Stage de Master 2 : La conjecture de Manin sur les surfaces de Châtelet

Université Paris 7 Diderot

Kévin Destagnol
Sous la direction de Régis de la Bretèche

9 septembre 2013

Table des matières

Résumé

On s'intéresse à la conjecture de Manin sous sa forme forte conjecturée par Peyre pour une famille de surfaces de Châtelet qui sont définies comme modèle minimal propre et lisse d'une surface affine de la forme

$$Y^2 + Z^2 = f(X),$$

où f est un polynôme de degré 3 ou 4 sur $\mathbb{Z}[X]$ produit de deux formes linéaires non proportionnelles par une forme quadratique irréductible sur $\mathbb{Q}[i]$. La résolution de ce problème par les torseurs universels repose essentiellement sur l'estimation asymptotique de sommes du type

$$S(X) = \sum_{\mathbf{x}\in\mathbb{Z}^2\cap X\mathcal{R}} r\big(L_1(\mathbf{x})\big)r\big(L_2(\mathbf{x})\big)r\big(Q(\mathbf{x})\big),$$

pour une région $\mathcal{R} \subset \mathbb{R}^2$ convenable, et où L_1 et L_2 sont deux formes linéaires binaires de $\mathbb{Z}[x_1, x_2]$ et Q est une forme quadratique de $\mathbb{Z}[x_1, x_2]$ irréductible sur $\mathbb{Q}[i]$ et où r désigne le nombre de représentations d'un entier comme somme de deux carrés. Ce travail permet essentiellement de terminer le programme de recherche initié par Tim Browning et Régis de la Bretèche concernant la conjecture de Manin sur les surfaces de Châtelet.

Remerciements

Je voudrais avant toute chose commencer ce rapport par quelques mots pour remercier mon directeur, Régis de la Bretèche, pour m'avoir fait découvrir avec enthousiasme pendant ce stage de M2 le monde de la recherche et les jolies mathématiques qui entourent la conjecture de Manin ainsi que pour sa disponinilité et sa patience face à mes nombreuses interrogations.

Introduction

L'objet de ce mémoire de M2 est l'étude d'équations diophantiennes particulières, autrement dit des points à coordonnées rationnelles de certains systèmes d'équations polynômiales. Plus précisément, étant donné V une variété algébrique de $\mathbb{P}^n$, on cherche à étudier l'ensemble $V(\mathbb{Q}) = V \cap \mathbb{P}^n(\mathbb{Q})$. On se restreint ici à des variétés dont l'ensemble des points rationnels est dense pour la topologie de Zariski. Cette hypothèse est en réalité assez générale dans le cas de la dimension 2 puisqu'un résultat de Segre, établi dans [1], montre que si V contient un point rationnel en dehors d'une droite incluse dans V, alors l'ensemble des points rationnels est nécessairement Zariski dense. L'ensemble $V(\mathbb{Q})$ est alors infini et la question naturelle qui se pose est celle de la complexité de cet ensemble, de sa "taille". On utilise alors des fonctions $H : \mathbb{P}^n(\mathbb{Q}) \to \mathbb{R}_*^+$ possédant des propriétés particulières appelées hauteurs qui seront précisées dans la suite du rapport et qui permettent de mesurer la "taille" d'un point $[x_0 : ... : x_n] \in \mathbb{P}^n(\mathbb{Q})$. En particulier, le cardinal

$$N_{U,H}(B) = \#\{x \in U(\mathbb{Q}) \quad | \quad H(x) \leqslant B\}$$

est bien défini (et donc fini) pour $B \geqslant 1$ et U un ouvert de Zariski de V.

Dans les années 1980 ([2]), Manin a mis en place un programme de recherche visant à comprendre le comportement asymptotique de $N_{U,H}(B)$ lorsque B tend vers $+\infty$ pour une classe particulière de variétés, les variétés de Fano et pour un ouvert U convenable. En effet, un principe général en géométrie arithmétique (conséquence notamment de la conjecture de Bombieri-Lang) prédit qu'une variété de type général, c'est-à-dire dont le faisceau canonique ω_V est ample, va contenir peu de points rationnels tandis qu'au contraire une variété de Fano, c'est-à-dire dont le faisceau anticanonique ω_V^{-1} est ample, devrait contenir beaucoup de points sur un corps de nombres assez gros. Ce programme a conduit à la conjecture de Manin qui est étudiée dans ce rapport dans un cas particulier. Si $V = W_1 \cap ... \cap W_r \subset \mathbb{P}^n$ est une intersecion complète non singulière de r hypersurfaces de degrés respectifs $d_1, ..., d_r$, cette conjecture prend la forme suivante. Si on pose $d = d_1 + ... + d_r$ et si $n \geqslant d$, alors il existe un ouvert U de V et une constante $c_{V,H}$ tels que, lorsque B tend vers $+\infty$,

$$N_{V,H}(B) = c_{V,H} B^{n+1-d} \log(B)^{\rho_V - 1}(1 + o(1)),$$

où ρ_V désigne le rang du groupe de Picard de V. En 1995 dans [3], Peyre a donné une expression conjecturale de la constante $c_{V,H}$ comme un produit

$$c_{V,H} = \alpha(V)\beta(V)\omega_H(\overline{V(\mathbb{Q})})$$

où $\alpha(V)$ est un coefficient dépendant de la géométrie de la variété, $\beta(V)$ un coefficient cohomologique et $\omega_H(\overline{V(\mathbb{Q})})$ un nombre de Tamagawa qui va s'interpréter comme un produit de densités archimédienne et $p-$adiques ou une somme de produit de telles densités.

On reviendra plus précisément sur cette expression dans le cœur du rapport. Le fait que la conjecture soit seulement formulée sur un ouvert de Zariski provient du fait qu'il peut exister des sous-variétés accumulatrices incluses dans la variété V qui sont susceptibles de dominer le comportement de $N_{V,H}(B)$. L'ouvert U est donc le complémentaire de toutes ces sous-variétés accumulatrices ([3]). Dans le cas de la dimension 2, la situation est particulièrement simple puisque les seules sous-variétés accumulatrices sont les droites qui contribuent de l'ordre de $O(B^2)$ et l'ouvert U est automatiquement le complémentaire de toutes les droites incluses dans la variété V étudiée. En dimension supérieure, la situation est plus délicate et explique, couplée au fait qu'on sache qu'il n'existe pas de méthode générale pour obtenir l'existence de points rationnels sur une variété quelonque, qu'une démonstration générale pour toute variété soit inenvisageable et que par conséquent la conjecture soit attaquée par classes de variétés.

Lorsque n est "grand" devant d, la méthode du cercle a permis d'obtenir des résultats comme le théorème de Birch ([4]) qui établit la conjecture sous sa forme forte dans le cas d'une hypersurface projective non singulière de degré d avec $n > (d-1)2^d$ et telle que le produit

$$\prod_p V(\mathbb{Q}_p) \times V(\mathbb{R})$$

soit non vide. Une deuxième approche utilisant l'analyse harmonique s'est révélée payante dans le cas de compactifications équivariantes de certains groupes algébriques comme dans [5] pour les variétés toriques ou dans [6] pour les compactifications équivariantes d'espaces affines. Malheureusement, lorsque la variété V n'est dans aucune des deux catégories précédentes, on ne dispose pas de méthode générale. L'idée a alors été de commencer par regarder la dimension 2 et de traiter différentes classes de variétés (comme les surfaces de del Pezzo [7], [8] et [9] ou [10] ou encore l'éclaté du plan projectif en quatre points dans [11]) en utilisant une méthode de comptage qui combine théorie analytique des nombres et méthodes de descente via les torseurs universels (qui ont été introduits par Colliot-Thélène et Sansuc dans [12], [13] et [14]) qui vont s'avérer être des variétés plus simples que la variété d'origine. C'est cette méthode qui est développée dans ce rapport dans le cas particulier des surfaces de Châtelet.

Le cas de la dimension 3 est beaucoup plus inexploré. Les deux seuls exemples publiés sont dû d'une part à Régis de la Bretèche pour la cubique de Segre [15] et d'autre part à Blomer, Brüdern et Salberger dans [16].

Les surfaces de Châtelet peuvent être vues comme le modèle propre et lisse des variétés affines dans $\mathbb{A}^3_{\mathbb{Q}}$ d'équations de la forme $X^2 - aY^2 = F(X,1) = f(X)$ où F est une forme binaire de degré 4 de discriminant non nul et a un entier. On se place dans le cadre de ce rapport dans le cas $a = -1$, bien que les cas $a < 0$ puissent se traiter de manière assez similaire mais en ajoutant un certain nombre de complications techniques aux places de mauvaises réduction dans le cas où le groupe de classes de $\mathbb{Q}(\sqrt{a})$ n'est pas trivial notamment. Ces surfaces apparaissent naturellement parmi les surfaces non triviales les plus simples dans la classification birationnelle des surfaces d'Iskovskikh ([17]) et comme désingularisations minimales de certaines surfaces de del Pezzo de degré 4 ([18], remarque 2.3). Les surfaces de Châtelet sont également arithmétiquement très riches puisque certaines de ces variétés ne satisfont ni le principe de Hasse ni le principe de l'approximation faible et correspondent à l'exemple historique donné par Swinnerton-Dyer en 1971. La

seule obstruction au principe de Hasse et à l'approximation faible pour ces surfaces est en effet l'obstruction de Brauer-Manin ([19] et [20]). L'étude du principe de Hasse pour les variétés projectives tire son origine du fait que pour les classes de variétés projectives le vérifiant, il existe un algorithme permettant de décider l'existence ou non de points rationnels. La recherche de contre-exemples à ce principe a alors été essentiellement motivée par la résolution du dixième problème de Hilbert sur $\mathbb{Q}$ qui reste encore aujourd'hui une question ouverte.

Considéré spécifiquement depuis 2005, le cas particulier des surfaces de Châtelet a donné lieu à une confirmation de la conjecture sous certaines conditions de factorisation pour la forme P — cf. notamment [21] et [18]. Désignons par $r(n)$ le nombre de décompositions d'un entier générique n comme somme de deux carrés et, pour toute une forme binaire $P \in \mathbb{Z}[X, Y]$ de degré 4, introduisons la quantité

$$S_P(X) := \sum_{\mathbf{x} \in \mathbb{Z}^2 \cap \mathcal{R}_P(X)} r(P(\mathbf{x}))$$

où l'on a posé

$$\mathcal{R}_P(X) := \{\mathbf{x} \in \mathbb{R}^2 : ||\mathbf{x}||_\infty \leqslant X,\ P(\mathbf{x}) > 0\} \qquad (X > 0).$$

L'évaluation asymptotique de $N_P(B)$ peut être reformulée en termes d'estimations de quantités plus générales, mais essentiellement de même nature que $S_P(X)$, sous réserve d'une uniformité suffisante en divers paramètres, notamment les coefficients de la forme P. La forme du résultat asymptotique conjecturé et les méthodes nécessaires pour l'obtenir sont subordonnées au type de factorisation de P dans $\mathbb{Q}$ et à la nature des facteurs dans $\mathbb{Q}[i]$. La liste suivante explicite tous les cas possibles :

(i) $P = L_1L_2L_3L_4$, où les L_j sont des formes linéaires de $\mathbb{Q}[X]$;

(ii) $P = L_1L_2Q$ où les L_j sont des formes linéaires, et Q une forme quadratique irréductible sur $\mathbb{Q}$ mais réductible sur $\mathbb{Q}[i]$;

(iii) $P = L_1L_2Q$ où les L_j sont des formes linéaires, et Q une forme quadratique irréductible sur $\mathbb{Q}[i]$;

(iv) $P = LC$, où L est une forme linéaire, et C est une forme cubique irréductible sur $\mathbb{Q}$;

(v) $P = Q_1Q_2$, où les Q_j sont des formes quadratiques irréductibles sur $\mathbb{Q}$, mais dont l'une au moins est réductible sur $\mathbb{Q}[i]$;

(vi) $P = Q_1Q_2$ où les Q_j sont des formes quadratiques irréductibles sur $\mathbb{Q}[i]$;

(vii) P est irréductible sur $\mathbb{Q}$, mais est réductible sur $\mathbb{Q}[i]$;

(viii) P est une forme irréductible sur $\mathbb{Q}[i]$.

Le premier exemple d'une formule asymptotique pour $S_P(X)$ lorsque $X \to \infty$ a été obtenu par Daniel [22] pour le polynôme $P(X, Y) = X^4 + Y^4$, qui est du type (vii). À la suite de ce travail, d'autres progrès ont été accomplis. Pour les formes de type (i), l'évaluation asymptotique de $S_P(X)$ a été traitée par Heath-Brown dans [23]. Les précisions nécessaires à l'approche de la conjecture de Manin ont été obtenues dans [24], ce qui a effectivement permis l'estimation asymptotique de $N_P(B)$ dans [18]. Ce cas constitue le premier cas où la conjecture de Manin a été obtenue par des méthodes différentes de l'analyse harmonique

dans le cas d'une variété ne vérifiant ni le principe de Hasse ni l'approximation faible. Les mêmes méthodes fonctionnent pour le type (iv) : les évaluations de $S_P(X)$ et de $N_P(B)$ ont ainsi été obtenues dans [21]. Avec Tenenbaum ([25] et [26]), Régis de la Bretèche a établi les cas dans lesquels P n'est pas divisible par une forme linéaire, autrement dit les types (vi) et (viii). Il reste donc certains cas dont le cas (iii) sachant que les cas (ii), (v) et (vii) peuvent être considérés comme des cas dégénérés.

L'objet de ce mémoire de M2 est alors de présenter, de compléter certains points et d'adapter les méthodes développées dans [24], [27], [26] et [18] afin de démontrer la conjecture dans le dernier cas (iii) restant afin de terminer le programme de recherche sur la conjecture de Manin sur les surfaces de Châtelet.

Chapitre 1

Ordre moyen du nombre de représentations en sommes de deux carrés des valeurs de certaines formes binaires quartiques de la forme L_1L_2Q

1.1 Motivation et lien avec la conjecture de Manin

On cherche dans ce rapport à s'intéresser à la conjecture de Manin pour une famille de surfaces de Châtelet qui sont définies comme modèle minimal propre et lisse d'une surface affine de la forme

$$Y^2 + Z^2 = f(X),$$

où f est un polynôme de degré 3 ou 4 sur $\mathbb{Z}$ produit de deux formes linéaires non proportionnelles par une forme quadratique irréductible sur $\mathbb{Q}[i]$. Comme mentionné dans l'introduction, la résolution de ce problème par les torseurs universels repose essentiellement sur l'estimation asymptotique de sommes du type

$$S(X) = \sum_{\mathbf{x}\in\mathbb{Z}^2\cap X\mathcal{R}} r\big(L_1(\mathbf{x})\big)r\big(L_2(\mathbf{x})\big)r\big(Q(\mathbf{x})\big),$$

pour une région $\mathcal{R} \subset \mathbb{R}^2$ convenable, et où L_1 et L_2 sont deux formes linéaires binaires et Q une forme quadratique entière irréductible sur $\mathbb{Q}[i]$ et où r désigne le nombre de représentations d'un entier comme somme de deux carrés.

1.2 Notations et résultats

On commence par préciser que dans les estimations qui vont suivre, ε désignera toujours un réel strictement positif. On autorisera systématiquement les constantes implicites dans les O à dépendre de ε. De plus, on autorisera la valeur de ε à changer d'une ligne à l'autre pour ne pas alourdir les notations.

On rappelle la définition du caractère multiplicatif χ non principal de Dirichlet modulo 4

$$\chi(p) = \begin{cases} 1 & \text{si } p \equiv 1[4] \\ -1 & \text{si } p \equiv 3[4] \\ 0 & \text{si } p = 2 \end{cases}$$

et celle de la fonction r :

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

On cherche donc à obtenir, pour $X \geqslant 1$, une estimation suffisamment **uniforme** en les coefficients des formes de la somme

$$S(X) = \sum_{\mathbf{x} \in \mathbb{Z}^2 \cap X\mathcal{R}} r\big(L_1(\mathbf{x})\big) r\big(L_2(\mathbf{x})\big) r\big(Q(\mathbf{x})\big), \tag{1.1}$$

où, si $\mathbf{x} = (x_1, x_2)$, L_1 et L_2 sont deux formes linéaires binaires dans $\mathbb{Z}[x_1, x_2]$, Q est 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** :

i) Les formes L_1 et L_2 ne sont pas proportionnelles ;

ii) La forme quadratique Q est irréductible sur $\mathbb{Q}[i]$ (et donc en particulier également sur $\mathbb{Q}$) ;

iii) $\forall \mathbf{x} \in \mathcal{R}, \quad L_1(\mathbf{x}) > 0, \quad L_2(\mathbf{x}) > 0$ et $Q(\mathbf{x}) > 0$.

iv) La région $\mathcal{R}$ est convexe, bornée avec une frontière continûment différentiable (par morceaux).

Ces conditions sont assez naturelles et n'imposent pas vraiment de restrictions sur les formes considérées. Elles seront vérifiées dans le cas notamment des surfaces de Châtelet qui nous intéressent ici. On définit

$$X\mathcal{R} = \{X\mathbf{x} \quad | \quad \mathbf{x} \in \mathcal{R}\}$$

et on pose

$$L_1(\mathbf{x}) = a_1x_1 + b_1x_2, \quad L_2(\mathbf{x}) = a_2x_1 + b_2x_2 \quad \text{et} \quad Q(\mathbf{x}) = a_3x_1^2 + b_3x_2^2 + c_3x_1x_2, \tag{1.2}$$

avec les a_i, b_i et c_3 entiers. On considére

$$\Delta = \operatorname{disc}(Q) = c_3^2 - 4a_3b_3 \neq 0, \tag{1.3}$$

puisque la forme quadratique Q est irréductible sur $\mathbb{Q}$,

$$\Delta_{12} = \operatorname{Res}(L_1, L_2) = a_1b_2 - a_2b_1 \neq 0, \tag{1.4}$$

puisque les deux formes ne sont pas proportionnelles,

$$\Delta_{i3} = \operatorname{Res}(L_i, Q) = a_3b_i^2 + b_3a_i^2 - c_3a_ib_i = Q(-b_i, a_i) \neq 0, \tag{1.5}$$

pour $i \in \{1, 2\}$ et car Q est irréductible sur $\mathbb{Q}$ et, pour $\mathbf{d} = (d_1, d_2, d_3) \in \mathbb{Z}^3_{\geqslant 0}$,

$$\Lambda(\mathbf{d}) = \{\mathbf{x} \in \mathbb{Z}^2 \quad | \quad d_i | L_i(\mathbf{x}), \quad d_3 | Q(\mathbf{x})\}, \tag{1.6}$$

où on note systématiquement (sauf mention contraire) $d_i|L_i(\mathbf{x})$ pour $d_1|L_1(\mathbf{x})$ et $d_2|L_2(\mathbf{x})$. On introduit alors la quantité essentielle

$$\rho(\mathbf{d}) = \rho(\mathbf{d}, L_1, L_2, Q) = \#\left(\Lambda(\mathbf{d}) \cap [0, d[^2\right) \tag{1.7}$$

soit

$$\rho(\mathbf{d}) = \#\{\mathbf{x} \in (\mathbb{Z}/d\mathbb{Z})^2 \quad | \quad d_i|L_i(\mathbf{x}), \quad d_3|Q(\mathbf{x})\}, \tag{1.8}$$

où on note à nouveau systématiquement $d = d_1d_2d_3$. Il est ici important de souligner que l'ensemble $\Lambda(\mathbf{d})$ n'est **pas** un réseau contrairement au cas traité par Régis de la Bretèche et Tim Browning dans [24] où le polynôme f est scindé en un produit de quatre formes linéaires binaires.

On pose également

$$L_\infty = L_\infty(L_1, L_2, Q) = \max(||L_1||, ||L_2||, ||Q||), \tag{1.9}$$

$$r_\infty = r_\infty(L_1, L_2, Q) = \sup_{\mathbf{x}\in\mathcal{R}} \max(|x_1|, |x_2|) \tag{1.10}$$

et

$$r' = r'(L_1, L_2, Q, \mathcal{R}) = \sup_{\mathbf{x}\in\mathcal{R}} \max\left(|L_1(\mathbf{x})|, |L_2(\mathbf{x})|, \sqrt{|Q(\mathbf{x})|}\right). \tag{1.11}$$

Le résultat principal obtenu est alors le suivant où l'on obtient bien mieux que la borne

$$S(X) \ll X^2 \tag{1.12}$$

fournie par [28]. On note

$$\mathcal{E} = \left\{n \in \mathbb{Z} \quad | \quad \exists \ell \in \mathbb{Z}_{\geqslant 0}, \quad n \equiv 2^\ell \left[\, 2^{\ell+2} \,\right]\right\}$$

et $\mathcal{E}_{2^n}$ sa projection modulo 2^n

$$\mathcal{E}_{2^n} = \left\{k \in \mathbb{Z}/2^n\mathbb{Z} \quad | \quad \exists \ell \in \mathbb{Z}_{\geqslant 0}, \quad k \equiv 2^\ell \left[\, 2^{\min(\ell+2,n)} \,\right]\right\},$$

et

$$\eta = 1 - \frac{1 + \log\log(2)}{\log(2)} = 0.086071...$$

Théorème 1. *On suppose que les formes L_1, L_2 et Q vérifient les hypothèses **NH** et soient $\varepsilon > 0$ et $X \geqslant 1$ tels que $r'X^{1-\varepsilon} \geqslant 1$. On a alors*

$$S(X) = 2\pi^3 \mathrm{vol}(\mathcal{R})\mathrm{X}^2 \prod_{\mathrm{p}} \sigma_{\mathrm{p}} + \mathrm{O}_\varepsilon\left(\frac{\mathrm{L}_\infty^\varepsilon(\mathrm{r}_\infty \mathrm{r}' + \mathrm{r}_\infty^2)\mathrm{X}^2}{(\log(\mathrm{X}))^{\eta-\varepsilon}}\right),$$

où

$$\sigma_p = \left(1 - \frac{\chi(p)}{p}\right)^3 \sum_{\boldsymbol{\nu}\in\mathbb{Z}^3_{\geqslant 0}} \frac{\chi(p)^{\nu_1+\nu_2+\nu_3}\rho\left(p^{\nu_1}, p^{\nu_2}, p^{\nu_3}\right)}{p^{2(\nu_1+\nu_2+\nu_3)}} \tag{1.13}$$

si $p > 2$ et

$$\sigma_2 = 4 \lim_{n\to+\infty} 2^{-2n} \# \left\{ \mathbf{x} \in (\mathbb{Z}/2^n\mathbb{Z})^2 \quad \middle| \quad \begin{array}{c} L_i(\mathbf{x}) \in \mathcal{E}_{2^n} \\ Q(\mathbf{x}) \in \mathcal{E}_{2^n} \end{array} \right\} \tag{1.14}$$

où le produit $\prod_{p>2} \sigma_P$ est absolument convergent.

Cependant, ce n'est pas directement de l'estimation de cette somme dont nous aurons besoin pour prouver la conjecture de Manin mais un de ces avatars. Pour cela on introduit l'ensemble

$$\mathfrak{D} = \{(\mathbf{d}, \mathbf{D}) \in \mathbb{Z}^6_{\geqslant 0} \quad | \quad d_i | D_i, \quad 2 \nmid d_i D_i\} \tag{1.15}$$

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

$$S(X, \mathbf{d}, \mathbf{D}) = \sum_{\mathbf{x} \in \Lambda(\mathbf{D}) \cap X\mathcal{R}} r\left(\frac{L_1(\mathbf{x})}{d_1}\right) r\left(\frac{L_2(\mathbf{x})}{d_2}\right) r\left(\frac{Q(\mathbf{x})}{d_3}\right). \tag{1.16}$$

En effet, cette somme est directement liée au comptage des points rationnels sur la variété affine de $\mathbb{A}^8$ d'équations

$$L_i(\mathbf{x}) = d_i(s_i^2 + t_i^2) \quad \text{et} \quad Q(\mathbf{x}) = d_3(s_3^2 + t_3^2), \tag{1.17}$$

où (x_1, x_2) sont restreints à un certain réseau, autrement dit au comptage des points rationnels sur un torseur associé à une surface de Châtelet du type que l'on souhaite étudier. On définit, toujours pour $(\mathbf{d}, \mathbf{D}) \in \mathfrak{D}$, $\delta(\mathbf{D})$ comme étant le plus grand entier δ tel que

$$\Lambda(\mathbf{D}) \subset \{\mathbf{x} \in \mathbb{Z}^2 \quad | \quad \delta | (x_1, x_2)\},$$

où on note (x_1, x_2) le plus grand diviseur commun des deux entiers x_1 et x_2. La fonction ρ a été abondamment étudiée, notamment par Daniel dans [22], Marasingha ([29] et [30]) ou La Bretèche et Browning dans [27] mais pour des formes primitives. On introduit donc les entiers ℓ_1, ℓ_2, q et les formes primitives L_1^*, L_2^* et Q^* telles que

$$L_i = \ell_i L_i^* \quad \text{et} \quad Q = qQ^*. \tag{1.18}$$

On considére alors $D = D_1 D_2 D_3$ et

$$\mathbf{D}' = \left(\frac{D_1}{(D_1, \ell_1)}, \frac{D_2}{(D_2, \ell_2)}, \frac{D_3}{(D_3, q)}\right), \tag{1.19}$$

$$a(\mathbf{D}, \mathbf{\Delta}) = (D_1, \Delta_{12}\Delta_{13})(D_2, \Delta_{12}\Delta_{23})(D_3, \Delta(\Delta_{13}, \Delta_{23})) \tag{1.20}$$

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

$$a'(\mathbf{D}, \mathbf{\Delta}) = a(\mathbf{D}', \mathbf{\Delta}') = (D_1', \Delta_{12}'\Delta_{13}')(D_2', \Delta_{12}'\Delta_{23}')(D_3', \Delta'(\Delta_{13}', \Delta_{23}')) \tag{1.21}$$

où

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

On notera la différence avec la quantité correspondante dans [27] qui n'est en réalité pas satisfaisante pour obtenir le Lemme 8 page 29 de [27]. On a alors le résultat suivant, crucial en vue de l'obtention de la conjecture de Manin :

Théorème 2. *Soient $\varepsilon > 0$ et $X \geqslant 1$ tels que $r' X^{1-\varepsilon} \geqslant 1$. Si on suppose que les formes L_1, L_2 et Q vérifient les hypothèses **NH** et que $(\mathbf{d}, \mathbf{D}) \in \mathfrak{D}$, alors*

$$S(X, \mathbf{d}, \mathbf{D}) = 2\pi^3 \mathrm{vol}(\mathcal{R}) \mathrm{X}^2 \prod_{\mathrm{p}} \sigma_{\mathrm{p}}(\mathbf{d}, \mathbf{D}) + \mathrm{O}_\varepsilon\left(\frac{\mathrm{L}_\infty^\varepsilon \mathrm{D}^\varepsilon (\mathrm{r}_\infty \mathrm{r}' + \mathrm{r}_\infty^2) \mathrm{a}'(\mathbf{d}, \mathbf{\Delta}) \mathrm{X}^2}{\delta(\mathbf{D}) \left(\log(\mathrm{X})\right)^{\eta - \varepsilon}}\right),$$

où

$$\sigma_p(\mathbf{d},\mathbf{D}) = \left(1-\frac{\chi(p)}{p}\right)^3 \sum_{\boldsymbol{\nu}\in\mathbb{Z}^3_{\geqslant 0}} \frac{\chi(p)^{\nu_1+\nu_2+\nu_3}\rho\left(p^{N_1},p^{N_2},p^{N_3}\right)}{p^{2(N_1+N_2+N_3)}} \tag{1.22}$$

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

$$\sigma_2(\mathbf{d},\mathbf{D}) = \sigma_2(\mathbf{d}) = 4\lim_{n\to+\infty} 2^{-2n} \# \left\{ \mathbf{x}\in(\mathbb{Z}/2^n\mathbb{Z})^2 \quad \middle| \quad \begin{array}{l} L_i(\mathbf{x}) \in d_i\mathcal{E}_{2^n} \\ Q(\mathbf{x}) \in d_3\mathcal{E}_{2^n} \end{array} \right\}. \tag{1.23}$$

De plus, on a

$$\prod_p \sigma_p(\mathbf{d},\mathbf{D}) \ll L_\infty^\varepsilon D^\varepsilon a'(\mathbf{d},\boldsymbol{\Delta}). \tag{1.24}$$

Pour terminer cette section, dans l'optique de vérifier la conjecture de Peyre, il est bon de réinterpréter la constante obtenue. On définit donc pour $\lambda = (\lambda_1,\lambda_2,\lambda_3) \in \mathbb{Z}^3_{\geqslant 0}$, $\mu = (\mu_1,\mu_2,\mu_3) \in \mathbb{Z}^3_{\geqslant 0}$ et p premier différent de 2 :

$$N_{\lambda,\mu}(p^n) = \# \left\{ (\mathbf{x},\mathbf{s},\mathbf{t}) \in (\mathbb{Z}/p^n\mathbb{Z})^8 \quad \middle| \quad \begin{array}{l} L_i(\mathbf{x}) \equiv p^{\lambda_i}(s_i^2+t_i^2)\,[p^n] \\ Q(\mathbf{x}) \equiv p^{\lambda_3}(s_3^2+t_3^2)\,[p^n] \\ p^{\mu_i}|L_i(\mathbf{x}), \quad p^{\mu_3}|Q(\mathbf{x}) \end{array} \right\} \tag{1.25}$$

et

$$\omega_{\lambda,\mu} = \lim_{n\to+\infty} p^{-5n-\lambda_1-\lambda_2-\lambda_3} N_{\lambda,\mu}(p^n) \tag{1.26}$$

qui existe bien et qui correspond à la densité p-adique associée à la variété (2.1). Pour le cas $p = 2$, on introduit

$$N_{\mathbf{d}}(2^n) = \# \left\{ (\mathbf{x},\mathbf{s},\mathbf{t}) \in (\mathbb{Z}/2^n\mathbb{Z})^8 \quad \middle| \quad \begin{array}{l} L_i(\mathbf{x}) \equiv d_i(s_i^2+t_i^2)\,[2^n] \\ Q(\mathbf{x}) \equiv d_3(s_3^2+t_3^2)\,[2^n] \end{array} \right\} \tag{1.27}$$

et

$$\omega_{\mathbf{d}}(2) = \lim_{n\to+\infty} 2^{-5n} N_{\mathbf{d}}(2^n). \tag{1.28}$$

Posant enfin $\omega_\infty(\mathcal{R})$ la densité archmédienne associée à cette même variété (2.1), on obtient le résultat suivant.

Théorème 3. *Supposons que les formes L_1, L_2 et Q vérifient les hypothèses **NH** et que $(\mathbf{d},\mathbf{D}) \in \mathfrak{D}$. On a $\omega_\infty(\mathcal{R}) = \pi^3\mathrm{vol}(\mathcal{R})$, pour tout premier $p > 2$, $\omega_{\lambda,\mu} = \sigma_p(\mathbf{d},\mathbf{D})$ avec $\lambda = (\nu_p(d_1),\nu_p(d_2),\nu_p(d_3))$ et $\mu = (\nu_p(D_1),\nu_p(D_2),\nu_p(D_3))$ et $\omega_{\mathbf{d}}(2) = 2\sigma_2$.*

1.3 Propriétés de la fonction ρ

Il résulte du théorème chinois que la fonction ρ est multiplicative dans le sens où si 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 on a

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

Il suffit donc de l'étudier sur les triplets de nombres premiers. Comme mentionné précédemment, cette fonction a été abondamment étudiée pour des formes primitives. Le lemme suivant permet de se ramener à ce cas.

Lemme 1. *Soient L_1, L_2 des formes linéaires non proportionnelles et Q une forme quadratique. Avec les notations de (1.18), on a pour $\mathbf{d} \in \mathbb{N}^3$,*

$$\frac{\rho(\mathbf{d}, L_1, L_2, Q)}{(d_1 d_2 d_3)^2} = \frac{\rho(\mathbf{d}', L_1^*, L_2^*, Q^*)}{(d_1' d_2' d_3')^2} \tag{1.29}$$

où $\mathbf{d}' = \left(\frac{d_1}{(d_1, \ell_1)}, \frac{d_2}{(d_2, \ell_2)}, \frac{d_3}{(d_3, q)} \right)$.

Démonstration.– Avec les notations (1.8), $d = d_1 d_2 d_3$ et $d' = d_1' d_2' d_3'$, on pose l'application

$$\varphi : \begin{array}{ccc} (\mathbb{Z}/d\mathbb{Z})^2 & \longrightarrow & (\mathbb{Z}/d'\mathbb{Z})^2 \\ \overline{\mathbf{x}}^d & \mapsto & \overline{\mathbf{x}}^{d'}. \end{array}$$

On voit facilement que

$$\# \left(\Lambda(\mathbf{d}) \cap [0, d_1 d_2 d_3[^2 \right) = \varphi^{-1} \left(\Lambda(\mathbf{d}') \cap [0, d_1' d_2' d_3'[^2 \right)$$

ce qui implique l'égalité

$$\rho(\mathbf{d}, L_1, L_2, Q) = \#\varphi^{-1}(\Lambda(\mathbf{d}') \cap [0, d_1' d_2' d_3'[^2) = \sum_{\mathbf{x} \in \Lambda(\mathbf{d}') \cap [0, d_1' d_2' d_3'[^2} \#\varphi^{-1}(\{\mathbf{x})$$

soit

$$\rho(\mathbf{d}, L_1, L_2, Q) = \rho(\mathbf{d}', L_1^*, L_2^*, Q^*)(d_1, \ell_1)^2 (d_2, \ell_2)^2 (d_3, q)^2$$

ce qui fournit le résultat. □

Cette quantité

$$\frac{\rho(\mathbf{d}, L_1, L_2, Q)}{(d_1 d_2 d_3)^2}$$

va jouer en quelque sorte le rôle de l'inverse du covolume dans le cas où f est scindé et où $\Lambda(\mathbf{d})$ est alors un réseau. L'étude de la fonction ρ pour des formes primitives repose alors sur celle de la fonction

$$\rho^*(\mathbf{d}) = \rho^*(\mathbf{d}, L_1, L_2, Q) = \# \left\{ \mathbf{x} \in \Lambda(\mathbf{d}) \cap [0, d_1 d_2 d_3[^2 \quad | \quad (x_1, x_2, d_1 d_2 d_3) = 1 \right\} \tag{1.30}$$

qui est également multiplicative, toujours grâce au théorème chinois. On a alors les résultats suivants.

