera les notations $\Delta_{ij} = \mathrm{Res}(F_i,F_j)$ et $\Delta_{43} = -\Delta_{34}$ qui généralisent (2.1) et (7.1). En particulier, $\Delta_{ij} = -\Delta_{ji}$. D'après [7, section 4] et en utilisant le formalisme développé dans [33, exemple 2.4.3], on sait que sur $\overline{\mathbb{Q}}$, un anneau de Cox de S est donné par

(7.5)
$$\overline{R} = \overline{\mathbb{Q}}[Z_i^+, Z_i^- \mid 0 \le i \le 4]/(\Delta_{jk}Z_i^+Z_i^- + \Delta_{ki}Z_j^+Z_j^- + \Delta_{ij}Z_k^+Z_k^-)_{1\le i<j<k\le 4}$$

où $\mathrm{div}(Z_0^{\pm}) = E^{\pm}$ et $\mathrm{div}(Z_i^{\pm}) = D_i^{\pm}$ pour $i \in [\![1,4]\!]$. Plus précisément,

$$(\Delta_{jk}Z_i^+Z_i^- + \Delta_{ki}Z_j^+Z_j^- + \Delta_{ij}Z_k^+Z_k^-)_{1\le i<j<k\le 4} = (P_{1,2,3}, P_{1,2,4})$$

où l'on note $P_{i,j,k}$ la forme quadratique $\Delta_{jk}Z_i^+Z_i^- + \Delta_{ki}Z_j^+Z_j^- + \Delta_{ij}Z_k^+Z_k^-$. Considérons alors les variables invariantes sous $\mathcal{G}$ suivantes :

$$X_k = \frac{Z_k^+ + Z_k^-}{2}, \qquad Y_k = \frac{Z_k^+ - Z_k^-}{2i}$$

pour $k \in \{0,1,2\}$ et

$$X_3 = \frac{Z_3^+ + Z_4^+ + Z_3^- + Z_4^-}{4}, \quad Y_3 = \frac{Z_3^+ - Z_3^- + Z_4^+ - Z_4^-}{4i},$$
$$X_4 = \frac{Z_3^+ - Z_4^+ + Z_3^- - Z_4^-}{4\sqrt{\Delta}}, \quad Y_4 = \frac{Z_3^+ + Z_4^- - Z_3^- - Z_4^+}{4\sqrt{\Delta}i}.$$

Par exemple, lorsque $a_3' \neq 0$, puisque

$$\phi_1^{(1,1,1,1)} = a_3' P_{1,2,4} - a_4' P_{1,2,3}, \quad \phi_2^{(1,1,1,1)} = \frac{1}{a_3'}(\Delta_{34} P_{1,2,3} + b_3' \phi_1^{(1,1,1,1)}),$$

une descente galoisienne garantit qu'un anneau de Cox pour S sur $\mathbb{Q}$ est donné par

$$R = \mathbb{Q}[X_i, Y_i \mid 0 \leq i \leq 4]/(\phi_1^{(1,1,1,1)}, \phi_2^{(1,1,1,1)}).$$

Par [36, corollaire 2.3.9], un torseur versel est unique à twist près par un élément de $H^1(\mathbb{Q}, \operatorname{Pic}(S_{\overline{\mathbb{Q}}}))$. On peut alors montrer en adaptant la preuve de [33, proposition 2.69] ou en utilisant [16, théorème 7.1] que pour tout cocycle $c \in H^1(\mathbb{Q}, \operatorname{Pic}(S_{\overline{\mathbb{Q}}}))$, l'anneau de Cox tordu par c est de la forme

$$R^c = \mathbb{Q}[X_i, Y_i \mid 0 \leq i \leq 4]/(\phi_1^{\boldsymbol{\beta}}, \phi_2^{\boldsymbol{\beta}})$$

pour un certain $\boldsymbol{\beta} \in \mathcal{B}$.

Finalement, il reste à établir le dernier point:

$$S(\mathbb{Q}) = \bigsqcup_{\boldsymbol{\beta} \in \mathcal{B}_M^{\Sigma}} \pi_{\boldsymbol{\beta}}(\mathcal{T}_{\boldsymbol{\beta}}(\mathbb{Q})).$$

Soit $P \in S(\mathbb{Q})$. Il existe alors un unique $(y,z,t,u,v) \in \mathbb{Z}^4$ tel que

$$\begin{cases} (y,z,t) = (u,v) = 1, \\ t > 0, \\ F_1(u,v) \geq 0, \\ t^2 F_1(u,v) F_2(u,v) F_3(u,v) = y^2 + z^2, \end{cases}$$

et $\pi_{\mathrm{spl}}((y,z,t,u,v)) = P$ avec π_{spl} l'application $\pi_{\mathrm{spl}} : \mathcal{T}_{\mathrm{spl}} \to S$ définie dans [7, définition 4.1]. Lorsque $F_1(u,v)F_2(u,v)F_3(u,v) > 0$, il existe un unique triplet $(\varepsilon_1, \varepsilon_2, \varepsilon_3) \in \{-1,+1\}^3$ avec $\varepsilon_1 = 1$ tel que $\varepsilon_1\varepsilon_2\varepsilon_3 = 1$ et

$$\varepsilon_i F_i(u,v) > 0.$$

Le fait que $F_1(u,v)F_2(u,v)F_3(u,v)$ soit une somme de deux carrés implique que, lorsque $p \equiv 3 \pmod 4$, on a

$$\begin{aligned} \nu_p(F_1(u,v)F_2(u,v)F_3(u,v)) &= \nu_p(F_1(u,v)) + \nu_p(F_2(u,v)) + \nu_p(F_3(u,v)) \\ &\equiv 0 \pmod 2. \end{aligned}$$

On pose alors

$$m_1 = \prod_{\substack{p\equiv 3 \pmod 4\\ \nu_p(F_1(u,v))\equiv 1 \pmod 2}} p, \quad m_2 = \prod_{\substack{p\equiv 3 \pmod 4\\ \nu_p(F_2(u,v))\equiv 1 \pmod 2}} p, \quad m_3 = \prod_{\substack{p\equiv 3 \pmod 4\\ \nu_p(F_3(u,v))\equiv 1 \pmod 2}} p,$$

de sorte que $m_i \mid F_i(u,v)$. On en déduit que si $p \mid m_1$, une seule des deux valeurs $\nu_p(F_2(u,v))$ et $\nu_p(F_3(u,v))$ est impaire. Donc $p \mid m_1$ et $p \mid m_2$ par exemple, et puisque $(u,v)=1$, cela implique que $p \mid \Delta_{12}^{(3)}$, si bien que

$$m_1 \mid [\Delta_{12}^{(3)}, \Delta_{13}^{(3)}], \quad m_2 \mid [\Delta_{12}^{(3)}, \Delta_{23}^{(3)}], \quad m_3 \mid [\Delta_{13}^{(3)}, \Delta_{23}^{(3)}], \quad (m_i, m_j) \mid \Delta_{ij}^{(3)},$$

et

$$\nu_p\left(\frac{F_i(u,v)}{m_i}\right) \equiv 0 \pmod 2$$

pour tous les nombres premiers $p \equiv 3 \pmod 4$. De plus, $m_1m_2m_3$ est un carré. Si par exemple $F_1(u,v)=0$, on note $\varepsilon_1 m_1$ l'unique entier sans facteur carré tel que $\varepsilon_1\varepsilon_2\varepsilon_3 m_1m_2m_3$ soit un carré.

On introduit alors $\beta_1 = \varepsilon_1 m_1$ et $\beta_2 = \varepsilon_2 m_2$. On note g le plus petit diviseur de $F_3(u,v)$ tel que $\varepsilon_3 F_3(u,v)/g$ soit une norme de L. Nécessairement, en posant $\beta_3' = \varepsilon_3 m_3$, on a $\beta_3' \mid g$ et on peut écrire $g = \beta_3' n$. Par définition de β_3', on constate alors que n est une norme sur $\mathbb{Q}[i]$. De plus, g est une norme sur K, on peut donc écrire $g = \beta_3\beta_4 = \beta_3' n$ avec $\tau(\beta_3) = \beta_4$. Ainsi, $\boldsymbol{\beta} \in \mathcal{B}_M^{\Sigma}$ et $(y,z,t,u,v) \in \hat{\pi_{\boldsymbol{\beta}}}(\mathcal{T}_{\boldsymbol{\beta}})$. On peut montrer que $\boldsymbol{\beta}$ est unique comme dans la preuve de [7, proposition 4.7]. ∎

En notant $\mathcal{X}_{\boldsymbol{\beta}}$ le sous-schéma de $\mathbb{A}^8_{\mathbb{Q}} = \mathrm{Spec}(\mathbb{Q}[X_i, Y_i \mid 1 \le i \le 4])$ défini par les équations $\phi_1^{\boldsymbol{\beta}}$ et $\phi_2^{\boldsymbol{\beta}}$, on constate donc que $\mathcal{T}_{\boldsymbol{\beta}} = \mathcal{X}_{\boldsymbol{\beta}} \times \mathbb{A}^2_{\mathbb{Q}}$. En notant $\mathcal{X}^{\circ}_{\boldsymbol{\beta}}$ le complémentaire de l'origine dans $\mathcal{X}_{\boldsymbol{\beta}}$, on a alors un isomorphisme entre l'intersection complète de $\mathbb{A}^{10}_{\mathbb{Q}} \setminus \{0\}$ donnée par les équations

$$\begin{aligned} &F_1(u,v) = \beta_1(X_1^2+Y_1^2), \qquad F_2(u,v) = \beta_2(X_2^2+Y_2^2),\\ &F_3(u,v) = \beta_3\beta_4\big[\big(X_3^2 - Y_3^2 - \Delta(X_4^2-Y_4^2)\big)^2 + (X_3Y_3 - \Delta X_4Y_4)^2\big], \end{aligned}$$

et le schéma $\mathcal{X}^{\circ}_{\boldsymbol{\beta}}$. Or, lors de la preuve de la conjecture de Manin, on s'est ramené à un problème de comptage sur certaines variétés de la forme (2.4)

$$F_i(u,v) = \beta_i(X_i^2+Y_i^2).$$

On n'a par conséquent pas utilisé une descente sur les torseurs versels mais sur des torseurs d'un type différent que l'on explicite dans la section suivante lors de notre preuve de la conjecture de Manin. Cette description facilitera grandement le traitement de la constante afin d'établir que celle-ci correspond à la prédiction de Peyre. De plus, il apparaît difficile *a priori* d'obtenir un système de représentants des classes d'isomorphisme de torseurs versels et de décrire précisément les ensembles du type $\pi_{\boldsymbol{\beta}}(\mathcal{T}_{\boldsymbol{\beta}}(\mathbb{Q}))$. En effet, pour ce faire, il faut caractériser les normes de l'extension biquadratique L.