Lemme 2. *Soient L_1, L_2 des formes linéaires primitives non proportionnelles et Q une forme quadratique primitive irréductible sur $\mathbb{Q}$.*

a) Pour tout premier p et $\nu \in \mathbb{Z}_{\geqslant 0}$, on a

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

b) Si $p \nmid 2 disc(Q)$, alors

$$\rho^*(1, 1, p^\nu) = \varphi(p^\nu) \left(1 + \left(\frac{disc(Q)}{p} \right) \right).$$

De plus, si p est un facteur impair de $disc(Q)$, on a

$$\rho^*(1, 1, p^\nu) \leqslant 2\varphi(p^\nu) p^{\min([\nu_p(disc(Q))]/2, [\nu/2])}$$

et si $p = 2$,

$$\rho^*(1, 1, 2^\nu) \leqslant 2^{\nu+2}.$$

c) Pour tout nombre premier p, on a

$$\rho(p^{\nu_1},p^{\nu_2},p^{\nu_3})=\sum_{0\leqslant k\leqslant \max(\nu_1,\nu_2,\lceil \nu_3/2\rceil)} \rho^*\left(p^{\max(\nu_1-k,0)},p^{\max(\nu_2-k,0)},p^{\max(\nu_3-2k,0)}\right)p^{m_k}$$

où $m_k=2(\min(\nu_1,k)+\min(\nu_2,k)+\min(\nu_3,2k)-k)$.

d) Pour tout nombre premier p, on a $\rho^*(p^{\nu_1},p^{\nu_2},p^{\nu_3})=0$ lorsqu'il existe $1\leqslant i<j\leqslant 3$ tels que $\nu_p(\Delta_{ij})<\min(\nu_i,\nu_j)$. En particulier, cette inégalité est vérifiée dès lors que $p\nmid \Delta_{12}\Delta_{13}\Delta_{23}$ et $\#\{i\,|\,\nu_i\geqslant 1\}\geqslant 2$.

e) Pour tout nombre premier p et $\nu_3\leqslant \max(\nu_1,\nu_2)$, on a

$$\rho^*(p^{\nu_1},p^{\nu_2},p^{\nu_3})\leqslant \varphi\left(p^{\nu_1+\nu_2+\nu_3}\right)p^{\nu_3+\min(\nu_1,\nu_2,\nu_p(\Delta_{12}))}$$

et lorsque $\nu_3>\max(\nu_1,\nu_2)$, on a

$$\rho^*(p^{\nu_1},p^{\nu_2},p^{\nu_3})\leqslant 8\varphi\left(p^{\nu_1+\nu_2+\nu_3}\right)p^{\nu_1+\nu_2}p^{\min([\nu_p(disc(Q)/2)],[\nu_3/2])}.$$

Démonstration.– La preuve se trouve dans [27]. □

On en déduit alors finalement les propriétés suivantes de la fontion ρ :

Lemme 3. *On se place sous les mêmes hypothèses que dans le lemme précédent.*

a) Pour tout nombre premier p, on a

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

b) Si $p\nmid 2disc(Q)$, alors

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

De plus, si p est un facteur impair de $disc(Q)$, on a

$$\rho(1,1,p^{\nu})\ll(\nu+1)p^{\nu+\min([\nu_p(disc(Q)/2)],[\nu/2])}$$

et si $p=2$,

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

c) Lorsque $\max(\nu_1,\nu_2)\leqslant\left\lceil\frac{\nu_3}{2}\right\rceil$ et p impair, on a

$$\rho(p^{\nu_1},p^{\nu_2},p^{\nu_3})\ll(\nu_3+1)p^{2(\nu_1+\nu_2)+\nu_3}p^{\min([\nu_p(disc(Q)/2)],[\nu_3/2])}$$

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 $\max(\nu_1,\nu_2)\leqslant\left\lceil\frac{\nu_3}{2}\right\rceil$, on a

$$\rho(2^{\nu_1},2^{\nu_2},2^{\nu_3})\ll 2^{2(\nu_1+\nu_2)+\nu_3}.$$

d) Lorsque $\left\lceil \frac{\nu_3}{2} \right\rceil \leqslant \min(\nu_1, \nu_2)$ *et pour tout nombre premier, 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 $\nu_j \leqslant \left\lceil \frac{\nu_3}{2} \right\rceil \leqslant \nu_3 \leqslant \nu_i$ *avec* $\{i,j\} = \{1,2\}$ *et pour tout nombre premier* p*, on a*

$$\rho(p^{\nu_1}, p^{\nu_2}, p^{\nu_3}) \ll \nu_3 p^{2\nu_j+\nu_i+\nu_3+[\nu_3/2]} \left(p^{\min(\lceil \nu_3/2 \rceil, \lceil \nu_p(\Delta_{i3})/2 \rceil)} + p^{r_p}\right),$$

où

$$r_p = \min\left(\nu_i - \lceil \nu_3/2 \rceil, \lceil \nu_p(\Delta_{i3})/2 \rceil\right) + \min\left([\nu_3/2], [\nu_p(disc(Q))/2]\right).$$

f) On a pour tout nombre premier p*, la majoration*

$$\rho(p^{\nu_1}, p^{\nu_2}, p^{\nu_3}) \ll \min\left(p^{2(\nu_2+\nu_3)+\nu_1}, p^{2(\nu_1+\nu_3)+\nu_2}, (\nu_3+1)p^{2(\nu_1+\nu_2)+3\frac{\nu_3}{2}}\right).$$

Démonstration.– La preuve des points a) à e) se trouve également dans [27]. Démontrons donc le point f). En négligeant les deux conditions

$$p^{\nu_1} | L_1(\mathbf{x}) \quad \text{et} \quad p^{\nu_3} | Q(\mathbf{x}),$$

on obtient les majorations

$$\rho(p^{\nu_1}, p^{\nu_2}, p^{\nu_3}) \leqslant p^{2(\nu_1+\nu_3)} \rho(1, p^{\nu_2}, 1) = p^{2(\nu_2+\nu_3)+\nu_1}.$$

On obtient alors la majoration

$$\rho(p^{\nu_1}, p^{\nu_2}, p^{\nu_3}) \leqslant p^{2(\nu_1+\nu_3)+\nu_2}$$

en inversant les rôles de L_1 et L_2 et en oubliant les deux conditions sur les formes linéaires, on obtient

$$\rho(p^{\nu_1}, p^{\nu_2}, p^{\nu_3}) \leqslant p^{2(\nu_1+\nu_2)} \rho(1, 1, p^{\nu_3})$$

et on conclut grâce au point b). □

On peut déduire de ces deux lemmes que la fonction

$$f(\mathbf{d}) = \frac{\rho(\mathbf{d})}{d_1 d_2 d_3}$$

est proche, au sens de la convolution, de la fonction $R : \mathbf{d} \mapsto R(\mathbf{d}) = r_\Delta(d_3)$ avec

$$r_\Delta(l) = \sum_{k|l} \chi_\Delta(k)$$

où $\chi_\Delta(n) = \left(\frac{\Delta}{n}\right)$ est le symbole de Kronecker. On pose également h la fonction arithmétique satisfaisant

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

Cette fonction h existe car R est inversible pour la convolution car non nulle en $(1,1,1)$.

Lemme 4. *Sous les hypothèses du Théorème 1, on a*

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

En particulier,

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

où on note que $L(1,\chi_\Delta\chi)\neq 0$. En particulier, la constante obtenue dans le Théorème 1 devant X^2 est bien non nulle.

Démonstration.– On commence par justifier que $L(1,\chi_\Delta\chi)$ est non nul, ce qui revient à justifier que $\chi_\Delta\chi$ est non principal. Or, on sait que les premiers p tels que $\left(\frac{a}{p}\right)=1$ sont de densité $\frac{1}{2}$ si a n'est pas un carré ([31]). On en déduit que $\chi_\Delta\chi$ est principal si, et seulement si, le disciminant de Q est l'opposé d'un carré, ce qui est exclu car Q a été supposée irréductible sur $\mathbb{Q}[i]$.

On a

$$\prod_{p>2}\sigma_p=\prod_p\left(1-\frac{\chi(p)}{p}\right)^3\sum_{\boldsymbol{\nu}\in\mathbb{N}^3}\frac{(h*R)(p^{\nu_1},p^{\nu_2},p^{\nu_3})\chi(p^{\nu_1+\nu_2+\nu_3})}{p^{\nu_1+\nu_2+\nu_3}}.$$

Or, on sait que les facteurs eulériens d'une convolution se multiplient donc

$$\prod_{p>2}\sigma_p=\prod_p\left(1-\frac{\chi(p)}{p}\right)^3\sum_{\boldsymbol{\nu}\in\mathbb{N}^3}\frac{h(p^{\nu_1},p^{\nu_2},p^{\nu_3})\chi(p^{\nu_1+\nu_2+\nu_3})}{p^{\nu_1+\nu_2+\nu_3}}\sum_{\boldsymbol{\nu}\in\mathbb{N}^3}\frac{R(p^{\nu_3})\chi(p^{\nu_1+\nu_2+\nu_3})}{p^{\nu_1+\nu_2+\nu_3}}.$$

Or,

$$\sum_{\boldsymbol{\nu}\in\mathbb{N}^3}\frac{R(p^{\nu_3})\chi(p^{\nu_1+\nu_2+\nu_3})}{p^{\nu_1+\nu_2+\nu_3}}=\sum_{\nu_1\geqslant 0}\frac{\chi(p)^{\nu_1}}{p^{\nu_2}}\sum_{\nu_2\geqslant 0}\frac{\chi(p)^{\nu_2}}{p^{\nu_2}}\sum_{\nu_3\geqslant 0}\frac{\chi(p)^{\nu_3}(\mathbf{1}*\chi_\Delta)(p)^{\nu_3}}{p^{\nu_3}}$$

en utilisant à nouveau que

$$\sum_{\nu_3\geqslant 0}\frac{\chi(p)^{\nu_3}(\mathbf{1}*\chi_\Delta)(p)^{\nu_3}}{p^{\nu_3}}=\sum_{\nu_3\geqslant 0}\frac{\chi(p)^{\nu_3}\chi_\Delta(p)^{\nu_3}}{p^{\nu_3}}\sum_{\nu_3\geqslant 0}\frac{\chi(p)^{\nu_3}}{p^{\nu_3}}$$

on en déduit l'égalité

$$\prod_{p>2}\sigma_p=\prod_p\left(1-\frac{\chi(p)}{p}\right)^3\left(1-\frac{\chi(p)}{p}\right)^{-3}\sum_{\boldsymbol{\nu}\in\mathbb{N}^3}\frac{h(p^{\nu_1},p^{\nu_2},p^{\nu_3})\chi(p^{\nu_1+\nu_2+\nu_3})}{p^{\nu_1+\nu_2+\nu_3}}\sum_{\nu_3\geqslant 0}\frac{\chi(p)^{\nu_3}\chi_\Delta(p)^{\nu_3}}{p^{\nu_3}}$$

soit

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

On a ici utilisé le fait que

$$L(1,\chi_\Delta\chi)\ll 1.$$

Ce passage est à justifier puisqu'a priori la constante dépend des coefficients des formes et qu'on cherche des estimations suffisamment uniforme en les coefficients de ces formes (cf après le Lemme 30 et avant le Théorème 6), où par suffisamment uniforme on veut

dire qu'on autorise la constante à dépendre de la classe d'équivalence des formes linéaires obtenues par des transformations linéaires $\mathbf{x} \mapsto E\mathbf{x}$ de la forme (1.63). Mais, un changement de variable linéaire $\mathbf{x} \mapsto \mathbf{M}\mathbf{x}$ avec $\mathbf{M}$ une matrice à coefficients entiers inversible donne lieu à une transformation du discriminant Δ en $\det(\mathbf{M})^2\Delta$ et donc $\chi_{\det(\mathbf{M})^2\Delta} = \chi_\Delta$ et la constante $L(1, \chi_\Delta\chi)$ est indépendante de la classe d'équivalence des formes par de telles transformations linéaires, ce qui est par conséquent convenable. De plus, comme par définition, $\sigma_2 \leqslant 4$, on en déduit que

$$\prod_p \sigma_p \ll L_\infty^\varepsilon.$$

Passons maintenant à la preuve de la première partie du lemme. Puisque les fonctions f et R sont multiplicatives, la fonction h l'est aussi et $|h|$ aussi et donc en notant la somme à majorer $P = P(L_1, L_2, Q)$

$$P = \prod_p \left(1 + \sum_{\boldsymbol{\nu} \in (\mathbb{N}^*)^3} \frac{|h(p^{\nu_1}, p^{\nu_2}, p^{\nu_3})|}{p^{\nu_1+\nu_2+\nu_3}}\right).$$

Commençons par nous ramener au cas de formes primitives. On note $P_p = P_p(L_1, L_2, Q)$ le facteur relatif au nombre premier p du produit ci-dessus. Lorsque $p \nmid \ell_1\ell_2 q$, le Lemme 1 donne, puisque $\mathbf{d}' = \mathbf{d}$, que

$$\rho(p^{n_1}, p^{n_2}, p^{n_3}, L_1, L_2, Q) = \rho(p^{n_1}, p^{n_2}, p^{n_3}, L_1^*, L_2^*, Q^*)$$

et donc

$$P(L_1, L_2, Q) = \prod_{p \nmid \ell_1\ell_2 q} P_p(L_1^*, L_2^*, Q^*) \prod_{p \mid \ell_1\ell_2 q} P_p(L_1, L_2, Q) = P'(L_1^*, L_2^*, Q^*) \prod_{p \mid \ell_1\ell_2 q} \frac{P_p(L_1, L_2, Q)}{P_p(L_1^*, L_2^*, Q^*)}.$$

On sait que l'inverse de la fonction

$$r_\Delta(n) = \sum_{k \mid n} \chi_\Delta(k)$$

est donnée par $\theta(1) = 1$ et

$$\theta(n) = -\sum_{\substack{d \mid n \\ d < n}} r_\Delta\left(\frac{n}{d}\right)\theta(d).$$

On en déduit en particulier que

$$\theta(p) = -r_\Delta(p) = \mu(p)(1 + \chi_\Delta(p)),$$

puis

$$\theta(p^2) = -r_\Delta(p^2) - r_\Delta(p)\theta(p) = -r_\Delta(p^2) + 1 + 2\chi_\Delta(p) + 1$$

car $\chi_\Delta(p)^2 = 1$. D'où,

$$\theta(p^2) = -1 - \chi_\Delta(p) - 1 + 2 + 2\chi_\Delta(p) = \chi_\Delta(p).$$

Passons alors aux cas $n \geqslant 3$,

$$\theta(p^3) = -r_\Delta(p^3) - r_\Delta(p^2)\theta(p) - r_\Delta(p)\theta(p^2)$$

soit

$$\begin{aligned}\theta(p^3) &= -r_\Delta(p^3) + r_\Delta(p^2)r_\Delta(p) - r_\Delta(p)\chi_\Delta(p)\\ &= -2 - \chi_\Delta(p) - \chi_\Delta(p) + 1 + 2 + 3\chi_\Delta(p) - 1 - \chi_\Delta(p) = 0\end{aligned}$$

car les puissances paires de $\chi_\Delta(p)$ valent 1 tandis que les puissances impaires valent $\chi_\Delta(p)$. On montre alors par récurrence que $\theta(p^n) = 0$ si $n \geqslant 3$. On l'a fait pour $n = 3$, supposons donc $n \geqslant 4$, alors par hypothèse de récurrence

$$\theta(p^n) = -r_\Delta(p^n) - r_\Delta(p^{n-1})\theta(p) = r_\Delta(p^{n-2})\theta(p^2)$$

et un calul similaire à ci-dessus fournit

$$\theta(p^n) = -r_\Delta(p^n) + r_\Delta(p^{n-1}) + (r_\Delta(p^n) - 1) - (r_\Delta(p^{n-1}) - 1) = 0.$$

En conclusion, on a démontré les relations

$$\theta(p^n) = \begin{cases} \mu(p^n)(1 + \chi_\Delta(p^n)) & \text{si } n = 1 \quad \text{ou } n \geqslant 3\\ \chi_\Delta(p) & \text{sinon.}\end{cases}$$

Montrons alors l'égalité

$$R^{(-1)}(d_1, d_2, d_3) = \mu(d_1)\mu(d_2)\theta(d_3).$$

On a

$$(R^{(-1)} * R)(\mathbf{d}) = \sum_{k_i|d_i} \mu(k_1)\mu(k_2)\theta(k_3) r_\Delta\left(\frac{d_3}{k_3}\right) = \sum_{k_1|d_1} \mu(k_1) \sum_{k_2|d_2} \mu(k_2) \sum_{k_3|d_3} \theta(k_3) r_\Delta\left(\frac{d_3}{k_3}\right)$$

donc

$$(R^{(-1)} * R)(\mathbf{d}) = \delta(d_1)\delta(d_2)\delta(d_3) = \delta(d_1 d_2 d_3),$$

ce qui montre bien le résultat. En particulier, on a donc $|R^{(-1)}(\mathbf{d})| \leqslant 2$ et plus précisément $|R^{(-1)}(\mathbf{d})| \leqslant R(\mathbf{d})$ donc

$$|h(p^{\nu_1}, p^{\nu_2}, p^{\nu_3})| = |(f * R^{(-1)})(p^{\nu_1}, p^{\nu_2}, p^{\nu_3})| \leqslant (f * R)(p^{\nu_1}, p^{\nu_2}, p^{\nu_3}).$$

On a donc

$$P_p \leqslant \left(1 + \sum_{\boldsymbol{\nu} \in (\mathbb{N}^*)^3} \frac{R(p^{\nu_1}, p^{\nu_2}, p^{\nu_3})}{p^{\nu_1+\nu_2+\nu_3}}\right) P'_p$$

avec

$$P'_p = P'_p(L_1, L_2, Q) = 1 + \sum_{\boldsymbol{\nu} \in (\mathbb{N}^*)^3} \frac{\rho(p^{\nu_1}, p^{\nu_2}, p^{\nu_3})}{p^{2(\nu_1+\nu_2+\nu_3)}}$$

puisqu'une convolution se transforme en produit en termes de séries de Dirichlet et en remplaçant f par son expression. En raisonnant comme dans le traitement de $S_{0,m}(X) \ll X(\log(X))^\varepsilon$ ci-dessous, en majorant R par $\tau(d_3)$, on obtient la majoration

$$\sum_{\substack{\boldsymbol{\nu} \in (\mathbb{N}^*)^3 \\ \nu_1+\nu_2+\nu_3 \geqslant 2}} \frac{R(p^{\nu_1}, p^{\nu_2}, p^{\nu_3})}{p^{\nu_1+\nu_2+\nu_3}} \ll \frac{1}{p^2}$$

ce qui permet de négliger ces termes. On traite alors

$$\sum_{\substack{\boldsymbol{\nu}\in(\mathbb{N}^*)^3\\ \nu_1+\nu_2+\nu_3=1}} \frac{R(p^{\nu_1},p^{\nu_2},p^{\nu_3})}{p} \ll 3\times\frac{2}{p}\ll 1$$

avec une constante C indépendante des formes. On en déduit que la contribution des

$$\prod_{p|\ell_1\ell_2 q}\left(1+\sum_{\boldsymbol{\nu}\in(\mathbb{N}^*)^3}\frac{R(p^{\nu_1},p^{\nu_2},p^{\nu_3})}{p^{\nu_1+\nu_2+\nu_3}}\right)$$

est

$$\ll L_\infty^{\varepsilon}$$

puisqu'on majore par une constante puissance $\omega(\ell_1\ell_2 q)$ et que $C^{\omega(n)}\ll n^{\varepsilon}$. Maintenant d'après l'étude de la fonction ρ effectuée ci-dessus, on a

$$\frac{\rho(p^{\nu_1+\nu_p(\ell_1)},p^{\nu_2+\nu_p(\ell_2)},p^{\nu_3+\nu_p(Q)})}{p^{2(\nu_1+\nu_2+\nu_3+\nu_p(\ell_1)+\nu_p(\ell_2)+\nu_p(Q))}}=\frac{\rho(p^{\nu_1},p^{\nu_2},p^{\nu_3};L_1^*,L_2^*,Q^*)}{p^{2(\nu_1+\nu_2+\nu_3)}}$$

donc

$$\frac{\rho(p^{\nu_1},p^{\nu_2},p^{\nu_3};L_1,L_2,Q)}{p^{2(\nu_1+\nu_2+\nu_3)}}\leqslant\frac{\rho(p^{\nu_1'},p^{\nu_2'},p^{\nu_3'};L_1^*,L_2^*,Q^*)}{p^{2(\nu_1'+\nu_2'+\nu_3')}}$$

avec

$$\nu_i'=\max(\nu_i-\nu_p(\ell_i),0)\quad\text{et}\quad\nu_3'=\max(\nu_3-\nu_p(q),0).$$

Si on se fixe tous les ν_i', on a au plus $(\nu_p(\ell_1)+1)(\nu_p(\ell_2)+1)(\nu_p(q)+1)$ triplets $\boldsymbol{\nu}$, donc en dénombrant selon les ν', on obtient l'inégalité

$$P_p'\leqslant(\nu_p(\ell_1)+1)(\nu_p(\ell_2)+1)(\nu_p(q)+1)\left(1+\sum_{\boldsymbol{\nu}'\in(\mathbb{N}^*)^3}\frac{\rho(p^{\nu_1'},p^{\nu_2'},p^{\nu_3'};L_1^*,L_2^*,Q^*)}{p^{2(\nu_1'+\nu_2'+\nu_3')}}\right).$$

De plus, utilisant le fait que $f=h*r$ et le comportement des facteurs eulériens vis-à-vis de la convolution, on déduit que

$$P_p'\leqslant(\nu_p(\ell_1)+1)(\nu_p(\ell_2)+1)(\nu_p(q)+1)P_p(L_1^*,L_2^*,Q^*)\left(1+\sum_{\boldsymbol{\nu}\in(\mathbb{N}^*)^3}\frac{R(p^{\nu_1},p^{\nu_2},p^{\nu_3})}{p^{\nu_1+\nu_2+\nu_3}}\right).$$

Finalement, on en déduit

$$P_p(L_1,L_2,Q)\leqslant(\nu_p(\ell_1)+1)(\nu_p(\ell_2)+1)(\nu_p(q)+1)P_p(L_1^*,L_2^*,Q^*)\left(1+\sum_{\boldsymbol{\nu}\in(\mathbb{N}^*)^3}\frac{R(p^{\nu_1},p^{\nu_2},p^{\nu_3})}{p^{\nu_1+\nu_2+\nu_3}}\right)^2$$

et donc

$$\prod_{p|\ell_1\ell_2 q}\frac{P_p(L_1,L_2,Q)}{P_p(L_1^*,L_2^*,Q^*)}\leqslant L_\infty^{\varepsilon}.$$

En effet,

$$(\nu_p(\ell_1)+1)(\nu_p(\ell_2)+1)(\nu_p(q)+1)\leqslant\tau(\ell_1)\tau(\ell_2)\tau(q)$$

et que chaque τ est $\ll L_\infty^\varepsilon$. On est donc ramené à démontrer dans le cas de formes primitives que

$$P(L_1^*, L_2^*, Q^*) \ll L_\infty^\varepsilon.$$

Dans la suite on suppose donc les formes L_1, L_2 et Q primitives et nous majorons P. On a puisque $h = f * R^{(-1)}$

$$h(p^\nu, 1, 1) = \sum_{k=0}^{\nu} \mu(p^{n-k}) \frac{\rho(p^k, 1, 1)}{p^k} = \rho(1, 1, 1) - \frac{\rho(p^n, 1, 1)}{p^n} = 0$$

d'après l'étude ci-dessus. De même, on obtient que $h(1, p^\nu, 1) = 0$. On suppose alors que $p \nmid 2\Delta$, alors

$$\begin{aligned} h(1, 1, p) &= f(1, 1, 1) r^{(-1)}(1, 1, p) + f(1, 1, p) r^{(-1)}(1, 1, 1) \\ &= -1 - \chi_\Delta(p) + \left(1 - \tfrac{1}{p}\right)(1 + \chi_\Delta(p)) + \tfrac{1}{p} \end{aligned}$$

toujours d'après l'étude de ρ. D'où

$$h(1, 1, p) = -\frac{1}{p} \chi_\Delta(p)$$

et

$$h(1, 1, p^\nu) = \sum_{k=0}^{\nu} f(1, 1, p^{\nu-k}) R^{(-1)}(1, 1, p^k)$$

donc

$$h(1, 1, p^\nu) = f(1, 1, p^\nu) R^{(-1)}(1, 1, 1) + f(1, 1, p^{\nu-1}) R^{(-1)}(1, 1, p) + f(1, 1, p^{\nu-2}) R^{(-1)}(1, 1, p^2)$$

les autres termes étant nuls. On a donc puisque $f(1, 1, p^k) \leqslant k + 1$ et $R^{(-1)}(\mathbf{d}) \leqslant 2$ que

$$h(1, 1, p^\nu) \leqslant 6(\nu + 1) \ll \nu + 1.$$

On peut en déduire, lorsque $p \nmid 2\Delta$, que la contribution dans la somme de P_p des termes tels $\#\{i | \nu_i \geqslant 1\} \leqslant 1$ est un $O(1/p^2)$. En effet, cette contribution est majorée d'après ce qui précède par

$$\ll \sum_{\nu \geqslant 2} \frac{\nu + 1}{p^\nu}.$$

De plus, on a

$$|h(p^{\nu_1}, p^{\nu_2}, p^{\nu_3})| \leqslant 2 \sum_{\substack{\mathbf{n} \in \mathbf{Z}^3_{\geqslant 0} \\ n_j \leqslant \nu_j}} f(p^{n_1}, p^{n_2}, p^{n_3})$$

soit

$$|h(p^{\nu_1}, p^{\nu_2}, p^{\nu_3})| \leqslant 2 \prod_{i=1}^{3} (\nu_i + 1) \max_{\substack{\mathbf{n} \in \mathbf{Z}^3_{\geqslant 0} \\ n_j \leqslant \nu_j}} f(p^{n_1}, p^{n_2}, p^{n_3})$$

et donc

$$|h(p^{\nu_1}, p^{\nu_2}, p^{\nu_3})| \ll \prod_{i=1}^{3} (\nu_i + 1)^2 p^{\nu_1 + \nu_2 + \nu_3 + k_p - \max(\nu_1 + \nu_2, \nu_1 + \lceil \nu_3/2 \rceil, \nu_2 + \lceil \nu_3/2 \rceil, \nu_3)}$$

où

$$k_p = [\nu_p(\Delta/2)] + \nu_p(\Delta_{12}\Delta_{13}\Delta_{23})$$

d'après toujours l'étude de ρ. En effet, commençons par établir que

$$f(p^{n_1}, p^{n_2}, p^{n_3}) \ll (n_3+1)p^{n_1+n_2+n_3+k_p-\max(n_1+n_2, n_1+\lceil n_3/2\rceil, n_2+\lceil n_3/2\rceil, n_3)}.$$

Dans un premier temps, on suppose que $n_1+n_2 \leqslant \min(n_1+\lceil n_3/2\rceil, n_2+\lceil n_3/2\rceil)$, ce qui implique que $\max(n_1,n_2) \leqslant \lceil n_3/2\rceil$, on a donc

$$f(p^{n_1}, p^{n_2}, p^{n_3}) \ll (n_3+1)p^{2n_1+2n_2+n_3+k_p-n_1-n_2-n_3} \ll (n_3+1)p^{n_1+n_2+k_p}.$$

Or, si les deux inégalités $n_i \leqslant \lceil n_3/2\rceil$ sont strictes , alors $n_1+n_2 \leqslant n_3$ et $\max(n_1+\lceil n_3/2\rceil, n_2+\lceil n_3/2\rceil) \leqslant n_3$ donc le max vaut n_3 et on a donc

$$(n_3+1)p^{n_1+n_2+n_3+k_p-\max(n_1+n_2, n_1+\lceil n_3/2\rceil, n_2+\lceil n_3/2\rceil, n_3)} = (n_3+1)p^{n_1+n_2+k_p}$$

qui convient donc. Le cas de $n_1 = n_2 = \lceil n_3/2\rceil$ est traité par le cas d) du Lemme 3 et le cas (l'autre se traitant par symétrie) où $n_1 = \lceil n_3/2\rceil$ et $n_2 < \lceil n_3/2\rceil$ est traité par le cas e) du Lemme 3. On a donc traité le cas $n_1+n_2 < \min(n_1+\lceil n_3/2\rceil, n_2+\lceil n_3/2\rceil)$.
On traite alors le cas où $n_1+n_2 \geqslant \min(n_1+\lceil n_3/2\rceil, n_2+\lceil n_3/2\rceil)$. On commence par le cas où $n_1+\lceil n_3/2\rceil \leqslant n_1+n_2$ et $n_2+\lceil n_3/2\rceil \leqslant n_1+n_2$. Cela implique que $\lceil n_3/2\rceil \leqslant \min(n_1,n_2)$ et puisque $n_3 \leqslant 2\lceil n_3/2\rceil \leqslant n_1+n_2$, le max est alors n_1+n_2. On a alors grâce au Lemme 3 que

$$f(p^{n_1}, p^{n_2}, p^{n_3}) \ll p^{n_1+n_2+2n_3+k_p-n_1-n_2-n_3} \ll (n_3+1)p^{n_3+k_p}$$

tandis que

$$(n_3+1)p^{n_1+n_2+n_3+k_p-\max(n_1+n_2, n_1+\lceil n_3/2\rceil, n_2+\lceil n_3/2\rceil, n_3)} = (n_3+1)p^{n_3+k_p}$$

ce qui convient.
On traite alors le cas $n_1+\lceil n_3/2\rceil \leqslant n_1+n_2 \leqslant n_2+\lceil n_3/2\rceil$ (on traite de même le cas symétrique en inversant les rôles de 1 et 2). Cela implique que $n_1 \leqslant \lceil n_3/2\rceil \leqslant n_2$. On suppose alors dans un premier temps que $n_1 \leqslant \lceil n_3/2\rceil \leqslant n_3 \leqslant n_2$ et on obtient

$$f(p^{n_1}, p^{n_2}, p^{n_3}) \ll p^{2n_1+n_2+n_3+[n_3/2]+k_p-n_1-n_2-n_3} \ll (n_3+1)p^{n_1+[n_3/2]+k_p}.$$

Le maximum vaut dans ce cas, $n_2+\lceil n_3/2\rceil$ donc

$$\begin{aligned}(n_3+1)p^{n_1+n_2+n_3+k_p-\max(n_1+n_2, n_1+\lceil n_3/2\rceil, n_2+\lceil n_3/2\rceil, n_3)} &= (n_3+1)p^{n_1+n_3-\lceil n_3/2\rceil+k_p}\\ &= (n_3+1)p^{n_1+[n_3/2]+k_p}\end{aligned}$$

ce qui convient. Il reste alors à traiter le cas où $n_1 \leqslant \lceil n_3/2\rceil \leqslant n_2 < n_3$ où le maximum reste inchangé et où

$$f(p^{n_1}, p^{n_2}, p^{n_3}) \ll 2n_3 p^{2n_1+n_2+n_3+[n_3/2]+k_p-n_1-n_2-n_3} \ll (n_3+1)p^{n_1+[n_3/2]+k_p}$$

(on majore p^{r_p} et $p^{\min([n_3/2],\lceil\nu_p(\Delta_{13})\rceil)}$ par p^{k_p} d'où l'apparition du 2) et on conclut comme ci-dessus. On a donc bien obtenu

$$f(p^{n_1}, p^{n_2}, p^{n_3}) \ll (n_3+1)p^{n_1+n_2+n_3+k_p-\max(n_1+n_2, n_1+\lceil n_3/2\rceil, n_2+\lceil n_3/2\rceil, n_3)}.$$

Montrons désormais la majoration

$$\max_{\substack{\mathbf{n}\in\mathbf{Z}^3_{\geqslant 0}\\ n_j\leqslant\nu_j}} f(p^{n_1},p^{n_2},p^{n_3}) \ll \max_{\substack{\mathbf{n}\in\mathbf{Z}^3_{\geqslant 0}\\ n_j\leqslant\nu_j}} (n_3+1)p^{n_1+n_2+n_3+k_p-\max(n_1+n_2,n_1+\lceil n_3/2\rceil,n_2+\lceil n_3/2\rceil,n_3)}$$

$$\ll (\nu_3+1)p^{\nu_1+\nu_2+\nu_3+k_p-\max(\nu_1+\nu_2,\nu_1+\lceil \nu_3/2\rceil,\nu_2+\lceil \nu_3/2\rceil,\nu_3)}$$

où il faut bien faire attention au fait que f (tout comme l'argument du maximum dans le membre de droite de l'inégalité ci-dessus) n'est pas croissante avec (n_1,n_2,n_3). Il faut aussi voir que l'indice qui réalise le maximum des trois entiers $(n_{1,0},n_{2,0},n_{3,0})$ où $(n_{1,0},n_{2,0},n_{3,0})$ réalise le maximum ci-dessus n'est pas nécessairement le même que celui qui réalise le maximum des trois entiers (ν_1,ν_2,ν_3). Supposons dans un premier temps que ν_3 est le maximum. Il s'agit alors de montrer que

$$\max_{\substack{\mathbf{n}\in\mathbf{Z}^3_{\geqslant 0}\\ n_j\leqslant\nu_j}} p^{n_1+n_2+n_3+k_p-\max(n_1+n_2,n_1+\lceil n_3/2\rceil,n_2+\lceil n_3/2\rceil,n_3)} \ll p^{\nu_1+\nu_2+\nu_3+k_p-\max(\nu_1+\nu_2,\nu_1+\lceil \nu_3/2\rceil,\nu_2+\lceil \nu_3/2\rceil,\nu_3)}$$

soit

$$\max_{\substack{\mathbf{n}\in\mathbf{Z}^3_{\geqslant 0}\\ n_j\leqslant\nu_j}} p^{n_1+n_2+n_3+k_p-\max(n_1+n_2,n_1+\lceil n_3/2\rceil,n_2+\lceil n_3/2\rceil,n_3)} \ll p^{\nu_1+\nu_2+k_p}.$$

Il faut alors à nouveau traiter tous les cas. Pour les indices tels que n_3 est le maximum, on a un terme

$$p^{n_1+n_2+k_p} \ll p^{\nu_1+\nu_2+k_p}.$$

Si, n_1+n_2 est le maximum, alors on a un terme

$$p^{n_3+k_p} \ll p^{n_1+n_2+k_p} \ll p^{\nu_1+\nu_2+k_p}$$

puisque $n_3 \leqslant n_1+n_2$. Lorsque $n_1+\lceil n_3/2\rceil$ est le maximum, on a de même

$$p^{n_2+[n_3/2]+k_p} \ll p^{n_1+n_2+k_p} \ll p^{\nu_1+\nu_2+k_p}$$

puisque $n_3 \leqslant n_1+\lceil n_3/2\rceil$, on a $[n_3/2]\leqslant n_1$, ce qui conclut ce premier cas. Supposons alors désormais que $\nu_1+\nu_2$ est le maximum. Il faut alors montrer l'inégalité

$$\max_{\substack{\mathbf{n}\in\mathbf{Z}^3_{\geqslant 0}\\ n_j\leqslant\nu_j}} p^{n_1+n_2+n_3+k_p-\max(n_1+n_2,n_1+\lceil n_3/2\rceil,n_2+\lceil n_3/2\rceil,n_3)} \ll p^{\nu_3+k_p}.$$

Lorsque n_3 est le maximum, on a

$$p^{n_1+n_2+k_p} \ll p^{n_3+k_p} \ll p^{\nu_3+k_p}$$

puis lorsque n_1+n_2 est le maximum, on a

$$p^{n_3+k_p} \ll p^{\nu_3+k_p}$$

et enfin lorsque $n_1+\lceil n_3/2\rceil$ est le maximum, on a

$$p^{n_2+[n_3/2]+k_p} \ll p^{n_3+k_p} \ll p^{\nu_3+k_p}$$

puisque $n_1+n_2 \leqslant n_1+\lceil n_3/2\rceil$ donc $n_2 \leqslant \lceil n_3/2\rceil$. Il reste alors à traiter le cas (l'autre se traitant par symétrie) où le maximum vaut $\nu_1+\lceil \nu_3/2\rceil$. On doit alors montrer la majoration

$$\max_{\substack{\mathbf{n}\in\mathbf{Z}^3_{\geqslant 0}\\ n_j\leqslant\nu_j}} p^{n_1+n_2+n_3+k_p-\max(n_1+n_2,n_1+\lceil n_3/2\rceil,n_2+\lceil n_3/2\rceil,n_3)} \ll p^{\nu_2+[\nu_3/2]+k_p}.$$

Lorsque n_3 est le maximum, on obtient

$$p^{n_1+n_2+k_p} \ll p^{n_2+[n_3/2]+k_p} \ll p^{\nu_2+[\nu_3/2]+k_p}$$

puisque $n_1+\lceil n_3/2\rceil \leqslant n_3$ donc $n_1 \leqslant [n_3/2]$. Ensuite, si n_1+n_2 est le maximum, on a

$$p^{n_3+k_p} \ll p^{n_2+[n_3/2]+k_p} \ll p^{\nu_2+[\nu_3/2]+k_p}$$

puisque $n_1+\lceil n_3/2\rceil \leqslant n_1+n_2$ donc $\lceil n_3/2\rceil \leqslant n_2$ et $n_3=\lceil n_3/2\rceil+[n_3/2]$. Et enfin, lorsque $n_1+\lceil n_3/2\rceil$ est le maximum, on obtient que

$$p^{n_2+[n_3/2]+k_p} \ll p^{\nu_2+[\nu_3/2]+k_p}$$

et lorsque $n_2+\lceil n_3/2\rceil$,

$$p^{n_1+[n_3/2]+k_p} \ll p^{\nu_2+[\nu_3/2]+k_p}$$

car $n_1+\lceil n_3/2\rceil \leqslant n_2+\lceil n_3/2\rceil$ donc $n_1 \leqslant n_2$ ce qui achève la preuve de la majoration

$$\max_{\substack{\mathbf{n}\in\mathbf{Z}^3_{\geqslant 0}\\ n_j\leqslant\nu_j}} f(p^{n_1},p^{n_2},p^{n_3}) \ll (\nu_3+1)p^{\nu_1+\nu_2+\nu_3+k_p-\max(\nu_1+\nu_2,\nu_1+\lceil\nu_3/2\rceil,\nu_2+\lceil\nu_3/2\rceil,\nu_3)}.$$

On utilisera lorsque $\max(\nu_1,\nu_2)=1=\nu_3$ et $p\nmid 2\Delta\Delta_{12}\Delta_{13}\Delta_{23}$ l'inégalité qui s'en déduit

$$|h(p^{\nu_1},p^{\nu_2},p^{\nu_3})| \ll p^{\nu_1+\nu_2+\nu_3-2}.$$

On regarde alors la contribution des termes tels que $\#\{i|\nu_i\geqslant 1\}\geqslant 2$. En effet, lorsque $p\nmid 2\Delta\Delta_{12}\Delta_{13}\Delta_{23}$, on a

$$\frac{|h(p^{\nu_1},p^{\nu_2},p^{\nu_3})|}{p^{\nu_1+\nu_2+\nu_3}} \ll \frac{1}{p^{\max(\nu_1+\nu_2,\nu_1+\lceil\nu_3/2\rceil,\nu_2+\lceil\nu_3/2\rceil,\nu_3)}}.$$

Mais la condition $\#\{i|\nu_i\geqslant 1\}\geqslant 2$ garantit que

$$\max(\nu_1+\nu_2,\nu_1+\lceil\nu_3/2\rceil,\nu_2+\lceil\nu_3/2\rceil,\nu_3)\geqslant 2$$

et donc on obtient du $1+O(1/p^2)$ ce qui fait que

$$\prod_{p\nmid 2\Delta\Delta_{12}\Delta_{13}\Delta_{23}} P_p \ll 1$$

et on montre comme ci-dessus que

$$\prod_{p|2\Delta\Delta_{12}\Delta_{13}\Delta_{23}}\left(1+\sum_{\boldsymbol{\nu}\in(\mathbb{N}^*)^3}\frac{R(p^{\nu_1},p^{\nu_2},p^{\nu_3})}{p^{\nu_1+\nu_2+\nu_)}}\right)\ll L_\infty^\varepsilon.$$

Pour conclure, il ne reste donc plus qu'à montrer que

$$\prod_{p|2\Delta\Delta_{12}\Delta_{13}\Delta_{23}} P'_p \ll L_\infty^\varepsilon.$$

Pour cela, on utilise à nouveau l'étude de la fonction ρ. On a dans le cas où $\max(\nu_1,\nu_2) \leqslant \lceil \nu_3/2 \rceil$ une contribution

$$\ll \sum_{\nu_3 \leqslant 1} (\nu_3+1) p^{\min([\nu_p(\Delta)],[\nu_3/2])-\nu_3}$$

puisque le terme $p^{2(\nu_1+\nu_2)+\nu_3}$ se simplifie avec le $p^{2(\nu_1+\nu_2+\nu_3)}$ au dénominateur. On a donc

$$\ll \sum_{\nu_3 \leqslant 1} (\nu_3+1) p^{-\lceil \nu_3/2 \rceil} \ll \frac{1}{p}.$$

De même, lorsque $\max(\lceil \nu_3/2 \rceil, 1) \leqslant \nu_2 \leqslant \nu_1$, on a une contribution

$$\ll \sum_{1 \leqslant \nu_2 \leqslant \nu_1} p^{\min(\nu_2,\nu_p(\Delta_{12}))-\nu_1-\nu_2}$$

soit

$$\ll \sum_{1 \leqslant \nu_2 \leqslant \nu_1} p^{-\nu_1} = \sum_{\nu_1 \geqslant 1} \sum_{1 \leqslant \nu_2 \leqslant \nu_1} p^{-\nu_1} = \sum_{\nu_1 \geqslant 1} \nu_1 p^{-\nu_1} \ll \frac{1}{p}$$

et de même en intervertissant les indices 1 et 2. Enfin, on traite les dernier cas de la même manière (point e) du Lemme 3 et cas où deux des ν_i sont nuls) pour obtenir que

$$P'_p = 1 + O\left(\frac{1}{p}\right)$$

et comme on l'a déjà vu, on peut en déduire que

$$\prod_{p|2\Delta\Delta_{12}\Delta_{13}\Delta_{23}} P'_p \ll \prod_{p|2\Delta\Delta_{12}\Delta_{13}\Delta_{23}} 1 + O\left(\frac{1}{p}\right) \ll L_\infty^\varepsilon.$$

□

1.4 Démonstration du Théorème 1

1.4.1 Quelques outils de théorie analytique des nombres

On note $\mathcal{M}(A,B)$ la classe des fonctions arithmétiques h telles pour tout p premier et tout entier ℓ

$$h(p^\ell) \leqslant A^\ell$$

pour une constante A et telles que pour tout $\varepsilon > 0$, pour tout entier naturel n,

$$h(n) \ll n^\varepsilon$$

pour une certaine fonction $B = B(\varepsilon)$. Soit $F \in \mathbb{Z}[x_1, x_2]$ une forme binaire non nulle de degré d, de discriminant non nul, que l'on met sous la forme

$$F(x_1, x_2) = x_1^{d_1} x_2^{d_2} G(x_1, x_2) \tag{1.31}$$

où d_1, $d_2 \in \{0, 1\}$ et G est une forme binaire de degré $d - d_1 - d_2$ de discriminant non nul et telle que $G(1, 0) = G(0, 1) \neq 0$. On considére également la quantité pour tout entier m non nul

$$\rho_F^*(m) = \frac{1}{\varphi(m)} \# \left\{ (n_1, n_2) \in]\!]0, m]\!]^2 \quad \middle| \quad \begin{array}{l} (n_1, n_2, m) = 1 \\ F(n_1, n_2) \equiv 0[m] \end{array} \right\}. \tag{1.32}$$

Enfin, on dit qu'un nombre premier p est un diviseur fixe pour un polynôme $f \in \mathbb{Z}[x]$ si $p | f(n)$ pour tout n.

Théorème 4. *Soient $h \in \mathcal{M}(A, B)$, X_1, $X_2 > 0$ et F comme ci-dessus. Alors, on a pour tout $\varepsilon > 0$:*

$$\sum_{|n_1| \leqslant X_1} \sum_{|n_2| \leqslant X_2} h(|F(n_1, n_2)|) \ll_{A,B,\varepsilon} ||F||^{\varepsilon} \left(X_1 X_2 E + \max X_1, {X_2}^{1+\varepsilon} \right), \tag{1.33}$$

où

$$E = \prod_{d < p \leqslant \min(X_1, X_2)} \left(1 + \frac{\rho_G^*(p)(h(p) - 1)}{p} \right) \prod_{i=1,2} \prod_{p \leqslant X_i} \left(1 + \frac{d_i(h(p) - 1)}{p} \right). \tag{1.34}$$

Démonstration.– La preuve constitue le cœur de l'article [28]. □

On a également besoin de l'amélioration suivante d'un théorème dû à Nair où Régis de la Bretèche et Tim Browning parviennent notamment à remplacer un terme exponentiel et à expliciter les dépendances en le discriminant.

Théorème 5. *Soient une fonction multiplicative $h \in \mathcal{M}(A, B)$ et f de degré d sans racine multiple et n'admettant aucun nombre premier comme diviseur fixe et $\delta \in]0, 1[$. Alors, il existe une constante $C = C(A, B, d, \delta)$ telle que*

$$\sum_{1 \leqslant n \leqslant X} h(|f(n)|) \ll_{A,B,\delta} X \prod_{p \leqslant X} \left(1 - \frac{\rho_f(p)}{p} \right) \sum_{1 \leqslant m \leqslant X} \frac{h(m)\rho_f(m)}{m}$$

pour $X \geqslant C||f||^{\delta}$.

Démonstration.– La preuve se trouve dans [28]. □

La preuve fait apparaître les résultats suivants sur les nombres premiers qui sont des diviseurs fixes dont on a besoin et qui sont tirés de [28]. On commence par remarquer qu'un premier qui est un diviseur fixe est nécessairement majoré par le degré du polynôme en question. En effet, soit p un tel nombre premier pour un polynôme f primitif de degré d. On a alors pour tout x entier

$$f(x) \equiv f_1(x) ... f_k(x) \equiv 0[p]$$

où les f_i sont des irréductibles de $\mathbb{F}_p[X]$ deux à deux non associés et où le fait d'être primitif implique que $f \not\equiv 0[p]$. En particulier, la fonction polynômiale associée à $f_1...f_k$ est nulle mais pas le polynôme f et on sait que le noyau du morphisme d'évaluation sur $\mathbb{F}_p[X]$ est engendré par $X^p - X$ donc on en déduit que $X^p - X$ divise $f_1...f_k$ dans $\mathbb{F}_p[X]$, d'où

$$p \leqslant \sum \deg(f_i) \leqslant d.$$

Le premier lemme qui suit a déjà été démontré dans ce qui précède :

Lemme 5. *Soient p un premier et $f \in \mathbb{Z}[x]$ primitif qui a p comme diviseur fixe. Alors il existe $e \geqslant 0$, $q, r \in \mathbb{Z}[x]$ tels que*

$$f(x) = (x^p - x)q(x) + pr(x), \tag{1.35}$$

avec

$$q(x) = \sum_{i=0}^{e} a_j x^j \quad \text{avec} \quad 0 \leqslant a_j < p$$

et $a_e \neq 0$.

On étudie ensuite l'effet de changements de variables de la forme $x \mapsto px + k$ pour $0 \leqslant k < p$:

Lemme 6. *Soient p un premier et $f \in \mathbb{Z}[x]$ primitif de la forme (1.35). Alors pour tout $0 \leqslant k < p$, il existe $\nu_k \in \mathbb{Z}$ tel que*

a) $0 \leqslant \nu_k \leqslant e$;

b) $f_k(x) = p^{-\nu_k - 1} f(px + k) \in \mathbb{Z}[x]$ est primitif;

c) Si f_k a p comme premier fixe et est de la forme (1.35) pour des polynômes q_k et r_k convenables, alors $e \geqslant p - 1$ et $deg(q_k) \leqslant e - p + 1$.

Démonstration.– On commence par faire la preuve dans le cas où $k = 0$. On part de l'identité

$$\frac{f(px)}{p} = x(p^{p-1}x^{p-1} - 1)q(px) + r(px)$$

et on pose b_j le j-ème coefficient de r. Alors le coefficient d'ordre $j + 1$ de $f(px)/p$ est

$$c_j := p^{p-1}p^{j-p+1}a_{j-p+1} - p^j a_j + p^{j+1}b_{j+1} = (a_{j-p+1} - a_j)p^j + p^{j+1}b_{j+1}$$

avec la convention $a_j = 0$ pour les indices négatifs. On introduit alors ν_0 la valuation p-adique du pgcd des coefficients de $f(px)/p$ et

$$f_0(x) = \frac{f(px)}{p^{\nu_0+1}} \in \mathbb{Z}[x].$$

On se convainc facilement que f_0 est primitif puisque f l'est et qu'on a divisé le pgcd par p. Les coefficients de $f(px)$ sont $p^i f_i$ donc le pgcd des coefficients est celui de ceux de f soit 1 multiplié par une puissance de p, à savoir p^{ν_0+1}. Si on pose e_0 le plus petit indice j tel que $a_j \neq 0$ dans q, alors $\nu_0 \leqslant e_0$, en effet sinon p^{ν_0+1} devrait diviser le coefficient

$$(a_{e_0-p+1} - a_{e_0})p^{e_0} + p^{e_0+1}b_{e_0+1} = a_{e_0}p^{e_0} + p^{e_0+1}b_{e_0+1}$$

par définition de e_0 ce qui est absurde par définition des a_j. On a en particulier $0 \leqslant \nu_0 \leqslant e_0$, ce qui suffit pour établir les deux premiers points du lemme. Si maintenant f_0 admet p pour premier fixe. On se place dans un premier temps dans le cas où $\nu_0 < e_0$. Alors pour $0 \leqslant j \leqslant \nu_0$, on a

$$c_j = b_j p^j$$

donc le coefficient de f_0 d'ordre j est

$$b_j p^{j-\nu_0}$$

qui est bien un entier car p^{ν_0} divise $b_j p^j$. Puis pour $j > \nu_0$, on a clairement que p divise c_j donc

$$f_0(x) \equiv g_0(x)[p]$$

où

$$g_0(x) = \sum_{j=0}^{\nu_0} b_j p^{j-\nu_0} x^j.$$

Si g_0 admet p comme premier fixe, alors on l'écrit sous la forme (1.35) pour certains q_0 et r_0 avec

$$0 \leqslant \deg(q_0) \leqslant \nu_0 - p < e_0 - p \leqslant e - p$$

ce qui permet de conclure. On traite alors le cas où $e_0 = \nu_0$. Le même raisonnemet fournit que

$$f_0(x) \equiv g_0(x)[p]$$

où

$$g_0(x) = -a_{e_0} x^{e_0+1} + \sum_{j=0}^{\nu_0} b_j p^{j-\nu_0} x^j$$

et on conclut de la même façon en écrivant g_0 sous la forme (1.35) avec

$$\deg(q_0) \leqslant e_0 + 1 - p \leqslant e + 1 - p.$$

Pour compléter la preuve, il faut maintenant en déduire le résultat pour $0 < k < p$. Pour ce faire, on pose $g(x) = f(x+k)$ qui vérifie les mêmes hypothèses que f et on est ramené au cas $k = 0$. □

On termine par un dernier lemme concernant les nombres premiers fixes qui repose sur les deux lemmes précédents :

Lemme 7. *Soit $f \in \mathbb{Z}[x]$ primitif, de discriminant non nul et de la forme (1.35) (en particulier p est premier fixe pour f). Alors il existe $0 \leqslant \delta \leqslant e$ et des entiers strictement positifs μ_0,..., μ_δ avec*

$$\mu_0 + ... + \mu_\delta \leqslant (e+1)^2$$

tels que le polynôme

$$g_{k_0,...,k_\delta}(x) = \frac{f\left(p^{\delta+1}x + p^\delta k_\delta + ... + pk_1 + k_0\right)}{p^{\mu_0+...+\mu_\delta}}$$

soit à coefficients entiers et n'admette pas p comme premier fixe pour tout $k_0, ..., k_\delta$ dans $\mathbb{Z} \cap [0, p[$.

Démonstration.– On raisonne par récurrence sur le degré e du polynôme q. Les transformations linéaires du type $x \mapsto ax+b$ préservent le degré dès que $a \neq 0$ et préservent la non-nullité du dsicriminant (on raisonne comme ci-dessus). Soit $0 \leqslant k_0 < p$ quelconque. Le lemme précédent implique qu'il existe $\nu_0 \in \mathbb{Z}$ tel que $0 \leqslant \nu_0 \leqslant e$ et

$$f_{k_0}(x) = p^{-\nu_0-1} f(px+k_0)$$

soit à coefficients entiers primitif. Si $e < p-1$, par contraposition du dernier point du lemme, on en déduit que f_{k_0} n'admet pas p comme premier fixe. On obtient donc le résultat pour $\delta = 0$, $\mu_0 = \nu_0 + 1$ et $g_{k_0} = f_{k_0}$, ce qui permet d'obtenir l'initialisation de notre récurrence. On suppose alors désormais $e \geqslant p-1$ et dans ce cas f_{k_0} admet p comme premier fixe. On peut donc écrire f_{k_0} sous la forme (1.35) pour eux polynômes q' et r' convenables avec $\deg(q') = e' \leqslant e-p+1$. Par hypothèse de récurrence, il existe $\delta' \leqslant e'$ et μ'_0,...,$\mu'_{\delta'}$ tels que

$$\mu'_0 + ... + \mu'_{\delta'} \leqslant (e'+1)^2$$

et

$$\frac{f_{k_0}\left(p^{\delta'+1}x + p^{\delta'}k'_{\delta'} + ... + pk'_1 + k'_0\right)}{p^{\mu'_0+...+\mu'_{\delta'}}} = \frac{f\left(p^{\delta'+2}x + p^{\delta'+1}k'_{\delta'} + ... + p^2k'_1 + pk'_0 + k_0\right)}{p^{\mu'_0+...+\mu'_{\delta'}+\nu_0+1}}$$

soit à coefficients entiers, primitif, et n'admette pas p comme premier fixe et ce pour tous k'_0,...,$k'_{\delta'}$ dans $\mathbb{Z} \cap [0,p[$. On pose alors $\delta = \delta'+1$, $k_{i+1} = k'_i$ pour $i \geqslant 0$ et $\mu_0 = \nu_0 + 1$, $\mu_i = \mu'_{i-1}$ pour $i \geqslant 1$ et on a bien que $g_{k_0,...,k_\delta}$ convient pour tous $k_0, ..., k_\delta$ dans $\mathbb{Z} \cap [0,p[$. Enfin, on a clairement

$$\delta \leqslant e'+1 \leqslant e+2-p \leqslant (e+1)^2$$

et

$$\mu_0 + ... + \mu_\delta \leqslant (e-p+2)^2 + (e+1) \leqslant e^2 + e + 1 \leqslant (e+1)^2$$

ce qui complète la preuve. □

1.4.2 Un outil de géométrie des nombres

On suit la méthode de [23], [27], [21] et [28] qui repose sur le lemme de géométrie des nombres suivant :

Lemme 8. *Soient $\varepsilon > 0$, L_1, L_2 et Q des formes vérifiant les hypothèses **NH**, $X \geqslant 1$, V_1, V_2, $V_3 \geqslant 2$ et $V = V_1V_2V_3$. Alors il existe une constante absolue $A > 0$ telle que*

$$\sum_{\substack{\mathbf{d}\in\mathbb{N}^3 \\ d_i \leqslant V_i}} \left| \#\left(\Lambda(\mathbf{d}) \cap X\mathcal{R}_{\mathbf{d}}\right) - \mathrm{vol}(\mathcal{R}_{\mathbf{d}})\mathrm{X}^2 \frac{\rho(\mathbf{d})}{(\mathrm{d}_1\mathrm{d}_2\mathrm{d}_3)^2} \right| \ll L_\infty^\varepsilon (r_\infty X\sqrt{V} + V)\log(V)^A,$$

où $\mathcal{R}_{\mathbf{d}} \subset \mathcal{R}$ est une région de frontière continûment différentiable (par morceaux) dépendant de $\mathbf{d}$.

Démonstration.– Les éléments de la preuve sont dans l'article [22] de Daniel ainsi que dans [29], [30] et [28] où il faut préciser en plus la dépendance par rapport aux formes et où il faut noter que la dépendance de la région par rapport à l'indice de sommation

ne change absolument rien dans la preuve. Il faut également noter que dans le cas où les formes linéaires s'annulent (la forme Q étant irréductible, elle ne peut pas s'annuler ailleurs qu'en $(0,0)$), on n'a pas nécessairement une condition de coprimalité, ce qui fait sortir un $\log(V)$ à la puissance 8 en plus par rapport à la preuve qui figure dans [28], ce qui n'est clairement pas gênant au vu du résultat énoncé. Dernier point, le lemme se démontre pour des formes primitives et on passe aux formes vérifiant **NH** en utilisant le Lemme 1. En effet, pour d' et l fixés, on a au plus $\tau(l)$ entiers d tels que $d' = \frac{d}{(d,l)}$. De plus, on constate que $\Lambda(\mathbf{d}, L_1, L_2, Q) = \Lambda(\ mathbf{d}', L_1^*, L_2^*, Q^*)$, ce qui permet de majorer la quantité

$$\sum_{\substack{\mathbf{d}\in\mathbb{N}^3\\ d_i\leqslant V_i}} \left| \#\left(\Lambda(\mathbf{d})\cap X\mathcal{R}_{\mathbf{d}}\right) - \mathrm{vol}(\mathcal{R}_{\mathbf{d}})\mathrm{X}^2\frac{\rho(\mathbf{d})}{(\mathrm{d}_1\mathrm{d}_2\mathrm{d}_3)^2}\right|$$

par

$$\tau(\ell_1)\tau(\ell_2)\tau(q)\sum_{\substack{\mathbf{d}'\in\mathbb{N}^3\\ d_i'\leqslant V_i}} \left| \#\left(\Lambda(\mathbf{d}')\cap X\mathcal{R}'_{\mathbf{d}'}\right) - \mathrm{vol}(\mathcal{R}'_{\mathbf{d}'})\mathrm{X}^2\frac{\rho(\mathbf{d}', \mathrm{L}_1^*, \mathrm{L}_2^*, \mathrm{Q}^*)}{(\mathrm{d}_1'\mathrm{d}_2'\mathrm{d}_3')^2}\right|.$$

Puisque $\tau(\ell_1)$, $\tau(\ell_2)$, $\tau(q) \ll L_\infty^\varepsilon$, le résultat sur les formes primitives permet de conclure. □

On pose $X' = r'X$ et $Y = (r'X)^{1/2}/(\log(X))^C$ pour une constante $C > 0$ que l'on fixera plus tard. L'idée est alors d'utiliser, si $m \equiv 1[4]$ et $0 \leqslant m \leqslant X'$, les décompositions suivantes qui permettent de restreindre les intervalles dans lesquels varient les variables de façon acceptable

$$r(m) = 4A_+(m) + 4A_-(m) \tag{1.36}$$

avec

$$A_+(m) = \sum_{\substack{d|m\\ d\leqslant\sqrt{X'}}} \chi(d) \quad \text{et} \quad A_-(m) = \sum_{\substack{e|m\\ m>e\sqrt{X'}}} \chi(e), \tag{1.37}$$

où la deuxième somme provient de la multiplicativité de χ, appliquée à $L_2(\mathbf{x})$,

$$r(m) = 4D_+(m) + 4D_-(m) \tag{1.38}$$

avec

$$D_+(m) = \sum_{\substack{d|m\\ d\leqslant X'}} \chi(d) \quad \text{et} \quad D_-(m) = \sum_{\substack{e|m\\ m>eX'}} \chi(e), \tag{1.39}$$

appliqué à $Q(\mathbf{x})$ et la décomposition

$$r(m) = 4B_+(m) + 4C(m) + 4B_-(m), \tag{1.40}$$

avec

$$B_+(m) = \sum_{\substack{d|m\\ d\leqslant Y}} \chi(d), \quad C(m) = \sum_{\substack{d|m\\ Y<d\leqslant X'/Y}} \chi(d) \quad \text{et} \quad B_-(m) = \sum_{\substack{e|m\\ m>eX'/Y}} \chi(e), \tag{1.41}$$

où on a à nouveau utilisé la multiplicativité de χ, appliquée à $L_1(\mathbf{x})$ cette fois. On notera que dans A_-, D_- et B_-, on a que $e \leqslant r'\sqrt{X}$, $e \leqslant r'X'$ et $e \leqslant Y$ respectivement. On introduit alors la quantité

$$S_{\pm,\pm,\pm} = \sum_{\mathbf{x}\in\mathbb{Z}^2\cap X\mathcal{R}} B_\pm\big(L_1(\mathbf{x})\big)A_\pm\big(L_2(\mathbf{x})\big)D_\pm\big(Q(\mathbf{x})\big), \tag{1.42}$$

de sorte quelque

$$S(X) = 4S_0 + 4^3\sum S_{\pm,\pm,\pm}, \tag{1.43}$$

avec

$$S_0 = \sum_{\mathbf{x}\in\mathbb{Z}^2\cap X\mathcal{R}} C\big(L_1(\mathbf{x})\big)r\big(L_2(\mathbf{x})\big)r\big(Q(\mathbf{x})\big). \tag{1.44}$$

On est donc ramené à l'étude de S_0 et des huit sommes $S_{\pm,\pm,\pm}$. Si on pose $V_1 = Y$, $V_2 = \sqrt{X'}$ et $V_3 = X'$ et pour $\mathbf{d} = (d_1, d_2, d_3) \in \mathbb{N}^3$,

$$\mathcal{R}_{4,\mathbf{d}} = \left\{\mathbf{x}\in\mathcal{R} \quad \middle| \quad Q(\mathbf{x}) > \frac{r'd_3}{X}, \quad L_1(\mathbf{x}) > r'd_1Y^{-1}, \quad L_2(\mathbf{x}) > (r')^{1/2}d_2X^{-1/2}\right\}, \tag{1.45}$$

de sorte que

$$X\mathcal{R}_{4,\mathbf{d}} = \left\{X\mathbf{x}\in X\mathcal{R} \,\middle|\, Q(\mathbf{x}) > X'd_3,\ L_1(\mathbf{x}) > d_1X'Y^{-1},\ L_2(\mathbf{x}) > d_2(X')^{1/2}\right\}. \tag{1.46}$$

On a alors

$$S_{-,-,-} = \sum_{\substack{\mathbf{d}\in\mathbb{N}^3\\ d_i\leqslant V_i}} \chi(d_1d_2d_3)\#\left(\Lambda(\mathbf{d})\cap X\mathcal{R}_{4,\mathbf{d}}\right) \tag{1.47}$$

par exemple et on est ramené à des quantités qu'on étudiera grâce au Lemme 5. Malheureusement, rien ne garantit que $L_i(\mathbf{x}) \equiv 1[4]$ et que $Q(\mathbf{x}) \equiv 1[4]$, ce qui est essentiel pour pouvoir appliquer ces décompositions car le caractère χ est trivial sur de tels entiers. Pour s'y ramener et pouvoir appliquer la méthode qu'on vient de décrire, on va extraire les valuations 2-adiques. Cette décomposition avec le Y est capitale pour obtenir le terme d'erreur souhaité.

1.4.3 Extraction des valuations 2-adiques

On effectue ici un raisonnement similaire à celui effectué dans [21]. En utilisant le fait que pour tout entier n, on ait $r(2n) = r(n)$, on obtient l'égalité

$$S(X) = \sum_{k_0\geqslant 0}\sum_{\substack{\mathbf{x}\in\mathbb{Z}^2\cap X\mathcal{R}\\ 2^{k_0}||\mathbf{x}}} r\big(L_1(\mathbf{x})\big)r\big(L_2(\mathbf{x})\big)r\big(Q(\mathbf{x})\big) = \sum_{k_0\geqslant 0} S^*\left(2^{-k_0}X\right), \tag{1.48}$$

où

$$S^*(X) = \sum_{\substack{\mathbf{x}\in\mathbb{Z}^2\cap X\mathcal{R}\\ 2\nmid(x_1,x_2)}} r\big(L_1(\mathbf{x})\big)r\big(L_2(\mathbf{x})\big)r\big(Q(\mathbf{x})\big). \tag{1.49}$$

En regroupant les termes selon la valuation 2−adique de $L_i(\mathbf{x})$ et de $Q(\mathbf{x})$, on a

$$S(X) = \sum_{k_0 \geqslant 0} \sum_{\mathbf{k}=(k_1,k_2,k_3)\in\mathbb{Z}^3_{\geqslant 0}} S_{\mathbf{k}}\left(2^{-k_0}X\right), \tag{1.50}$$

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

$$\nu_2(L_i(\mathbf{x})) = k_i \quad \text{et} \quad 2^{-k_i}L_i(\mathbf{x}) \equiv 1[4]$$

et

$$\nu_2(Q(\mathbf{x})) = k_3 \quad \text{et} \quad 2^{-k_3}Q(\mathbf{x}) \equiv 1[4]$$

et $2 \nmid \mathbf{x}$ et où les dernières conditions sont nécessaires si l'on veut un terme non nul dans $S^*(X)$. On a clairement que $2^{k_i} \leqslant L_i(\mathbf{x}) \leqslant X'$ donc

$$k_i \ll \log(X') \tag{1.51}$$

Utilisant à nouveau le fait que

$$\forall \mathbf{x} \in \mathbb{Z}^2, \quad \forall l \in \mathbb{N}, \quad r\left(2^l L_1(\mathbf{x})\right) = r\left(L_1(\mathbf{x})\right),$$

on peut supposer quitte à diviser par la plus grande puissance de 2 qui divise tous les coefficients de L_1 que a_1 ou b_1 est impair. Traitons le cas a_1 impair, le cas où a_1 est pair et b_1 impair se traitant par symétrie en échangeant les rôles de x_1 et x_2. La première condition

$$2^{-k_1}L_1(\mathbf{x}) \equiv 1[4]$$

équivaut à l'existence de x_1' tel que $x_1' \equiv 1[4]$ et tel que $x_1 = cx_2 + c'2^{k_1}x_1'$ où $c' \in \{\pm 1\}$ tel que $c' \equiv a_1[4]$ et $c \in [\![0, 2^{k_1+2}[\![$ tel que $a_1 c \equiv -b_1 \left[2^{k_1+2}\right]$ (on rappelle que a_1 est supposé impair). En effet, si on pose $z = 2^{-k_1}L_1(\mathbf{x}) \equiv 1[4]$, on a clairement que

$$x_1 \equiv cx_2 + \overline{a_1}2^{k_1}z \left[2^{k_1+2}\right]$$

où on notera $\overline{a_1}$ pour l'inverse multiplicatif de a_1. On a donc, puisque $c' \equiv \overline{a_1}[4]$, l'existence d'un entier l tel que $\overline{a_1} = c' + 4l$ et d'un entier m tels que

$$x_1 = cx_2 + c'2^{k_1}(z + 4(m + l))$$

ce qui permet de conlure en posant $x_1' = z + 4(m + l) \equiv 1[4]$. Si $k_1 = 0$, on a alors automatiquement que $2 \nmid \mathbf{x}$ et sinon, cette condition devient équivalente au fait que x_2 soit impair. Intéressons-nous à présent à la deuxième condition

$$2^{-k_2}L_2(\mathbf{x}) \equiv 1 \equiv x_1'[4].$$

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

$$L_2\left(cx_2 + c'2^{k_1}x_1', x_2\right) \equiv 2^{k_2}x_1' \left[2^{k_2+2}\right].$$

On considère alors $L(X,Y) = L_2\left(cY + c'2^{k_1}X, Y\right) = aX + bY$ pour a et b deux entiers. On pose alors $k_1' = \min(\nu_2(a), \nu_2(b))$, $k_2' = k_2 - k_1'$ et $L_0(X,Y) = 2^{-k_1'}L(X,Y)$ de sorte qu'on obtient

$$L_0(x_1', x_2) \equiv 2^{k_2'}x_1' \left[2^{k_2'+2}\right].$$

On peut alors écrire $x_2 \equiv \alpha x_1' \left[2^{k_2'+2}\right]$ pour un unique $\alpha \in [\![0, 2^{k_2'+2}[\![$ pour obtenir

$$L_0(1,\alpha) \equiv 2^{k_2'} \left[2^{k_2'+2}\right]. \tag{1.52}$$

Finalement, lorsque la première condition est vérifiée, la deuxième l'est si, et seulement si, on a $x_2 = \alpha x_1' + 2^{k_2'+2} x_2'$ pour α solution de (1.52) où si $k_1 = 0$, α doit être choisi impair pour vérifier la condition $2 \nmid \mathbf{x}$. Avec des notations évidentes, le même raisonnement conduit à montrer que si la première condition est remplie, la troisième l'est si, et seulement si, il existe $\beta \in [\![0, 2^{k_3'+2}[\![$ solution de

$$Q_0(1,\beta) \equiv 2^{k_3'} \left[2^{k_3'+2}\right] \tag{1.53}$$

tel que $x_2 = \beta x_1' + 2^{k_3'+2} x_2''$, β devant éventuellement être choisi impair. Pour traiter le cas où les trois conditions sont remplies simultanément, posons $k^- = \min(k_2', k_3')$ et $k^+ = \max(k_2', k_3')$. D'après ce qui précède, il existe α_1 solution de (1.52), α_2 solution de (1.53), $x_{2,1}$ et $x_{2,2}$ deux entiers tels que

$$x_2 = \alpha_1 x_1' + 2^{k_2'+2} x_{2,1} = \alpha_2 x_1' + 2^{k_3'+2} x_{2,2}.$$

On a donc en passant modulo 2^{k^-} que

$$x_2 \equiv \alpha_1 x_1' \equiv \alpha_2 x_1' \left[2^{k^-+2}\right]$$

soit, puisque x_1' n'est pas divisible par 2, $\alpha_1 \equiv \alpha_2 \left[2^{k^-+2}\right]$. On peut donc écrire, en notant toujours α^+ le α_i correspondant à k^+ et α^- celui correspondant à k^-, que $\alpha^- = \alpha^+ + 2^{k^-+2} m$ pour un certain entier m. On a par conséquent que x_2 est de la forme

$$x_2 = \alpha^+ x_1' + 2^{k^++2} x_2^+ = \alpha^+ x_1' + 2^{k^-+2} x_2^-$$

pour deux entiers x_2^+ et x_2^- tels que $2^{k^+-k^-} | x_2^-$. Cette condition est bien sûr équivalente à $x_2 = \alpha^+ x_1' + 2^{k^++2} x_2'$ pour un certain entier x_2' et où α^+ est une racine de (1.52) et (1.53). En effet, supposons que $\alpha^+ = \alpha_1$, l'autre cas étant tout à fait symétrique. Alors par définition, α^+ est racine de (1.52) mais puisque $\alpha^- = \alpha^+ + 2^{k^-+2} m$, on a également

$$Q(1,\alpha^+) \equiv 0 \left[2^{k_3'+2}\right].$$

On vient donc de montrer que les conditions

$$\nu_2(L_i(\mathbf{x})) = k_i \quad \text{et} \quad 2^{-k_i} L_i(\mathbf{x}) \equiv 1[4]$$

et

$$\nu_2(Q(\mathbf{x})) = k_3 \quad \text{et} \quad 2^{-k_3} Q(\mathbf{x}) \equiv 1[4]$$

et $2 \nmid \mathbf{x}$ peuvent s'écrire $\mathbf{x} = \mathbf{M}\mathbf{x}'$ avec $x_1' \equiv 1[4]$ et

$$\mathbf{M} = \mathbf{M}_\alpha = \begin{pmatrix} c' 2^{k_1} & c \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \alpha & 2^{\max(k_2', k_3')+2} \end{pmatrix} = \begin{pmatrix} c' 2^{k_1} + c\alpha & c 2^{\max(k_2', k_3')+2} \\ \alpha & 2^{\max(k_2', k_3')+2} \end{pmatrix}, \tag{1.54}$$

où $\alpha \in [\![0, 2^{\max(k_2',k_3')+2}[\![$ est une racine de (1.52) et (1.53) qui doit de plus être choisie impaire lorsque $k_1 \geqslant 1$. On notera $n(k_1, k_2, k_3)$ le nombre de tels α et on remarque que

$$|\det(\mathbf{M})| = 2^{k_1+\max(k_2',k_3')+2}. \tag{1.55}$$

On peut remarquer que $\min(k_i, k_j) > \nu_2(\Delta_{i,j})$. En effet, il est clair dans le cas où $\{i, j\} = \{1, 2\}$, que si on pose $k = \min(k_1, k_2)$, on a

$$\begin{aligned} a_1x_1 + b_1x_2 &\equiv 0 \left[2^k\right] \\ a_2x_1 + b_2x_2 &\equiv 0 \left[2^k\right] \end{aligned}$$

ce qui implique que, si on suppose par exemple que $2 \nmid x_1$ (le cas $2 \nmid x_2$ se traitant exactement de la même façon)

$$x_1(a_1b_2 - a_2b_1) \equiv 0 \left[2^k\right],$$

ce qui entraîne bien que nécessairement $\min(k_i, k_j) \leqslant \nu_2(\Delta_{i,j})$. Traitons alors les cas $i \in \{1, 2\}$ et $j = 3$. Avec les mêmes notations, on a

$$\begin{aligned} a_ix_1 + b_ix_2 &\equiv 0 \left[2^k\right] \\ Q(x_1, x_2) &\equiv 0 \left[2^k\right] \end{aligned}.$$

Or, on a vu qu'on pouvait supposer que a_i ou b_i était impair, sans perte de généralité on va supposer qu'il s'agit de a_i. On obtient donc grâce à la première congruence que

$$x_1 \equiv -\overline{a_i}b_ix_2 \left[2^k\right] \tag{1.56}$$

soit en réinjectant dans la seconde

$$x_2^2Q(-\overline{a_i}b_i, 1) \equiv 0 \left[2^k\right].$$

Mais (1.56) implique que si $2|x_2$, alors $2|x_1$ si $k > 0$, ce qui est exclu. On a donc dans le cas $k > 0$ que x_2 est inversible modulo 2^k et donc que

$$Q(-\overline{a_i}b_i, 1) \equiv 0 \left[2^k\right] \quad \text{soit} \quad Q(-b_i, a_i) \equiv 0 \left[2^k\right]$$

ce qui prouve bien que nécessairement $\min(k_i, k_j) \leqslant \nu_2(\Delta_{i,j})$, le cas où $k = 0$ étant trivialement vrai.

On cherche maintenant à estimer la taille de la quantité $n(k_1, k_2, k_3)$. On utilise pour cela le lemme suivant. On définit le contenu d'un polynôme f à coefficients entiers comme le pgcd de tous ses coefficients et on définit pour tout entier naturel non nul n :

$$\rho_f(n) = \{x \in \mathbb{Z}/n\mathbb{Z} \quad | \quad f(x) \equiv 0[n]\}. \tag{1.57}$$

Il s'agit d'une fonction multiplicative qu'il suffit donc d'étudier sur les puissances de nombres premiers.

Lemme 9. *Soient $f \in \mathbb{Z}[x]$ de degré $d \geqslant 2$ et p un nombre premier qui ne divise pas le contenu de f et tel que $p^\mu || disc(f)$. Alors, pour tout $\nu \geqslant 1$, on a*

$$\rho_f(p^\nu) \leqslant d \min\left(p^{\frac{\mu}{2}}, p^{\left(1-\frac{1}{d}\right)\nu}, p^{\nu-1}\right).$$

Démonstration.– La preuve se trouve dans [21]. □

Démontrons alors

Lemme 10. *On a* $n(k_1,k_2,k_3) \ll 1$.