Il est à noter plus généralement que dans les cas des articles [7], [6] et [8], le même type de calculs fournissent que le seul cas de la conjecture de Manin pour les surfaces de Châtelet où l'on utilise une méthode de descente sur les torseurs versels est celui pour lequel F est scindé. Dans tous les autres cas, on utilise une descente sur des torseurs d'un type différent dont la construction est analogue à celle de la section qui suit.

7.3. Les torseurs utilisés dans la preuve de la conjecture de Manin. On décrit explicitement dans cette section les torseurs qui sont utilisés dans la preuve du Théorème 1.1, c'est-à-dire les torseurs qui correspondent aux variétés de la forme (2.4). Cette description repose sur le formalisme développé dans [33] et [22].

Soit T le tore algébrique dont le groupe des caractères est donné par

$$\hat{T} = [E^+]\mathbb{Z} \oplus [D_1^+]\mathbb{Z} \oplus [D_2^+]\mathbb{Z} \oplus [D_3^+ + D_4^+]\mathbb{Z} \oplus [D_1^-]\mathbb{Z} \tag{7.6}$$

ainsi que l'injection $\lambda : \hat{T} \hookrightarrow \mathrm{Pic}(S_{\overline{\mathbb{Q}}})$.

Lemme 7.4. *La $\mathbb{Q}$-algèbre $R' := \mathbb{Q}[X_i, Y_i \mid 0 \leq i \leq 3]/(f_1)$ avec*

$$f_1 = X_3^2 + Y_3^2 - \frac{1}{\varDelta_{12}^2}\big(\varDelta_{23}(X_1^2+Y_1^2) + \varDelta_{31}(X_2^2+Y_2^2)\big) \times \big(\varDelta_{24}(X_1^2+Y_1^2) + \varDelta_{41}(X_2^2+Y_2^2)\big)$$

est un anneau de Cox de S de type λ défini en (7.6).

Démonstration. D'après (7.4), on a $[\omega_S^{-1}] \in \lambda(\hat{T})$ et ainsi l'image de λ contient la classe d'un diviseur ample. Suivant la preuve de [33, proposition 2.71], un anneau de Cox R' de type λ est donné par l'anneau des invariants sous le groupe de Galois $\mathcal{G}$ de

$$\bigoplus_{m \in \hat{T}} \overline{R}_m,$$

où $\overline{R}$ a été défini en (7.5) et $\overline{R}_m$ correspond aux éléments homogènes de degré m de $\overline{R}$. Supposons $m \in \hat{T}$ donné tel que

$$m = [a_0 E^+ + a_1 D_1^+ + a_2 D_2^+ + a_3(D_3^+ + D_4^+) + a_4 D_1^-]$$

avec $a_i \in \mathbb{Z}$. Pour déterminer $\overline{R}_m$, on cherche à résoudre le système linéaire donné par

$$\Big[e_0^+ E^+ + e_0^- E^- + \sum_{j=1}^4 (e_j^+ D_j^+ + e_j^- D_j^-)\Big] = [a_0 E^+ + a_1 D_1^+ + a_2 D_2^+ + a_3(D_3^+ + D_4^+) + a_4 D_1^-],$$

où $e_j^{\pm} \geq 0$ pour tout j. Grâce aux relations (7.2) et (7.3), ce dernier est équivalent à

$$\begin{cases} a_0 = e_0^+ + e_0^-, \\ a_1 = \sum_{j=2}^4 e_j^- + e_1^+ - e_0^-, \\ a_2 = e_2^+ - e_2^- + e_0^-, \\ a_3 = e_3^+ - e_3^- + e_0^- = e_4^+ - e_4^- + e_0^-, \\ a_4 = \sum_{j=1}^4 e_j^- - 2e_0^-. \end{cases}$$

En résolvant ce système en les $e_j^{\pm}$ pour $0 \leq j \leq 4$, il vient que $\overline{R'}$ est isomorphe au sous-anneau de $\overline{R}$ engendré par les variables

$$Z_0^{\pm}, \quad Z_1^{\pm}, \quad Z_2^{\pm}, \quad Z_3^+ Z_4^+, \quad Z_3^- Z_4^-$$

vérifiant la relation suivante (d'après (7.5)) :

$$\begin{aligned}(Z_3^+ Z_4^+)(Z_3^- Z_4^-) &= (Z_3^+ Z_3^-)(Z_4^+ Z_4^-) \\ &= \frac{1}{\Delta_{12}^2}(\Delta_{23} Z_1^+ Z_1^- + \Delta_{31} Z_2^+ Z_2^-)(\Delta_{24} Z_1^+ Z_1^- + \Delta_{41} Z_2^+ Z_2^-).\end{aligned}$$

Cette dernière relation est bien invariante par le groupe de Galois $\mathcal{G}$. En considérant les variables $\mathcal{G}$-invariantes suivantes :

$$X_k = \frac{Z_k^+ + Z_k^-}{2}, \qquad Y_k = \frac{Z_k^+ - Z_k^-}{2i}$$

pour $k \in \{0, 1, 2\}$ et

$$X_3 = \frac{Z_3^+ Z_4^+ + Z_3^- Z_4^-}{2}, \qquad Y_3 = \frac{Z_3^+ Z_4^+ - Z_3^- Z_4^-}{2i},$$

il vient alors bien

$$R' = \mathbb{Q}[X_i, Y_i \mid 0 \leq i \leq 3]/(f_1). \ \blacksquare$$

À nouveau d'après [36, corollaire 2.3.9], un torseur de type λ est unique à twist près par un élément de $H^1(\mathbb{Q}, \hat{T})$. Le lemme suivant explicite ce groupe de cohomologie.

Lemme 7.5. *On a la série d'isomorphismes*

$$H^1(\mathbb{Q}, \hat{T}) \cong H^1(\mathrm{Gal}(\mathbb{Q}[i]/\mathbb{Q}), \hat{T}) \cong \mathbb{Z}/2\mathbb{Z}.$$

Démonstration. Le point clé concernant les torseurs de type λ est que l'action de la conjugaison τ dans K est triviale si bien que

$$H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}[i]), \hat{T}) = \{0\}.$$

Ainsi, la suite exacte de restriction-inflation

$$0 \to H^1(\mathrm{Gal}(\mathbb{Q}[i]/\mathbb{Q}), \hat{T}) \to H^1(\mathbb{Q}, \hat{T}) \to H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}[i]), \hat{T})$$

fournit l'isomorphisme $H^1(\mathbb{Q}, \hat{T}) \cong H^1(\mathrm{Gal}(\mathbb{Q}[i]/\mathbb{Q}), \hat{T})$. Puisque le groupe $\mathrm{Gal}(\mathbb{Q}[i]/\mathbb{Q})$ est cyclique d'ordre 2 engendré par la conjugaison complexe σ, le groupe de cohomologie $H^1(\mathrm{Gal}(\mathbb{Q}[i]/\mathbb{Q}), \hat{T})$ coïncide avec l'homologie du complexe

$$\hat{T} \xrightarrow{\mathrm{Id}+\sigma} \hat{T} \xrightarrow{\mathrm{Id}-\sigma} \hat{T}.$$

Autrement dit,

$$H^1(\mathrm{Gal}(\mathbb{Q}[i]/\mathbb{Q}), \hat{T}) \cong \mathrm{Ker}(\sigma + \mathrm{Id})/\mathrm{Im}(\mathrm{Id} - \sigma).$$

On obtient alors aisément le fait que $\mathrm{Ker}(\sigma + \mathrm{Id})$ est engendré par

$$[D_1^+] - [D_1^-], \quad [D_1^+] - [D_2^+], \quad 2[D_1^+] - [D_3^+ + D_4^+],$$

et que $\mathrm{Im}(\mathrm{Id} - \sigma)$ est engendré par

$$[D_1^+] - [D_1^-], \quad 2[D_2^+] - [D_1^+] - [D_1^-], \quad 2[D_3^+ + D_4^+] - 2[D_1^+] - 2[D_1^-].$$

Il vient alors immédiatement que $H^1(\mathrm{Gal}(\mathbb{Q}[i]/\mathbb{Q}), \hat{T}) \cong \mathbb{Z}/2\mathbb{Z}$ engendré par la classe de $[D_1^+] - [D_2^+]$. ∎

On est désormais en mesure de décrire tous les anneaux de Cox de S de type λ. On s'inspire ici des deux preuves de [33, propositions 2.69–2.70]. Tout élément de $H^1(\mathbb{Q}, \hat{T})$ est représenté par un cocycle $c : \mathrm{Gal}(\mathbb{Q}[i]/\mathbb{Q}) \to \hat{T}$, lui-même déterminé par l'image $c_\sigma \in \mathrm{Hom}_{\mathbb{Z}}(T, \mathbb{Q}[i]^\times)$ de la conjugaison complexe.