Démonstration.– On commence par traiter le cas où $k_1 \geqslant 1$ dans lequel on sait que α doit être impair. On se ramène à des quantités de type ρ_f que l'on sait estimer. On a clairement que

$$n(k_1,k_2,k_3) \leqslant \#\left\{\alpha \in [\![0,2^{k_1+\max(k_2,k_3)}[\![\quad \middle| \quad \begin{array}{l} L_2(c\alpha+c'2^{k_1},\alpha) \equiv 2^{k_2}\left[2^{k_2+2}\right], \\ Q(c\alpha+c'2^{k_1},\alpha) \equiv 2^{k_3}\left[2^{k_3+2}\right] \end{array}\right\}$$

donc

$$n(k_1,k_2,k_3) \leqslant \#\left\{\alpha \in [\![0,2^{k_1+\max(k_2,k_3)}[\![\quad \middle| \quad \begin{array}{l} L_2(c\alpha+c'2^{k_1},\alpha) \equiv 0\left[2^{k_2}\right], \\ Q(c\alpha+c'2^{k_1},\alpha) \equiv 0\left[2^{k_3}\right] \end{array}\right\}.$$

Mais, puisque α est inversible, on a que les deux congruences sont équivalentes à

$$\left\{\begin{array}{l} L_2(c+c'2^{k_1}\overline{\alpha},1) \equiv 0\left[2^{k_2}\right], \\ Q(c+c'2^{k_1}\overline{\alpha},1) \equiv 0\left[2^{k_3}\right] \end{array}\right. .$$

En remarquant que

$$c+c'2^{k_1}\overline{\alpha} \equiv c \equiv -b_1\overline{a_1}\left[2^{k_1}\right],$$

on en déduit la majoration suivante

$$n(k_1,k_2,k_3) \leqslant \#\left\{x \in [\![0,2^{k_1+\max(k_2,k_3)+2}[\![\quad \middle| \quad \begin{array}{l} x \equiv -b_1\overline{a_1}\left[2^{k_1}\right], \\ L_2(x,1) \equiv 0\left[2^{k_2}\right], \\ Q(x,1) \equiv 0\left[2^{k_3}\right] \end{array}\right\}.$$

Notons N l'ensemble dont le membre de droite de l'inégalité ci-dessus correspond au cardinal. Supposons alors que $\max(k_2,k_3) \leqslant k_1$ et considérons $x \in N$. On a alors $x \equiv -b_1\overline{a_1}\left[2^{k_1}\right]$ et donc cette congruence reste vraie modulo 2^{k_2} et modulo 2^{k_3} en particulier et donc on a

$$L_2(-b_1\overline{a_1},1) \equiv 0\left[2^{k_2}\right] \quad \text{soit} \quad L_2(-b_1,a_1) = \mathrm{Res}(L_1,L_2) \equiv 0\left[2^{k_2}\right]$$

et de même

$$Q(-b_1,a_1) = \mathrm{Res}(L_1,Q) \equiv 0\left[2^{k_3}\right].$$

Soit ces conditions ne sont pas vérifiées et on a donc aucun élément dans N, soit elles sont vérifiées et tous les éléments de $\mathbb{Z}/2^{k_1+\max(k_2+k_3)}\mathbb{Z}$ congrus à $-b_1\overline{a_1}$ modulo 2^{k_1} sont solutions. On a donc que dans ce cas

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

En utilisant le fait que $\min(k_i,k_1) \leqslant \nu_2(\Delta_{i,1})$ pour $i \in \{2,3\}$, on en déduit, si on pose $H = \Delta_{12}\Delta_{13}\Delta_{23}\Delta$, que

$$n(k_1,k_2,k_3) \ll 2^{\nu_2(H)}.$$

Comme dans la preuve du Lemme 4, pour pouvoir appliquer notre estimation de la somme dans le cadre du Théorème 2, il faut que la constante soit indépendante du changement de variables, on autorise donc la constante à dépendre des quantités dépendant des formes tant que celles-ci sont invariantes sous le changement de variables E défini dans la preuve du Théorème 2 en (1.63). Or, $\det(E) = eD''$ et par hypothèse $\det(E)$ est impair. De plus, comme les discriminants ou les résultants vont être multipliés par une puissance du déterminant de E sous le changement de variables, on voit que la quantité $2^{\nu_2(H)}$ est bien invariante et donc on peut écrire

$$n(k_1, k_2, k_3) \ll 1.$$

Passons aux cas où $\max(k_2, k_3) > k_1$. On traite tout d'abord les cas $k_3 = \max(k_2, k_3)$, soit les cas $k_3 > k_1 \geqslant k_2$ et $k_3 \geqslant k_2 \geqslant k_1$. On a alors la majoration

$$n(k_1, k_2, k_3) \leqslant \#\left\{x \in [\![0, 2^{k_1+\max(k_2,k_3)}[\![\quad \middle| \quad Q(x,1) \equiv 0 \left[2^{k_3}\right]\right\}.$$

Or, on a $\rho_{Q(x,1)}\left(2^{k_3}\right)$ solutions à $Q(x,1) \equiv 0 \left[2^{k_3}\right]$ modulo 2^{k_3} et on cherche le nombre de solutions modulo $2^{k_1+\max(k_2,k_3)}$. Il suffit de prendre les éléments de $\mathbb{Z}/2^{k_1+\max(k_2+k_3)}\mathbb{Z}$ qui sont congrus modulo 2^{k_3} à une solution, on obtient donc la majoration

$$n(k_1, k_2, k_3) \ll \frac{2^{k_1+k_3}}{2^{k_3}} \rho_{Q(x,1)}\left(2^{k_3}\right) \ll 2^{k_1} \rho_{Q(x,1)}\left(2^{k_3}\right) \ll 2^{k_1+\frac{\nu_2(\Delta)}{2}}$$

en utilisant le Lemme 6 puisqu'on a bien un discriminant non nul et qu'on a vu qu'on pouvait supposer que 2 ne divise pas le contenu de Q grâce à la propriété $r(2n) = r(n)$. On a donc

$$n(k_1, k_2, k_3) \ll 2^{\frac{3\nu_2(H)}{2}} \ll 1$$

car $\Delta | H$ et $k_1 = \min(k_1, k_2) \leqslant \nu_2(H)$. De la même manière, dans les cas où $k_2 = \max(k_2, k_3)$, on obtient

$$n(k_1, k_2, k_3) \ll 2^{k_1} \rho_{L_2(x,1)}\left(2^{k_2}\right).$$

On ne peut pas ici appliquer le Lemme 6 puisque L_2 est de degré 1. On peut supposer que $2 \nmid (a_2, b_2)$ et la congruence se réécrit

$$a_2 x_1 \equiv b_2 \left[2^{k_2}\right].$$

Si $k_2 > 0$, on ne peut pas avoir $2|a_2$ sinon $2|b_2$ ce qui est exclu donc a_2 est inversible et on a une solution exactement. On a donc que dans ce dernier cas

$$n(k_1, k_2, k_3) \ll 2^{k_1} \ll 1,$$

par un raisonnement similaire à ce qui précède. Il reste à majorer $n(k_1, k_2, k_3)$ lorsque $k_1 = 0$, dans ce cas, on procède de même que ci-dessus pour les α impairs et on a éventuellement à ajouter tous les α pairs de $[\![0, 2^{\max(k_2,k_3)}[\![$ qui vérifient (1.52) et (1.53). Le nombre de ces α est majoré par celui des β tels que

$$Q_0(1, \beta) \equiv 0 \left[2^{\max(k_2', k_3')}\right].$$

Par le Lemme 6, cette quantité est majorée par $2^{\nu_2(\mathrm{disc}(Q_0))}$. Or, puisque $k_1 = 0$, on a que $Q_0(X, Y) = 2^{-k_1'} Q(cY + c'X, Y)$ où k_1' est la valuation 2-adique du pgcd des coefficients

de $(X,Y) \mapsto Q(cY+c'X,Y)$. En particulier, les coefficients de Q_0 ne dépendent que des coefficients de Q et donc on a $2^{\nu_2(\mathrm{disc}(Q_0))} \ll 1$. On a donc démontré que dans tous les cas, on a

$$n(k_1,k_2,k_3) \ll 1.$$

□

On relie maintenant les quantités $n(k_1,k_2,k_3)$ et la constante σ_2 qui apparaît dans le Théorème 1.

Lemme 11. *On a*

$$\sigma_2 = \sum_{k_0 \geqslant 0} \frac{1}{2^{2k_0}} \sum_{k_1,k_2,k_3 \geqslant 0} \frac{n(k_1,k_2,k_3)}{2^{k_1+\max(k_2',k_3')+2}} = \frac{1}{3} \sum_{k_1,k_2,k_3 \geqslant 0} \frac{n(k_1,k_2,k_3)}{2^{k_1+\max(k_2',k_3')}}. \tag{1.58}$$

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

$$\sigma_2 = 4 \lim_{n\to+\infty} 2^{-2n} \sum_{k_0=0}^{n} \sum_{0\leqslant k_1,k_2,k_3 \leqslant n} \# \left\{ \mathbf{x} \in \left(\mathbb{Z}/2^{n-k_0}\mathbb{Z}\right)^2, \quad 2 \nmid \mathbf{x} \quad \middle| \quad \begin{array}{l} L_1(\mathbf{x}) \equiv 2^{k_1}\left[2^{\min(k_1+2,n-k_0)}\right] \\ L_2(\mathbf{x}) \equiv 2^{k_2}\left[2^{\min(k_2+2,n-k_0)}\right] \\ Q(\mathbf{x}) \equiv 2^{k_3}\left[2^{\min(k_3+2,n-k_0)}\right] \end{array} \right\}.$$

On peut déjà commencer par remarquer que la contribution des termes tels que pour au moins un des k_i, $i \in \{1,2,3\}$ on ait $k_i+2 > n-k_0$ à la triple somme intérieure est majorée par

$$\# \left\{ \mathbf{x} \in \left(\mathbb{Z}/2^{n-k_0}\mathbb{Z}\right)^2 \quad \middle| \quad \begin{array}{l} L_1(\mathbf{x}) \equiv 0\left[2^{n-k_0}\right] \\ L_2(\mathbf{x}) \equiv 0\left[2^{\min(k_2+2,n-k_0)}\right] \\ Q(\mathbf{x}) \equiv 0\left[2^{\min(k_3+2,n-k_0)}\right] \end{array} \right\} \leqslant \# \left\{ \mathbf{x} \in \left(\mathbb{Z}/2^{n-k_0}\mathbb{Z}\right)^2 \quad \middle| \quad L_1(\mathbf{x}) \equiv 0\left[2^{n-k_0}\right] \right\}$$

si on suppose que $k_1+2 > n-k_0+1$ et où on suppose toujours que $2 \nmid \mathbf{x}$. La condition $L_1(\mathbf{x}) \equiv 0\left[2^{n-k_0}\right]$ donne au plus 2^{n-k_0} choix de $\mathbf{x}$, une fois x_2 fixé, on raisonne comme ci-dessus à propos de $\rho_{L_2(x,1)}$ pour obtenir au plus une valeur de x_1 et une majoration du type

$$4 \lim_{n\to+\infty} 2^{-2n} n^2 \sum_{k_0=0}^{n} k_0 2^{n-k_0} = 0.$$

Pour $k_1+2 = n-k_0+1$, on a la condition $L_1(\mathbf{x}) \equiv 0\left[2^{n-k_0-1}\right]$ et on raisonne de la même façon. On traite de manière tout à fait analogue la cas où $k_2+2 > n-k_0$. Il reste donc le cas $k_3 > n-k_0$ à traiter et pour ce faire, on a besoin de majorer

$$\# \left\{ \mathbf{x} \in \left(\mathbb{Z}/2^{n-k_0}\mathbb{Z}\right)^2 \quad \middle| \quad Q(\mathbf{x}) \equiv 0\left[2^{n-k_0}\right] \right\} = \rho(1,1,2^{n-k_0}) \ll (n-k_0+1)2^{n-k_0}$$

ce qui donne un terme

$$4 \lim_{n\to+\infty} 2^{-2n} n^2 \sum_{k_0=0}^{n} k_0 (n-k_0+1) 2^{n-k_0} = 0.$$

On peut donc s'intéresser uniquement aux triplets tels que $\max(k_1,k_2,k_3)\leqslant n-k_0$. On découpe alors la triple somme sur k_1, k_2 et k_3 selon le plus grand des trois indices. Traitons par exemple le cas où $k_1=\max(k_1,k_2,k_3)$, ce qui revient à estimer

$$4\lim_{n\to+\infty}2^{-2n}\sum_{k_0=0}^{n}\sum_{0\leqslant k_2,k_3\leqslant k_1\leqslant n-k_0}\#\left\{\mathbf{x}\in\left(\mathbb{Z}/2^{n-k_0}\mathbb{Z}\right)^2,\quad 2\nmid\mathbf{x}\quad\middle|\quad\begin{array}{l}L_1(\mathbf{x})\equiv 2^{k_1}\left[2^{k_1+2}\right]\\L_2(\mathbf{x})\equiv 2^{k_2}\left[2^{k_2+2}\right]\\Q(\mathbf{x})\equiv 2^{k_3}\left[2^{k_3+2}\right]\end{array}\right\}.$$

On constate alors que les trois conditions de congruences ne dépendent que de la classe de $\mathbf{x}$ modulo 2^{k_1+2}. Il suffit de déterminer le cardinal de l'ensemble intérieur pour $\mathbf{x}\in\left(\mathbb{Z}/2^{k_1+2}\mathbb{Z}\right)^2$ et d'en déduire tous les couples de $\left(\mathbb{Z}/2^{n-k_0}\mathbb{Z}\right)^2$ congrus à un couple solution de $\left(\mathbb{Z}/2^{k_1+2}\mathbb{Z}\right)^2$. Autrement dit, on obtient

$$4\lim_{n\to+\infty}2^{-2n}\sum_{k_0=0}^{n}\sum_{0\leqslant k_2,k_3\leqslant k_1\leqslant n-k_0}2^{2(n-k_0-k_1-2)}\#\left\{\mathbf{x}\in\left(\mathbb{Z}/2^{k_1+2}\mathbb{Z}\right)^2,\quad 2\nmid\mathbf{x}\quad\middle|\quad\begin{array}{l}L_1(\mathbf{x})\equiv 2^{k_1}\left[2^{k_1+2}\right]\\L_2(\mathbf{x})\equiv 2^{k_2}\left[2^{k_2+2}\right]\\Q(\mathbf{x})\equiv 2^{k_3}\left[2^{k_3+2}\right]\end{array}\right\}.$$

soit

$$\lim_{n\to+\infty}\sum_{k_0=0}^{n}\frac{1}{2^{2k_0}}\sum_{0\leqslant k_2,k_3\leqslant k_1\leqslant n-k_0}\frac{1}{2^{2k_1+2}}\#\left\{\mathbf{x}\in\left(\mathbb{Z}/2^{k_1+2}\mathbb{Z}\right)^2,\quad 2\nmid\mathbf{x}\quad\middle|\quad\begin{array}{l}L_1(\mathbf{x})\equiv 2^{k_1}\left[2^{k_1+2}\right]\\L_2(\mathbf{x})\equiv 2^{k_2}\left[2^{k_2+2}\right]\\Q(\mathbf{x})\equiv 2^{k_3}\left[2^{k_3+2}\right]\end{array}\right\}.$$

En raisonnant comme ci-dessus, on a vu que les condition impliquent que

$$x_1\equiv-\overline{a_1}b_1x_2+2^{k_1}\overline{a_1}\left[2^{k_1+2}\right]$$

et donc x_1 est entièrement déterminé par la valeur de x_2. On sait alors que si on pose $x_2\equiv\alpha\left[2^{\max(k_2',k_3')+2}\right]$, α est une des $n(k_1,k_2,k_3)$ solution de (1.52) et (1.53) dans $[\![0,2^{\max(k_2',k_3')+2}[\![$. On a donc $n(k_1,k_2,k_3)$ valeurs de x_2 possibles dans $\mathbb{Z}/2^{\max(k_2',k_3')+2}\mathbb{Z}$, ce qui en donne

$$2^{k_1-\max(k_2',k_3')}n(k_1,k_2,k_3)$$

dans $\mathbb{Z}/2^{k_1+2}\mathbb{Z}$. Cela fournit donc un terme

$$\lim_{n\to+\infty}\sum_{k_0=0}^{n}\frac{1}{2^{2k_0}}\sum_{0\leqslant k_2,k_3\leqslant k_1\leqslant n-k_0}\frac{1}{2^{2k_1+2}}2^{k_1-\max(k_2',k_3')}n(k_1,k_2,k_3)$$

soit

$$\lim_{n\to+\infty}\sum_{k_0=0}^{n}\frac{1}{2^{2k_0}}\sum_{0\leqslant k_2,k_3\leqslant k_1\leqslant n-k_0}\frac{n(k_1,k_2,k_3)}{2^{k_1+\max(k_2',k_3')+2}}.$$

Traitons maintenant le cas où $k_2=\max(k_1,k_2,k_3)$ qui donne une contribution

$$\lim_{n\to+\infty}\sum_{k_0=0}^{n}\frac{1}{2^{2k_0}}\sum_{0\leqslant k_1,k_3\leqslant k_2\leqslant n-k_0}\frac{1}{2^{2k_2+2}}\#\left\{\mathbf{x}\in\left(\mathbb{Z}/2^{k_2+2}\mathbb{Z}\right)^2,\quad 2\nmid\mathbf{x}\quad\middle|\quad\begin{array}{l}L_1(\mathbf{x})\equiv 2^{k_1}\left[2^{k_1+2}\right]\\L_2(\mathbf{x})\equiv 2^{k_2}\left[2^{k_2+2}\right]\\Q(\mathbf{x})\equiv 2^{k_3}\left[2^{k_3+2}\right]\end{array}\right\}.$$

On a de même que x_1 est déterminé par le choix de x_2 modulo 2^{k_1}. Le même raisonnement que ci-dessus donne exactement $n(k_1,k_2,k_3)$ x_2 modulo $2^{\max(k_2',k_3')+2}$ (où il est à noter qu'on

ne sait pas si on a encore $k_2' \geqslant k_3'$) ce qui donne $2^{k_2-\max(k_2',k_3')}$ valeurs de x_2 modulo 2^{k_2+2} puis pour chacune de ces valeurs on a $2^{k_2-k_1}$ valeurs de x_1, ce qui fournit là encore

$$\lim_{n\to+\infty}\sum_{k_0=0}^{n}\frac{1}{2^{2k_0}}\sum_{0\leqslant k_1,k_3\leqslant k_2\leqslant n-k_0}\frac{n(k_1,k_2,k_3)}{2^{k_1+\max(k_2',k_3')+2}}.$$

On traite le dernier cas de la même façon et en regroupant les trois contributions, on obtient finalement que

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

□

On a vu qu'on avait k_1, k_2 et $k_3 \ll \log(X')$ mais cela ne sera pas suffisant et on a besoin de réduire l'intervalle dans lequel varient les k_i de façon à le rendre acceptable. On écrit pour ce faire

$$S(X)=\sum_{k_0\geqslant 0}\sum_{0\leqslant k_1,k_2,k_3\leqslant \log\log X}S_{\mathbf{k}}\left(2^{-k_0}X\right)+\sum_{k_0\geqslant 0}\sum_{\log\log X<k_i}S_{\mathbf{k}}\left(2^{-k_0}X\right)$$

où la notation $\log\log X < k_i$ signifie ici qu'au moins un des k_i est stritement supérieur à $\log\log X$. D'après ce qu'on a fait ci-dessus, on a également

$$S_{\mathbf{k}}\left(2^{-k_0}X\right)=\sum_{\alpha}S_{\mathbf{k},\alpha}\left(2^{-k_0}X\right)$$

où α parcourt les $n(k_1,k_2,k_3)$ possibilités et où

$$S_{\mathbf{k},\alpha}(X)=\sum_{\substack{\mathbf{x}'\in\mathbb{Z}^2\cap X\mathcal{R}_{\mathbf{M}}\\ x_1'\equiv 1[4]}}r\left(L_1\left(\mathbf{M}\mathbf{x}'\right)\right)r\left(L_2\left(\mathbf{M}\mathbf{x}'\right)\right)r\left(Q\left(\mathbf{M}\mathbf{x}'\right)\right),$$

avec $\mathcal{R}_{\mathbf{M}}=\{\mathbf{x}'\in\mathbb{R}^2 \quad | \quad \mathbf{M}\mathbf{x}'\in\mathcal{R}\}$. On a que $\mathbf{M}\mathbb{Z}^2=\{\mathbf{M}\mathbf{x}' \quad | \quad \mathbf{x}'\in\mathbb{Z}^2\}$ est un réseau de covolume

$$\det(\mathbf{M}\mathbb{Z}^2)=\det(\mathbf{M})\det(\mathbb{Z}^2)=\det(\mathbf{M}).$$

On peut donc en considérer une base réduite $(\mathbf{e}_1,\mathbf{e}_2)$, c'est-à-dire une base telle que

$$\mathbf{e}_1=\text{arginf}_{\mathbf{x}\in\mathbf{M}\mathbb{Z}^2}||\mathbf{x}|| \quad \text{et} \quad \mathbf{e}_1=\text{arginf}_{\mathbf{x}\in\mathbf{M}\mathbb{Z}^2\setminus\mathbf{e}_1\mathbb{Z}}||\mathbf{x}||$$

où $||\mathbf{x}||=\max(|x_1|,|x_2|)$. On écrit donc tout $\mathbf{x}\in\mathbb{Z}^2\cap X\mathcal{R}$,

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

pour deux entiers λ et μ. On pose alors $L_i'(\lambda,\mu)=L_i(\mathbf{x})$ et $Q'(\lambda,\mu)=Q(\mathbf{x})$, de sorte qu'on ait

$$S_{\mathbf{k},\alpha}(X)\ll\sum_{\substack{\lambda\ll X/||\mathbf{e}_1||\\ \mu\ll X/||\mathbf{e}_2||}}r\left(L_1'(\lambda,\mu)\right)r\left(L_2'(\lambda,\mu)\right)r\left(Q'(\lambda,\mu)\right).$$

On utilise ici un cas particulier d'un résultat de Davenport ([32]).

Lemme 12. *Soit Γ un réseau de $\mathbb{R}^2$ et $(\mathbf{e}_1, \mathbf{e}_2)$ une base réduite. Alors si $(x_1, x_2) = \lambda\mathbf{e}_1 + \mu\mathbf{e}_2 \in \Gamma$, on a*

$$\lambda \ll \frac{||\mathbf{x}||}{||\mathbf{e}_1||} \quad et \quad \mu \ll \frac{||\mathbf{x}||}{||\mathbf{e}_2||}. \tag{1.59}$$

Démonstration.– On pose $s_1 = ||\mathbf{e}_1||$ et $s_2 = ||\mathbf{e}_2||$. On a $\det(\Gamma) = s_1 s_2 \sin(\theta)$ où θ est l'angle entre les vecteurs $\mathbf{e}_1$ et $\mathbf{e}_2$ et $s_1 s_2 \leqslant \frac{2}{\sqrt{3}} \det(\Gamma)$. On a que

$$d(\mathbf{e}_1, \mathrm{Vect}(\mathbf{e}_2))^2 = ||\mathbf{e}_1 - \mathbf{e}_1.\mathbf{e}_2||^2 = s_1^2 \sin^2(\theta),$$

d'où

$$d(\mathbf{e}_1, \mathrm{Vect}(\mathbf{e}_2)) = \frac{\det(\Gamma)}{s_2}.$$

On obtient

$$d(\mathbf{x}, \mathrm{Vect}(\mathbf{e}_2)) = d(\lambda\mathbf{e}_1 + \mu\mathbf{e}_2, \mathrm{Vect}(\mathbf{e}_2)) = d(\lambda\mathbf{e}_1, \mathrm{Vect}(\mathbf{e}_2)) = |\lambda| \frac{\det(\Gamma)}{s_2}.$$

On a donc, puisque $(0,0) \in \mathrm{Vect}(\mathbf{e}_2)$, que

$$||\mathbf{x}|| = ||\mathbf{x} - (0,0)|| \geqslant d(\mathbf{x}, \mathrm{Vect}(\mathbf{e}_2)) = |\lambda| \frac{\det(\Gamma)}{s_2} \geqslant \frac{\sqrt{3}}{2} [\lambda| s_1$$

ce qui implique

$$\lambda \leqslant |\lambda| \ll \frac{||\mathbf{x}||}{s_1}.$$

On démontrerait de même la deuxième inégalité en regardant des projections sur $\mathrm{Vect}(\mathbf{e}_1)$. □

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

$$\forall p \in \mathbb{P}, \forall \nu \geqslant 1, \quad r_1(p^\nu) = \begin{cases} r_0(p) = 1 + \chi(p) & \text{si } \nu = 1 \\ (1+\nu)^3 & \text{sinon.} \end{cases}$$

On a ainsi que pour tous k, m et n entiers,

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

En effet, par multiplicativité, il suffit de le vérifier sur $k = p^{\nu_1}$, $m = p^{\nu_2}$ et $n = p^{\nu_3}$. Or,

$$r_0(p^{\nu_1}) r_0(p^{\nu_2}) r_0(p^{\nu_3}) = \begin{cases} 0 & \text{si } p = 2 \\ (\nu_1+1)(\nu_2+1)(\nu_2+1) & \text{si } p \equiv 1[4] \\ \frac{(1-(-1)^{\nu_1})(1-(-1)^{\nu_2})(1-(-1)^{\nu_3})}{8} & \text{sinon.} \end{cases}$$

puisque

$$r_0(p^\nu) = \sum_{i=0}^{\nu} \chi(p)^i = \begin{cases} 0 & \text{si } p = 2 \\ \nu + 1 & \text{si } p \equiv 1[4] \\ \frac{1-(-1)^\nu}{2} & \text{sinon.} \end{cases}$$

Si $p = 2$ ou $p \equiv 1[4]$, on a trivialement

$$r_0(p^{\nu_1}) r_0(p^{\nu_2}) r_0(p^{\nu_3}) \leqslant r_1(p^{\nu_1+\nu_2+\nu_3})$$

puisque

$$(\nu_1+1)(\nu_2+1)(\nu_2+1) \leqslant (\nu_1+\nu_2+\nu_3+1)^3$$

comme on le constate en développant. Enfin, si $p \equiv 3[4]$, on a $r_0(p^\nu)$ positif et $r_0(p^\nu) \leqslant (\nu+1)$ et donc le résultat reste vrai. On déduit de cela la majoration

$$S_{\mathbf{k},\alpha}\left(2^{-k_0}X\right) \ll \sum_{\substack{\lambda \ll X/||\mathbf{e}_1|| \\ \mu \ll X/||\mathbf{e}_2||}} r_1\left(F(\lambda,\mu)\right)$$

où $F = L_1' L_2' Q'$ est un polynôme de $\mathbb{Z}[x_1,x_2]$ de degré 4. On a alors

$$\max(||L_i'||, ||Q'||) \leqslant ||\mathbf{M}||^2 L_\infty$$

où $||\mathbf{M}||$ désigne le plus grand coefficient de la marice en valeur absolue. Ici, à partir de l'expression de la matrice $\mathbf{M}$ et des intervalles dans lesquels sont chacune des variables, on voit immédiatement que $||M|| \leqslant 2^{k_1+\max(k_2,k_3)}$. On a donc les inégalités

$$||F|| \leqslant 2^{4(k_1+\max(k_2,k_3))} L_\infty^3 \leqslant (2^{k_1+\max(k_2,k_3)} L_\infty)^4.$$

On souhaite alors utiliser le Théorème 4 avec la fonction r_1 qui appartient clairement à la classe des fonctions multiplicatives admissibles et avec F. On a alors besoin du lemme suivant qui est crucial mais pourtant jamais démontré dans aucune des références connues de l'auteur.

Lemme 13. *On a dans ce cas $E \ll (\det(\mathbf{M}) L_\infty)^\varepsilon$, où E est donnée par (1.63).*

Démonstration.– En utilisant la définition de E, on a

$$E = \prod_{d<p\leqslant \min(X_1,X_2)} \left(1+\frac{\rho_F^*(p)\chi(p)}{p}\right) \prod_{i=1,2} \prod_{p\leqslant X_i} \left(1+\frac{d_i\chi(p)}{p}\right)$$

On commence par remarquer que

$$\prod_p \left(1+\frac{\chi(p)}{p}\right) = \frac{2}{\pi}$$

(on le déduit de $L(1,\chi)$ et de $\zeta(2)$ sur $1-1/4$). On a donc que les produits

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

puisqu'on rappelle que $d_i \in \{0,1\}$. Étudions maintenant la quantité

$$\rho_L^*(p) = \frac{1}{p-1} \# \left\{ (n_1,n_2) \in]\!]0,p]\!]^2 \quad \middle| \quad \begin{array}{l} (n_1,n_2,p)=1 \\ L(n_1,n_2) \equiv 0[p] \end{array} \right\},$$

pour $L(x_1,x_2) = ax_1+bx_2$ une forme binaire de degré 1 quelconque. Soit $p|(a,b)$ et dans ce cas là tous les couples tels que $(x_1,x_2,p) = 1$ sont solutions, on en a donc $(p-1)^2+2(p-1) = (p+1)(p-1)$, soit $p \nmid a$ ou $p \nmid b$ et dans ce cas, on partitionne les

solutions telles que $p|x_1$ et $p \nmid x_2$, celles telles que $p|x_2$ et $p \nmid x_1$ et celles telles que x_2 et x_1 soient inversibles. Dans le premier cas, on a que

$$ax_1 + bx_2 \equiv 0[p]$$

équivaut à

$$ax_1 \equiv 0[p]$$

ce qui donne que si $p|a$, alors on a $p-1$ choix de x_1 inversible et comme x_2 est fixé, on obtient $p-1$ solutions et zéro sinon, de même on obtient $p-1$ solutions si $p|b$ dans le deuxième cas et zéro sinon. Enfin, dans le dernier cas, on est ramené à résoudre dans un corps

$$L(1, \overline{x_1}x_2) \equiv 0[p]$$

On a donc autant de solutions que de choix de x_2 inversible car $p \nmid b$ car sinon p diviserait aussi a ce qui est exclu, soit $p-1$ solutions. On a par conséquent

$$\rho_L^*(p) = \begin{cases} p+1 & \text{si } p|(a,b) \\ 1 & \text{si } p|a \quad \text{et} \quad p \nmid b \\ 1 & \text{si } p|b \quad \text{et} \quad p \nmid a \\ 1 & \text{si } p \nmid a \quad \text{et} \quad p \nmid b. \end{cases}$$

Étudions alors

$$\rho_Q^*(p) = \frac{1}{p-1} \# \left\{ (n_1, n_2) \in]\!]0, p]\!]^2 \quad \middle| \quad \begin{array}{l} (n_1, n_2, p) = 1 \\ L(n_1, n_2) \equiv 0[p] \end{array} \right\},$$

pour une forme quadratique $Q(\mathbf{x}) = ax_1^2 + bx_2^2 + cx_1x_2$ irréductible sur $\mathbb{Q}[i]$. Le même raisonnement que pour une forme linéaire selon que les couples sont inversibles ou que l'une des deux composantes est divisible par p donne

$$\rho_Q^*(p) = \begin{cases} p+1 & \text{si } p|(a,b,c) \\ 2 & \text{si } p|a,b \quad \text{et} \quad p \nmid c \\ 1 & \text{si } p|a,c \quad \text{et} \quad p \nmid b \\ 1 & \text{si } p|b,c \quad \text{et} \quad p \nmid a \\ \rho_{Q(x,1)}(p) & \text{si } p \nmid a,b,c. \end{cases}$$

En effet, si p divise a et b et pas c, on voit que x_1 ou x_2 vaut 0 et l'autre est inversible donc on a $2(p-1)$ solutions par exemple, dans le dernier cas, tout le monde est inversible et on est ramené à résoudre

$$Q(\overline{x_2}x_1, 1) \equiv 0[p]$$

qui donne $p-1$ choix de x_2 fois le nombre de solutions. On relie à présent la quantité $\rho^*_{L_1'L_2'Q'}$ à des quantités du même type que celles que l'on vient d'étudier. On peut commencer par remarquer que le fait $L_i'(\lambda, \mu) = L_i(\mathbf{x})$ et que le changement de variables via $\mathbf{M}_e$ (la matrice de $\mathbf{e}_1$, $\mathbf{e}_2$) soit dans $\mathrm{GL}_2(\mathbb{Q})$ impliquent que Q', L_i' vérifient les mêmes hypothèses que les L_i et Q. On commence alors par étudier les nombres premiers p ne divisant aucun des contenus de L_1, L_2 et Q et les couples tels que

$$L_1'(x_1, x_2) \equiv 0[p] \quad \text{et} \quad Q'(x_1, x_2) \equiv 0[p].$$

Supposons que a_1 soit inversible modulo p, on a donc $x_1 \equiv -\overline{a_1}b_1x_2[p]$, ce qui donne que

$$x_2^2\mathrm{Res}(L_1, Q) \equiv 0[p].$$

Puisqu'on doit avoir $(x_1, x_2, p) = 1$, soit $\mathrm{Res}(L_1, Q)$ est divisible par p et on a $p-1$ couples dans l'intersection, soit on en a zéro car si p divise x_2, il divise x_1. On étudie désormais, pour le même ensemble de nombres premiers, les couples tels que

$$L_1'(x_1, x_2) \equiv 0[p] \quad \text{et} \quad L_2'(x_1, x_2) \equiv 0[p].$$

Si a_1 et a_2 sont inversibles, alors on a

$$x_1 \equiv -\overline{a_1}b_1x_2 \equiv -\overline{a_2}b_2x_2[p].$$

Soit donc $\mathrm{Res}(L_1, L_2)$ est divisible par p et on a $p-1$ couples dans l'intersection, soit on en a zéro. Le cas où b_1 et b_2 sont inversibles est analogue. Supposons donc que a_1 et b_2 soient inversibles. On a donc

$$x_1 \equiv -\overline{a_1}b_1x_2[p] \quad \text{et} \quad x_2 \equiv -\overline{b_2}a_2x_1[p].$$

On en déduit que $x_1 \equiv \overline{a_1}b_1\overline{b_2}a_2x_1[p]$, ce qui fournit à nouveau $p-1$ solutions si $\mathrm{Res}(L_1, L_2)$ est divisible par p et zéro sinon. D'après ce qu'on vient de voir, pour qu'il y ait des solutions telles que

$$L_1'(x_1, x_2) \equiv 0[p] \quad , \quad L_2'(x_1, x_2) \equiv 0[p] \quad \text{et} \quad Q'(x_1, x_2) \equiv 0[p].$$

pour ces nombres premiers, il est nécessaire que p divise tous les résultants et dans ce cas on obtient $p-1$ solutions.

On est maintenant presqu'en mesure de montrer que sous nos hypothèses, $E \ll (\det(\mathbf{M})L_\infty)^\varepsilon$. On rappelle qu'il restait à étudier

$$\prod_{4<p\leqslant X}\left(1+\frac{\rho^*_{L_1'L_2'Q'}(p)\chi(p)}{p}\right).$$

Si p divise $\delta = c(L_1')c(L_2')c(Q')$, alors tous les couples sont solutions, on a donc une contribution de tels premiers majorée par

$$0 \leqslant \prod_{\substack{4<p\\ p|\delta}}\left(1+\frac{(p+1)\chi(p)}{p}\right) \leqslant \prod_{p|\delta}\left(1+\frac{p+1}{p}\right) \leqslant 3^{\omega(\delta)} \ll \delta^\varepsilon \ll (\det(\mathbf{M})L_\infty)^\varepsilon.$$

Intéressons-nous maintenant aux premiers p qui ne divisent pas δ. On a par l'étude qui précède

$$\rho^*_{L_1'L_2'Q'}(p) = \rho^*_{L_1'}(p) + \rho^*_{L_2'}(p) + \rho^*_{Q'}(p) - c_p(p-1)$$

où c_p est une constante positive telle que $c_p \in \{0, 1, 2\}$ (on doit enlever les contributions des couples solutions de deux et pas de la troisième et rajouter ceux qui sont solutions des trois) nulle dès que p ne divise aucun des résultants. On en déduit une contribution des p divisant le produit R des résultants majorée par

$$\prod_{\substack{p|R\\ p\nmid\delta}}(1+c_p) \ll 3^{\omega(R)} \ll (\det(\mathbf{M})L_\infty)^\varepsilon.$$

Il reste donc une contribution de

$$\prod_{\substack{4<p\leqslant X\\ p\nmid\delta}}\left(1+\frac{(\rho^*_{L'_1}(p)+\rho^*_{L'_2}(p)+\rho^*_{Q'}(p))\chi(p)}{p}\right).$$

La suite d'inégalité

$$\log\left(\prod_p\left(1+\frac{\chi(p)\rho^*(p)}{p}\right)\right)=\sum_p\log\left(1+\frac{\chi(p)\rho^*(p)}{p}\right)\leqslant\sum_p\frac{\chi(p)\rho^*(p)}{p}.$$

permet de majorer (en fait les raisonnement précédents montrent qu'on peut se restreindre en plus aux premiers qui ne divisent aucun des coefficients des formes) cette contribution par

$$\sum_p\frac{(\rho^*_{L'_1}(p)+\rho^*_{L'_2}(p)+\rho^*_{Q'}(p))\chi(p)}{p}$$

où la somme porte en réalité sur l'ensemble $\mathbb{P}$ des nombres premiers privé d'un nombre fini de premiers ce qui ne change rien à la convergence. Or, d'après ce qui précède, on a

$$\sum_p\frac{\rho^*_{L'_i}(p)\chi(p)}{p}=\sum_p\frac{\chi(p)}{p}\ll 1$$

et

$$\sum_p\frac{\rho^*_{Q'}(p)\chi(p)}{p}=\sum_p\frac{\rho_{Q(x,1)}(p)\chi(p)}{p}$$

où là encore la somme porte en réalité sur l'ensemble $\mathbb{P}$ des nombres premiers privé d'un nombre fini de premiers. Il nous reste donc pour pouvoir conclure à montrer que

$$\sum_p\frac{\rho_{Q(x,1)}(p)\chi(p)}{p}\ll 1$$

sous l'hypothèse que Q est irréductible sur $\mathbb{Q}[i]$. On commence pour ce faire par constater que si $Q(X,Y)\in k[X,Y]$ est homogène et irrductible sur un corps k, alors $Q(1,X)$ est irréductible sur $k[X]$. En effet, si

$$Q(1,X)=R(X)S(X),$$

on homogénéise R et S en $\tilde{R}$ et $\tilde{S}$ de sorte que

$$Q(1,X)=\tilde{R}(1,X)\tilde{S}(1,X).$$

On a alors $Q(X,Y)=\tilde{R}(X,Y)\tilde{S}(X,Y)$. Dans $k(X,Y)$, on a

$$Y^{-2}Q(X,Y)=Q(1,X/Y)=\tilde{R}(1,X/Y)\tilde{S}(1,X/Y)$$

donc

$$Q(X,Y)=\tilde{R}(X,Y)\tilde{S}(X,Y).$$

Puis, si f est irréductible sur $\mathbb{Q}[i]$ de degré 2, on peut obtenir une formule explicite pour $\rho_f(p)$ et obtenir la convergence souhaitée. En effet, une équation du second degré modulo

p différent de 2 repose sur le discriminant de f tout comme sur $\mathbb{R}$ ou $\mathbb{C}$. Un tel f est irréductible sur $\mathbb{Q}$ si, et seulement si, elle n'a pas de racine dans $\mathbb{Q}$ ce qui équivaut au fait que le discriminant de f soit strictement positif et ne soit pas un carré ou qu'il soit négatif strictement. Ensuite la forme est réductible sur $\mathbb{Q}[i]$ si, et seulement si, ce discriminant est strictement négatif et que son opposé est un carré. De plus, on voit tout de suite que

$$\rho_f(p) = 1 + \left(\frac{\mathrm{disc}(f)}{p}\right)$$

où $\left(\frac{\cdot}{p}\right)$ désigne le symbole de Legendre modulo p. On décompose $\mathrm{disc}(f) = \varepsilon_f u_f v_f$ où $\varepsilon_f \in \{-1, 1\}$, v_f est un carré et u_f est positif sans facteur carré. On a alors par multiplicativité

$$\rho_f(p) = 1 + \chi(p)^{\frac{1-\varepsilon_f}{2}} \left(\frac{u_f}{p}\right).$$

On voit donc que si la forme est irréductible sur $\mathbb{Q}[i]$, on a soit $\varepsilon_f = 1$ soit $\varepsilon_f = -1$ et dans les deux cas $u_f \neq 1$. Dans le premier cas, on a

$$\sum_p \frac{\chi(p)\rho_f(p)}{p} = \sum_p \frac{\chi(p)\left(1 + \left(\frac{u_f}{p}\right)\right)}{p}$$

On a donc affaire à un caractère de Dirichlet modulo u_f non principal car sinon on aurait $u_f = 1$. Or, on sait que pour tout caractère de Dirichlet ψ non principal, on a

$$\sum_p \frac{\psi(p)}{p} \ll 1,$$

où on justifie l'invariance de la constante (qui dépend a priori des formes) par transformations linéaires comme dans la preuve du Lemme 4. On a donc bien

$$\sum_p \frac{\chi(p)\rho_f(p)}{p} \ll 1.$$

Le cas où ε_f se traite de façon analogue en ajoutant un facteur $\chi(p)$. En revanche, lorsque f est réductible sur $\mathbb{Q}[i]$, on a $\varepsilon_f = -1$ et $u_f = 1$ et donc

$$\rho_f(p) = 1 + \chi(p)$$

et

$$\sum_{p\leqslant x} \chi_0(p)\rho_{x^2+1}(p) = \sum_{p\leqslant x}(1+\chi(p)) = 2\sum_{p\equiv 1[4]} 1 = 2\frac{\mathrm{Li}(x)}{\varphi(4)} + O\left(x\exp(-c\sqrt{\log(x)})\right),$$

où χ_0 désigne le caractère principal, tandis que

$$\sum_{p\leqslant x} \chi(p)\rho_{x^2+1}(p) = \sum_{p\leqslant x} 1 + \sum_{p\leqslant x}\chi(p) = \mathrm{Li}(x) + O\left(x\exp(-c\sqrt{\log(x)})\right),$$

pour une certaine constante $c > 0$ d'après le théorème des nombres premiers et le fait que

$$\left|\sum_{p\leqslant x}\chi(p)\right| \leqslant 4.$$

Remarque : On a également, si k $(= \mathbb{Q}[i])$ est un corps de nombres et que f est un polynôme irréductible sur $\mathbb{Z}$, que si $p \nmid f_0\mathrm{disc}(f)$ avec f_0 le coefficient dominant de f, alors en utilisant la décomposition en produit d'irrréductibles deux à deux non associés de la réduction de f modulo p

$$f(x) \equiv f_1(x)^{e_1}...f_r(x)^{e_r}[p],$$

les polynomes f_i étant de degré $r_i = N_{k/\mathbb{Q}}(\mathfrak{P}_\mathfrak{i})$ où $\mathfrak{P}_\mathfrak{i} = (p, f_i(x))$. Les polynômes étant iréductibles, on en déduit que le polynôme f admet autant de racines modulo p qu'il n'y a de i tels que $r_i = 1$. D'où,

$$\rho_f(p) = \#\left\{\mathfrak{P} \quad | \quad N_{k/\mathbb{Q}}(\mathfrak{P}) = p\right\},$$

et donc l'étude de

$$\sum_p \chi(p)\rho_f(p)$$

est reliée à celle de la fonction L :

$$L_k(s,\chi) = \sum_{\mathfrak{A}} \frac{\chi\left(N_{k/\mathbb{Q}}(\mathfrak{A})\right)}{N_{k/\mathbb{Q}}(\mathfrak{A})^s}.$$

On aurait alors pu utiliser le résultat suivant qui est démontré dans le survol d'Heilbronn [33] si on suppose de plus la forme irréductible sur $\mathbb{Q}[i]$, où on note χ_0 le caractère principal :

$$\sum_{p\leqslant x}\chi_0(p)\rho_{Q(1,x)}(p) = \frac{x}{\log(x)} + o\left(\frac{x}{\log(x)}\right)$$

et

$$\sum_{p\leqslant x}\chi(p)\rho_{Q(1,x)}(p) = o\left(\frac{x}{\log(x)}\right)$$

si le caractère χ n'est pas principal. On peut même améliorer les termes d'erreur par

$$\sum_{p\leqslant x}\chi_0(p)\rho_{Q(1,x)}(p) = \mathrm{Li}(x) + 0\left(x\exp(-c\sqrt{\log(x)})\right)$$

et

$$\sum_{p\leqslant x}\chi(p)\rho_{Q(1,x)}(p) \ll x\exp(-c\sqrt{\log(x)})$$

avec c une constante qui dépend des coefficients de la forme. Il est à noter que la première expression reste vraie si la forme est réductible sur $\mathbb{Q}[i]$ mais pas la deuxième comme on l'a vu.

Pour revenir à la preuve, on obtient finalement que

$$\sum_p \frac{\rho_{Q(x,1)}(p)\chi(p)}{p} \ll 1,$$

ce qui permet de conclure la preuve du Lemme. □

Appliquant alors le Théorème 4 et le Lemme 13, on déduit la majoration

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

pour tout $\varepsilon > 0$. Or, on sait que pour tout réseau Γ, on a

$$\det(\Gamma) \leqslant s_1 s_2 \ll \det(\Gamma)$$

en reprenant les notations de la preuve du Lemme 12. On a donc

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

ce qui fournit finalement

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

Or, on avait écrit la décomposition suivante

$$S(X) = \sum_{k_0 \geqslant 0} \sum_{0 \leqslant k_1,k_2,k_3 \leqslant \log\log X} S_{\mathbf{k}}\left(2^{-k_0}X\right) + \sum_{k_0 \geqslant 0} \sum_{\log\log X > k_i} S_{\mathbf{k}}\left(2^{-k_0}X\right).$$

On déduit donc de ce qui précéde

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

puis d'après l'estimation de $n(k_1,k_2,k_3) \ll 1$ obtenue ci-dessus

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

On utilise alors cette majoration pour estimer les termes tels que $k_i > \log\log(X)$. Traitons par exemple le cas de la somme

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

On a

$$\sum_{k_0 \geqslant 0} \sum_{k_2,k_3 \leqslant \log\log(X)} \sum_{k_1 > \log\log(X)} 2^{\varepsilon(k_1+\max(k_2,k_3))} L_\infty^\varepsilon \left(\frac{X^2}{2^{2k_0+\max(k_1,k_2,k_3)}} \right)$$
$$= \frac{4}{3} L_\infty^\varepsilon X^2 \sum_{k_2,k_3 \leqslant \log\log(X)} 2^{\varepsilon \max(k_2,k_3)} \sum_{k_1 > \log\log(X)} 2^{(\varepsilon-1)k_1}$$

car $k_1 = \max(k_1,k_2,k_3)$. Quitte à prendre $\varepsilon < 1$, on a

$$\sum_{k_1 > \log\log(X)} 2^{(\varepsilon-1)k_1} \sim_{+\infty} 2 \times 2^{(\varepsilon-1)\log\log(X)} = 2(\log(X))^{-(1-\varepsilon)\log(2)}$$

et

$$\sum_{k_2,k_3\leqslant \log\log(X)} 2^{\varepsilon \max(k_2,k_3)} \leqslant \sum_{k_2,k_3\leqslant \log\log(X)} 2^{\varepsilon(k_2+k_3)}.$$

Or, toujours avec la formule donnant la somme partielle d'une série géométrique, on voit que

$$\sum_{k\leqslant \log\log(X)} 2^{\varepsilon k} \sim_{+\infty} 2^{\varepsilon \log\log(X)} = (\log(X))^{\varepsilon\log(2)}.$$

On obtient donc finalement la majoration

$$\sum_{k_2,k_3\leqslant \log\log(X)} 2^{\varepsilon \max(k_2,k_3)} \sum_{k_1>\log\log(X)} 2^{(\varepsilon-1)k_1} \ll (\log(X))^{3\varepsilon\log(2)-\log(2)}$$

et

$$\sum_{k_0\geqslant 0}\sum_{k_2,k_3\leqslant \log\log(X)}\sum_{k_1>\log\log(X)} 2^{\varepsilon(k_1+\max(k_2,k_3))} L_\infty^\varepsilon\left(\frac{X^2}{2^{2k_0+\max(k_1,k_2,k_3)}}\right)$$
$$\ll L_\infty^\varepsilon X^2(\log(X))^{3\varepsilon\log(2)-\log(2)} \ll L_\infty^\varepsilon X^2(\log(X))^{3\varepsilon\log(2)-\eta}$$

puisque $\eta<\log(2)$. On peut donc écrire une majoration du type

$$L_\infty^\varepsilon X^2(\log(X))^{\varepsilon-\eta}$$

pour ε assez petit, ce qui est convenable. On passe désormais à l'étude de

$$\sum_{k_0\geqslant 0}\sum_{k_2,k_3\leqslant \log\log(X)}\sum_{k_1>\log\log(X)} 2^{\varepsilon(k_1+\max(k_2,k_3))} L_\infty^\varepsilon\left(2^{-k_0}X\right)^{1+\varepsilon} \ll L_\infty^\varepsilon X^{1+\varepsilon}\sum_{k_2,k_3\leqslant \log\log(X)}\sum_{k_1>\log\log(X)} 2^{\varepsilon(k_1+k_2+k_3)}.$$

Le même raisonnement fournit

$$\sum_{k_2,k_3\leqslant \log\log(X)} 2^{\varepsilon(k_2+k_3)} \ll (\log(X))^{2\varepsilon\log(2)}$$

et en utilisant que $\log\log(X)<k_1\ll\log(X)$ et la formule donnant la série géométrique, on obtient

$$\sum_{k_1>\log\log(X)} 2^{\varepsilon k_1} \ll 2^{\varepsilon\log(X)} = X^{\varepsilon\log(2)}.$$

Finalement, on a

$$\sum_{k_0\geqslant 0}\sum_{k_2,k_3\leqslant \log\log(X)}\sum_{k_1>\log\log(X)} 2^{\varepsilon(k_1+\max(k_2,k_3))} L_\infty^\varepsilon\left(2^{-k_0}X\right)^{1+\varepsilon} \ll L_\infty^\varepsilon X^{1+\varepsilon(1+\log(2))}(\log(X))^{2\varepsilon\log(2)}$$

où

$$(\log(X))^{2\varepsilon\log(2)} \ll (\log(X))^{2\varepsilon\log(2)}$$

et

$$X^{1+\varepsilon(1+\log(2))} \ll X^2\log(X)^{-\eta}$$

pour ε assez petit. On a donc obtenu que pour ε assez petit, on a bien

$$S_1 \ll L_\infty^\varepsilon X^2(\log(X))^{\varepsilon-\eta}.$$

On traite de manière exactement analogue les cas $k_2 > \log\log(X)$, $k_1, k_3 \leqslant \log\log(X)$ et $k_3 > \log\log(X)$, $k_1, k_2 \leqslant \log\log(X)$. Ensuite si ε' est plus grand que le "assez petit" dont on a besoin, puisque

$$(\log(X))^{\varepsilon-\eta} \ll (\log(X))^{\varepsilon'-\eta},$$

on en déduit

$$S_1 \ll L_\infty^\varepsilon X^2 (\log(X))^{\varepsilon-\eta}$$

pour tout $\varepsilon > 0$. Passons à l'étude du cas

$$S_2 := \sum_{k_0 \geqslant 0} \sum_{k_3 \leqslant \log\log(X)} \sum_{k_1, k_2 > \log\log(X)} S_{\mathbf{k}}\left(2^{-k_0} X\right).$$

On étudie donc

$$L_\infty^\varepsilon X^{1+\varepsilon} \sum_{k_3 \leqslant \log\log(X)} \sum_{k_1, k_2 > \log\log(X)} 2^{\varepsilon(k_1+k_2+k_3)}$$

pour obtenir facilement une contribution

$$\ll L_\infty^\varepsilon X^{1+\varepsilon} (\log(X))^{\varepsilon\log(2)} X^{2\varepsilon\log(2)}$$

qui est convenable pour ε assez petit. On traite ensuite

$$\sum_{k_3 \leqslant \log\log(X)} \sum_{k_1, k_2 > \log\log(X)} 2^{\varepsilon(k_1+k_2+k_3) - \max(k_1,k_2,k_3)}.$$

En effet, $\max(k_2, k_3) \leqslant k_2 + k_3$ et ensuite on regarde

$$\sum_{k_3 \leqslant \log\log(X)} \sum_{k_1 > \log\log(X)} \sum_{\log\log(X) < k_2 \leqslant k_1} 2^{\varepsilon(k_1+k_2+k_3) - k_1}.$$

Le terme

$$\sum_{\log\log(X) < k_2 \leqslant k_1} 2^{\varepsilon k_2} \ll \sum_{k_2 \leqslant k_1} 2^{\varepsilon k_2} \ll 2^{\varepsilon k_1}$$

donc

$$\sum_{k_1 > \log\log(X)} \sum_{\log\log(X) < k_2 \leqslant k_1} 2^{\varepsilon(k_1+k_2) - k_1} \ll \sum_{k_1 > \log\log(X)} 2^{(2\varepsilon-1)k_1} \ll 2(\log(X))^{-(1-2\varepsilon)\log(2)}$$

tandis que

$$\sum_{k_3 \leqslant \log\log(X)} 2^{\varepsilon k_3} \ll (\log(X))^{\varepsilon\log(2)}.$$

On obtient finalement un terme en

$$L_\infty^\varepsilon X^2 (\log(X))^{3\varepsilon\log(2) - \log(2)}$$

qui est à nouveau convenable pour ε assez petit. On obtient le même terme d'erreur pour les termes de la somme tels que $k_1 \leqslant k_2$. On traite de même la somme où on inverse les rôles de k_2, k_3 et pour celle où on inverse les rôles de k_1, k_3 puisqu'une fois $k_1 + \max(k_2, k_3)$ majoré par la somme des trois, les rôles sont symétriques. Enfin, il reste à traiter

$$S_3 := \sum_{k_0 \geqslant 0} \sum_{k_1, k_2, k_3 > \log\log(X)} S_{\mathbf{k}}\left(2^{-k_0} X\right).$$

La partie de la somme faisant intervenir le $X^{1+\varepsilon}$ ne pose pas de problème et se traite exactement de la même manière mais en faisant apparaître un facteur 3. Il suffit donc d'étudier

$$L_\infty^\varepsilon X^2 \sum_{k_1,k_2,k_3>\log\log(X)} 2^{\varepsilon(k_1+k_2+k_3)-\max(k_1,k_2,k_3)}.$$

On sépare selon le maximum des k_i et on est ramené à l'étude de

$$\sum_{k_1>\log\log(X)} \sum_{\log\log(X)<k_2\leqslant k_1} \sum_{\log\log(X)<k_3\leqslant k_1} 2^{\varepsilon(k_1+k_2+k_3)-k_1}$$

et tout marche comme ci-dessus.
On a donc

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

qui donne bien

$$S(X) = \sum_{k_0\geqslant 0} \sum_{0\leqslant k_1,k_2,k_3\leqslant\log\log(X)} S_{\mathbf{k}}\left(2^{-k_0}X\right) + O\left(\frac{L_\infty^\varepsilon (r_\infty r' + r_\infty^2)X^2}{(\log(X))^{\eta-\varepsilon}}\right)$$

où

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

où α parcourt les $n(k_1,k_2,k_3)$ solutions de (1.52) et (1.53) et où

$$S_{\mathbf{k},\alpha}(X) = \sum_{\substack{\mathbf{x}'\in\mathbb{Z}^2\cap X\mathcal{R}_{\mathbf{M}}\\ x_1'\equiv 1[4]}} r\left(L_{1,\mathbf{M}}(\mathbf{x}')\right) r\left(L_{2,\mathbf{M}}(\mathbf{x}')\right) r\left(Q_{\mathbf{M}}(\mathbf{x}')\right)$$

avec les notations qui ont été introduites plus haut et

$$L_{i,\mathbf{M}}(\mathbf{x}') = L_i(\mathbf{M}\mathbf{x}') \quad \text{et} \quad Q_{\mathbf{M}}(\mathbf{x}') = Q(\mathbf{M}\mathbf{x}').$$

Cette fois-ci, on a bien dans les sommes $S_{\mathbf{k},\alpha}$ la condition $x_1' \equiv 1[4]$ qui permet d'appliquer la décomposition exposée dans la section précédente. On a donc

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

où

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

et

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

1.4.4 Traitement de S_0

On commence par traiter la contribution des $S_0(X;\mathbf{k},\alpha)$ qui donne un terme d'erreur, le terme principal provenant de la contribution des $S_{\pm,\pm,\pm}(X;\mathbf{k},\alpha)$. La contribution des sommes $S_0(X;\mathbf{k},\alpha)$ est

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

On a clairement que

$$S_0\left(2^{-k_0}X;\mathbf{k},\alpha\right)\ll \sum_{\substack{\mathbf{x}'\in\mathbb{Z}^2\cap X\mathcal{R}_{\mathbf{M}}\\ x_1'\equiv 1[4]}} \left|C\left(L_{1,\mathbf{M}}(\mathbf{x}')\right)\right| r\left(L_{2,\mathbf{M}}(\mathbf{x}')\right) r\left(Q_{\mathbf{M}}(\mathbf{x}')\right).$$

On pose alors

$$E=\{m\in\mathbb{Z}\quad|\quad \exists d|m,\quad \text{tel que}\quad Y<d\leqslant XY^{-1}\},$$

(sinon $C(m)$ est nul)

$$E_{k_0}=\{m\in\mathbb{Z}\quad|\quad \exists \mathbf{x}\in 2^{-k_0}X\mathcal{R}\quad \text{tel que}\quad L_1(\mathbf{x})=m\}$$

et

$$\mathcal{B}_{k_0}=E\cap E_{k_0}$$

de sorte que

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

où

$$S_{0,m}(X)=\sum_{\substack{\mathbf{x}\in\mathbb{Z}^2\cap X\mathcal{R}\\ L_1(\mathbf{x})=m}} r\left(L_2(\mathbf{x})\right) r\left(Q(\mathbf{x})\right).$$

On en déduit donc que

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

On utilise alors le lemme suivant

Lemme 14. *Pour $2^{k_0}\leqslant\sqrt{X}$, on a*

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

Démonstration.– On applique le Lemme 6 de [24] pour obtenir la majoration

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

Mais la condition $2^{k_0}\leqslant\sqrt{X}$ implique l'inégalité

$$\sqrt{X}\leq 2^{-k_0}X$$

et par conséquent

$$\frac{r'2^{-k_0}X\log\log(X')^{9/4}}{(\log(2^{-k_0}X'))^{\eta}} \ll \frac{r'2^{-k_0}X\log\log(X')^{9/4}}{(\log(X'))^{\eta}},$$

ce qui est convenable. □

On en déduit la majoration

$$S_0(X) \ll \frac{r'X\log\log(X')^{21/4}}{(\log(X'))^{\eta}} \sum_{k_0\geqslant 0} 2^{-k_0} \max_{m\in\mathbb{N}} \left|S_{0,m}\left(2^{-k_0}X\right)\right|,$$

dans le cas où $2^{k_0} \leqslant \sqrt{X}$. Dans le cas contraire, où $2^{k_0} > \sqrt{X}$, la majoration triviale (1.12) fournit

$$S_0(X) \ll X^2 \sum_{2^{k_0}>\sqrt{X}} 2^{-2k_0} \ll X$$

qui fournit un terme convenable en vue du Théorème 1. On montre alors le lemme suivant qui permet de conclure que la contribution de S_0 donne un terme d'erreur convenable.

Lemme 15. *Il existe une constante absolue $c_0 > 0$ telle que*

$$S_{0,m}(X) \ll L_\infty^{\varepsilon} r_\infty X(\log\log(X'))^{c_0}.$$

Démonstration.– On adapte ici la démonstration donnée dans [24]. On rappelle que

$$S_{0,m}(X) = \sum_{\substack{\mathbf{x}\in\mathbb{Z}^2\cap X\mathcal{R}\\ L_1(\mathbf{x})=m}} r\left(L_2(\mathbf{x})\right) r\left(Q(\mathbf{x})\right).$$

On sait que L_1 est non nulle donc $a_1b_1 \neq 0$. Supposons que $a_1 \neq 0$, le cas où $a_1 = 0$ et $b_1 \neq 0$ se traitant de manière analogue. Si on a $L_1(\mathbf{x}) = m$, alors on a

$$x_1 = \frac{m - b_1x_2}{a_1}$$

et donc

$$L_2(\mathbf{x}) = \frac{A_2m + B_2n}{a_1} = L_2'(m,n)$$

avec $A_2 = a_2$, $B_2 = a_1b_2 - a_2b_1 = \mathrm{Res}(L_1, L_2)$ et $n = x_2$ et

$$Q(\mathbf{x}) = \frac{A_3m^2 + B_3n^2 + C_3mn}{a_1^2} = Q'(m,n)$$

avec $n = x_2$ et $A_3 = a_3$, $B_3 = a_3b_1^2 + b_3a_1^2 - c_3b_1a_1 = \mathrm{Res}(L_1, Q)$ et
$C_3 = c_3a_1 - 2a_3b_1 = \mathrm{Res}\left(L_1, \partial_1 Q\right)$. On peut remarquer que $B_2B_3 \neq 0$ par hypothèse et puisque

$$\forall (k,l) \in \mathbb{N}, \quad r(l) \leqslant r(k^2l)$$

qui résulte du fait que si $l = a^2 + b^2$, alors $k^2l = (ka)^2 + (kb)^2$ et que pour deux décompositions distinctes de l on en obtient deux distinctes de k^2l. On en déduit les inégalités

$$r(L_2'(m,n)) \leqslant r(a_1(A_2m + B_2n)) \quad \text{et} \quad r(Q'(m,n)) \leqslant r(A_3m^2 + B_3n^2 + C_3mn).$$

On pose alors

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

et

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

de sorte que $(B_2', A_2'(m)) = (B_3', A_3'(m), C_3'(m)) = 1$ et

$$a_1(A_2 m + B_2 n) = a_1 \gcd(A_2 m, B_2)(A_2'(m) + B_2' n)$$

et

$$A_3 m^2 + B_3 n^2 + C_3 mn = \gcd(A_3 m^2, B_3, C_3 m)(A_3'(m) + B_3' n^2 + C_3'(m) n).$$

On introduit enfin $h = 2 \times 3 \times a_1 B_2 B_3 H$ avec les notations précédentes et la fonction multiplicative définie pour p premier et ν un entier naturel par

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

Comme on l'a démontré plus haut (cf après le Lemme 12), le choix de cette fonction implique que

$$\forall (m,n) \in \mathbb{N}^2, \quad r(m) r(n) \leqslant 16 r_2(mn).$$

On en déduit

$$r(L_2(\mathbf{x}))\, r(Q(\mathbf{x})) \leqslant 16 r_2(F_m(n))$$

où

$$F_m(n) = a_1 \gcd(A_2 m, B_2) \gcd(A_3 m, B_3, C_3 m)(A_2'(m) + B_2' n)(A_3'(m) + B_3' n^2 + C_3'(m) n)$$

est un polynôme à coefficients entiers de degré 3. On pose

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

qui est de degré 3 et primitif. En effet, par définition, les deux polynômes dont G_m est le produit le sont et on sait que le contenu du produit de deux polynômes est le produit des contenus. De plus,

$$a_1 \gcd(A_2 m, B_2) \gcd(A_3 m, B_3, C_3 m) | h.$$

Montrons donc à présent que si k est un entier naturel et l est un autre entier naturel divisant h, alors

$$r_2(kl) \leqslant \tau(k)^2 r_2(l).$$

En effet, si $(k,l) = 1$, alors

$$r_2(kl) = r_2(k) r_2(l) = \tau(k)^2 r_2(l)$$

puisque dans ce cas $r_2(k) = \tau(k)^2$. Sinon, on peut écrire $l = l' l''$ avec $(l'', h) = 1$ et

$$r_2(kl) = r_2(kl') r_2(l'')$$

par multiplicativité. On a alors puisque $r_2(kl') = \tau(kl')^2$ et que $\tau(kl') \leqslant \tau(k)\tau(l')$ comme on le voit en écrivant la formule

$$\tau(l')\tau(k) = \prod_{p^\mu || l'} (\mu + 1) \prod_{p^\nu || k} (\nu + 1)$$

et

$$\tau(kl') = \prod_{p^{\mu+\nu} || kl'} (\mu + \nu + 1).$$

On a donc bien

$$r_2(kl) \leqslant \tau(k)^2 \tau(l')^2 r_2(l'')$$

où $\tau(l')^2 = r_2(l')$ et $(l', l'') = 1$ donc par multiplicativité

$$r_2(kl) \leqslant \tau(k)^2 r_2(l'l'') = \tau(k)^2 r_2(l).$$

On applique donc cela pour obtenir la suite d'inégalités

$$r\left(L_2(\mathbf{x})\right) r\left(Q(\mathbf{x})\right) \leqslant 16\tau(h)^2 r_2(G_m(n)) \ll L_\infty^\varepsilon r_2(G_m(n))$$

où on a encore utilisé le fait que $\tau(n) \ll n^\varepsilon$. On remarque enfin que $n \leqslant r_\infty X$ et donc

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

On veut alors appliquer le Théorème 5. On montre donc que G_m n'a pas de racine multiple. Tout d'abord, pour ce faire, on remarque que par définition, il suffit de le montrer pour

$$F_m(n) = (A_2 m^2 + B_2 n)(A_3 m^2 + B_3 n^2 + C_3 mn).$$

Mais on a $A_3 m^2 + B_3 n^2 + C_3 mn = a_1^2 Q\left(\frac{m - b_1 x_2}{a_1}, n\right)$ et donc si $A_3 m^2 + B_3 n^2 + C_3 mn$ était réductible, on aurait l'existence de deux polynômes P_m et R_m tels que

$$A_3 m^2 + B_3 n^2 + C_3 mn = P_m(n) R_m(n) = a_1^2 Q\left(\frac{m - b_1 x_2}{a_1}, n\right)$$

donc

$$a_1^2 Q(\mathbf{x}) = P_{L_1(\mathbf{x})}(x_2) R_{L_1(\mathbf{x})}(x_2)$$

et en particulier $Q(1, x)$ serit réductible ce qui est exclu. On en déduit donc que $A_3 m^2 + B_3 n^2 + C_3 mn$ est irréductible sur $\mathbb{Q}$ et donc puisqu'en caractristique nulle, tout polynôme irréductible est séparable, on en déduit que $A_3 m^2 + B_3 n^2 + C_3 mn$ n'a pas de racine multiple. Pour conclure, il faut voir que $A_3 m^2 + B_3 n^2 + C_3 mn$ et $A_2 m^2 + B_2 n$ n'ont pas de racines en commun. S'il en avait une (m_0, n_0), alors on aurait $\mathbf{x}_0 = \left(\frac{m_0 - b_1 n_0}{a_1}, n_0\right)$ tel que $L_2(\mathbf{x}_0) = Q(\mathbf{x}_0) = 0$ ce qui viendrait contredire le fait que $\mathrm{Res}(L_2, Q) \neq 0$. On a donc bien obtenu le résultat annoncé, à savoir que G_m n'a que des racines simples. D'après la section 1.4.1, le polynôme étant primitif de degré 3, seuls $p = 2$ et $p = 3$ peuvent être des premiers fixes. Si 3 est fixe par G_m, on est en mesure d'appliquer le Lemme 7 à G_m. Dans ce cas, puisque G_m est de degré 3, le degré de q dans (1.35) est nécessairement 0 donc $\delta = 0$, $\mu_0 = 1$ et

$$G_{m,1}(x) = \frac{G_m(3x + 1)}{3}$$

(on fixe les k_i tous égaux à 1) est à coefficient entier, est primitif et n'admet pas 3 comme premier fixe. La remarque page 8 de [24] permet de voir qu'un premier non fixé reste non fixé après une telle transformation comme on le démontre juste ci-dessous. Si maintenant $G_{m,1}$ admet 2 comme premier fixe, le degré de q est inférieur à 1 donc il existe $\delta' \in \{0,1\}$ et

$$\mu = \mu_0 + \mu_1 \leqslant 4$$

tels que

$$G_{m,2}(x) = \frac{G_{m,1}(2^{\delta'+1}x + 2^{\delta'} + 1)}{2^\mu} = \frac{G_m(3 \times 2^{\delta'+1}x + 3 \times 2^{\delta'} + 4)}{3 \times 2^\mu},$$

(où on n'a éventuellement pas de +1 si $\delta' = 0$) autrement dit

$$G_{m,2}(x) = \frac{G_m(3 \times 2^{\delta'+1}x + k)}{3 \times 2^\mu}$$

pour un certain entier $k \leqslant 3 \times 2 + 4 \leqslant 10$ est à coefficients entiers, primitif et n'admettant pas 2 comme premier fixe. Il faut alors pouvoir garantir que cette transformation conserve la propriété que 3 n'est pas un premier fixe. Or, lorsque x décrit toutes les classes modulo 3, on sait qu'il existe une valeur telle que $G_{m,1}(x)$ soit non nul et 3 étant inversible modulo 2, on en déduit que $x \mapsto 2^{\delta'+1}x + 2^{\delta'} + 1$ est une bijecton de $\mathbb{Z}/3\mathbb{Z}$ et donc on en déduit qu'il existe x tel que $G_{m,1}(2^{\delta'+1}x + 2^{\delta'} + 1) \not\equiv 0[3]$ et ainsi on a bien que 3 n'est pas fixe pour $G_{m,2}$.

Ainsi

$$r_2(G_m(n)) = r_2(3 \times 2^\mu G_{m,2}(3 \times 2^\mu n + k)) \leqslant \tau(3)^2 \tau(2^\mu)^2 r_2(G_{m,2}(3 \times 2^\mu n + k))$$

puisque 2 et 3 divisent h par le même raisonnement que ci-avant. On en déduit, avec la majoration de μ donnée précédemment, que

$$r_2(G_m(n)) \ll r_2(G_{m,2}(3 \times 2^\mu n + k)).$$

Enfin, on note que lorsque $n \leqslant r_\infty X$,

$$3 \times 2^\mu n + k \leqslant 3 \times 16 r_\infty X + 10 \ll r_\infty X$$

pour X assez grand. On en déduit finalement la majoration

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

où on est désormais en mesure d'appliquer le Théorème 5 puisqu'on n'a pas introduit de racines multiples en se ramenant à un polynôme sans premier fixe. On remarque que les coefficients de G_m (et donc ceux de $G_{m,2}$) vérifient

$$L_\infty(G_m) \ll (X')^3 L_\infty^3.$$

Si $r_\infty X \gg_\delta L_\infty^{3\delta} X^{3\delta}$ (puisqu'a fortiori on aura $r_\infty X \gg_\delta ||G_{m,2}||^\delta$), on peut donc appliquer le Théorème 5. On peut choisir $\delta = \frac{\varepsilon}{3}$ de sorte qu'on va appliquer le Théorème 5 pour $r_\infty X \gg L_\infty \varepsilon X^\varepsilon$. On en déduit donc dans ce cas la majoration

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

ce qui donne par multiplicativité

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

On majore alors

$$\sum_{\nu \geqslant 1} \frac{r_2(p^\nu)\rho_{G_{m,2}}(p^\nu)}{p^\nu} \leqslant \frac{2}{p} + \frac{9}{p} + \sum_{\nu \geqslant 3} \frac{(\nu+1)^2}{p^{\frac{\nu}{3}}}$$

en utilisant le Lemme 9. Or, on a pour tout $0 < x < 1$

$$\sum_{\nu \geqslant 3} (\nu+1)^2 x^\nu = \frac{x^3(9x^2 - 23x + 16)}{(1-x)^3}.$$

On en déduit

$$\sum_{\nu \geqslant 3} \frac{(\nu+1)^2}{p^{\frac{\nu}{3}}} = \frac{1}{p} \frac{((3/p)^2 - 23/p + 16)}{(1-1/p)^3}.$$

On peut, en étudiant la fonction $x \mapsto \frac{9x^2-23x+16}{(1-x)^3}$ montrer qu'elle est décroissante sur $\left[0, \frac{1}{2}\right]$ et qu'elle vaut 54 en $x = \frac{1}{2}$ donc

$$\sum_{\nu \geqslant 1} \frac{r_2(p^\nu)\rho_{G_{m,2}}(p^\nu)}{p^\nu} \leqslant \frac{2}{p} + \frac{9}{p} + \frac{54}{p} = \frac{c_0}{p}$$

où $c_0 = 65$. On déduit de tout cela, en considéant les nombres premiers p qui divisent le discriminant de $G_{m,2}$ ont une contribution à $S_{0,m}(X)$

$$\ll L_\infty^\varepsilon r_\infty X \prod_{p | \mathrm{disc}(G_{m,2})} \left(1 + \frac{c_0}{p}\right)$$

en majorant $1 - \frac{\rho_{G_{m,2}}(p)}{p}$ par 1. Or,

$$\prod_{p | \mathrm{disc}(G_{m,2})} \left(1 + \frac{c_0}{p}\right) \leqslant \prod_{p | \mathrm{disc}(G_{m,2})} \left(1 + \frac{1}{p}\right)^{c_0}.$$

On utilise ici le lemme suivant.