Lemme 7.6. *Tout anneau de Cox pour S de type λ est isomorphe à une $\mathbb{Q}$-algèbre de la forme*

$$R'_{\mathbf{n}} := \mathbb{Q}[X_i, Y_i \mid 0 \leq i \leq 3]/(f_1^{\mathbf{n}})$$

avec

$$f_1^{\mathbf{n}} = n_3(X_3^2 + Y_3^2) - \frac{1}{\varDelta_{12}^2}\big(\varDelta_{23} n_1(X_1^2 + Y_1^2) + \varDelta_{31} n_2(X_2^2 + Y_2^2)\big) \times \big(\varDelta_{24} n_1(X_1^2 + Y_1^2) + \varDelta_{41} n_2(X_2^2 + Y_2^2)\big) \tag{7.7}$$

et $\mathbf{n} = (n_1, n_2, n_3) \in (\mathbb{Z} \smallsetminus \{0\})^3$ tels que $n_1 n_2 n_3$ soit une somme de deux carrés.

Démonstration. On sait que, pour tout anneau de Cox R'_λ pour S de type λ, il existe un cocycle $c : \mathrm{Gal}(\mathbb{Q}[i]/\mathbb{Q}) \to \hat{T}$ tel que R'_λ soit un twist de R' défini en (7.4). D'après [33, proposition 2.41], l'action de la conjugaison complexe sur $\overline{R'}$ est la suivante :

$$\sigma(Z_0^-) = c_\sigma([E^+]) Z_0^+, \qquad \forall j \in \{1, 2\}, \quad \sigma(Z_j^-) = c_\sigma([D_j^+]) Z_j^+,$$
$$\sigma(Z_3^- Z_4^-) = c_\sigma([D_3^+ + D_4^+]) Z_3^+ Z_4^+.$$

En prenant les nouvelles variables suivantes, invariantes sous l'action du groupe de Galois $\mathrm{Gal}(\mathbb{Q}[i]/\mathbb{Q})$:

$$X_0 = \frac{c_\sigma([E^+])Z_0^+ + Z_0^-}{2}, \quad Y_0 = \frac{c_\sigma([E^+])Z_0^+ - Z_0^-}{2i},$$
$$X_k = \frac{c_\sigma([D_k^+])Z_k^+ + Z_k^-}{2}, \quad Y_k = \frac{c_\sigma([D_k^+])Z_k^+ - Z_k^-}{2i},$$

pour $k \in \{1,2\}$ et

$$X_3 = \frac{c_\sigma([D_3^+ + D_4^+])Z_3^+Z_4^+ + Z_3^-Z_4^-}{2},$$
$$Y_3 = \frac{c_\sigma([D_3^+ + D_4^+])Z_3^+Z_4^+ - Z_3^-Z_4^-}{2i},$$

il vient

$$R'_\lambda \cong \mathbb{Q}[X_i, Y_i \mid 0 \leq i \leq 3]/(f_1^c)$$

avec

$$f_1^c = n_{31}^c(X_3^2 + Y_3^2) - \frac{1}{\Delta_{12}^2}\big(\Delta_{23}(X_1^2 + Y_1^2) + \Delta_{31}n_{21}^c(X_2^2 + Y_2^2)\big)$$
$$\times \big(\Delta_{24}(X_1^2 + Y_1^2) + \Delta_{41}n_{21}^c(X_2^2 + Y_2^2)\big)$$

et $n_{21}^c = c_\sigma([D_1^+ - D_2^+])$ et $n_{31}^c = c_\sigma([2D_1^+ - D_3^+ - D_4^+])$. Le fait que c soit un cocycle et les relations (7.2) et (7.3) impliquent que $\sigma(n_{i1}) = n_{i1}$ si bien que $n_{i1} \in \mathbb{Q}^\times$ pour $i \in \{2,3\}$. En écrivant $n_{21}^c = n_2/n_1$ et $n_{31}^c = n_3/{n_1}^2$ pour trois entiers n_1, n_2 et n_3 non nuls, on obtient bien

$$R'_\lambda \cong \mathbb{Q}[X_i, Y_i \mid 0 \leq i \leq 3]/(f_1^{\mathbf{n}}).$$

Pour conclure, il reste à établir le fait que $n_1n_2n_3$ est une somme de deux carrés. On a

$$n_1n_2n_3 = n_1^4 n_{21}^c n_{31}^c.$$

Puisque les conditions de cocycle s'écrivent

$$c_\sigma([E^+])\sigma(c_\sigma([E^-])) = 1, \quad \forall k \in \{1,2\}, \quad c_\sigma([D_k^+])\sigma(c_\sigma([D_k^-])) = 1,$$

et

$$c_\sigma([D_3^+ + D_4^+])\sigma(c_\sigma([D_3^- + D_4^-])) = 1,$$

les relations (7.2) et (7.3) fournissent

$$n_1n_2n_3 = n_1^4 c_\sigma([E^+ + 2D_1^+])\sigma(c_\sigma([E^+ + 2D_1^+]))$$

si bien que $n_1n_2n_3$ est bien une somme de deux carrés. On peut établir plus précisément, en suivant [33, proposition 2.70], qu'étant donné (n_1, n_2, n_3) dans $\mathbb{Q}^\times$, il existe un cocycle $c : \mathrm{Gal}(\mathbb{Q}[i]/\mathbb{Q}) \to \hat{T}$ tel que $n_{21}^c = n_2/n_1$ et $n_{31}^c = n_3/n_1^2$ si, et seulement si, $n_1n_2n_3$ est une somme de deux carrés. ∎

De façon analogue au Lemme 7.3, on voit que pour $\mathbf{n} \in \mathbb{N}^3$ tel que $n_1n_2n_3$ soit une somme de deux carrés, le sous-ensemble constructible $\mathcal{T}_{\mathbf{n}}$ de $\mathbf{A}^8_{\mathbb{Q}} = \mathrm{Spec}(\mathbb{Q}[X_i, Y_i \mid 0 \leq i \leq 3])$ défini par l'équation $f^{\mathbf{n}}$ donnée en (7.7) et les relations

$$\forall i \neq j \in [\![0,3]\!]^4, \qquad ((X_i, Y_i), (X_j, Y_j)) \neq ((0,0),(0,0))$$

est un torseur de type λ au-dessus de S. Pour toute extension finie k de $\mathbb{Q}$ et tout $(x_i, y_i)_{0\leq i\leq 3}$ dans $\mathcal{T}_{\mathbf{n}}(k)$, à l'aide de

$$u = \frac{1}{\Delta_{12}}(b_2n_1(x_1^2+y_1^2) - b_1n_2(x_2^2+y_2^2)),$$
$$v = \frac{1}{\Delta_{12}}(-a_2n_1(x_1^2+y_1^2) + a_1n_2(x_2^2+y_2^2)),$$

on peut définir comme en section précédente un morphisme $\pi_{\mathbf{n}} : \mathcal{T}_{\mathbf{n}} \to S$. Lorsque $\mathbf{n}$ est de la forme

$$\forall i \in [\![1,3]\!], \quad n_i = \varepsilon_i m_i$$

pour un certain $(\boldsymbol{\varepsilon}, \mathbf{m}) \in \Sigma \times M$, on note $\mathcal{T}_{\mathbf{n}} = \mathcal{T}_{\mathbf{m},\boldsymbol{\varepsilon}}$ et $\pi_{\mathbf{n}} = \pi_{\mathbf{m},\boldsymbol{\varepsilon}}$. On peut alors montrer comme lors de la preuve du Lemme 7.3 que

$$S(\mathbb{Q}) = \bigsqcup_{(\boldsymbol{\varepsilon},\mathbf{m})\in\Sigma\times M} \pi_{\mathbf{m},\boldsymbol{\varepsilon}}(\mathcal{T}_{\mathbf{m},\boldsymbol{\varepsilon}}(\mathbb{Q})). \tag{7.8}$$

De plus,

$$\begin{aligned} &\pi_{\mathbf{m},\boldsymbol{\varepsilon}}(\mathcal{T}_{\mathbf{m},\boldsymbol{\varepsilon}}(\mathbb{Q})) \\ &= \left\{ [tu^2 : tuv : tv^2 : x_3 : x_4] \in \mathbb{P}^4_{\mathbb{Q}} \;\middle|\; \begin{array}{l} (t,u,v,x_3,x_4) \in \mathbb{Z}^5, \\ (t,u,v) = (x_3,x_4) = 1, \\ t \geq 0, x_3^2 + x_4^2 = t^2F(u,v), \\ \varepsilon_i F_i(u,v) > 0, \\ \nu_p(F_i(u,v)) - \mu_i \equiv 0 \pmod 2, \\ F_i(u,v) \in \varepsilon_i m_i \mathcal{E} \end{array} \right\} \\ &\sqcup \left\{ [tu^2 : tuv : tv^2 : x_3 : x_4] \in \mathbb{P}^4_{\mathbb{Q}} \;\middle|\; \begin{array}{l} (t,u,v,x_3,x_4) \in \mathbb{Z}^5, \\ (t,u,v) = (x_3,x_4) = 1, \\ t \geq 0, x_3^2 + x_4^2 = t^2F(u,v), \\ \varepsilon_i F_i(-u,-v) > 0, \\ \nu_p(F_i(u,v)) - \mu_i \equiv 0 \pmod 2, \\ F_i(-u,-v) \in \varepsilon_i m_i \mathcal{E} \end{array} \right\}. \end{aligned} \tag{7.9}$$

En effet, un point de S admet exactement deux représentants de la forme $[tu^2 : tuv : tv^2 : x_3 : x_4]$ avec $(t,u,v,x_3,x_4) \in \mathbb{Z}^5$ et $(t,u,v) = (x_3,x_4) = 1$.