Lemme 16. *Soit* $\mathbf{M} \in \mathcal{M}_2(\mathbb{Z}) \cap GL_2(\mathbb{R})$, *alors*

$$disc(\mathbf{x} \mapsto F(\mathbf{M}\mathbf{x})) = \det(\mathbf{M})^{d(d-1)} disc(F)$$

où d est le degré de F.

Démonstration.– La preuve figure dans [24]. □

Dans notre cas, on passe de F_m à $G_{m,2}$ en utilisant des transformations linéaires qui font apparaître un m et les coefficients des formes initiales. On a donc d'après le Lemme

16 que $\mathrm{disc}(G_{m,2}) \leqslant L_\infty^{12} m^{24}$. On remarque alors que la quantité $1+\frac{1}{p}$ est décroissante en p et donc

$$\prod_{p|\mathrm{disc}(G_{m,2})} \left(1+\frac{1}{p}\right) \leqslant \prod_{i\leqslant \omega(L_\infty^{12} m^{24})} \left(1+\frac{1}{p_i}\right)$$

où p_i désigne le i-ème nombre premier. Par la formule de Mertens, on obtient

$$\prod_{p|\mathrm{disc}(G_{m,2})} \left(1+\frac{1}{p}\right) \ll \log(\omega(L_\infty^{12} m^{24})).$$

Puis, on sait que si $n = p_1^{\alpha_1}...p_r^{\alpha_r}$, alors $2^r \leqslant n$ et donc $\omega(n) \ll \log(n)$. On en déduit donc

$$\prod_{p|\mathrm{disc}(G_{m,2})} \left(1+\frac{1}{p}\right) \ll \log\log(L_\infty^{12} m^{24}) \ll L_\infty^{\varepsilon} \log\log(m)$$

et donc

$$L_\infty^{\varepsilon} r_\infty X \prod_{p|\mathrm{disc}(G_{m,2})} \left(1+\frac{c_0}{p}\right) \ll L_\infty^{\varepsilon} r_\infty X (\log\log(m))^{c_0}.$$

Or, on a vu que pour que $S_{0,m}(X)$ soit non nulle, il est nécessaire que $m \leqslant X'$ donc

$$L_\infty^{\varepsilon} r_\infty X \prod_{p|\mathrm{disc}(G_{m,2})} \left(1+\frac{c_0}{p}\right) \ll L_\infty^{\varepsilon} r_\infty X (\log\log(X'))^{c_0}.$$

On traite maintenant la contribution des p qui ne divisent pas le discriminant. Pour ces premiers, on a une meilleure majoration de $\rho_{G_{m,2}}(p^\nu) \ll 1$ puisque $\mu = 0$. On en déduit de la même façon que ci-dessus les majorations

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

ce qui permet de négliger tous les exposants $\nu \leqslant 2$ qui donnent des termes convergents. Le raisonnement effectué dans la preuve du Lemme 13 donne que si $p \geqslant 5$, puisqu'alors $\rho_{G_{m,2}}(p) = \rho_{G_m}(p)$ et que G_m est le produit d'une forme linéaire et d'une forme quadratique irréductible sur $\mathbb{Q}[i]$, on a

$$\prod_{p\leqslant r_\infty X} \left(1+\frac{\chi(p)\rho_{G_m}(p)}{p}\right) \ll 1.$$

On en déduit donc finalement

$$S_{0,m}(X) \ll L_\infty^{\varepsilon} r_\infty X (\log\log(X'))^{c_0} \prod_{\substack{p\leqslant r_\infty X \\ p\nmid \mathrm{disc}(G_{m,2})}} \left(1-\frac{\rho_{G_{m,2}}(p)}{p}\right)\left(1+\frac{r_2(p)\rho_{G_{m,2}}(p)}{p}\right)$$

où les deux termes qui apparaissent sont ceux pour $\nu = 0$ et $\nu = 1$. On obtient donc

$$\begin{aligned} S_{0,m}(X) &\ll L_\infty^{\varepsilon} r_\infty X (\log\log(X'))^{c_0} \prod_{\substack{p\leqslant r_\infty X \\ p\nmid \mathrm{disc}(G_{m,2})}} \left(1+\frac{(r_2(p)-1)\rho_{G_{m,2}}(p)}{p}\right) \\ &\ll L_\infty^{\varepsilon} r_\infty X (\log\log(X'))^{c_0} \prod_{p\leqslant r_\infty X} \left(1+\frac{\chi(p)\rho_{G_{m,2}}(p)}{p}\right) \ll L_\infty^{\varepsilon} r_\infty X (\log\log(X'))^{c_0} \end{aligned}$$

par définition de r_2, ce qui prouve le lemme dans le cas où $r_\infty X \gg L_\infty^\varepsilon X^\varepsilon$. Dans le cas contraire, où on a $n \leqslant L_\infty^\varepsilon X^\varepsilon$, on ne peut plus appliquer le Théorème 5 mais on a

$$r_2(n) \ll n^\varepsilon$$

pour tout $\varepsilon > 0$. D'où,

$$r_2(G_{m,2}(n)) \ll G_{m,2}(n)^\varepsilon \ll L_\infty^{3\varepsilon}(X')^{3\varepsilon} L_\infty^\varepsilon X^\varepsilon \ll L_\infty^\varepsilon X^\varepsilon$$

puisque les coefficients de $G_{m,2}$ sont en $O\left((X')^3 L_\infty^3\right)$. D'où,

$$S_{0,m}(X) \ll L_\infty^\varepsilon X^\varepsilon \ll L_\infty^\varepsilon X (\log\log(X'))^{c_0}$$

pour ε assez petit. Dans tous les cas, on en déduit bien le résultat. On a donc pour conclure (où on peut toujours se restreindre aux indices tels que $2^{k_0} \leq \sqrt{X}$ comme dans le Lemme 14)

$$S_0(X) \ll \frac{L_\infty^\varepsilon r_\infty r' X^2 \log\log(X')^{21/4+c_0}}{(\log(X'))^\eta} \sum_{k_0 \geqslant 0} 2^{-2k_0} \ll \frac{L_\infty^\varepsilon r_\infty r' X^2 \log\log(X')^{21/4+c_0}}{(\log(X'))^\eta}.$$

On utilise alors que

$$\log\log(X')^{21/4+c_0} \ll \log(X')^\varepsilon$$

et donc

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

ce qui est convenable puisque l'hypothèse $r' X^{1-\varepsilon} \geqslant 1$ garantit que

$$\log(X') \ll \log(X).$$

Ceci achève le traitement de S_0.

1.4.5 Traitement des $S_{\pm,\pm\pm}$ et fin de la preuve

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 toujours $V_1 = Y$, $V_2 = \sqrt{X'}$, $V_3 = X'$ et

$$\mathcal{R}_{\mathbf{M},4,\mathbf{d}}^{-,-,-,} = \left\{ \mathbf{x}' \in \mathcal{R}_{\mathbf{M}} \;\middle|\; \begin{array}{l} Q(\mathbf{M}\mathbf{x}') > \frac{r' d_3}{X}, \\ L_1(\mathbf{M}\mathbf{x}') > r' d_1 Y^{-1}, \\ L_2(\mathbf{M}\mathbf{x}') > (r')^{1/2} d_2 X^{-1/2}, \\ x_1' \equiv 1[4] \end{array} \right\}. \tag{1.60}$$

On a

$$S_{-,-,-}(X; \mathbf{k}, \alpha) = \sum_{\substack{\mathbf{d} \in \mathbb{N}^3 \\ d_i \leqslant V_i}} \chi(d_1 d_2 d_3) \#\left(\Lambda_{\mathbf{M}}(\mathbf{d}) \cap X \mathcal{R}_{\mathbf{M},4,\mathbf{d}}^{-,-,-,}\right) \tag{1.61}$$

où $\Lambda_{\mathbf{M}}(\mathbf{d}) = \Lambda(\mathbf{d}, L_{1,\mathbf{M}}, L_{2,\mathbf{M}}, Q_{\mathbf{M}})$. En appliquant le Lemme 8 de géométrie des nombres, on obtient l'égalité

$$S_{-,-,-}(X; \mathbf{k}, \alpha) = \sum_{\substack{\mathbf{d} \in \mathbb{N}^3 \\ d_i \leqslant V_i}} \chi(d_1 d_2 d_3) \frac{X^2}{2^{k_1 + \max(k_2', k_3') + 2}} \frac{\mathrm{vol}(\mathcal{R}_{\mathbf{d}}^{-,-,-})}{4} \frac{\rho(\mathbf{d})}{(d_1 d_2 d_3)^2}$$

$$+O\left(2^{\varepsilon(k_1+k_2+k_3)}L_\infty^\varepsilon(r_\infty X\sqrt{V}+V)\log(V)^A\right)$$

où

$$\mathcal{R}_{\mathbf{d}}^{-,-,-}=\left\{\mathbf{x}\in\mathcal{R}\quad\middle|\quad Q(\mathbf{x})>\frac{r'd_3}{X},\quad L_1(\mathbf{x})>r'd_1Y^{-1},\quad L_2(\mathbf{x})>(r')^{1/2}d_2X^{-1/2}\right\}.$$

On commence par montrer que le terme d'erreur est convenable. En remplaçant V par son expression, on obtient qu'il vaut

$$T:=2^{\varepsilon(k_1+k_2+k_3)}L_\infty^\varepsilon(r_\infty X(X'^2Y)^{1/2}+X'Y)\log(X'Y)^A.$$

Or, on a que

$$X(X'^2Y)^{1/2}=r'\frac{X^2}{(\log(X))^{C/2}}$$

et

$$X'^2Y=(r')^2\frac{X^2}{(\log(X'))^C}.$$

D'où on tire

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

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

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

On remarque alors en utilisant le Théorème 4 que

$$\begin{aligned}T&\ll S_{+,-,+}(X;\mathbf{k},\alpha)\ll\textstyle\sum_{\mathbf{x}\leqslant r_\infty X}\tau(L_1(\mathbf{x}))\tau(L_2(\mathbf{x}))\tau(Q(\mathbf{x}))\\&\ll 2^{\varepsilon(k_1+k_2+k_3)}L_\infty^\varepsilon r_\infty^2X^2(\log(X))^3.\end{aligned}$$

Pour ce faire, on introduit la fonction multiplicative

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

On sait qu'alors

$$S_{+,-,+}(X;\mathbf{k},\alpha)\ll\sum_{\mathbf{x}\leqslant r_\infty X}\tau_0(L_1(\mathbf{x})L_2(\mathbf{x})Q(\mathbf{x}))$$

et le résultat provient simplement du Théorème 4 où on a utilisé ici la majoration triviale de E par $(\log(X))^3$ puisque

$$\prod_p\left(1+\frac{\rho_G^*(p)(\tau_0(p)-1)}{p}\right)\leqslant\prod_p\left(1+\frac{1}{p}\right)\ll\log(X)$$

et

$$\prod_{p\leqslant X}\left(1+\frac{d_i(\tau_0(p)-1)}{p}\right)\ll\log(X).$$

On en déduit donc que si $r' \geqslant r_\infty(\log(X))^{A+1}$, alors

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

Or, on peut toujours augmenter le A dans le résultat du Lemme 8 et supposer que $A \geqslant 5$, 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

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

En utilisant $n(k_1,k_2,k_3) \ll 1$, 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 $\varepsilon \leqslant 1/\log(2)$. Ceci est satisfaisant dans l'optique du Théorème 1. On peut noter qu'il s'est avéré crucial d'avoir restreint les intervalles de sommation des k_i pour ici obtenir une puissance de log et non une puissance de X.

On passe maintenant à l'étude du terme principal. On pourrait raisonner comme dans [23] mais dans notre cas il y a bon nombre de complications techniques et l'expression de $\rho(1,1,h)$ empêche la méthode d'aboutir. On exploite donc plutôt les deux lemmes élémentaires suivants sur les séries de Dirichlet associées à des convolutions pour étudier

$$\sum_{d_i \leqslant V_i} \chi(d_1d_2d_3) \frac{\rho(d_1,d_2,d_3)}{(d_1d_2d_3)^2}. \tag{1.62}$$

Lemme 17. *Soient $A > 0$, g, h deux fonctions arithmétiques et C, C', C'' trois constantes telles que*

$$\sum_{d=1}^{+\infty} \frac{|h(d)|\log(2d)^A}{d} \leqslant C'' \quad \text{et} \quad \sum_{d \leqslant x} \frac{g(d)}{d} = C + O\left(\frac{C'}{(\log(2x))^A}\right).$$

On a alors que

$$\sum_{n \leqslant x} \frac{(g*h)(n)}{n} = C \sum_{d=1}^{+\infty} \frac{h(d)}{d} + O\left(\frac{C''(C+C')}{(\log(2x))^A}\right).$$

Démonstration– On écrit

$$\sum_{n \leqslant x} \frac{(g*h)(n)}{n} = \sum_{d \leqslant x} \frac{h(d)}{d} \sum_{m \leqslant \frac{x}{d}} \frac{g(m)}{m}$$

et donc

$$\sum_{n \leqslant x} \frac{(g*h)(n)}{n} = \sum_{d \leqslant \sqrt{x}} \frac{h(d)}{d} \sum_{m \leqslant \frac{x}{d}} \frac{g(m)}{m} + \sum_{\sqrt{x} < d \leqslant x} \frac{h(d)}{d} \sum_{m \leqslant \frac{x}{d}} \frac{g(m)}{m}.$$

On approche alors

$$\sum_{m\leqslant \frac{x}{d}} \frac{g(m)}{m} = C + O\left(\frac{C'}{(\log(2\sqrt{x}))^A}\right)$$

car $\sqrt{x} \leqslant \frac{x}{d}$. On a donc un terme

$$C\sum_{d\leqslant\sqrt{x}} \frac{h(d)}{d} + O\left(\frac{C'}{(\log(2\sqrt{x}))^A}\sum_{d\leqslant\sqrt{x}} \frac{|h(d)|}{d}\right)$$

où

$$O\left(\frac{C'}{(\log(2\sqrt{x}))^A}\sum_{d\leqslant\sqrt{x}} \frac{|h(d)|}{d}\right) = O\left(\frac{C'C''}{(\log(2\sqrt{x}))^A}\right).$$

Maintenant,

$$C\sum_{d\leqslant\sqrt{x}} \frac{h(d)}{d} = C\sum_{d=1}^{+\infty} \frac{h(d)}{d} - C\sum_{d>\sqrt{x}}^{+\infty} \frac{h(d)}{d}.$$

Or,

$$\sum_{d>\sqrt{x}}^{+\infty} \frac{h(d)}{d} \leqslant \sum_{d>\sqrt{x}}^{+\infty} \frac{h(d)}{d}\frac{(\log(2d))^A}{(\log(2\sqrt{x}))^A} \ll \frac{C''}{(\log(2\sqrt{x}))^A}$$

ce qui permet aisément de conclure la preuve du lemme. □

Lemme 18. *Soient g, h deux fonctions arithmétiques et C, C', C'' trois constantes telles que*

$$\sum_{d=1}^{+\infty} \frac{|h(d)|\log(2d)}{d} \leqslant C'' \quad et \quad \sum_{d\leqslant x} \frac{g(d)}{d} = C\log(x) + O\left(C'\right).$$

On a alors que

$$\sum_{n\leqslant x} \frac{(g*h)(n)}{n} = C\log(x)\sum_{d=1}^{+\infty} \frac{h(d)}{d} + O\left(C''(C+C')\right).$$

Démonstration– La preuve est très similaire à celle du Lemme précédent et nous ne la rédigeons pas ici. □

On a maintenant tous les outils pour pouvoir estimer la somme (1.62). On établit alors le lemme suivant.

Lemme 19. *Si on note $V_M = \max(V_i)$, $V_m = \min(V_i)$ et $V_r = \{V_1, V_2, V_3\} \setminus \{V_M, V_m\}$, on a*

$$\sum_{d_i\leqslant V_i} \chi(d_1d_2d_3)\frac{\rho(d_1,d_2,d_3)}{(d_1d_2d_3)^2} = \left(\frac{\pi}{4}\right)^3 \prod_{p>2}\sigma_p + O\left(L_\infty^\varepsilon\left(\frac{\log(V_m)\log(V_r)}{\log(V_M)^A} + \frac{\log(V_m)}{\log(V_r)^A} + \frac{1}{\log(V_m)^A}\right)\right),$$

pour tout $A > 0$.

Démonstration– On utilise les notations du Lemme 4 pour écrire

$$\sum_{d_i \leqslant V_i} \chi(d_1d_2d_3)\frac{\rho(d_1,d_2,d_3)}{(d_1d_2d_3)^2} = \sum_{d_i \leqslant V_i} \chi(d_1d_2d_3)\frac{(h*R)(d_1,d_2,d_3)}{d_1d_2d_3}$$

où

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

Supposons que V_3 soit le maximum des V_i. On commence alors par sommer sur d_3 et e_3 si bien qu'on doit estimer la somme suivante

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

Le Lemme 17, avec $g = \chi r_\Delta$ et $h = \chi h$ où h est vue simplement comme fonction de sa troisième variable ici, et certains arguments de la preuve du Lemme 4 fournissent alors que cette somme est

$$L(1,\chi)L(1,\chi\chi_\Delta)\sum_{k_3}\frac{\chi(k_3)h\left(\frac{d_1}{e_1},\frac{d_2}{e_2},k_3\right)}{k_3} + O\left(\frac{1}{\log(V_3)^A}\sum_{k_3}\frac{\left|h\left(\frac{d_1}{e_1},\frac{d_2}{e_2},k_3\right)\right|\log(2k_3)^A}{k_3}\right).$$

Or, on a

$$\chi(2n) = 0 \quad \text{et} \quad \chi(2n+1) = (-1)^n$$

et par conséquent

$$L(1,\chi) = \sum_n \frac{\chi(n)}{n} = \sum_n \frac{(-1)^n}{2n+1} = \arctan(1) = \frac{\pi}{4}.$$

On obtient donc

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

Supposons alors que $V_r = V_2$. On va alors maintenant sommer sur d_2 et e_2. Le terme principal ci-dessus, devient par une nouvelle application du Lemme 17 avec le même h vue comme fonction de la deuxième variable uniquement mais avec $g = \chi$ cette fois

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

Pour traiter le terme d'erreur de la sommation sur d_3 et e_3, on va utiliser le Lemme 18 avec $g = 1$ et $h = |h|$ vue comme fonction de sa deuxième variable pour obtenir

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

On effectue alors la même manipulation sur la somme sur d_1 et e_1 et on remarque qu'une modification mineure de la preuve du Lemme 4 qui est d'ailleurs effectuée dans [27] dans le cas $3A = 1$ permet d'obtenir que les quantités de la forme

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

ont une contribution

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

ce qui permet de conclure la preuve du Lemme en utilisant l'expression obtenue dans le Lemme 4

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

L'argument clé pour effectuer cette modification est de majorer

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

par $P'/(\log(2))^A$ où

$$P' = P'(L_1,L_2,Q) = \prod_p \left(1 + \sum_{\boldsymbol{\nu}\in\mathbb{Z}^3_{\geqslant 0}} \frac{|h(p^{\nu_1},p^{\nu_2},p^{\nu_3})| \log(p^{\nu_1+\nu_2+\nu_3})^A}{p^{\nu_1+\nu_2+\nu_3}}\right)$$

qui provient de l'inégalité (où on utilise le fait que pour $p > 2$, $\log(p) > 1$)

$$\log(d) \leq \frac{\prod_{p^\nu \| d} \log(p^\nu)}{\log(2)}.$$

Le reste des arguments n'étant presque pas modifiés. Pour conclure, il suffit maintenant de voir que les autres cas se traitent de manière parfaitement analogue. □

Il ne reste donc plus qu'à introduire le terme $\mathrm{vol}(\mathcal{R}_{\mathbf{d}}^{-,-,-})$. Pour ce faire, on écrit

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

En réinjectant et en intervertissant les sommations, on aboutit à

$$\int\int_{\mathbf{x}\in\mathcal{R}} \sum_{\substack{d_1\leqslant \min(Y,L_1(\mathbf{x})r'^{-1}Y),d_2\leqslant\min(r'\sqrt{X},L_2(\mathbf{x})r'^{-1}\sqrt{X}) \\ d_3\leqslant\min(r'X',Q(\mathbf{x})r'^{-2}X)}} \frac{\chi(d_1d_2d_2)\rho(\mathbf{d})}{(d_1d_2d_3)^2}\mathrm{d}\mathbf{x}.$$

Or, on a que

$$L_i(\mathbf{x})r'^{-1} \leqslant 1, \quad \text{et} \quad Q(\mathbf{x})r'^{-2} \leqslant 1$$

donc on obtient en choisissant $A = 3$ dans le Lemme 19,

$$\sum_{d_i \leqslant V_i} \frac{\chi(d_1 d_2 d_2)\rho(\mathbf{d})\mathrm{vol}(\mathcal{R}_{\mathbf{d}}^{-,-,-})}{(d_1 d_2 d_3)^2} = \left(\frac{\pi}{4}\right)^3 \mathrm{vol}(\mathcal{R}) \prod_{\mathrm{p}>2} \sigma_{\mathrm{p}} +$$

$$O\left(L_\infty^\varepsilon \int\int_{\mathbf{x}\in\mathcal{R}} \frac{1}{\log(\max(L_1(\mathbf{x})r'^{-1}Y, L_2(\mathbf{x})r'^{-1/2}\sqrt{X}, Q(\mathbf{x})r'^{-1}X))} \mathrm{d}\mathbf{x}\right).$$

On a donc

$$O\left(L_\infty^\varepsilon \int\int_{\mathbf{x}\in\mathcal{R}} \frac{1}{\log(Q(\mathbf{x})r'^{-1}X)} \mathrm{d}\mathbf{x}\right) = O\left(\frac{L_\infty^\varepsilon r_\infty^2}{(\log(X))^\eta}\right).$$

En effet, effectuant un changement de variables $\mathbf{x} = r_\infty \mathbf{z}$, on obtient que

$$\int\int_{\mathbf{x}\in\mathcal{R}} \frac{1}{\log(Q(\mathbf{x})r'^{-1}X)} \mathrm{d}\mathbf{x} \leqslant r_\infty^2 \int\int_{||\mathbf{x}||1} \frac{1}{\log(Q(\mathbf{x})r_\infty^2 r'^{-1}X + 2)} \mathrm{d}\mathbf{x}.$$

On peut alors constater qu'un changement de variables $\mathbf{z} = E\mathbf{x}$ fait sortir l'inverse de $\det(E)$ que l'on peut majorer par 1. Ainsi, on peut intégrer plutôt sur la forme J définie par $J(\mathbf{x}) = Q(E\mathbf{x})$ et obtenir grâce à l'inégalité (lorsque $a + b > 0$)

$$\frac{1}{a+b} \leqslant \frac{1}{\sqrt{|ab|}},$$

la majoration

$$\int\int_{\mathbf{x}\in\mathcal{R}} \frac{1}{\log(Q(\mathbf{x})r'^{-1}X)} \mathrm{d}\mathbf{x} \leqslant \frac{r_\infty^2}{\sqrt{\log(r_\infty^2 r'^{-2}X)}} \int\int_{||\mathbf{x}||1} \frac{1}{\sqrt{|\log(J(\mathbf{x})+2)|}} \mathrm{d}\mathbf{x} \ll \frac{r_\infty^2}{\sqrt{\log(r_\infty^2 r'^{-2}X)}},$$

puisqu'on a vu qu'on autorisait la constante à dépendre de la classe d'équivalence des formes sous certaines transformations linéaires E. Le même raisonnement que ci-dessus permet d'obtenir

$$\frac{r_\infty^2}{\sqrt{\log(r_\infty^2 r'^{-2}X)}} \ll \frac{r_\infty^2}{(\log(X))^{\frac{1}{4}}} \frac{1}{|\log(r_\infty^2 r'^{-2})|^{\frac{1}{4}}}.$$

Mais les inégalités $r'/(2L_\infty) \leqslant r_\infty \leqslant 2L_\infty r'$ où la première majoration est évidente et la seconde provient des relations

$$x_1 = \frac{b_2 L_1(\mathbf{x}) - b_1 L_2(\mathbf{x})}{b_2 a_1 - b_1 a_2} \quad \text{et} \quad x_2 = \frac{a_2 L_1(\mathbf{x}) - a_1 L_2(\mathbf{x})}{b_1 a_2 - b_2 a_1},$$

permettent de montrer la majoration

$$\frac{1}{|\log(r_\infty^2 r'^{-2})|^{\frac{1}{4}}} \ll L_\infty^\varepsilon$$

qui permet de conclure. Pour traiter les autres cas, on obtient de la même façon

$$O\left(L_\infty^\varepsilon \int\int_{\mathbf{x}\in\mathcal{R}} \frac{1}{\log(L_2(\mathbf{x})r'^{-1/2}X)} \mathrm{d}\mathbf{x}\right) \ll \frac{L_\infty^\varepsilon r_\infty^2}{\sqrt{\log(r_\infty r'^{-1}\sqrt{X})}}$$

qui se traite comme ci-dessus ou du type

$$O\left(L_\infty^\varepsilon \int\int_{\mathbf{x}\in\mathcal{R}} \frac{1}{\log(L_1(\mathbf{x})r'^{-1}Y)}\mathrm{d}\mathbf{x}\right) \ll \frac{L_\infty^\varepsilon r_\infty^2}{\sqrt{\log(r_\infty r'^{-1}Y)}}$$

et pour conclure, il reste à remarquer que le terme

$$\frac{1}{(\log(Y))^{\frac{1}{4}}}$$

qu'on obtient est convenable grâce à la définition de Y. On en déduit que

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

En combinant tous les résultats obtenus, on conclut à l'égalité

$$S(X) = \sum_{k_0\geqslant 0}\sum_{k_1,k_2,k_3\geqslant 0} 8\times 4^3\left(\frac{2^{-2k_0}X^2 n(k_1,k_2,k_3)}{2^{k_1+\max(k_2',k_3')+2}}\left(\frac{\pi}{4}\right)^3\frac{\mathrm{vol}(\mathcal{R})}{4}\prod_{p>2}\sigma_p + O_\varepsilon\left(L_\infty^\varepsilon(r_\infty r' + r_\infty^2)\frac{2^{-2k_0}X^2}{\log(X)^{\eta-\varepsilon}}\right)\right)$$

D'après le Lemme 11, on aboutit au bon terme principal

$$2\pi^3\mathrm{vol}(\mathcal{R})\mathrm{X}^2\sigma_2\prod_{\mathrm{p}>2}\sigma_{\mathrm{p}}$$

tandis que pour le terme d'erreur, les indices pour lesquels on a un $k_i > \log\log(X)$ donnent le bon terme d'erreur comme on l'a vu plus haut et les indices $k_i \leqslant \log\log(X)$ font apparaître un terme

$$L_\infty^\varepsilon(r_\infty r' + r_\infty^2)\frac{X^2\log\log(X)^3}{\log(X)^{\eta-\varepsilon}}$$

qui en utilisant l'inégalité $\log\log(X) \ll \log(X)^\varepsilon$ est convenable. Ceci achève la preuve du Théorème 1.

1.5 Démonstration du Théorème 2

1.5.1 Changement de variables

L'idée principale est bien sûr de se ramener au Théorème 1. On va commencer par se ramener au cas où $(D_i,\ell_i) = (D_3,q) = 1$ et relier les ensembles $\Lambda(\mathbf{D})$ à des réseaux en s'inspirant du travail de Daniel dans [22] et de La Bretèche et Browning dans [27]. Avec les notations de la première section, on a clairement

$$\Lambda(\mathbf{D};L_1,L_2,Q) = \Lambda(\mathbf{D}';L_1^*,L_2^*,Q^*).$$

On a également, en posant

$$\Lambda^*(\mathbf{D}') = \left\{\mathbf{x}\in\Lambda(\mathbf{D};' L_1^*,L_2^*,Q^*) \quad | \quad (x_1,x_2,D_1'D_2'D_3') = 1\right\},$$

que

$$\Lambda(\mathbf{D}') = \bigsqcup_{b|\psi(\mathbf{D}')} b\Lambda^*(\mathbf{D}''; L_1', L_2', Q')$$

où

$$\psi(\mathbf{D}') = \prod_{p|D_1'D_2'D_3'} p^{\max(\nu_p(D_1'),\nu_p(D_2'),\lceil \nu_p(D_3')/2\rceil)}$$

et

$$\mathbf{D}'' = \left(\frac{D_1'}{(D_1', b)}, \frac{D_2'}{(D_2', b)}, \frac{D_3'}{(D_3', b^2)}\right)$$

et enfin

$$L_i' = \frac{bL_i}{(D_i', b)} \quad \text{et} \quad Q' = \frac{b^2 Q}{(D_3', b^2)}.$$

En effet, on a

$$\Lambda(\mathbf{D}') = \left\{\mathbf{x} \in \mathbb{Z}^2 \quad | \quad D_i'|L_i^*(\mathbf{x}), \quad D_3'|Q^*(\mathbf{x})\right\}$$

et on partitionne cet ensemble suivant les valeurs de $\gcd(\psi(\mathbf{D}'), x_1, x_2)$ qui parcourt tous les diviseurs de $\psi(\mathbf{D}')$ lorsque $\mathbf{x}$ décrit $\mathbb{Z}^2$. On a donc

$$\Lambda(\mathbf{D}') = \bigsqcup_{b|\psi(\mathbf{D}')} \left\{\mathbf{x} \in \mathbb{Z}^2 \quad | \quad \gcd(\psi(\mathbf{D}'), x_1, x_2) = b, \quad D_i'|L_i^*(\mathbf{x}), \quad D_3'|Q^*(\mathbf{x})\right\}.$$

En écrivant que $x_i = bx_i'$, $D_i' = (b, D_i')D_i''$ et $D_3' = (b^2, D_3')D_3''$, on obtient que les conditions deviennent

$$\Lambda(\mathbf{D}') = \bigsqcup_{b|\psi(\mathbf{D}')} b\left\{\mathbf{x}' \in \mathbb{Z}^2 \quad | \quad D_i''|\frac{bL_i(\mathbf{x}')}{(b, D_i')}, \quad D_3''|\frac{b^2Q(\mathbf{x}')}{(b^2, D_3')} \quad (D_1''D_2''D_3'', x_1', x_2') = 1\right\}$$

car on remarque que $b^{-1}\psi(\mathbf{D}') = \psi(\mathbf{D}'')$ et que $(\psi(\mathbf{D}''), x_1, x_2) = 1$ si, et seulement si, $(D_1''D_2''D_3'', x_1, x_2) = 1$. On a donc bien

$$\Lambda(\mathbf{D}') = \bigsqcup_{b|\psi(\mathbf{D}')} b\Lambda^*(\mathbf{D}''; L_1', L_2', Q').$$

On rappelle que la somme que l'on veut estimer est

$$S(X, \mathbf{d}, \mathbf{D}) = \sum_{\mathbf{x}\in\Lambda(\mathbf{D})\cap X\mathcal{R}} r\left(\frac{L_1(\mathbf{x})}{d_1}\right) r\left(\frac{L_2(\mathbf{x})}{d_2}\right) r\left(\frac{Q(\mathbf{x})}{d_3}\right)$$

donc on peut la réécrire en utilisant ce qui précède

$$S(X, \mathbf{d}, \mathbf{D}) = \sum_{b|\psi(\mathbf{D}')} \sum_{\mathbf{x}\in\Lambda^*(\mathbf{D}'')\cap(X/b)\mathcal{R}} r\left(\frac{L_1(b\mathbf{x})}{d_1}\right) r\left(\frac{L_2(b\mathbf{x})}{d_2}\right) r\left(\frac{Q(b\mathbf{x})}{d_3}\right)$$

donc

$$S(X, \mathbf{d}, \mathbf{D}) = \sum_{b|\psi(\mathbf{D}')} \sum_{\mathbf{x}\in\Lambda^*(\mathbf{D}'')\cap(X/b)\mathcal{R}} r\left(\frac{bL_1(\mathbf{x})}{d_1}\right) r\left(\frac{bL_2(\mathbf{x})}{d_2}\right) r\left(\frac{b^2Q(\mathbf{x})}{d_3}\right)$$

et finalement

$$S(X,\mathbf{d},\mathbf{D}) = \sum_{b|\psi(\mathbf{D}')} \sum_{\mathbf{x}\in\Lambda^*(\mathbf{D}'')\cap(X/b)\mathcal{R}} r\left(l'_1\frac{L'_1(\mathbf{x})}{d'_1}\right) r\left(l'_2\frac{L'_2(\mathbf{x})}{d'_2}\right) r\left(q'\frac{Q'(\mathbf{x})}{d'_3}\right)$$

où

$$\mathbf{d}' = \left(\frac{d_1}{(d_1,\ell_1,b)}, \frac{d_2}{(d_2,\ell_2,b)}, \frac{d_3}{(d_3,q,b^2)}\right)$$

et où

$$l'_i = \frac{(b,D'_i)}{(b,d_i,\ell_i)} = \frac{(b,D_i,\ell_i)}{(b,d_i,\ell_i)} \quad \text{et} \quad q' = \frac{(b^2,D'_3)}{(b^2,d_3,q)} = \frac{(b^2,D_3,q)}{(b^2,d_3,q)}$$

qui sont bien des entiers puisque $d_i|D_i$. On pose alors $D' = D'_1D'_2D'_3$ et $D'' = D''_1D''_2D''_3$ et on définit la relation d'équivalence suivante sur $\mathbf{x}\in\mathbb{Z}^2$ tel que $(x_1,x_2,D'')=1$ par

$$\mathbf{x}\sim\mathbf{y} \quad \Longleftrightarrow \quad \exists\lambda\in\mathbb{Z} \quad \text{tel que} \quad \mathbf{x}\equiv\lambda\mathbf{y}[D''].$$

On vérifie aisément qu'il s'agit d'une relation d'équivalence, la symétrie provenant du fait que le λ vérifie nécessairement $(\lambda,D'')=1$ car si p divise D'' et λ, alors ce p divise x_1 et x_2 ce qui est absurde. On note $\mathcal{U}(D'')$ l'ensemble des classes d'équivalence et pour $\mathbf{y}\in\mathcal{A}$, avec$\mathcal{A}\in\mathcal{U}(D'')$, on a

$$\mathcal{A} = \{\mathbf{x}\in\mathbb{Z}^2 \quad | \quad \mathbf{x}\equiv a\mathbf{y}[D''] \quad \text{avec} \quad a\in\mathbb{Z} \quad \text{et} \quad (a,D'')=1\}.$$

On peut constater que soit $\mathcal{A}\subset\Lambda^*(\mathbf{D}'')$ soit $\mathcal{A}\cap\Lambda^*(\mathbf{D}'')=\varnothing$ puisque par exemple

$$L_i(a\mathbf{y}) = aL_i(\mathbf{y}) \equiv 0[D''_i]$$

si

$$L_i(\mathbf{y}) \equiv 0[D''_i].$$

On peut donc poser

$$\mathcal{V}(\mathbf{D}'') = \{\mathcal{A}\in\mathcal{U}(D'') \quad | \quad \mathcal{A}\subset\Lambda^*(\mathbf{D}'')\},$$

et définir pour $\mathcal{A}\in\mathcal{V}(\mathbf{D}'')$ et $\mathbf{y}_0\in\mathcal{A}$,

$$G(\mathcal{A}) = \{\mathbf{x}\in\mathbb{Z}^2 \quad | \quad \exists a\in\mathbb{Z} \quad \text{tel que} \quad \mathbf{x}\equiv a\mathbf{y}_0[D'']\}.$$

L'interêt de l'ensemble $G(\mathcal{A})$ est qu'il s'agit d'un réseau de déterminant D'' et

$$\mathcal{A} = \{\mathbf{x}\in G(\mathcal{A}) \quad | \quad (x_1,x_2,D'')=1)\}.$$

Il s'agit clairement d'un sous-$\mathbb{Z}$-module de $\mathbb{Z}^2$ non réduit à zéro. On a

$$G(\mathcal{A}) = \{(ay_{0,1}+kD'', ay_{0,2}+lD'') \quad | \quad (a,k,l)\in\mathbb{Z}^3\}$$

mais où en fait a est défini modulo D'' seulement. On montre plus bas dans la preuve du Lemme 21 que l'application

$$f : \left\{ \begin{array}{lll} \mathbb{Z}/D''\mathbb{Z} & \to & (\mathbb{Z}/D''\mathbb{Z})^2 \\ \overline{a} & \mapsto & (ay_{0,1}, ay_{0,2}) \end{array} \right.$$

est injective (c'est là que l'hypothèse de coprimalité intervient). On en déduit que

$$\mathbb{Z}/D''\mathbb{Z} \cong \mathrm{Im}(f).$$

Or, clairement $\mathrm{Im}(f)$ est l'image de $G(\mathcal{A})$ par la projection

$$\pi : \mathbb{Z}^2 \to \left(\mathbb{Z}/D''\mathbb{Z}\right)^2$$

et donc ($D''\mathbb{Z} \times D''\mathbb{Z}$ est bien un sous-module de $G(\mathcal{A})$)

$$G(\mathcal{A})/(D''\mathbb{Z} \times D''\mathbb{Z}) \cong \mathrm{Im}(f)$$

ce qui conduit à

$$\det(G(\mathcal{A})) = \#\left(\mathbb{Z}^2/G(\mathcal{A})\right) = \frac{\#\left(\mathbb{Z}/D''\mathbb{Z}\right)^2}{\#G(\mathcal{A})/(D''\mathbb{Z} \times D''\mathbb{Z})} = D''.$$

On peut donc utiliser le fait que

$$\Lambda^*(\mathbf{D}'') = \bigsqcup_{\mathcal{A} \in \mathcal{V}(\mathbf{D}'')} \mathcal{A}$$

pour réécrire

$$S(X, \mathbf{d}, \mathbf{D}) = \sum_{b|\psi(\mathbf{D}')} \sum_{\mathcal{A} \in \mathcal{V}(\mathbf{D}'')} \sum_{\mathbf{x} \in \mathcal{A} \cap (X/b)\mathcal{R}} r\left(l'_1 \frac{L'_1(\mathbf{x})}{d'_1}\right) r\left(l'_2 \frac{L'_2(\mathbf{x})}{d'_2}\right) r\left(q' \frac{Q'(\mathbf{x})}{d'_3}\right)$$

et en utilisant une inversion de Möbius pour exprimer la condition de coprimalité dans

$$\mathcal{A} = \{\mathbf{x} \in G(\mathcal{A}) \quad | \quad (x_1, x_2, D'') = 1)\}$$

on obtient finalement l'égalité

$$S(X, \mathbf{d}, \mathbf{D}) = \sum_{b|\psi(\mathbf{D}')} \sum_{\mathcal{A} \in \mathcal{V}(\mathbf{D}'')} \sum_{e|D''} \mu(e) \sum_{\mathbf{x} \in G_e(\mathcal{A}) \cap (X/b)\mathcal{R}} r\left(l'_1 \frac{L'_1(\mathbf{x})}{d'_1}\right) r\left(l'_2 \frac{L'_2(\mathbf{x})}{d'_2}\right) r\left(q' \frac{Q'(\mathbf{x})}{d'_3}\right)$$

où

$$G_e(\mathcal{A}) = G(\mathcal{A}) \cap e\mathbb{Z}^2 = \{\mathbf{x} \in \mathbb{Z}^2 \quad | \quad \exists a \in e\mathbb{Z} \quad \text{tel que} \quad \mathbf{x} \equiv a\mathbf{y}_0[D'']\}.$$

Il s'agit d'un réseau de covolume eD'' (à préciser également). On a donc

$$S(X, \mathbf{d}, \mathbf{D}) = \sum_{b|\psi(\mathbf{D}')} \sum_{\mathcal{A} \in \mathcal{V}(\mathbf{D}'')} \sum_{e|D''} \mu(e) T(X, \mathcal{A}, e)$$

avec

$$T(X, \mathcal{A}, e) = \sum_{\mathbf{x} \in G_e(\mathcal{A}) \cap (X/b)\mathcal{R}} r\left(l'_1 \frac{L'_1(\mathbf{x})}{d'_1}\right) r\left(l'_2 \frac{L'_2(\mathbf{x})}{d'_2}\right) r\left(q' \frac{Q'(\mathbf{x})}{d'_3}\right),$$

et on est donc ramené à un problème de comptage sur un réseau. On utilise alors notre premier théorème pour estimer $T(X, \mathcal{A}, e)$. Pour ce faire, on effectue un changement de variables E de sorte que

$$\mathbf{x} \in G_e(\mathcal{A}) \quad \Longleftrightarrow \quad \mathbf{x} = E\mathbf{v} \quad \text{avec} \quad \mathbf{v} \in \mathbb{Z}^2, \tag{1.63}$$

où $E = (\mathbf{e}_1, \mathbf{e}_2)$ est la matrice d'une base réduite de vecteurs du réseau $G_e(\mathcal{A})$. Par définition d'une base réduite, comme on a pu le voir plus haut, $||\mathbf{e}_1||$ et $||\mathbf{e}_2||$ sont les minima successifs des éléments du réseau $G_e(\mathcal{A})$. On a $G_e(\mathcal{A}) \subset \delta(\mathbf{D})\mathbb{Z}^2$, et puisque $\delta(\mathbf{D})|\mathbf{e}_1$, que

$$\delta(\mathbf{D}) \leqslant ||\mathbf{e}_1|| \leqslant ||\mathbf{e}_2||$$

et on a comme on l'a déjà vu

$$eD'' = \det(G_e(\mathcal{A})) \ll ||\mathbf{e}_1||||\mathbf{e}_2||.$$

Si on pose $\mathcal{R}'_E = \{\mathbf{v} \in \mathbb{R}^2 \quad | \quad E\mathbf{v} \in \mathcal{R}/b\}$, on a clairement

$$\mathrm{vol}(\mathcal{R}'_{\mathrm{E}}) = \frac{\mathrm{vol}(\mathcal{R})}{\mathrm{b}^2 \det(\mathrm{E})} = \frac{\mathrm{vol}(\mathcal{R})}{\mathrm{b}^2 \mathrm{eD}''}.$$

On peut donc écrire

$$T(X, \mathcal{A}, e) = \sum_{\mathbf{v} \in \mathbb{Z}^2 \cap \mathcal{R}'_E} r\left(M_1(\mathbf{v})\right) r\left(M_2(\mathbf{v})\right) r\left(M_3(\mathbf{v})\right)$$

avec $M_i(\mathbf{v}) = l'_i L'_i(E\mathbf{v})/d'_i$ et $M_3(\mathbf{v}) = q'Q'(E\mathbf{v})/d'_3$. Il est maintenant utile de savoir comment se comportent les quantités intervenant dans le terme d'erreur du Théorème 1. On a

$$r'(\mathbf{M}, \mathcal{R}'_E) = \sup_{\mathbf{v} \in \mathcal{R}'_E} \max\left(|M_1(\mathbf{v})|, |M_2(\mathbf{v})|, \sqrt{|M_3(\mathbf{v})|}\right)$$

$$= \sup_{\mathbf{x} \in \mathcal{R}/b} \max\left(|l'_1 L'_1(\mathbf{x})|/d'_1, |l'_2 L'_2(\mathbf{x})|/d'_2, \sqrt{|q'Q'(\mathbf{x})|/d'_3}\right)$$

et en raisonnant comme ci-dessus pour passer de L_i/d_i à $l'_i L'_i/d'_i$, on obtient

$$= \sup_{\mathbf{x} \in \mathcal{R}} \max\left(|L_1(\mathbf{x})|/d_1, |L_2(\mathbf{x})|/d_2, \sqrt{|Q(\mathbf{x})|/d_3}\right) = r'_{\mathbf{d}}(L_1, L_2, Q, \mathcal{R}) = r'_{\mathbf{d}}.$$

On a d'autre part

$$L_\infty(\mathbf{M}) = \max(||M_i||) \leqslant D^2 ||E|| \max(||L_1||, ||L_2||, ||Q||).$$

Or, on a aussi

$$eD'' = \det(G_e(\mathcal{A})) \gg ||\mathbf{e}_1||||\mathbf{e}_2||$$

et en utilisant le fait que $||E||$ est le maximum des coefficients de $\mathbf{e}_1$ et $\mathbf{e}_2$ en valeur absolue, on en déduit la majoration

$$||E|| \ll eD'' = \det(G_e(\mathcal{A})).$$

On en tire donc

$$L_\infty(\mathbf{M}) \ll D^2 eD'' L_\infty \leqslant D^4 L_\infty$$

car $e|D''|D$. Enfin, on a

$$r_\infty(\mathcal{R}'_E) = \sup_{\mathbf{v} \in \mathcal{R}'_E} \max(|v_1|, |v_2|) \ll \frac{r_\infty(\mathcal{R})}{b} = \frac{r_\infty}{b}.$$

En effet, on a

$$r_\infty(\mathcal{R}'_E) = \sup_{\mathbf{x}\in\mathcal{R}/b} ||E^{-1}\mathbf{x}||$$

et en utilisant la relation

$$E^{-1} = \frac{1}{\det(E)}\,{}^t\tilde{E}$$

où $\tilde{E}$ désigne la comatrice de E, on obtient

$$r_\infty(\mathcal{R}'_E) = \frac{1}{b\det(E)} \sup_{\mathbf{x}\in\mathcal{R}} ||{}^t\tilde{E}\mathbf{x}||.$$

Enfin, pour des matrices de taille 2, $||{}^t\tilde{E}|| = ||E||$ et en utilisant la multiplicativité des normes matricielles,

$$r_\infty(\mathcal{R}'_E) \leqslant \frac{||E||}{b\det(E)} \sup_{\mathbf{x}\in\mathcal{R}} ||\mathbf{x}||,$$

ce qui donne bien

$$r_\infty(\mathcal{R}'_E) \ll \frac{r_\infty}{b}$$

en utilisant à nouveau $||E|| \ll \det(E)$. Posant

$$\sigma_p(E) = \left(1 - \frac{\chi(p)}{p}\right)^3 \sum_{\boldsymbol{\nu}\in\mathbb{Z}^3_{\geqslant 0}} \frac{\chi(p)^{\nu_1+\nu_2+\nu_3}\rho(p^{\nu_1}, p^{\nu_2}, p^{\nu_3}; \mathbf{M})}{p^{2(\nu_1+\nu_2+\nu_3)}}$$

pour $p > 2$ et

$$\sigma_2(E) = 4 \lim_{n\to+\infty} 2^{-2n} \left\{ \mathbf{x} \in (\mathbb{Z}/2^n\mathbb{Z})^2 \quad \middle| \quad \begin{array}{c} M_i(\mathbf{x}) \in \mathcal{E}_{2^n} \\ M_3(\mathbf{x}) \in \mathcal{E}_{2^n} \end{array} \right\},$$

le Théorème 1 nous fournit, puisque les formes M_i vérifient bien les hypothèses **NH** le Lemme suivant.

Lemme 20. *Si on a $r'_{\mathbf{d}} X^{1-2\varepsilon} \geqslant 1$, alors*

$$T(X, \mathcal{A}, e) = 2\pi^3 \mathrm{vol}(\mathcal{R})\mathrm{X}^2\mathrm{W}(\mathrm{E}) + \mathrm{O}\left(\frac{\mathrm{L}^\varepsilon_\infty \mathrm{D}^\varepsilon(\mathrm{r}_\infty \mathrm{r}'_{\mathbf{d}} + \mathrm{r}^2_\infty)\mathrm{X}^2}{\mathrm{b}(\log(\mathrm{X}))^{\eta-\varepsilon}}\right),$$

où

$$W(E) = \frac{1}{b^2 e D''} \prod_p \sigma_p(E)$$

L'objectif est maintenant de voir qu'on ne somme pas trop de termes et qu'on obtient bien après sommation le bon terme principal. On commence par démontrer le lemme suivant.

Lemme 21. *On a*

$$\#\mathcal{V}(\mathcal{D}) \leqslant 8^{\omega(D_1D_2D_3)} a(\mathbf{D}, \boldsymbol{\Delta}).$$

Démonstration.– On utilise la relation

$$\#\mathcal{V}(\mathcal{D}) = \frac{\rho^*(\mathbf{D})}{\varphi(D_1D_2D_3)}.$$

En effet, si $\mathcal{A} \in \mathcal{V}(\mathcal{D})$ et $\mathbf{y}_0$ est fixé dans $\mathcal{A}$, alors il existe par définition a entier tel que $\mathbf{x} \equiv a\mathbf{y}_0[D]$ et la classe de a modulo D est uniquement déterminé par $\mathbf{y}$ car $(y_{0,1}, y_{0,2}, D) = 1$. En effet, si $y_{0,1} = (y_{0,1}, D)y'_{0,1}$, alors nécessairement $(y_{0,1}, D)$ divise x_1 et

$$a \equiv \frac{x_1}{(y_{0,1}, D)} \overline{\left(\frac{y_{0,1}}{(y_{0,1}, D)}\right)} \left[\frac{D}{(y_{0,1}, D)}\right]$$

et de même sur la deuxième composante

$$a \equiv \frac{x_2}{(y_{0,2}, D)} \overline{\left(\frac{y_{0,2}}{(y_{0,2}, D)}\right)} \left[\frac{D}{(y_{0,2}, D)}\right].$$

Or,

$$(y_{0,2}, D) | \frac{D}{(y_{0,1}, D)}$$

(par la condition de coprimalité) donc on a

$$a \equiv \frac{x_1}{(y_{0,1}, D)} \overline{\left(\frac{y_{0,1}}{(y_{0,1}, D)}\right)} [(y_{0,2}, D)]$$

et

$$a \equiv \frac{x_2}{(y_{0,2}, D)} \overline{\left(\frac{y_{0,2}}{(y_{0,2}, D)}\right)} \left[\frac{D}{(y_{0,2}, D)}\right],$$

où

$$\left(\frac{D}{(y_{0,2}, D)}, (y_{0,2}, D)\right) = 1$$

donc par le théorème chinois, on connaît la classe de a modulo le produit des deux, soit modulo D. Ainsi,

$$\rho^*(\mathbf{D}) = \sum_{\mathcal{A} \in \mathcal{V}(\mathbf{D})} \#\left(\mathcal{A} \cap]0, D]^2\right) = \varphi(D)\#\mathcal{V}(\mathbf{D})$$

étant donné qu'on a

$$\varphi(D) = \#\left(\mathcal{A} \cap]0, D]^2\right)$$

puisqu'un élément $\mathbf{x} \equiv \lambda\mathbf{y}_0[D]$ est entièrement déterminé par la classe de λ inversible modulo D. On a donc obtenu la formule souhaitée. Par multiplicativité, on en déduit que

$$\#\mathcal{V}(\mathcal{D}) = \prod_{p^{\nu_i} || D_i} \frac{\rho^*(p^{\nu_1}, p^{\nu_2}, p^{\nu_3})}{\varphi(p^{\nu_1+\nu_2+\nu_3})},$$

ce qui permet de restreindre l'étude à des puissances de nombres premiers. D'après l'étude de la fonction ρ^* faite plus haut, il est nécessaire que

$$\nu_p(\Delta_{12}) \geqslant \min(\nu_1, \nu_2) \quad \text{et} \quad \nu_p(\Delta_{i3}) \geqslant \min(\nu_i, \nu_3)$$

pour que $\rho^*(p^{\nu_1}, p^{\nu_2}, p^{\nu_3}) \neq 0$. Il faut alors à nouveau traiter tous les cas. On en traite deux typiques, les autres s'obtiennent de la même façon. Supposons que $\nu_1 \geqslant \nu_2 \geqslant \nu_3$, alors

$$\frac{\rho^*(p^{\nu_1}, p^{\nu_2}, p^{\nu_3})}{\varphi(p^{\nu_1+\nu_2+\nu_3})} \leqslant p^{\nu_3+\min(\nu_1,\nu_2,\nu_p(\Delta_{12}))} = p^{\nu_3+\nu_2} \leqslant 8p^{\nu_p(a(\mathbf{D},\mathbf{\Delta}))}$$

car

$$\nu_p(a(\mathbf{D},\mathbf{\Delta})) = \min(\nu_1, \nu_p(\Delta_{12}))+\min(\nu_2, \nu_p(\Delta_{12}))+\min(\nu_3, \nu_p(\Delta)+\min(\nu_p(\Delta_{23}), \nu_p(\Delta_{13}))),$$

et ici $\min(\nu_2, \nu_p(\Delta_{12})) = \nu_2$ et $\nu_3 = \min(\nu_3, \nu_p(\Delta) + \min(\nu_p(\Delta_{23}), \nu_p(\Delta_{13})))$ puisqu'en particulier $\nu_3 \leqslant \min(\Delta_{13}, \Delta_{23})$. Supposons alors maintenant que $\nu_3 > \max(\nu_1, \nu_2)$. On obtient

$$\frac{\rho^*(p^{\nu_1}, p^{\nu_2}, p^{\nu_3})}{\varphi(p^{\nu_1+\nu_2+\nu_3})} \leqslant 8p^{\nu_1+\nu_2}p^{\min([\nu_p(\mathrm{disc}(Q))/2],[\nu_3/2])} \leqslant 8p^{\nu_p(a(\mathbf{D},\mathbf{\Delta}))}.$$

En effet, $\nu_i \leqslant \nu_p(\Delta_{i3})$ donc $\nu_i \leqslant \min(\nu_i, \nu_p(\Delta_{i3}) + \nu_p(\Delta_{ij}))$ avec $\{i, j\} = \{1, 2\}$. □

Sous la condition $r'_{\mathbf{d}}X^{1-2\varepsilon} \geqslant 1$,on a donc

$$S(X, \mathbf{d}, \mathbf{D}) = 2\pi^3 \mathrm{vol}(\mathcal{R})\mathrm{W}\mathrm{X}^2 + \mathrm{O}\left(\frac{\mathrm{L}_\infty^\varepsilon \mathrm{D}^\varepsilon \mathrm{a}'(\mathbf{D},\mathbf{\Delta})(\mathrm{r}_\infty \mathrm{r}'_{\mathbf{d}} + \mathrm{r}_\infty^2)\mathrm{X}^2}{(\log(\mathrm{X}))^{\eta-\varepsilon}}\right)$$

où

$$W = \sum_{b|\psi(\mathbf{D}')} \sum_{\mathcal{A}\in\mathcal{V}(\mathbf{D}'')} \sum_{e|D''} \mu(e)W(E).$$

En effet, on majore $\mu(e)$ par 1 en valeur absolue, ce qui fait sortir un $\tau(D'') \leqslant \tau(D) \ll D^\varepsilon$, puis la deuxième somme fait sortir un $\#\mathcal{V}(\mathbf{D}'')$ que l'on peut majorer d'après le Lemme 21 par

$$\#\mathcal{V}(\mathbf{D}'') \leqslant 8^{\omega(D'_1D'_2D'_3)}a'(\mathbf{D},\mathbf{\Delta})$$

puisque les D''_i divisent les D'_i (et car avec $\mathbf{D}''$ on a les formes primitives) et enfin on a alors une

$$\sum_{b|\psi(\mathbf{D}')} \frac{1}{b} \leqslant \sum_{b|\psi(\mathbf{D}')} 1 = \tau(\psi(\mathbf{D}')) \leqslant \tau(D'_1D'_2D'_3) \ll D^\varepsilon,$$

ce qui fournit bien le résultat escompté. Il ne reste alors plus qu'à traiter le $r'_{\mathbf{d}}$, introduire le terme $\delta(\mathbf{D})$ et calculer W. On introduit alors la fonction multiplicative suivante

$$\psi_0(p^{\beta_1}, p^{\beta_2}, p^{\beta_3}) = \max_{1\leqslant\beta\leqslant\max(\beta_1,\beta_2,\lceil\beta_3/2\rceil)} p^{\min(\beta,\beta_1)+\min(\beta,\beta_2)+\min(2\beta,\beta_3)-2\beta}.$$

Si on suppose que D_3 est sans facteur carré, on a toujours $\beta_3 = 1$ et $\lceil\beta_3/2\rceil = 0$ et les termes tels que $\beta \leqslant \min(\beta_1, \beta_2)$ donnent des facteurs 1, tandis que si on suppose que $\beta_1 \geqslant \beta_2$, alors $\beta \leqslant \beta_1$ et les termes $\beta_2 \leqslant \beta \leqslant \beta_1$ donnent des facteurs

$$p^{\beta_2-\beta+1}$$

puisque $2\beta \geqslant \beta_3 = 1$. Le maximum de ces exposants pour $\beta_2 \leqslant \beta \leqslant \beta_1$ vaut 1 et donc on a obtenu

$$\psi_0(D_1, D_2, D_3) = \prod_{\substack{p|D_1,p|D_2\\p|D_3}} p = (D_1, D_2, D_3)$$

puisque D_3 est sans facteur carré. De plus, on a

$$\psi_0(D_1, D_2, D_3) \leqslant (D_1 D_2 D_3)^{1/2}$$

puisqu'on a

$$\min(\beta, \beta_1) + \min(\beta, \beta_2) + \min(2\beta, \beta_3) \leqslant 2\beta + \frac{\beta_1 + \beta_2 + \beta_3}{2}$$

que l'on peut vérifier cas par cas. On a également besoin de l'inégalité

$$\psi_0(D_1', D_2', D_3') \geqslant \frac{(D_1', b)(D_2', b)(D_3', b^2)}{b^2}.$$

En effet, on a

$$\frac{(D_1', b)(D_2', b)(D_3', b^2)}{b^2} = \prod_p p^{\min(\nu_p(D_1'),\nu_p(b))+\min(\nu_p(D_2'),\nu_p(b))+\min(\nu_p(D_3'),2\nu_p(b))-2\nu_p(b)}$$

et $b|\psi(\mathbf{D}')$ donc $\nu_p(b) \leqslant \max(\nu_p(D_1'), \nu_p(D_2'), \lceil \nu_p(D_3')/2 \rceil)$ et cela découle de la défintion de ψ_0. On a donc

$$D'' b^2 = \frac{b^2 D'}{(D_1', b)(D_2', b)(D_3', b^2)} \geqslant \frac{D'}{\psi_0(D_1', D_2', D_3')}.$$

On a alors besoin d'utiliser le Lemme 4 pour se débarrasser de $r'_{\mathbf{d}}$ et passer à du r'. En majorant $W(E)$ par

$$L_\infty^\varepsilon \frac{\psi_0(D_1', D_2', D_3')}{D'}$$

grâce au Lemme 4 et à la remarque précédente pour majorer $1/D''b^2$, on obtient de la même façon qu'on a traité la sommation du terme d'erreur dans le Théorème 1 que

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

puisque

$$\frac{\psi_0(D_1', D_2', D_3')}{D'} \leqslant \frac{(D')^{1/2}}{D'} \leqslant 1.$$

Or, on a clairement la suite d'inégalités

$$\frac{r'}{d_1 d_2 d_3} \leqslant r'_{\mathbf{d}} \leqslant r'$$

ce qui permet remplacer $r'_{\mathbf{d}}$ par r' dans le terme d'erreur. De plus, lorsque $d_1 d_2 d_3 \leqslant X^\varepsilon$, la condition $r'_{\mathbf{d}} X^{1-2\varepsilon} \geqslant 1$ est une conséquence de $r' X^{1-\varepsilon} \geqslant 1$ et lorsque $d_1 d_2 d_3 > X^\varepsilon$, en passant aux logarithmes, on a

$$1 \ll_\varepsilon \frac{D^\varepsilon}{\log(X)}.$$

On cherche ici à obtenir la même estimation que celle qui découle du Théorème 1 sous la condition $r' X^{1-\varepsilon} \geqslant 1$, à savoir :

$$S(X, \mathbf{d}, \mathbf{D}) = O\left(\frac{L_\infty^\varepsilon D^\varepsilon a'(\mathbf{D}, \mathbf{\Delta}) r_\infty^2 X^2}{\log(X)}\right).$$

Or, le même raisonnement que dans le traitement de $S_{\pm,\pm,\pm}$ en majorant par la somme des τ fournit que

$$S(X,\mathbf{d},\mathbf{D}) \ll L_\infty^\varepsilon r_\infty^2 X^2 (\log(X))^3 \ll L_\infty^\varepsilon D^\varepsilon r_\infty^2 \frac{X^2}{\log(X)}$$

et donc on a bien le résultat voulu dans ce cas-là également, ce qui fait que pour $r'X^{1-\varepsilon} \geqslant 1$, on a

$$S(X,\mathbf{d},\mathbf{D}) = 2\pi^3 \mathrm{vol}(\mathcal{R})\mathrm{WX}^2 + \mathrm{O}\left(\frac{\mathrm{L}_\infty^\varepsilon \mathrm{D}^\varepsilon \mathrm{a}'(\mathbf{D},\boldsymbol{\Delta})(\mathrm{r}_\infty \mathrm{r}' + \mathrm{r}_\infty^2)\mathrm{X}^2}{(\log(\mathrm{X}))^{\eta-\varepsilon}}\right).$$

Ensuite, en ce qui concerne le $\delta(\mathbf{D})$ (ce ne sera nécessaire en réalité dans notre obtention de la conjecture de Manin), il suffit de remarquer que

$$S(X,\mathbf{d},\mathbf{D};L_1,L_2,Q,\mathcal{R}) = S(X,\mathbf{d},\mathbf{D};\delta L_1,\delta L_2,\delta^2 Q,\mathcal{R}/\delta)$$

avec $\delta = \delta(\mathbf{D})$ (car tous les éléments de $\Lambda(\mathbf{D})$ sont de la forme $(x_1,x_2) = \delta(x_1',x_2')$ avec $\mathbf{x}' \in \mathcal{R}/\delta$ par définition de δ) et que r' est alors inchangé par cette transformation quand r_∞ se retrouve divisé par δ. Les $\mathbf{D}$ et $\mathbf{d}$ et X sont inchangés, on a donc du $1/\delta$ qui apparaît du $r'r_\infty$ et du $1/\delta^2 \leqslant 1/\delta$ du r_∞^2. De plus, le L_∞ est multiplié par δ ou δ^2 mais on fait alors apparaître un $\delta^\varepsilon \leqslant D^\varepsilon$ car $\delta | D_1D_2D_3 \in \Lambda(\mathbf{D})$ qui ne pose pas de problème. En ce qui concerne le terme principal, on a

$$\mathrm{vol}(\mathcal{R}/\delta) = \frac{\mathrm{vol}(\mathcal{R})}{\delta^2}.$$

Ensuite, on montre que $W(\delta L_i,\delta^2 Q) = \delta^2 W$ ce qui achève de montrer que le terme principal reste inchangé. On voit en effet avec la définition de W qu'il suffit de montrer que

$$W(E;\delta L_i,\delta^2 Q) = \delta^2 W(E).$$

On s'intéresse donc aux $\sigma_p(E;\delta L_i,\delta^2 Q)$. On commence par remarquer que si $p \nmid \delta$, alors

$$\rho(p^{\nu_1},p^{\nu_2},p^{\nu_3},\delta L_i,\delta^2 Q) = \rho(p^{\nu_1},p^{\nu_2},p^{\nu_3},L_i,Q)$$

donc

$$\sigma_p(E;\delta L_i,\delta^2 Q) = \sigma_p(E).$$

Ensuite pour $p|\delta$, on a

$$\rho(p^{\nu_1},p^{\nu_2},p^{\nu_3},\delta L_i,\delta^2 Q) = \rho(p^{\nu_1},p^{\nu_2},p^{\nu_3},p^{\nu_p(\delta)}L_i,p^{2\nu_p(\delta)}Q)$$

et

$$\frac{\rho(p^{\nu_1},p^{\nu_2},p^{\nu_3},p^{\nu_p(\delta)}L_i,p^{2\nu_p(\delta)}Q)}{p^{2(\nu_1+\nu_2+\nu_3)}} = p^{2\nu_p(\delta)}\frac{\rho(p^{\nu_1},p^{\nu_2},p^{\nu_3},L_i,Q)}{p^{2(\nu_1+\nu_2+\nu_3)}}$$

puisque

$$\Lambda(p^{\nu_i},\delta L_i,\delta^2 Q) = p^{\nu_p(\delta)}\Lambda(p^{\nu_i},L_i,Q).$$

On obtient bien donc que

$$W(E;\delta L_i,\delta^2 Q) = \prod_p \sigma_p(E;\delta L_i,\delta^2 Q) = \delta^2 W(E)$$

ce qui permet de conclure. On a ainsi

$$S(X,\mathbf{d},\mathbf{D}) = 2\pi^3 \mathrm{vol}(\mathcal{R})\mathrm{WX}^2 + \mathrm{O}\left(\frac{\mathrm{L}_\infty^\varepsilon \mathrm{D}^\varepsilon \mathrm{a}'(\mathbf{D},\boldsymbol{\Delta})(\mathrm{r}_\infty \mathrm{r}' + \mathrm{r}_\infty^2)\mathrm{X}^2}{\delta(\mathbf{D})(\log(\mathrm{X}))^{\eta-\varepsilon}}\right).$$

1.5.2 Une majoration uniforme de $S(X, \mathbf{d}, \mathbf{D})$ dans l'optique de la conjecture de Manin

On donne maintenant une majoration uniforme de $S(X, \mathbf{d}, \mathbf{D})$ qui sera nécessaire dans la deuxième section.

Lemme 22. *Soit $\varepsilon > 0$. Lorsque L_1, L_2 et Q vérifient les hypothèses du Théorème 2 et $(\mathbf{d}, \mathbf{D}) \in \mathfrak{D}$, on a*

$$S(X, \mathbf{d}, \mathbf{D}) \ll (DL_\infty)^\varepsilon a'(\mathbf{d}, \mathbf{\Delta}) \left(\frac{\psi_0(D_1', D_2', D_3')}{D_1' D_2' D_3'} r_\infty^2 X^2 + \frac{(r_\infty X)^{1+\varepsilon}}{\delta(\mathbf{D})} \right).$$

Démonstration– On pose classiquement la fonction multiplicative suivante

$$r''(p^\nu) = \begin{cases} 1 + \chi(p) & \text{si } \nu = 1 \\ (\nu+1)^3 & \text{sinon} \end{cases}$$

de sorte qu'on ait

$$T(X, \mathcal{A}, e) \ll \sum_{\substack{\mathbf{v} \in \mathbb{Z}^2 \\ v_2 \ll r_\infty X/(|\mathbf{e}_2| b) \\ v_1 \ll r_\infty X/(|\mathbf{e}_1| b)}} r'' \left(M_1(\mathbf{v}) M_2(\mathbf{v}) M_3(\mathbf{v}) \right).$$

Appliquant le Théorème 4 et utilisant le fait que $E \ll (DL_\infty)^\varepsilon$, on obtient la majoration

$$T(X, \mathcal{A}, e) \ll \frac{(DL_\infty)^\varepsilon}{D'' b^2} r_\infty^2 X^2 + (DL_\infty)^\varepsilon \frac{(r_\infty X)^{1+\varepsilon}}{\delta(\mathbf{D})}$$

car

$$r_\infty X/(|\mathbf{e}_1| b) \times r_\infty X/(|\mathbf{e}_2| b) \leqslant \frac{r_\infty^2 X^2}{D'' e b^2}$$

et on majore $1/e$ par 1 et dans la deuxième partie de l'inégalité, on utilise le fait que

$$\delta(\mathbf{D}, L_1, L_2, Q) = \delta(\mathbf{D}', L_1^*, L_2^*, Q^*) \leqslant b \delta(\mathbf{D}'', L_1', L_2', Q')$$

pour majorer

$$\frac{(r_\infty X)^{1+\varepsilon}}{(D'' e b^2)^{1+\varepsilon}} \leqslant \frac{(r_\infty X)^{1+\varepsilon}}{(D'' e b^2)}$$

et

$$\frac{1}{b} \leqslant \frac{\delta(\mathbf{D}'', L_1', L_2', Q')}{\delta(\mathbf{D}, L_1, L_2, Q)} \leqslant \frac{D'' e}{\delta(\mathbf{D}, L_1, L_2, Q)}$$

pour obtenir la formule annoncée. Il ne reste alors plus qu'à sommer. Le nombre de termes à sommer est majoré par

$$\tau(\psi(\mathbf{D}') \# \mathcal{V}(\mathbf{D}'')) \tau(D'') \leqslant D^\varepsilon a'(\mathbf{d}, \mathbf{\Delta})$$

ce qui permet, avec la majoration que l'on a obtenu sur ψ_0, d'obtenir le résultat du lemme, où, d'après ce qu'on a déjà démontré,

$$\frac{\psi_0(D_1', D_2', D_3')}{D_1' D_2' D_3'} \leqslant 1.$$

□

1.5.3 Calcul de W et fin de la preuve

Il ne reste plus qu'à calculer W pour obtenir l'expression souhaitée pour conclure la preuve du Théorème 2. Pour ce faire, on étudie les termes sommés dans $\sigma_p(E)$. On introduit quelques notations supplémentaires :

$$\mu_i' = \nu_p(D_i'), \quad \mu_i'' = \nu_p(D_i''), \quad \lambda_i' = \nu_p(d_i'), \quad \mu = \nu_p(D), \quad \mu' = \nu_p(D'),$$

$$\mu'' = \nu_p(D''), \quad \varepsilon = \nu_p(e), \quad \beta = \nu_p(b), \quad \text{et} \quad \nu = \nu_1 + \nu_2 + \nu_3,$$

où pour alléger les notations, on omettra la dépendance en p de ces valuations. On a alors

$$\rho(p^{\nu_1}, p^{\nu_2}, p^{\nu_3}, \mathbf{M}) = \#\left(\Lambda'(p^{\nu_1}, p^{\nu_2}, p^{\nu_3}) \cap \mathcal{B}(p^{\nu})\right)$$

où

$$\Lambda'(p^{\nu_1}, p^{\nu_2}, p^{\nu_3}) = \{\mathbf{x} \in \mathbb{Z}^2 \quad | \quad p^{\nu_i+\lambda_i} | p^{\beta} L_i(\mathbf{x}) \quad \text{et} \quad p^{\nu_3+\lambda_3} | p^{2\beta} Q(\mathbf{x})\}$$

et

$$\mathcal{B}(p^{\nu}) = \{E\mathbf{v} \quad | \quad 0 \leqslant v_i < p^{\nu}\}$$

puisque

$$\rho(p^{\nu_1}, p^{\nu_2}, p^{\nu_3}, \mathbf{M}) = \{\mathbf{v} \in [\![0, p^{\nu}[\![^2 \quad | \quad p^{\nu_i} | M_i(\mathbf{v}) \quad \text{et} \quad p^{\nu_3} | M_3(\mathbf{v})\}.$$

et il suffit alors de remplacer les M_i par leurs expressions. Par le théorème de la base adaptée, on peut trouver une base $(\mathbf{e}_1, \mathbf{e}_2)$ de $\mathbb{Z}^2$ telle qu'il existe $(\delta_1 p^{m_1}, \delta_2 p^{m_2}) \in \mathbb{N}^2$ pour lequel la famille $(\delta_1 p^{m_1}\mathbf{e}_1, \delta_2 p^{m_2}\mathbf{e}_2)$ est une $\mathbb{Z}$-base de $E\mathbb{Z}^2$ avec $(\delta_1\delta_2, p) = 1$. De plus, on a

$$\delta_1\delta_2 p^{m_1+m_2} = \det(E) = D''b^2$$

puisque le déterminant est invariant par changement de base. On a donc en particulier $m_1 + m_2 = \mu'' + \varepsilon$. On peut alors remplacer $\mathcal{B}(p^{\nu})$ par

$$\{\mathbf{w} = w_1\delta_1 p^{m_1}\mathbf{e}_1 + w_2\delta_2 p^{m_2}\mathbf{e}_2 \quad | \quad 0 \leqslant w_i < p^{\nu}\}$$

puis par

$$\mathcal{B}'(p^{m_1+\nu}, p^{m_2+\nu}) = \{\mathbf{w} = w_1 p^{m_1}\mathbf{e}_1 + w_2 p^{m_2}\mathbf{e}_2 \quad | \quad 0 \leqslant w_i < p^{\nu}\}$$

car la condition de coprimalité implique que

$$w_i \mapsto w_i\delta_i$$

est une isomorphisme de $\mathbb{Z}/p^{\nu}\mathbb{Z}$ sur lui-même et où

$$\mathcal{B}'(p^{k_1}, p^{k_2}) = \{\mathbf{w}' = w_1'\mathbf{e}_1 + w_2'\mathbf{e}_2 \in E\mathbb{Z}^2 \quad | \quad 0 \leqslant w_j' < p^{k_j}\}.$$

On en déduit alors

$$\begin{aligned}\rho(p^{\nu_1}, p^{\nu_2}, p^{\nu_3}, \mathbf{M}) &= \#\left(\Lambda'(p^{\nu_1}, p^{\nu_2}, p^{\nu_3}) \cap \mathcal{B}'(p^{m_1+\nu}, p^{m_2+\nu})\right) \\ &= \frac{\#\left(\Lambda'(p^{\nu_1}, p^{\nu_2}, p^{\nu_3}) \cap \mathcal{B}'(p^{m_1+m_2+\nu}, p^{m_1+m_2+\nu})\right)}{p^{m_1+m_2}}.\end{aligned}$$

Ensuite d'après ce qui précède

$$\rho(p^{\nu_1},p^{\nu_2},p^{\nu_3},\mathbf{M})=\frac{\#\left(\Lambda'(p^{\nu_1},p^{\nu_2},p^{\nu_3})\cap\mathcal{B}'(p^{\mu''+\varepsilon+\nu},p^{\mu''+\varepsilon+\nu})\right)}{p^{\mu''+\varepsilon}}.$$