À nouveau de la même façon qu'en section précédente, on montre, en notant $\mathcal{Y}_{\mathbf{n}}$ le sous-schéma de $\mathbf{A}^8_{\mathbb{Q}} = \mathrm{Spec}(\mathbb{Q}[X_i, Y_i \mid 1 \leq i \leq 3])$ défini par l'équation $f^{\mathbf{n}}$ donnée en (7.7), que $\mathcal{T}_{\mathbf{n}} = \mathcal{Y}_{\mathbf{n}} \times \mathbf{A}^2_{\mathbb{Q}}$. Si $\mathcal{Y}^\circ_{\mathbf{n}}$ est le complémentaire de l'origine dans $\mathcal{Y}_{\mathbf{n}}$, on a alors un isomorphisme entre l'intersection complète de $\mathbf{A}^8_{\mathbb{Q}} \setminus \{0\}$ donnée par les équations

$$F_i(u,v) = n_i(X_i^2 + Y_i^2) \qquad (1 \leq i \leq 3)$$

et $\mathcal{Y}^\circ_{\mathbf{n}}$. On retrouve ainsi une variété de la forme (2.4) et il s'agit donc bel et bien des torseurs utilisés dans la preuve de la conjecture de Manin en section 6.

On donne alors deux derniers lemmes qui permettent d'exprimer la constante conjecturée par Peyre de manière adéquate à notre traitement du problème de comptage.

Lemme 7.7. *On a* $Ш^1(\mathbb{Q}, T) = \{0\}$ *où*

$$Ш^1(\mathbb{Q}, T) = \mathrm{Ker}\Big(H^1(\mathbb{Q}, T) \to H^1(\mathbb{R}, T) \prod_p H^1(\mathbb{Q}_p, T)\Big).$$

Démonstration. Le théorème de Tate fournit l'accouplement naturel non dégénéré

$$Ш^1(\mathbb{Q}, T) \times Ш^2(\mathbb{Q}, \hat{T}) \to \mathbb{Q}/\mathbb{Z}$$

si bien qu'il suffit d'établir que $Ш^2(\mathbb{Q}, \hat{T}) = \{0\}$. Puisque

$$H^1\big(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}[i]), \hat{T}\big) = \{0\},$$

la suite de restriction-inflation d'ordre 2 fournit

$$0 \to H^2\big(\mathrm{Gal}(\mathbb{Q}[i]/\mathbb{Q}), \hat{T}\big) \to H^2(\mathbb{Q}, \hat{T}) \to H^2\big(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}[i]), \hat{T}\big).$$

Montrons à présent que $H^2(\mathrm{Gal}(\mathbb{Q}[i]/\mathbb{Q}), \hat{T}) = \{0\}$. Le groupe de Galois $\mathrm{Gal}(\mathbb{Q}[i]/\mathbb{Q})$ étant cyclique engendré par la conjugaison complexe σ, il vient que

$$H^2\big(\mathrm{Gal}(\mathbb{Q}[i]/\mathbb{Q}), \hat{T}\big) = \hat{T}^{\langle \sigma \rangle}/\mathrm{Im}(\mathrm{Id} + \sigma) = \mathrm{Ker}(\sigma - \mathrm{Id})/\mathrm{Im}(\mathrm{Id} + \sigma).$$

On établit comme lors de la preuve du Lemme 7.5 que $\mathrm{Ker}(\sigma - \mathrm{Id})$ est de rang 2 engendré par $[D_1^+] + [D_1^-]$ et $[\omega_S^{-1}]$. Or,

$$\begin{aligned} [D_1^+] + [D_1^-] &= (\mathrm{Id} + \sigma)([D_1^+]), \\ [\omega_S^{-1}] &= (\mathrm{Id} + \sigma)([E^+] + 2[D_1^+]), \end{aligned}$$

si bien que $\mathrm{Ker}(\sigma - \mathrm{Id}) = \mathrm{Im}(\mathrm{Id} + \sigma)$ et $H^2(\mathrm{Gal}(\mathbb{Q}[i]/\mathbb{Q}), \hat{T}) = \{0\}$. On a donc le diagramme commutatif

$$\begin{tikzcd}
 & Ш^2(\mathbb{Q},\hat{T}) \arrow[d] & Ш^2(\mathbb{Q}[i],\hat{T}) \arrow[d] \\
0 \arrow[r] & H^2(\mathbb{Q},\hat{T}) \arrow[r] \arrow[d] & H^2(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}[i]),\hat{T}) \arrow[d] \\
 & \prod_{v\in \mathrm{val}(\mathbb{Q})} H^2(\mathbb{Q}_v,\hat{T}) \arrow[r] & \prod_{v\in \mathrm{val}(\mathbb{Q}[i])} H^2(\mathbb{Q}[i]_v,\hat{T})
\end{tikzcd}$$

qui implique que tout élément de $Ш^2(\mathbb{Q},\hat{T})$ appartient à $Ш^2(\mathbb{Q}[i],\hat{T})$. Or, sur $\mathbb{Q}[i]$, on a $\hat{T}\cong\mathbb{Z}^5$ avec action triviale si bien que $Ш^2(\mathbb{Q}[i],\hat{T})=\{0\}$ d'après [35, lemme 1.9], ce qui permet de conclure la preuve. ∎

Lemme 7.8. *On a l'égalité*

$$S(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}(S)}=\bigsqcup_{(\mathbf{m},\boldsymbol{\varepsilon})\in M\times\varSigma}\pi_{\mathbf{m},\boldsymbol{\varepsilon}}(\mathcal{T}_{\mathbf{m},\boldsymbol{\varepsilon}}(\mathbb{A}_{\mathbb{Q}})),$$

où $\mathbb{A}_{\mathbb{Q}}$ désigne l'anneau des adèles de $\mathbb{Q}$.

Démonstration. Tout d'abord, d'après [36, théorème 6.1.2] et le Lemme 7.6, il vient

$$S(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}_\lambda(S)}=\bigcup_{\substack{\mathbf{n}\in\mathbb{N}^3\\ n_1n_2n_3=\square+\square}}\pi_{\mathbf{n}}(\mathcal{T}_{\mathbf{n}}(\mathbb{A}_{\mathbb{Q}})),$$

où $\mathrm{Br}_\lambda(S)=r^{-1}(\lambda_*(H^1(\mathbb{Q},\hat{T})))$, $\lambda_*:H^1(\mathbb{Q},\hat{T})\to H^1(\mathbb{Q},\mathrm{Pic}(S_{\overline{\mathbb{Q}}}))$ est associée à l'injection λ et $r:\mathrm{Br}(S)\to H^1(\mathbb{Q},\mathrm{Pic}(S_{\overline{\mathbb{Q}}}))$ est l'application canonique issue de la suite spectrale de Hochschild–Serre

$$H^p(\mathbb{Q},H^q(S_{\overline{\mathbb{Q}}},\mathbb{G}_{\mathrm{m}}))\to H^{p+q}(S,\mathbb{G}_{\mathrm{m}}).$$

On a ici utilisé le fait que la surface S est géométriquement rationnelle, auquel cas $\mathrm{Br}_1(S)=\mathrm{Br}(S)$.

De la suite exacte courte

$$0\to\hat{T}\to\mathrm{Pic}(S_{\overline{\mathbb{Q}}})\to\mathrm{Pic}(S_{\overline{\mathbb{Q}}})/\hat{T}\to 0$$

on tire la suite exacte

$$(\mathrm{Pic}(S_{\overline{\mathbb{Q}}})/\hat{T})^{\mathcal{G}}\to H^1(\mathbb{Q},\hat{T})\xrightarrow{\lambda_*}H^1(\mathbb{Q},\mathrm{Pic}(S_{\overline{\mathbb{Q}}})).$$

Or, on montre facilement que $\mathrm{Pic}(S_{\overline{\mathbb{Q}}})/\hat{T}$ est de rang 1 engendré par la classe de $[D_3^+]$ si bien que

$$(\mathrm{Pic}(S_{\overline{\mathbb{Q}}})/\hat{T})^{\mathcal{G}}=\{0\}$$

et λ_* est injective. Le Lemme 7.5 et la valeur de $\beta(S)$ impliquent par conséquent

$$\lambda_*(H^1(\mathbb{Q},\hat{T}))=H^1(\mathbb{Q},\mathrm{Pic}(S_{\overline{\mathbb{Q}}})),$$

de sorte que $\mathrm{Br}_\lambda(S) = \mathrm{Br}(S)$.

On a ainsi

$$S(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}(S)} = \bigcup_{\substack{\mathbf{n}\in\mathbb{N}^3\\ n_1n_2n_3=\square+\square}} \pi_\mathbf{n}(\mathcal{T}_\mathbf{n}(\mathbb{A}_\mathbb{Q}))$$

et en particulier

$$\bigcup_{(\mathbf{m},\boldsymbol{\varepsilon})\in M\times\Sigma} \pi_{\mathbf{m},\boldsymbol{\varepsilon}}(\mathcal{T}_{\mathbf{m},\boldsymbol{\varepsilon}}(\mathbb{A}_\mathbb{Q})) \subset S(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}(S)}.$$

D'autre part, d'après [15], il vient $\overline{S(\mathbb{Q})} = S(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}(S)}$ et par continuité de l'application $\mathcal{T}_{\mathbf{m},\boldsymbol{\varepsilon}}(\mathbb{Q}) \to S(\mathbb{Q})$ induite par $\pi_{\mathbf{m},\boldsymbol{\varepsilon}}$ ainsi que (7.8), il s'ensuit

$$\overline{S(\mathbb{Q})} = S(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}(S)} = \bigcup_{(\mathbf{m},\boldsymbol{\varepsilon})\in M\times\Sigma} \pi_{\mathbf{m},\boldsymbol{\varepsilon}}(\overline{\mathcal{T}_{\mathbf{m},\boldsymbol{\varepsilon}}(\mathbb{Q})}) \subset \bigcup_{(\mathbf{m},\boldsymbol{\varepsilon})\in M\times\Sigma} \pi_{\mathbf{m},\boldsymbol{\varepsilon}}(\mathcal{T}_{\mathbf{m},\boldsymbol{\varepsilon}}(\mathbb{A}_\mathbb{Q})),$$

si bien qu'on peut conclure à l'égalité

$$S(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}(S)} = \bigcup_{(\mathbf{m},\boldsymbol{\varepsilon})\in M\times\Sigma} \pi_{\mathbf{m},\boldsymbol{\varepsilon}}(\mathcal{T}_{\mathbf{m},\boldsymbol{\varepsilon}}(\mathbb{A}_\mathbb{Q})).$$

Suivant alors l'argument utilisé dans [34, preuve du lemme 6.17], on a que tout point de $S(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}(S)}$ appartient à exactement $\#\text{Ш}^1(\mathbb{Q},T)$ ensembles de la forme $\pi_{\mathbf{m},\boldsymbol{\varepsilon}}(\mathcal{T}_{\mathbf{m},\boldsymbol{\varepsilon}}(\mathbb{A}_\mathbb{Q}))$ avec $(\mathbf{m},\boldsymbol{\varepsilon}) \in M\times\Sigma$. Le Lemme 7.7 permet alors d'en déduire que l'union est disjointe et de conclure la preuve. ∎

7.4. Expression de la constante de Peyre. Le Lemme 7.8 fournit

$$c_S = \alpha(S)\beta(S) \sum_{\substack{\boldsymbol{\varepsilon}\in\Sigma\\ \mathbf{m}\in M}} \omega_H(\pi_{\boldsymbol{\varepsilon},\mathbf{m}}(\mathcal{T}_{\boldsymbol{\varepsilon},\mathbf{m}}(\mathbb{A}_\mathbb{Q}))).$$

On a $\alpha(S)\beta(S) = 1$ et on écrit

$$\omega_H(\pi_{\boldsymbol{\varepsilon},\mathbf{m}}(\mathcal{T}_{\boldsymbol{\varepsilon},\mathbf{m}}(\mathbb{A}_\mathbb{Q}))) = \omega_\infty(\boldsymbol{\varepsilon},\mathbf{m}) \prod_p \omega_p(\boldsymbol{\varepsilon},\mathbf{m}),$$

où, en passant comme dans [6] aux densités sur le torseur intermédiaire $\mathcal{T}_{\mathrm{spl}}$ défini par (6.3) et au vu de (7.9), on a

$$\omega_p(\boldsymbol{\varepsilon},\mathbf{m}) = \lim_{n\to\infty} \frac{1}{p^{4n}} \# \left\{ (u,v,y,z,t) \in (\mathbb{Z}/p^n\mathbb{Z})^5 \;\middle|\; \begin{array}{l} F(u,v) \equiv y^2+z^2 \pmod{p^n}, \\ p\nmid(u,v),\ p\nmid(y,z,t), \\ 2|\nu_p(F_i(u,v)) - \mu_i \end{array} \right\}$$

pour $p \neq 2$. Pour tout entier d et $F \in \mathbb{Z}[x_1,x_2]$, on introduit alors

$$\rho^*(d) = \rho^*(d;F) = \#\{\mathbf{x} \in [0,d[^2 \mid d \mid F(\mathbf{x}),\ (x_1,x_2,d)=1\}.$$

Exactement le même type de raisonnements que dans [8, section 8.2] conduit, lorsque $p \nmid \Delta_{12}^{(3)}\Delta_{13}^{(3)}\Delta_{23}^{(3)}$, aux expressions

$$\omega_p(\boldsymbol{\varepsilon},\mathbf{m}) = \left(1-\frac{1}{p^2}\right)\left(1-\frac{1}{p^2}+\sum_{\nu\geq 1}\frac{\chi(p^\nu)\rho^*(p^\nu;F)}{p^{2\nu}}\right)$$

lorsque $p \equiv 3 \pmod 4$, et

$$\omega_p(\boldsymbol{\varepsilon},\mathbf{m}) = \left(1-\frac{1}{p^2}\right)^2 + \left(1-\frac{1}{p}\right)^2\sum_{\nu\geq 1}\frac{\chi(p^\nu)\rho^*(p^\nu;F)}{p^{2\nu}}$$

lorsque $p \equiv 1 \pmod 4$. En particulier, $\omega_p(\boldsymbol{\varepsilon},\mathbf{m}) = \omega_p$ ne dépend ni de $\boldsymbol{\varepsilon}$ ni de $\mathbf{m}$. Dans le cas $p|\Delta_{12}^{(3)}\Delta_{13}^{(3)}\Delta_{23}^{(3)}$ et $p \equiv 3 \pmod 4$, on a $(t,p)=1$ et donc

$$\omega_p(\boldsymbol{\varepsilon},\mathbf{m}) \\ = \lim_{n\to\infty}\frac{1-\frac{1}{p}}{p^{3n}}\#\left\{(u,v,y,z)\in(\mathbb{Z}/p^n\mathbb{Z})^4 \;\middle|\; \begin{array}{l} F(u,v)\equiv y^2+z^2 \pmod{p^n}, \\ p\nmid (u,v), \\ 2|\nu_p(F_i(u,v))-\mu_i \end{array}\right\}.$$

Pour $p=2$, on a

$$\omega_2(\boldsymbol{\varepsilon},\mathbf{m}) \\ = \lim_{n\to\infty}\frac{1}{2^{4n}}\#\left\{(u,v,y,z,t)\in(\mathbb{Z}/2^n\mathbb{Z})^5 \;\middle|\; \begin{array}{l} F(u,v)\equiv y^2+z^2 \pmod{2^n}, \\ 2\nmid (u,v),\ 2\nmid (y,z,t), \\ F_i(u,v)\in \varepsilon_i m_i\mathcal{E}_{2^n} \end{array}\right\} \\ + \lim_{n\to\infty}\frac{1}{2^{4n}}\#\left\{(u,v,y,z,t)\in(\mathbb{Z}/2^n\mathbb{Z})^5 \;\middle|\; \begin{array}{l} F(u,v)\equiv y^2+z^2 \pmod{2^n}, \\ 2\nmid (u,v),\ 2\nmid (y,z,t), \\ F_i(-u,-v)\in \varepsilon_i m_i\mathcal{E}_{2^n} \end{array}\right\}.$$

On a également $(2,t)=1$ et donc, grâce au Lemme 5.1, on aboutit à l'expression

$$\omega_2(\boldsymbol{\varepsilon},\mathbf{m}) = 2\lim_{n\to\infty}2^{-2n}\#\left\{(u,v)\in(\mathbb{Z}/2^n\mathbb{Z})^2 \;\middle|\; \begin{array}{l} 2\nmid (u,v), \\ F_i(u,v)\in \varepsilon_i m_i\mathcal{E}_{2^n} \end{array}\right\}.$$

Noter ici qu'on a une dépendance en $\boldsymbol{\varepsilon}$ et en $\mathbf{m}$.

Enfin on traite le cas de la densité archimédienne. Grâce à la symétrie du problème, on peut se restreindre à $y,z>0$. En utilisant une forme de Leray en paramétrant en z, on obtient

$$\omega_\infty(\boldsymbol{\varepsilon},\mathbf{m}) = 4\lim_{B\to\infty}\frac{1}{B\log(B)}\int_D \frac{du\,dv\,dt\,dy}{2\sqrt{t^2F(u,v)-y^2}}$$

avec

$$D=\left\{(u,v,y,t)\in\mathbb{R}^4 \;\middle|\; \begin{array}{l}(u,v)\in R^{(\varepsilon_1,\varepsilon_2,\varepsilon_3)}(\sqrt{B/t})\sqcup R^{(-\varepsilon_1,-\varepsilon_2,\varepsilon_3)}(\sqrt{B/t}),\\ 0<y<t\sqrt{F(u,v)},\ 1<t<B\end{array}\right\}.$$

La formule (5.2) fournit alors immédiatement

$$\omega_\infty(\boldsymbol{\varepsilon},\mathbf{m})=\pi\big(\mathrm{Vol}(R^{(\varepsilon_1,\varepsilon_2,\varepsilon_3)}(1))+\mathrm{Vol}(R^{(-\varepsilon_1,-\varepsilon_2,\varepsilon_3)}(1))\big)=2\pi\,\mathrm{vol}(\mathcal{R}),$$

qui ne dépend que de $\boldsymbol{\varepsilon}$ mais pas de $\mathbf{m}$. On obtient ainsi l'égalité

$$c_S=\sum_{\substack{\boldsymbol{\varepsilon}\in\Sigma\\ \mathbf{m}\in M}}2\pi\,\mathrm{vol}(\mathcal{R})\prod_p\omega_p(\boldsymbol{\varepsilon},\mathbf{m}). \tag{7.10}$$

7.5. Transformation de la constante c_0. On revient dans cette section à l'expression de la constante c_0 obtenue grâce au Théorème 6.1 que l'on met sous une forme similaire à celle de c_S en (7.10). On réécrit cette constante sous la forme

$$\begin{aligned}c_0=\frac{\pi^2}{2^4}\sum_{d\in\mathcal{D}}\frac{\mu(d)r_0(d)\varphi^\dagger(d)}{d}\sum_{\boldsymbol{\varepsilon}\in\Sigma}\mathrm{vol}(\mathcal{R})\\ \times\sum_{\substack{\mathbf{d},\mathbf{d}'\in\mathcal{D}^3\\ d=d_1d_2d_3,d_i'\mid\Delta_{jk}}}\sum_{\mathbf{m}\in M}\mu(d_1'd_2')\mu(d_3')\sum_{\substack{k_4k_1k_1'\mid\gcd(\Delta_{23},d)\\ k_4k_2k_2'\mid\gcd(\Delta_{13},d)\\ k_4k_3k_3'\mid\gcd(\Delta_{12},d)}}\\ \times\sum_{\substack{k_4k_4'\mid\gcd(\Delta_{12},\Delta_{13},\Delta_{23},d)\\ k_5k_5'\mid\gcd(\Delta_{12},d_1'd_2')}}\frac{\mu(k_1')\mu(k_2')\mu(k_3')\mu(k_4')\mu(k_5')}{3^{\omega(k_4)}2^{\omega(k_5)+\omega(k_1)+\omega(k_2)+\omega(k_3)}}\sigma_*^{\boldsymbol{\varepsilon}}(\mathbf{e},\mathbf{E}),\end{aligned} \tag{7.11}$$

où

$$\sigma_*^{\boldsymbol{\varepsilon}}(\mathbf{e},\mathbf{E})=\sum_{e=1}^{\infty}\frac{\mu(e)}{e^2}\sigma^{\boldsymbol{\varepsilon}}(\mathbf{e},\mathbf{E},e). \tag{7.12}$$

Par multiplicativité en e de la quantité $\sigma^{\boldsymbol{\varepsilon}}(\mathbf{e},\mathbf{E},e)$, on peut écrire $\sigma_*^{\boldsymbol{\varepsilon}}(\mathbf{e},\mathbf{E})$ sous forme d'un produit eulérien

$$\sigma_*^{\boldsymbol{\varepsilon}}(\mathbf{e},\mathbf{E})=\prod_p\sigma_{*,p}^{\boldsymbol{\varepsilon}}(\mathbf{e},\mathbf{E}). \tag{7.13}$$

Pour $p>2$, le facteur eulérien est donné par

$$\sigma_{*,p}^{\boldsymbol{\varepsilon}}(\mathbf{e},\mathbf{E})=\left(1-\frac{\chi(p)}{p}\right)^3\sum_{\boldsymbol{\nu}\in\mathbb{N}^3}\frac{\chi(p)^{\nu_1+\nu_2+\nu_3}\tilde{\rho}(p^{N_1},p^{N_2},p^{N_3};F_1,F_2,F_3)}{p^{2(N_1+N_2+N_3+1)}}$$

où les N_i sont définis lors du Lemme 6.4 et avec

$$\tilde{\rho}(p^{N_1},p^{N_2},p^{N_3};F_1,F_2,F_3)=\#\{\mathbf{x}\in(\mathbb{Z}/p^{N_1+N_2+N_3+1}\mathbb{Z})^2\mid p^{N_i}\mid F_i(\mathbf{x}),\ p\nmid\mathbf{x}\},$$

tandis que pour $p=2$, on obtient un facteur eulérien

$$\sigma^{\boldsymbol{\varepsilon}}_{*,2}(\mathbf{e},\mathbf{E}) = 8 \lim_{n\to\infty} 2^{-2n} \#\left\{ \mathbf{x}\in(\mathbb{Z}/2^n\mathbb{Z})^2 \;\middle|\; \begin{array}{l} F_i(\mathbf{x})\in e_i\varepsilon_i\mathcal{E}_{2^n}, \\ 2\nmid \mathbf{x} \end{array} \right\}. \tag{7.14}$$

On écrit alors

$$c_0 = \sum_{\substack{\boldsymbol{\varepsilon}\in\Sigma \\ \mathbf{m}\in M}} \mathrm{vol}(\mathcal{R}) c_0(\boldsymbol{\varepsilon},\mathbf{m})$$

avec

$$c_0(\boldsymbol{\varepsilon},\mathbf{m}) = \frac{\pi^2}{2^4}\sum_{d\in\mathcal{D}} \frac{\mu(d)r_0(d)\varphi^\dagger(d)}{d} \sum_{\substack{\mathbf{d},\mathbf{d}'\in\mathcal{D}^3 \\ d=d_1d_2d_3,\, d_i'|\Delta_{jk}}} \mu(d_1'd_2')\mu(d_3')$$

$$\times \sum_{\substack{k_4k_1k_1'|\gcd(\Delta_{23},d) \\ k_4k_2k_2'|\gcd(\Delta_{13},d) \\ k_4k_3k_3'|\gcd(\Delta_{12},d)}} \sum_{\substack{k_4k_4'|\gcd(\Delta_{12},\Delta_{13},\Delta_{23},d) \\ k_5k_5'|\gcd(\Delta_{12},d_1'd_2')}} \frac{\mu(k_1')\mu(k_2')\mu(k_3')\mu(k_4')\mu(k_5')}{3^{\omega(k_4)}2^{\omega(k_5)+\omega(k_1)+\omega(k_2)+\omega(k_3)}}\sigma^{\boldsymbol{\varepsilon}}_{*}(\mathbf{e},\mathbf{E}),$$

où $\sigma^{\boldsymbol{\varepsilon}}_{*,p}(\mathbf{e},\mathbf{E})$ a été défini en (7.12). De plus, en utilisant les notations (6.11) et en posant

$$\begin{aligned}
e_1' &= d_1d_2'd_3' \quad e_2' = d_2d_1'd_3', \quad e_3' = d_3d_1'd_2', \\
E_1' &= [e_1', k_4k_2k_2', k_4k_3k_3', k_4k_4', d_1k_5k_5'], \\
E_2' &= [e_2', k_4k_1k_1', k_4k_3k_3', k_4k_4', d_2k_5k_5'], \\
E_3' &= [e_3', k_4k_1k_1', k_4k_2k_2', k_4k_4'], \\
e_1'' &= E_1'' = m_1 \quad e_2'' = E_2'' = m_2, \quad e_3'' = E_3'' = m_3,
\end{aligned}$$

on a les décompositions $e_i = e_i'e_i''$ et $E_i = E_i'E_i''$. Alors $N_i = \max\{\nu_p(e_i')+\nu_i, \nu_p(E_i')\}$ lorsque $p\equiv 1 \pmod 4$ et $N_i = \max\{\nu_p(e_i'')+\nu_i, \nu_p(E_i'')\}$ lorsque $p\equiv 3 \pmod 4$. Enfin,

$$\begin{aligned}
\sigma^{\boldsymbol{\varepsilon}}_{*,2}(\mathbf{e},\mathbf{E}) &= \sigma^{\boldsymbol{\varepsilon}}_{*,2}(\mathbf{m}) \\
&= 8 \lim_{n\to\infty} 2^{-2n} \#\left\{ \mathbf{x}\in(\mathbb{Z}/2^n\mathbb{Z})^2 \;\middle|\; \begin{array}{l} F_i(\mathbf{x})\in m_i\varepsilon_i\mathcal{E}_{2^n}, \\ 2\nmid \mathbf{x} \end{array} \right\}.
\end{aligned}$$

On pose alors

$$V_1(\mathbf{d},\mathbf{d}') = \sum_{\substack{k_4k_1k_1'|\gcd(\Delta_{23},d) \\ k_4k_2k_2'|\gcd(\Delta_{13},d) \\ k_4k_3k_3'|\gcd(\Delta_{12},d)}} \sum_{\substack{k_4k_4'|\gcd(\Delta_{12},\Delta_{13},\Delta_{23},d) \\ k_5k_5'|\gcd(\Delta_{12},d_1'd_2')}} \frac{\mu(k_1')\mu(k_2')\mu(k_3')\mu(k_4')\mu(k_5')}{3^{\omega(k_4)}2^{\omega(k_5)+\omega(k_1)+\omega(k_2)+\omega(k_3)}}$$
$$\times \prod_{p\equiv 1 \,(\mathrm{mod}\, 4)} \sigma_{*,p}(\mathbf{e}',\mathbf{E}'),$$

puis

$$V_3(\mathbf{m}) = \prod_{p \equiv 3 \pmod 4} \sigma_{*,p}(\mathbf{e}'', \mathbf{E}'')$$

et enfin

$$V_2(\boldsymbol{\varepsilon}, \mathbf{m}) = \tfrac{1}{4}\sigma_{*,2}^{\boldsymbol{\varepsilon}}(\mathbf{m}),$$

de sorte que

$$c_0(\boldsymbol{\varepsilon}, \mathbf{m}) = 2\pi \prod_p \left(1 + \frac{\chi(p)}{p}\right)\left(1 - \frac{\chi(p)}{p}\right)^{-2} c_1 \times V_2(\boldsymbol{\varepsilon}, \mathbf{m})V_3(\mathbf{m})$$

avec

$$c_1 = \sum_{d \in \mathcal{D}} \frac{\mu(d)r_0(d)\varphi^\dagger(d)}{d} \sum_{\substack{\mathbf{d},\, \mathbf{d}' \in \mathcal{D}^3 \\ d = d_1 d_2 d_3,\, d_i' \mid \Delta_{jk}}} \mu(d_1'd_2')\mu(d_3')V_1(\mathbf{d}, \mathbf{d}').$$

On a ici utilisé la décomposition en produit eulérien

$$\frac{\pi}{8} = \prod_p \left(1 + \frac{\chi(p)}{p}\right)\left(1 - \frac{\chi(p)}{p}\right)^{-2}.$$

La stratégie pour conclure à la validation de la conjecture de Peyre est alors, suivant [8, section 9.5], de décomposer $c_0(\boldsymbol{\varepsilon}, \mathbf{m})$ sous la forme

$$c_0(\boldsymbol{\varepsilon}, \mathbf{m}) = 2\pi \prod_p c_p(\boldsymbol{\varepsilon}, \mathbf{m})$$

et d'établir que $c_p(\boldsymbol{\varepsilon}, \mathbf{m}) = \omega_p(\boldsymbol{\varepsilon}, \mathbf{m})$ pour tout nombre premier p.

7.6. Fin de la preuve de la conjecture de Peyre. On pose $c_2(\boldsymbol{\varepsilon}, \mathbf{m}) = V_2(\boldsymbol{\varepsilon}, \mathbf{m})$ de sorte que $c_2(\boldsymbol{\varepsilon}, \mathbf{m}) = \omega_2(\boldsymbol{\varepsilon}, \mathbf{m})$. Dans le cas $p \equiv 1 \pmod 4$, on pose $\delta_i' = \nu_p(d_i')$ et

$$\begin{aligned}
N_1' &= \nu_1 + \delta_1 + \delta_2' + \delta_3', \\
N_1 &= \max\{N_1', \kappa_4 + \kappa_2 + \kappa_2', \kappa_4 + \kappa_3 + \kappa_3', \kappa_4 + \kappa_4', \kappa_5 + \kappa_5'\}, \\
N_2' &= \nu_2 + \delta_2 + \delta_1' + \delta_3', \\
N_2 &= \max\{N_2', \kappa_4 + \kappa_1 + \kappa_1', \kappa_4 + \kappa_3 + \kappa_3', \kappa_4 + \kappa_4', \kappa_5 + \kappa_5'\}, \\
N_3' &= \nu_3 + \delta_3 + \delta_1' + \delta_2', \\
N_3 &= \max\{N_3', \kappa_4 + \kappa_1 + \kappa_1', \kappa_4 + \kappa_2 + \kappa_2', \kappa_4 + \kappa_4'\}.
\end{aligned}$$

Puisque $r_0(p) = 2$ et par définition de $\varphi^\dagger$, on a alors

$$c_p(\boldsymbol{\varepsilon}, \mathbf{m}) = \left(1 - \frac{1}{p^2}\right) \sum_{0 \le \delta \le 1} \left(-\frac{2}{p+1}\right)^\delta \sum_{\substack{0 \le \delta_1, \delta_2, \delta_3 \le 1 \\ \delta_1 + \delta_2 + \delta_3 = \delta}} f_p(\boldsymbol{\delta})$$

avec
(7.15)

$$f_p(\boldsymbol{\delta}) = \sum_{\substack{0\leq\delta'_i\leq\min\{\nu_p(\Delta_{jk}),1\}\\ \delta'_1\delta'_2=0}} (-1)^{\delta'_1+\delta'_2+\delta'_3} \sum_{\substack{\kappa_4,\kappa'_4\geq 0\\ \kappa_4+\kappa'_4\leq\min\{\delta,\nu_p(\Delta_{12}),\nu_p(\Delta_{13}),\nu_p(\Delta_{23})\}}} \frac{(-1)^{\kappa'_4}}{3^{\kappa_4}}$$
$$\times \sum_{i=1}^{3} \sum_{\substack{\kappa_i,\kappa'_i\geq 0\\ \kappa_4+\kappa_i+\kappa'_i\leq\min\{\delta,\nu_p(\Delta_{jk})\}}} \frac{(-1)^{\kappa'_i}}{2^{\kappa_i}} \sum_{\substack{\kappa_5,\kappa'_5\geq 0\\ \kappa_5+\kappa'_5\leq\min\{\delta'_1+\delta'_2,\nu_p(\Delta_{12})\}}} \frac{(-1)^{\kappa'_5}}{2^{\kappa_5}}$$
$$\times \sum_{\boldsymbol{\nu}\in\mathbb{N}^3} \frac{\tilde{\rho}(p^{N_1},p^{N_2},p^{N_3};F_1,F_2,F_3)}{p^{2(N_1+N_2+N_3+1)}}$$

et $\{i,j,k\}=\{1,2,3\}$. Enfin, dans le cas $p\equiv 3 \pmod 4$, si l'on note $\mu_i = \nu_p(m_i)$, on pose

$$c_p(\boldsymbol{\varepsilon},\mathbf{m}) = \left(1-\frac{1}{p^2}\right) g(\boldsymbol{\mu}),$$

où

$$g(\boldsymbol{\mu}) = \sum_{\boldsymbol{\nu}\in\mathbb{N}^3} \frac{(-1)^{\nu_1+\nu_2+\nu_3}\tilde{\rho}(p^{N_1},p^{N_2},p^{N_3};F_1,F_2,F_3)}{p^{2(N_1+N_2+N_3+1)}},$$

et $N_1=\mu_1+\nu_1$, $N_2=\mu_2+\nu_2$ et $N_3=\mu_3+\nu_3$. On a ainsi

$$c_0(\boldsymbol{\varepsilon},\mathbf{m}) = 2\pi \prod_p c_p(\boldsymbol{\varepsilon},\mathbf{m}).$$

Il s'agit à présent de remonter la formule d'éclatement du Lemme 6.2 utilisée dans le passage aux torseurs. On distingue selon la congruence de p modulo 4. On commence par le cas $p\equiv 1 \pmod 4$ et on étudie la quantité

$$c'_p(\boldsymbol{\varepsilon},\mathbf{m}) = \left(1-\frac{1}{p^2}\right)^{-1} c_p(\boldsymbol{\varepsilon},\mathbf{m}).$$

Pour ce faire, on ne considère dans un premier temps que la quantité

$$f'_p(\boldsymbol{\delta},\boldsymbol{\delta}') = \sum_{\substack{\kappa_4,\kappa'_4\geq 0\\ \kappa_4+\kappa'_4\leq\min\{\delta,\nu_p(\Delta_{ij})\}}} \frac{(-1)^{\kappa'_4}}{3^{\kappa_4}} \sum_{\substack{\kappa_1,\kappa'_1\geq 0\\ \kappa_4+\kappa_1+\kappa'_1\leq\min\{\delta,\nu_p(\Delta_{23})\}}} \frac{(-1)^{\kappa'_1}}{2^{\kappa_1}}$$
$$\times \sum_{\substack{\kappa_2,\kappa'_2\geq 0\\ \kappa_4+\kappa_2+\kappa'_2\leq\min\{\delta,\nu_p(\Delta_{13})\}}} \frac{(-1)^{\kappa'_2}}{2^{\kappa_2}} \sum_{\substack{\kappa_3,\kappa'_3\geq 0\\ \kappa_4+\kappa_3+\kappa'_3\leq\min\{\delta,\nu_p(\Delta_{12})\}}} \frac{(-1)^{\kappa'_3}}{2^{\kappa_3}}$$
$$\times \sum_{\substack{\kappa_5,\kappa'_5\geq 0\\ \kappa_5+\kappa'_5\leq\min\{\delta'_1+\delta'_2,\nu_p(\Delta_{12})\}}} \frac{(-1)^{\kappa'_5}}{2^{\kappa_5}} \sum_{\boldsymbol{\nu}\in\mathbb{N}^3} \frac{\tilde{\rho}(p^{N_1},p^{N_2},p^{N_3};F_1,F_2,F_3)}{p^{2(N_1+N_2+N_3+1)}}.$$

On raisonne comme dans [8, section 9.5] et on utilise, pour a et b entiers naturels, la formule

$$\sum_{\substack{\kappa,\kappa'\geq 0\\ \kappa+\kappa'\leq\min\{a,b\}\\ 0\leq\kappa'\leq 1}} \frac{(-1)^{\kappa'}}{z^{\kappa}} = \frac{1}{z^{\min\{a,b\}}}.$$

On commence par se placer dans le cas d'un nombre premier $p \equiv 1 \pmod 4$ qui divise tous les résultants $\varDelta_{ij}$. On obtient alors l'égalité

$$f'_p(\boldsymbol{\delta},\boldsymbol{\delta}') = \sum_{\boldsymbol{\nu}\in\mathbb{N}^3} \frac{(\nu_1+1)(\nu_2+1)(\nu_3+1)\rho^{\dagger}(p^{N'_1},p^{N'_2},p^{N'_3};F_1,F_2,F_3)}{C(\delta,N'_1,N'_2,N'_3)2^{\min\{\delta'_1+\delta'_2,N'_1,N'_2,N'_3\}}p^{2(N'_1+N'_2+N'_3+1)}},$$

où

$$C(\delta,N'_1,N'_2,N'_3) = (3/8)^{\min\{\delta,N'_1,N'_2,N'_3\}}2^{\min\{\delta,N'_2,N'_3\}+\min\{\delta,N'_1,N'_3\}+\min\{\delta,N'_2,N'_3\}}$$

et, lorsque $(a_1,a_2,a_3)\in\mathbb{N}^3$,

$$\rho^{\dagger}(p^{a_1},p^{a_2},p^{a_3};F_1,F_2,F_3) = \#\left\{(u,v)\in(\mathbb{Z}/p^{a_1+a_2+a_3+1}\mathbb{Z})^2 \;\middle|\; \begin{array}{l} p^{a_i}\parallel F_i(u,v),\\ p\nmid (u,v)\end{array}\right\}.$$

Il reste à voir sur quels $\boldsymbol{\delta}' = (\delta'_1,\delta'_2,\delta'_3)$ on somme. D'après (7.15), on somme sur les triplets suivants:

$$(0,0,0),\quad (0,0,1),\quad (1,0,1),\quad (0,1,1),\quad (1,0,0),\quad (0,1,0),$$

si bien que

$$\begin{aligned} f_p(\boldsymbol{\delta}) = \sum_{\boldsymbol{\nu}\in\mathbb{N}^3} &\frac{\rho^{\dagger}(p^{N''_1},p^{N''_2},p^{N''_3};F_1,F_2,F_3)}{C(\delta,N''_1,N''_2,N''_3)p^{2(N''_1+N''_2+N''_3+1)}}\big((\nu_1+1)(\nu_2+1)(\nu_3+1)\\ &- \nu_1\nu_2(\nu_3+1) + \tfrac{1}{2}\nu_1\nu_3(\nu_2-1) + \tfrac{1}{2}\nu_2\nu_3(\nu_1-1)\\ &- \tfrac{1}{2}\nu_2\nu_3(\nu_1+1) - \tfrac{1}{2}\nu_1\nu_3(\nu_2+1)\big)\\ = \sum_{\boldsymbol{\nu}\in\mathbb{N}^3} &(\nu_1+\nu_2+\nu_3+1)\frac{\rho^{\dagger}(p^{N''_1},p^{N''_2},p^{N''_3};F_1,F_2,F_3)}{C(\delta,N''_1,N''_2,N''_3)p^{2(N''_1+N''_2+N''_3+1)}}, \end{aligned}$$

avec $N''_i = \nu_i+\delta_i$. En remarquant que pour N''_i fixés, il y a $C(\delta,N''_1,N''_2,N''_3)$ triplets $\boldsymbol{\delta}$ tels que $N''_i = \nu_i+\delta_i$, on peut conclure exactement comme dans [8, section 9.5] que l'on obtient la quantité adéquate.

Sans être complètement exhaustif, on traite ensuite un cas éloquent dont l'adaptation aux cas restants ne pose aucune difficulté. Tout d'abord, on se place dans un cas où $\nu_p(\varDelta_{12}) = 0$. Supposons alors par exemple que $\nu_p(\varDelta_{13}) = 0$ et $\nu_p(\varDelta_{23}) \geq 1$. Dans ce cas de figure, on a clairement

$$\begin{aligned} &\min\{\delta'_1+\delta'_2,\nu_p(\varDelta_{12}),N'_1,N'_2,N'_3\}\\ &\qquad = \min\{\delta,\nu_p(\varDelta_{12}),\nu_p(\varDelta_{13}),\nu_p(\varDelta_{23}),N'_1,N'_2,N'_3)\} = 0, \end{aligned}$$

et un examen des conditions sur les $\boldsymbol{\delta}'$ dans la formule (7.15) montre que la somme sur les $\boldsymbol{\delta}'$ porte sur les triplets $(0,0,0)$ et $(1,0,0)$, si bien que

$$f_p(\boldsymbol{\delta}) = \sum_{\boldsymbol{\nu}\in\mathbb{N}^3} \frac{\rho^\dagger(p^{N_1'}, p^{N_2'}, p^{N_3'}; F_1, F_2, F_3)}{C'(\delta, N_1', N_2', N_3')p^{2(N_1'+N_2'+N_3'+1)}} \times \big((\nu_1+1)(\nu_2+1)(\nu_3+1) - \nu_2\nu_3(\nu_1+1)\big),$$

où

$$C'(\delta, N_1', N_2', N_3') = 2^{\min\{\delta,N_2',N_3'\}+\min\{\delta,N_1',N_3'\}+\min\{\delta,N_2',N_3'\}}.$$

Mais, le fait que p ne divise ni $\varDelta_{12}$ ni $\varDelta_{13}$ implique que nécessairement $\nu_1\nu_2 = \nu_1\nu_3 = 0$, de sorte que

$$\begin{aligned}(\nu_1+1)(\nu_2+1)(\nu_3+1) - \nu_2\nu_3(\nu_1+1) &= \nu_1+\nu_2+\nu_3+1+\nu_1\nu_2+\nu_1\nu_3\\ &= \nu_1+\nu_2+\nu_3+1,\end{aligned}$$

et on peut à nouveau conclure comme dans [8, section 9.5].

Pour finir, dans le cas $p \equiv 3 \pmod 4$, on a

$$g(\boldsymbol{\mu}) = \sum_{\boldsymbol{\nu}\in\mathbb{N}^3} \frac{\rho^\dagger(p^{2\nu_1+\mu_1}, p^{2\nu_2+\mu_2}, p^{2\nu_3+\mu_3}; F_1, F_2, F_3)}{p^{2(2\nu_1+2\nu_2+2\nu_3+1)}},$$

que l'on traite comme dans [8, section 9.5]. Cela permet finalement de conclure à l'égalité

$$c_0 = \sum_{\substack{\boldsymbol{\varepsilon}\in\varSigma\\ \mathbf{m}\in M}} \omega_\infty(\boldsymbol{\varepsilon}, \mathbf{m}) \prod_p \omega_p(\boldsymbol{\varepsilon}, \mathbf{m})$$

et achève la preuve du fait que $c_0 = c_S$.

Remerciements. L'auteur tient ici à exprimer toute sa gratitude à son directeur de thèse Régis de la Bretèche pour ses conseils, son soutien et ses relectures tout au long de ce travail, ainsi qu'à Tim Browning, Cyril Demarche, Ulrich Derenthal, Dan Loughran, Emmanuel Peyre et Marta Pieropan pour de nombreuses discussions éclairantes.

Références

[1] V. Batyrev and Y. Tschinkel, *Tamagawa numbers of polarized algebraic varieties*, Astérisque 251 (1998), 299–340.

[2] R. de la Bretèche and T. Browning, *Sums of arithmetic functions over values of binary forms*, Acta Arith. 125 (2007), 291–304.

[3] R. de la Bretèche and T. Browning, *On Manin's conjecture for singular del Pezzo surfaces of degree four, I*, Michigan Math. J. 55 (2007), 51–80.

[4] R. de la Bretèche and T. Browning, *Binary linear forms as sums of two squares*, Compos. Math. 144 (2008), 1375–1402.

[5] R. de la Bretèche et T. Browning, *Le problème des diviseurs pour des formes binaires de degré 4*, J. Reine Angew. Math. 646 (2010), 1–44.

[6] R. de la Bretèche and T. Browning, *Binary forms as sums of two squares and Châtelet surfaces*, Israel J. Math. 191 (2012), 973–1012.

[7] R. de la Bretèche, T. Browning and E. Peyre, *On Manin's conjecture for a family of Châtelet surfaces*, Ann. of Math. 175 (2012), 1–47; une version plus longue : arXiv:1002.0255.

[8] R. de la Bretèche et G. Tenenbaum, *La conjecture de Manin pour certaines surfaces de Châtelet*, J. Inst. Math. Jussieu 12 (2013), 759–819.

[9] T. D. Browning, *Linear growth for Châtelet surfaces*, Math. Ann. 346 (2010), 41–50.

[10] F. Châtelet, *Points rationnels sur certaines courbes et surfaces cubiques*, Enseign. Math. (2) 5 (1959), 153–170.

[11] F. Châtelet, *Points rationnels sur certaines surfaces cubiques*, dans : Les tendances géométriques en algèbre et théorie des nombres (Clermont-Ferrand, 1964), Éditions CNRS, Paris, 1966, 67–75.

[12] J.-L. Colliot-Thélène et J.-J. Sansuc, *La descente sur une variété rationnelle définie sur un corps de nombres*, C. R. Acad. Sci. Paris Sér. A 284 (1977), 1215–1218.

[13] J.-L. Colliot-Thélène et J.-J. Sansuc, *La descente sur les variétés rationnelles*, dans : Journées de géométrie algébrique d'Angers (Angers, 1979), Sijthoff & Noordhoff, 1980, 223–237.

[14] J.-L. Colliot-Théléne et J.-J. Sansuc, *La descente sur les variétés rationnelles II*, Duke Math. J. 54 (1987), 375–492.

[15] J.-L. Colliot-Thélène, J.-J. Sansuc and H. P. F. Swinnerton-Dyer, *Intersections of two quadrics and Châtelet surfaces I*, J. Reine Angew. Math. 373 (1987), 37–101.

[16] J.-L. Colliot-Thélène, J.-J. Sansuc and H. P. F. Swinnerton-Dyer, *Intersections of two quadrics and Châtelet surfaces II*, J. Reine Angew. Math. 374 (1987), 72–168.

[17] S. Daniel, *On the divisor-sum problem for binary forms*, J. Reine Angew. Math. 507 (1999), 107–129.

[18] H. Davenport, *Cubic forms in sixteen variables*, Proc. Roy. Soc. Ser. A 272 (1963), 285–303.

[19] U. Derenthal, *Geometry of universal torsors*, PhD Thesis, 2006.

[20] U. Derenthal, A.-S. Elsenhans and J. Janhel, *On the factor alpha in Peyre's constant*, Math. Comput. 286 (2014), 965–977.

[21] U. Derenthal, M. Joyce and Z. Teitler, *The nef cone volume of generalized del Pezzo surfaces*, Algebra Number Theory 2 (2008), 157–182.

[22] U. Derenthal and M. Pieropan, *Cox rings over nonclosed fields*, arXiv:1408.5358 (2014).

[23] U. Derenthal and Y. Tschinkel, *Universal torsors over Del Pezzo surfaces and rational points*, dans : Equidistribution in Number Theory, an Introduction, NATO Sci. Ser. II Math. Phys. Chem. 237, Springer, 2007, 169–196.

[24] D. R. Heath-Brown, *Linear relations amongst sums of two squares*, dans : Number Theory and Algebraic Geometry, London Math. Soc. Lecture Note Ser. 303, Cambridge Univ. Press, 133–176, 2003.

[25] V. A. Iskovskih, *Minimal models of rational surfaces over arbitrary fields*, Math. USSR-Izv. 14 (1980), 17–39.

[26] P. Le Boudec, *Manin's conjecture for a cubic surface with $2A_2 + A_1$ singularity type*, Math. Proc. Cambridge Philos. Soc. 153 (2012), 419–455.

[27] G. Marasingha, *On the representation of almost primes by pairs of quadratic forms*, Acta Arith. 124 (2008), 327–355.

[28] G. Marasingha, *Almost primes represented by binary forms*, J. London Math. Soc. (2010), 295–316.

[29] T. Ono, *On the Tamagawa number of algebraic tori*, Ann. of Math. 78 (1963), 47–73.
[30] E. Peyre, *Hauteurs et mesures de Tamagawa sur les variétés de Fano*, Duke Math. J. 79 (1995), 101–218.
[31] E. Peyre, *Points de hauteur bornée, topologie adélique et mesures de Tamagawa*, J. Théor. Nombres Bordeaux 15 (2003), 319–349.
[32] E. Peyre, *Counting points on varieties using universal torsors*, Ann. of Math. 175 (2012), 61–81.
[33] M. Pieropan, *Torsors and generalized Cox rings for Manin's conjecture*, PhD Thesis, 2015, http://edok01.tib.uni-hannover.de/edoks/e01dh15/828227667.pdf.
[34] P. Salberger, *Tamagawa measures on universal torsors and points of bounded height on Fano varieties*, dans : Nombre et répartition de points de hauteur bornée (Paris, 1996), Astérisque 251 (1998), 91–258.
[35] J.-J. Sansuc, *Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres*, J. Reine Angew. Math. 327 (1980), 12–80.
[36] A. Skorobogatov, *Torsors and Rational Points*, Cambridge Univ. Press, Cambridge, 2001.

Kevin Destagnol
Institut de Mathématiques de Jussieu-Paris Rive Gauche
UMR 7586
Université Paris Diderot-Paris 7
Case postale 6052
Bâtiment Sophie Germain
75205 Paris Cedex 13, France
E-mail: kevin.destagnol@imj-prg.fr
URL: webusers.imj-prg.fr/~kevin.destagnol/