On réécrit alors cette relation

$$\begin{aligned}\frac{\rho(p^{\nu_1},p^{\nu_2},p^{\nu_3},\mathbf{M})}{p^{2\nu_2+2\nu_2+2\nu_3+\nu_p(eD'')}}&=\frac{\#\left(\Lambda'(p^{\nu_1},p^{\nu_2},p^{\nu_3})\cap\mathcal{B}'(p^{\mu''+\varepsilon+\nu},p^{\mu''+\varepsilon+\nu})\right)}{p^{2(\mu''+\varepsilon+\nu)}}\\&=\frac{\#\left(\Lambda'(p^{\nu_1},p^{\nu_2},p^{\nu_3})\cap\mathcal{B}'(p^{\mu''+1+\nu},p^{\mu''+1+\nu})\right)}{p^{2(\mu''+1+\nu)}}.\end{aligned}$$

Justifions la dernière égalité qui est un peu subtile. Tout d'abord, la présence du $\mu(e)$ nous permet de nous restreindre aux entiers sans facteurs multiples et donc ε ne peut prendre que les valeurs 0 ou 1. Le résultat est clair dans le second cas et il ne reste qu'à le justifier lorsque $\varepsilon=0$. Pour cela, on observe que les conditions de $\Lambda'(p^{\nu_1},p^{\nu_2},p^{\nu_3})$ ne dépendent que des valeurs des coordonnées modulo $p^{\nu+\mu''}$. En effet, si par exemple

$$p^{\nu_i+\lambda_i}|p^{\beta}L_i(\mathbf{x}),$$

alors

$$p^{\beta}L_i(\mathbf{x}+p^{\nu+\mu''}\mathbf{k})=p^{\beta}L_i(\mathbf{x})+p^{\beta}p^{\nu+\mu''+\nu_p(\ell_i)}L_i^*(\mathbf{k})$$

et $\nu_i+\lambda_i\leqslant\nu+\mu''+\beta+\nu_p(\ell_i)$. En effet, on montre que $\lambda_i\leqslant\mu_i''+\beta+\nu_p(\ell_i)$. On sait que

$$\lambda_i=\lambda_i'+\min(\lambda_i,\beta,\nu_p(\ell_i))\leqslant\lambda_i'+\nu_p(\ell_i)$$

donc il suffit maintenant d'établir que $\lambda_i'\leqslant\mu_i''+\beta$. Or, on a

$$\lambda_i'\leqslant\mu_i'$$

et par conséquent il suffit de montrer que $\mu_i'\leqslant\mu_i''+\beta$. Or, $\mu_i''=\mu_i'-\min(\beta,\mu_i')$ et puisque

$$\beta-\min(\beta,\mu_i')\geqslant 0,$$

on a bien le résultat et

$$p^{\nu_i+\lambda_i}|p^{\beta}L_i(\mathbf{x}+p^{\nu+\mu''}\mathbf{k}).$$

On voit donc que $\mathbf{x}\in\Lambda'(p^{\nu_1},p^{\nu_2},p^{\nu_3})$ si, et seulement si, sa classe modulo $p^{\nu+\mu''}$ y est. On en déduit que

$$p^2\#\left(\Lambda'(p^{\nu_1},p^{\nu_2},p^{\nu_3})\cap\mathcal{B}'(p^{\mu''+\nu},p^{\mu''+\nu})\right)=\#\left(\Lambda'(p^{\nu_1},p^{\nu_2},p^{\nu_3})\cap\mathcal{B}'(p^{m_1+m_2+\nu},p^{\mu''+1+\nu})\right)$$

puisque dans le second ensemble, on trie les élèments selon leur classe modulo $p^{\nu+\mu''}$ et on a $\#\left(\Lambda'(p^{\nu_1},p^{\nu_2},p^{\nu_3})\cap\mathcal{B}'(p^{m_1+m_2+\nu},p^{\mu''+\nu})\right)$ éléments qui vont convenir que l'on relève chacun en p^2 éléments dans $\mathbb{Z}/p^{\nu+\mu''+1}\mathbb{Z}$. On en déduit donc lorsque $\varepsilon=0$ que

$$\begin{aligned}\frac{\rho(p^{\nu_1},p^{\nu_2},p^{\nu_3},\mathbf{M})}{p^{2\nu_2+2\nu_2+2\nu_3+\nu_p(eD'')}}&=\frac{\#\left(\Lambda'(p^{\nu_1},p^{\nu_2},p^{\nu_3})\cap\mathcal{B}'(p^{\mu''+\nu},p^{\mu''+\nu})\right)}{p^{2(\mu''+\nu)}}\\&=\frac{\#\left(\Lambda'(p^{\nu_1},p^{\nu_2},p^{\nu_3})\cap\mathcal{B}'(p^{\mu''+\nu},p^{\mu''+\nu})\right)}{p^{2(\mu''+\nu)+2}}\end{aligned}$$

ce qui permet de conclure. On va alors sommer par rapport à e, $\mathcal{A} \in \mathcal{V}(\mathbf{D}'')$ et b. On a supprimé la dépendance en e, il reste alors le $\mu(e)$ qui par multipilicativité donne pour un p donné $(-1)^{\varepsilon}$ puisqu'on a vu qu'on pouvait supposer e sans facteur multiple et donc on obtient que (tout est multiplicatif, même les sommes sur $b|\psi(D'')$)

$$W(E) = \prod_p w_p$$

où

$$w_p = \left(1 - \frac{\chi(p)}{p}\right)^3 \sum_{\beta \leqslant B'} \sum_{\mathcal{A} \in \mathcal{V}(p^{\mu_1''}, p^{\mu_2''}, p^{\mu_3''})} \sum_{\varepsilon \leqslant \min(1,\mu'')} \sum_{\boldsymbol{\nu} \in \mathbb{Z}^3_{\geqslant 0}} (-1)^{\varepsilon} p^{-2\beta} \frac{\chi(p)^{\nu_1+\nu_2+\nu_3} \rho(p^{\nu_1}, p^{\nu_2}, p^{\nu_3}, \mathbf{M})}{p^{2\nu_2+2\nu_2+2\nu_3+\nu_p(eD'')}}$$

et où $B' = \max(\mu_1', \mu_2', \lceil \mu_3'/2 \rceil)$. On a donc d'après ce qui précède

$$w_p = \left(1 - \frac{\chi(p)}{p}\right)^3 \times$$

$$\sum_{\beta \leqslant B'} \sum_{\mathcal{A} \in \mathcal{V}(p^{\mu_1''}, p^{\mu_2''}, p^{\mu_3''})} \sum_{\varepsilon \leqslant \min(1,\mu'')} \sum_{\boldsymbol{\nu} \in \mathbb{Z}^3_{\geqslant 0}} (-1)^{\varepsilon} p^{-2\beta} \chi(p)^{\nu_1+\nu_2+\nu_3} \frac{\#\left(\Lambda'(p^{\nu_1}, p^{\nu_2}, p^{\nu_3}) \cap \mathcal{B}'(p^{\mu''+1+\nu}, p^{\mu''+1+\nu})\right)}{p^{2(\mu''+1+\nu)}}$$

où on se sert du fait qu'on ait fait disparaître la dépendance en ε dans l'ensemble dans lequel on compte (attention cependant on a encore une dépendance en ε cachée dans l'ensemble $\mathcal{B}$) de manière essentielle pour estimer

$$\sum_{\varepsilon \leqslant \min(1,\mu'')} (-1)^{\varepsilon} \frac{\#\left(\Lambda'(p^{\nu_1}, p^{\nu_2}, p^{\nu_3}) \cap \mathcal{B}'(p^{\mu''+1+\nu}, p^{\mu''+1+\nu})\right)}{p^{2(\mu''+1+\nu)}}.$$

On suppose ici $\mu'' \geqslant 1$ et on a donc

$$\sum_{\varepsilon \leqslant \min(1,\mu'')} (-1)^{\varepsilon} \frac{\#\left(\Lambda'(p^{\nu_1}, p^{\nu_2}, p^{\nu_3}) \cap \mathcal{B}'(p^{\mu''+1+\nu}, p^{\mu''+1+\nu})\right)}{p^{2(\mu''+1+\nu)}} =$$

$$\frac{1}{p^{2(\mu''+1+\nu)}} \left(\#\left\{ \mathbf{w}' = w_1\mathbf{e}_1 + w_2'\mathbf{e}_2 \in G(\mathcal{A}), \quad 0 \leqslant w_i' < p^{\nu+\mu''+1} \quad | \quad \mathbf{w}' \in \Lambda'(p^{\nu_1}, p^{\nu_2}, p^{\nu_3}) \right\} - \right.$$

$$\left. \#\left\{ \mathbf{w}' = w_1\mathbf{e}_1 + w_2'\mathbf{e}_2 \in G(\mathcal{A}), \quad 0 \leqslant w_i' < p^{\nu+\mu''+1}, \quad p|\mathbf{w}' \quad | \quad \mathbf{w}' \in \Lambda'(p^{\nu_1}, p^{\nu_2}, p^{\nu_3}) \right\} \right)$$

($\varepsilon = 0$ car $E\mathbb{Z}^2 = G_1(\mathcal{A}) = G(\mathcal{A})$ pour $\mathcal{A} \in \mathcal{V}(p^{\mu_1''}, p^{\mu_2''}, p^{\mu_3''})$ moins $\varepsilon = 1$ car $E\mathbb{Z}^2 = G_p(\mathcal{A}) = \{\mathbf{x} \in G(\mathcal{A}) \quad | \quad p|\mathbf{x}\}$). On obtient donc

$$\frac{1}{p^{2(\mu''+1+\nu)}} \left(\#\left\{ \mathbf{w}' = w_1\mathbf{e}_1 + w_2'\mathbf{e}_2 \in G(\mathcal{A}), \quad 0 \leqslant w_i' < p^{\nu+\mu''+1} \quad p \nmid \mathbf{w}' \quad | \quad \mathbf{w}' \in \Lambda'(p^{\nu_1}, p^{\nu_2}, p^{\nu_3}) \right\} \right).$$

On a ici utilisé de façon crucial le fait qu'on n'ait pas des $p^{\nu+\mu''}$ et des $p^{\nu+\mu''+1}$ qui nous auraient empêché de comparer les deux quantités. On remarque alors que $\mathbf{w}' = M(w_1', w_2')$ avec $M = (\mathbf{e}_1, \mathbf{e}_2)$ qui est dans $\mathrm{GL}_2(\mathbb{Z})$ au sens où son inverse est aussi à coefficients entiers. On en déduit que $|\det(M)| = 1$ et donc en particulier pour tout p, M est inversible dans $\mathcal{M}\left(\mathbb{Z}/p^{\nu+\mu''+1}\mathbb{Z}\right)$. On en déduit un isomorphisme via M de $\left(\mathbb{Z}/p^{\nu+\mu''+1}\mathbb{Z}\right)^2$ sur lui-même

qui implique qu'il y a une bijection entre les $\mathbf{w}'$ que l'on considère dans notre comptage et les

$$(t_1, t_2) + p^{\nu+\mu''+1}(r_1, r_2)$$

avec (t_1, t_2) qui décrit $\left(\mathbb{Z}/p^{\nu+\mu''+1}\mathbb{Z}\right)^2$ et pour certains $(r_1, r_2) \in \mathbb{Z}^2$. De plus, on voit que $\mathbf{w}'$ est dans $G(\mathcal{A})$ et dans $\Lambda'(p^{\nu_1}, p^{\nu_2}, p^{\nu_3})$ si, et seulement si, (t_1, t_2) y est et qu'il est non divisible par p si, et seulement si, $p \nmid \mathbf{t}$. On en déduit donc qu'on a

$$\sum_{\varepsilon \leqslant \min(1,\mu'')} (-1)^{\varepsilon} \frac{\#\left(\Lambda'(p^{\nu_1}, p^{\nu_2}, p^{\nu_3}) \cap \mathcal{B}'(p^{\mu''+1+\nu}, p^{\mu''+1+\nu})\right)}{p^{2(\mu''+1+\nu)}} =$$

$$\frac{1}{p^{2(\mu''+1+\nu)}} \left(\# \left\{ \mathbf{t} \in G(\mathcal{A}) \cap \left(\mathbb{Z}/p^{\nu+\mu''+1}\mathbb{Z}\right)^2, \quad p \nmid \mathbf{t} \quad | \quad \mathbf{t} \in \Lambda'(p^{\nu_1}, p^{\nu_2}, p^{\nu_3}) \right\} \right).$$

Or, la condition $\mathbf{t} \in G(\mathcal{A})$ et $p \nmid \mathbf{t}$ implique que $\mathbf{t} \in \mathcal{A}$ et donc en sommant sur les $\mathcal{A} \in \mathcal{V}(p^{\mu_1''}, p^{\mu_2''}, p^{\mu_3''})$ et en le faisant apparaître comme une union disjointe et puisque l'union des tels $\mathcal{A}$ est $\Lambda^*(p^{\mu_1''}, p^{\mu_2''}, p^{\mu_3''})$, on obtient

$$\sum_{\mathcal{A} \in \mathcal{V}(p^{\mu_1''}, p^{\mu_2''}, p^{\mu_3''})} \sum_{\varepsilon \leqslant \min(1,\mu'')} (-1)^{\varepsilon} \frac{\#\left(\Lambda'(p^{\nu_1}, p^{\nu_2}, p^{\nu_3}) \cap \mathcal{B}'(p^{\mu''+1+\nu}, p^{\mu''+1+\nu})\right)}{p^{2(\mu''+1+\nu)}} =$$

$$\frac{1}{p^{2(\mu''+1+\nu)}} \left(\# \left\{ \mathbf{t} \in \Lambda^*(p^{\mu_1''}, p^{\mu_2''}, p^{\mu_3''}) \cap \left(\mathbb{Z}/p^{\nu+\mu''+1}\mathbb{Z}\right)^2 \quad | \quad \mathbf{t} \in \Lambda'(p^{\nu_1}, p^{\nu_2}, p^{\nu_3}) \right\} \right).$$

Remplaçant les expressions de Λ^* et de L_i' et Q' et Λ' et en utilisant que $D_i'|L_i^*$ si, et seulement si, $D_i|L_i$, on voit qu'on compte les $\mathbf{t} \in [\![0, p^{\nu+\mu''+1}[\![^2$ tels que

$$p^{\nu_i+\lambda_i}|L_i(\mathbf{t}) \quad \text{et} \quad p^{\nu_3+\lambda_3}|Q(\mathbf{t})$$

et

$$p^{\mu_i}|L_i(\mathbf{t}) \quad \text{et} \quad p^{\mu_3}|Q(\mathbf{t}).$$

Finalement, on a donc obtenu que

$$w_p = \left(1 - \frac{\chi(p)}{p}\right)^3 \sum_{\beta \leqslant B'} \sum_{\boldsymbol{\nu} \in \mathbb{Z}^3_{\geqslant 0}} \frac{\chi(p)^{\nu_1+\nu_2+\nu_3} \rho'(p^{\nu_1}, p^{\nu_2}, p^{\nu_3}; p^{\nu+\mu''+1})}{p^{2(\nu+\mu''+1+\beta)}}$$

où

$$\rho'(p^{\nu_1}, p^{\nu_2}, p^{\nu_3}; p^k) = \{\mathbf{t} \in [\![0, p^k[\![^2 \quad | \quad p^{N_i}|L_i(\mathbf{t}), \quad p^{N_3}|Q(\mathbf{t}), \quad p \nmid \mathbf{t}\},$$

avec $N_i = \max(\mu_i, \nu_i + \lambda_i)$.
Si $\mu'' = 0$, on connaît le cardinal de $\mathcal{V}(1,1,1) = 1$, et $\varepsilon = 0$. Ainsi, on obtient bien, puisque $\Lambda^*(1,1,1) = \{\mathbf{x} \in \mathbb{Z}^2 \quad | \quad (x_1, x_2, 1) = 1\} = \mathbb{Z}^2$ (et donc dans ce cas $m_1 = m_2 = 0$ et $(\mathbf{e}_i)$ est la base canonique),

$$\sum_{\mathcal{A} \in \mathcal{V}(p^{\mu_1''}, p^{\mu_2''}, p^{\mu_3''})} \sum_{\varepsilon \leqslant \min(1,\mu'')} (-1)^{\varepsilon} \frac{\#\left(\Lambda'(p^{\nu_1}, p^{\nu_2}, p^{\nu_3}) \cap \mathcal{B}'(p^{\mu''+1+\nu}, p^{\mu''+1+\nu})\right)}{p^{2(\mu''+1+\nu)}} =$$

$$\frac{1}{p^{2(\mu''+1+\nu)}} \left(\# \left\{ \mathbf{t} \in \mathbb{Z}^2 \cap \left(\mathbb{Z}/p^{\nu+\mu''+1}\mathbb{Z}\right)^2 \quad | \quad \mathbf{t} \in \Lambda'(p^{\nu_1}, p^{\nu_2}, p^{\nu_3}) \right\} \right)$$

où la condition $p^{\mu_i}|L_i(\mathbf{x})$ est équivalente à $p^{\mu_i'}|L_i^*(\mathbf{x})$ et où puisque $\mu_i''=0$, on a que $p^{\mu_i'}=p^{\min(\beta,\mu_i')}$ par définition de D_i' donc $\mu_i'\leqslant\beta$ et $\mu_3'\leqslant 2\beta$ et donc en fait $\beta=B'$ nécessairement. La condition $p^{\mu_i}|p^{\beta}L_i(\mathbf{x})$ est donc automatique, ce qui entraîne qu'on a :

$$w_p=\left(1-\frac{\chi(p)}{p}\right)^3\sum_{\boldsymbol{\nu}\in\mathbb{Z}^3_{\geqslant 0}}\frac{\chi(p)^{\nu_1+\nu_2+\nu_3}\rho''(p^{\nu_1},p^{\nu_2},p^{\nu_3};p^{\nu+\mu''+1})}{p^{2(\nu+\mu''+1+B')}}$$

où

$$\rho''(p^{\nu_1},p^{\nu_2},p^{\nu_3};p^k)=\{\mathbf{t}\in[\![0,p^k[\![^2\quad|\quad p^{N_i}|p^{B'}L_i(\mathbf{t}),\quad p^{N_3}|p^{2B'}Q(\mathbf{t})\}.$$

où $B'=\nu_p((p^{B'}t_1,p^{B'}t_2,\psi(p^{\mu_1'},p^{\mu_2'},p^{\mu_3'})))$ et donc ce cas-là rentre dans le raisonnement qui suit.
Ensuite, si $k\geqslant\nu+1$, on voit comme ci-dessus que

$$\frac{\rho'(p^{\nu_1},p^{\nu_2},p^{\nu_3};p^k)}{p^{2k}}$$

est indépendant de k et donc puisque $\mu''\leqslant\mu'+B'-\beta$, on peut réécrire

$$w_p=\left(1-\frac{\chi(p)}{p}\right)^3\sum_{\beta\leqslant B'}\sum_{\boldsymbol{\nu}\in\mathbb{Z}^3_{\geqslant 0}}\frac{\chi(p)^{\nu_1+\nu_2+\nu_3}\rho'(p^{\nu_1},p^{\nu_2},p^{\nu_3};p^{\nu+\mu'+B'-\beta+1})}{p^{2(\nu+\mu'+B'+1)}}.$$

En faisant alors le changement de variables $p^{\beta}\mathbf{t}=\mathbf{w}$ (la valeur de β correspondant à la valuation p-adique de $(p^{\beta}t_1,p^{\beta}t_2,\psi(p^{\mu_1'},p^{\mu_2'},p^{\mu_3'}))$). La somme en β (qui revient séparer le comptage selon la valuation-p-adique) devient donc ($\mathbf{w}\in[\![0,p^{\nu+\mu'+1+B'}[\![^2$ quand on multiplie $\mathbf{w}'$ par p^{β})

$$\frac{1}{p^{2(\nu+\mu'+1+B')}}\#\left\{\mathbf{w}\in[\![0,p^{\nu+\mu'+1+B'}[\![^2\quad|\quad p^{N_i}|L_i(\mathbf{w}),\quad p^{N_3}|Q(\mathbf{w})\right\}$$

$$=\frac{1}{p^{2(N_1+N_2+N_3)}}\#\left\{\mathbf{w}\in[\![0,p^{N_1+N_2+N_3}[\![^2\quad|\quad p^{N_i}|L_i(\mathbf{w}),\quad p^{N_3}|Q(\mathbf{w})\right\}$$

puisque les conditions de congruences qui définissent cet ensemble ne dépendent que de la classe modulo $N_1+N_2+N_3$. On a donc bien obtenu ce qu'on souhaitait, à savoir

$$w_p=\sigma_p(\mathbf{d},\mathbf{D}).$$

Ceci conclut la preuve du Théorème 2.

1.6 Démonstration du Théorème 3 : interprétation de la constante

Ce théorème est capital dans l'optique d'obtenir la forme de la constante conjecturée par Peyre pour la conjecture de Manin.

1.6.1 Un Lemme utile

On commence par le lemme suivant.

Lemme 23. *Pour $A \in \mathbb{Z}$, $\alpha \in \mathbb{Z}_{\geqslant 0}$ et p^n une puissance d'un nombre premier, on pose*

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

Si $\alpha \leqslant n$, on a

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

lorsque $\alpha \leqslant \nu_p(A)$ et $S_\alpha(A; p^n) = 0$ sinon. Il suffit donc de traiter le cas $\alpha = 0$ et dans ce cas, on a

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

si $p \equiv 1[4]$. Lorsque $p \equiv 3[4]$, on a

$$S_0(A; p^n) = \begin{cases} p^{2[n/2]} & si\ \nu_p(A) \geqslant n \\ p^n(1+1/p) & si\ \nu_p(A) < n \quad et\ 2|\nu_p(A) \\ 0 & sinon \end{cases}$$

et enfin, das le cas $p = 2$, on a

$$S_0(A; 2^n) = \begin{cases} 2^n & si\ \nu_2(A) \geqslant n-1 \\ 2^{n+1} & si\ \nu_p(A) < n-1 \quad et\ 2^{-\nu_2(A)}A \equiv 1[4] \\ 0 & sinon. \end{cases}$$

Démonstration.– La preuve est esquissée dans [24]. □

1.6.2 Le cas $p \equiv 1[4]$

On commence par traiter le cas $p \equiv 1[4]$. On pose alors

$$M_{\boldsymbol{\nu}}(p^n) = \#\{\mathbf{x} \in (\mathbb{Z}/p^n\mathbb{Z})^2 \quad | \quad \nu_p(L_i(\mathbf{x})) = \nu_i, \quad \nu_p(Q(\mathbf{x})) = \nu_3\}$$

et

$$M'_{\boldsymbol{\nu}}(p^n) = \#\{\mathbf{x} \in (\mathbb{Z}/p^n\mathbb{Z})^2 \quad | \quad \nu_p(L_i(\mathbf{x})) \geqslant \nu_i, \quad \nu_p(Q(\mathbf{x})) \geqslant \nu_3\}.$$

On a clairement lorsque $n \geqslant \nu_1 + \nu_2 + \nu_3$ que

$$M'_{\boldsymbol{\nu}}(p^n) = p^{2n-2\nu_1-2\nu_2-2\nu_3}\rho(p^{\nu_1}, p^{\nu_2}, p^{\nu_3})$$

et

$$M_{\boldsymbol{\nu}}(p^n) = \sum_{\mathbf{e}\in\{0,1\}^3} (-1)^{e_1+e_2+e_3} M'_{\boldsymbol{\nu}+\mathbf{e}}(p^n).$$

En effet, on compte ceux dont la valuation est supérieure à ν_i puis on enlève ceux pour lesquels un indice est supérieur à $\nu_i + 1$ mais faisant ceci on enlève deux fois ceux pour lesquels on a deux indices supérieurs à $\nu_i + 1$ donc on les rajoute mais alors on a enlevé trois fois et rajouté deux parmi trois fois, c'est-à-dire trois fois ceux pour lesquels les trois

indices sont supérieurs à $\nu_i + 1$ et donc il faut les enlever à nouveau, ce qui donne bien la formule ci-dessus. Posant $m_j = \max(\lambda_j, \mu_j)$, on obtient (ici $\chi(p) = 1$) que

$$N_{\lambda,\mu}(p^n) = p^{3n+\lambda_1+\lambda_2+\lambda_3}(1-1/p)^3 \sum_{m_j \leqslant \nu_j < n} M_{\boldsymbol{\nu}}(p^n) \prod_{1 \leqslant j \leqslant 3} (1 + \nu_j - \lambda_j) + O(n^3 p^{4n}).$$

Pour obtenir cette formule, on fixe la valuation p-adique et on utilise les formules de $S_\alpha(A; p^n)$ pour compter. On ne regarde pour commencer que les valuations strictement inférieures à n qui vont donner le terme principal. Pour des valuations fixés, qui sont nécessairement plus grandes que m_j car p^{μ_i} divise L_j et p^{μ_3} divise Q et on peut supposer $n > \lambda_j$ puisque la formule est asymptotique et donc on a des relations du type

$$L_i(\mathbf{x}) \equiv p^{\lambda_j}(s_i^2 + t_i^2)[p^n]$$

qui impliquent que $\lambda_j \leqslant \nu_j$. On a alors $M_{\boldsymbol{\nu}}(p^n)$ tels $\mathbf{x}$ et pour chacun de ces $\mathbf{x}$, le nombre de (s_i, t_i) convenant est de $S_{\lambda_i}(L_i(\mathbf{x}); p^n)$ et celui de (s_3, t_3) est $S_{\lambda_3}(Q(\mathbf{x}); p^n)$. Or, on a puisque $\nu_i < n$,

$$S_{\lambda_i}(L_i(\mathbf{x}); p^n) = p^{2\lambda_i}(1 + \nu_i - \lambda_i)p^{n+\lambda_i}(1 - 1/p)$$

ce qui fournit bien le terme

$$p^{3n+\lambda_1+\lambda_2+\lambda_3}(1-1/p)^3 \sum_{m_j \leqslant \nu_j < n} M_{\boldsymbol{\nu}}(p^n) \prod_{1 \leqslant j \leqslant 3} (1 + \nu_j - \lambda_j).$$

Maintenant, il ne reste plus qu'à prendre en compte la contribution des termes telles qu'il existe un indice i tel que $\nu_i \geqslant n$. Pour cet indice, on a

$$S_{\lambda_i}(L_i(\mathbf{x}); p^n) \ll np^{n+\lambda_i}$$

et pour les indices qui sont éventuellement $\nu_i < n$, on a toujours

$$S_{\lambda_i}(L_i(\mathbf{x}); p^n) = (1 + \nu_i)p^{n+\lambda_i} \ll np^{n+\lambda_i}$$

donc dans tous les cas, on obtient une contribution des termes restant

$$\ll n^3 p^{3n+\lambda_1+\lambda_2+\lambda_3} \sum_{\substack{\nu_j \geqslant m_j \\ \exists \nu_i > n}} M_{\boldsymbol{\nu}}(p^n).$$

On montre alors que la contribution des termes restants est

$$O(n^4 p^{4n+\lambda_1+\lambda_2+\lambda_3} p^{[\nu_p(\Delta)/2]}).$$

On traite d'abord l'un des deux cas parfaitement symétriques où $\nu_1 > n$ (repectivement $\nu_2 > n$), peu importe les autres indices. Alors les $\mathbf{x}$ comptés dans la somme sur les $\boldsymbol{\nu}$ des $M_{\boldsymbol{\nu}}(p^n)$ est majorée par $\rho(p^n, 1, 1)$ (respectivement $\rho(1, p^n, 1)$). On obtient donc que

$$\sum_{\substack{\nu_j \geqslant m_j \\ \exists \nu_i > n}} M_{\boldsymbol{\nu}}(p^n) \ll p^n$$

ce qui fournit avec ce qui précède

$$O(n^3 p^{4n+\lambda_1+\lambda_2+\lambda_3})$$

ce qui est satisfaisant. Si maintenant, on a $\nu_3 > n$, alors on obtient

$$\sum_{\substack{\nu_j \geqslant m_j \\ \exists \nu_i > n}} M_{\boldsymbol{\nu}}(p^n) \ll (n+1)p^n p^{[\nu_p(\Delta)/2]}$$

ce qui fournit bien l'estimation annoncée

$$O(n^4 p^{4n+\lambda_1+\lambda_2+\lambda_3} p^{[\nu_p(\Delta)/2]}).$$

En utilisant les remarques précédentes, on obtient que dans le terme principal

$$M_{\boldsymbol{\nu}}(p^n) = p^{2n} \sum_{\mathbf{e}\in\{0,1\}^3} (-1)^{e_1+e_2+e_3} \frac{\rho(p^{\nu_1+e_1}, p^{\nu_2+e_2}, p^{\nu_3+e_3})}{p^{2(\nu_1+e_1+\nu_2+e_2+\nu_3+e_3)}}$$

si bien que ce terme principal devient

$$p^{5n+\lambda_1+\lambda_2+\lambda_3}(1-1/p)^3 \sum_{m_j\leqslant\nu_j<n} \sum_{\mathbf{e}\in\{0,1\}^3} (-1)^{e_1+e_2+e_3} \frac{\rho(p^{\nu_1+e_1}, p^{\nu_2+e_2}, p^{\nu_3+e_3})}{p^{2(\nu_1+e_1+\nu_2+e_2+\nu_3+e_3)}} \prod_{1\leqslant j\leqslant 3} (1+\nu_j-\lambda_j)$$

En divisant par $p^{5n+\lambda_1+\lambda_2+\lambda_3}$ et faisant tendre n vers l'infini, on en déduit l'expression

$$\omega_{\lambda,\mu}(p) = (1-1/p)^3 \sum_{m_j\leqslant\nu_j} \sum_{\mathbf{e}\in\{0,1\}^3} (-1)^{e_1+e_2+e_3} \frac{\rho(p^{\nu_1+e_1}, p^{\nu_2+e_2}, p^{\nu_3+e_3})}{p^{2(\nu_1+e_1+\nu_2+e_2+\nu_3+e_3)}} \prod_{1\leqslant j\leqslant 3} (1+\nu_j-\lambda_j)$$

où on a bien convergence puisqu'on sait que $\omega_{\lambda,\mu}(p)$ existe et est fini. On effectue alors le changement de variable $n_j = \nu_j + e_j - \lambda_j$ pour obtenir puisque $\nu_i + e_i \leqslant m_i + e_i \leqslant m_i$

$$\omega_{\lambda,\mu}(p) = (1-1/p)^3 \sum_{m_j-\lambda_j\leqslant n_j} \frac{\rho(p^{n_1+\lambda_1}, p^{n_2+\lambda_2}, p^{n_3+\lambda_3})}{p^{2(n_1+\lambda_1+n_2+\lambda_2+n_3+\lambda_3)}} \sum_{0\leqslant e_j\leqslant \min(1,\lambda_j+n_j-m_j)} (-1)^{e_1+e_2+e_3} \prod_{1\leqslant j\leqslant 3} (1+n_j-e_j).$$

Or, on a

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

La deuxième ligne de l'affirmaton est claire puisqu'on a un seul terme où $e = 0$ et que $n = m - \lambda$. La première ligne est claire aussi puisque dans ce cas, on a

$$1 + n - (1 + n - 1) = 1.$$

Or, $1+m-\lambda = \#\mathbb{Z}\cap[0, m-\lambda]$, on voit que dans la somme ci-dessus, on obtient l'égalité

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

On aboutit donc à

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

soit

$$\omega_{\lambda,\mu}(p) = (1-\chi(p)/p)^3 \times$$
$$\sum_{n_i \geqslant 0} \frac{\chi(p)^{\max(\mu_1,\lambda_1+n_1)+\max(\mu_2,\lambda_2+n_2)+\max(\mu_3,\lambda_3+n_3)} \rho(p^{\max(\mu_1,\lambda_1+n_1)}, p^{\max(\mu_2,\lambda_2+n_2)}, p^{\max(\mu_3,\lambda_3+n_3)})}{p^{2(\max(\mu_1,\lambda_1+n_1)+\max(\mu_2,\lambda_2+n_2)+\max(\mu_3,\lambda_3+n_3))}}$$

soit

$$\omega_{\lambda,\mu}(p) = \sigma_p(\mathbf{d}, \mathbf{D})$$

qui est bien ce qu'on cherchait à obtenir.

1.6.3 Le cas $p \equiv 3[4]$

Passons maintenant à la preuve du même résultat dans le cas où $p \equiv 3[4]$. Le même raisonnement que ci-dessus amène

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

puisque 2 doit diviser $\nu_p(L_i(\mathbf{x})/p^{\lambda_i})$ pour que

$$S_{\lambda_i}(L_i(\mathbf{x}); p^n) \neq 0$$

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

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

car $2|\nu_i - \lambda_i = n_i - e_i$. On a alors

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

En effet, pour la première ligne, on ne prend nécessairement qu'un seul terme dans la somme pour pouvoir respecter la congruence $e \equiv n[2]$ et si n est pair, on garde $e=0$ alors que si n est impair, on va garder $e=1$ ce qui donne bien le résultat annoncé de $(-1)^n$. Si maintenant $\lambda+n-m=0$, alors, si $2|m-\lambda$, on a que $2|n$ et donc $e=0$ convient et on obtient bien 1 tandis que dans le cas contraire, $e=0$ ne remplit pas les conditions, on a donc une somme vide qui vaut 0. Puisque

$$\sum_{0\leqslant n\leqslant m-\lambda} (-1)^n = \begin{cases} 0 & \text{si } 2\nmid m-\lambda \\ 1 & \text{sinon,} \end{cases}$$

on déduit l'égalité

$$\sum_{\substack{0\leqslant e_i \leqslant \min(1,\lambda_i+n_i-m_i) \\ e_i \equiv n_i[2]}} (-1)^{e_1+e_2+e_3} \frac{\rho(p^{m_1}, p^{m_2}, p^{m_3})}{p^{2(m_1+m_2+m_3)}}$$

$$= \sum_{n_i \leqslant m_i - \lambda_i} (-1)^{n_1+n_2+n_3} \frac{\rho(p^{\max(m_1,\lambda_1+n_1)}, p^{\max(m_2,\lambda_2+n_2)}, p^{\max(m_3,\lambda_3+n_3)})}{p^{2(\max(m_1,\lambda_1+n_1)+\max(m_2,\lambda_2+n_2)+\max(m_3,\lambda_3+n_3))}}.$$

On obtient alors donc

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

soit

$$\omega_{\lambda,\mu}(p) = (1-\chi(p)/p)^3 \times$$
$$\sum_{n_i \geqslant 0} \frac{\chi(p)^{n_1+n_2+n_3} \rho(p^{\max(\mu_1,\lambda_1+n_1)}, p^{\max(\mu_2,\lambda_2+n_2)}, p^{\max(\mu_3,\lambda_3+n_3)})}{p^{2(\max(\mu_1,\lambda_1+n_1)+\max(\mu_2,\lambda_2+n_2)+\max(\mu_3,\lambda_3+n_3))}}$$

soit

$$\omega_{\lambda,\mu}(p) = \sigma_p(\mathbf{d}, \mathbf{D})$$

qui est bien ce qu'on cherchait à obtenir.

1.6.4 Le cas $p = 2$

On traite maintenant le cas de $p = 2$. On montre que

$$\omega_{\mathbf{d}}(2) = 2\sigma_2(\mathbf{d})$$

où

$$\sigma_2(\mathbf{d}) = 4 \lim_{n \to +\infty} 2^{-2n} \# \left\{ \mathbf{x} \in (\mathbb{Z}/2^n\mathbb{Z})^2 \quad \middle| \quad \begin{array}{c} L_i(\mathbf{x}) \in d_i \mathcal{E}_{2^n} \\ Q(\mathbf{x}) \in d_3 \mathcal{E}_{2^n} \end{array} \right\}.$$

On obtient de l'étude de $S_\alpha(A; 2^n)$ en séparant $N_{\mathbf{d}}(2^n)$ comme ci-dessus selon que la valuation soit supérieure à $n-1$ pour donner un terme qui tend vers 0 et un terme concernant les valuations inférieures à $n-1$ qui est donné par

$$2^{3(n+1)} \# \left\{ \mathbf{x} \in (\mathbb{Z}/2^n\mathbb{Z})^2 \quad \middle| \quad \begin{array}{c} L_i(\mathbf{x}) \in d_i \mathcal{E}_{2^n} \\ Q(\mathbf{x}) \in d_3 \mathcal{E}_{2^n} \end{array} \right\}.$$

En divisant par 2^{5n} et en passant à la limite, on obtient

$$\omega_{\mathbf{d}}(2) = \lim_{n \to +\infty} 2^{-2n+3} \# \left\{ \mathbf{x} \in (\mathbb{Z}/2^n\mathbb{Z})^2 \quad \middle| \quad \begin{array}{c} L_i(\mathbf{x}) \in d_i \mathcal{E}_{2^n} \\ Q(\mathbf{x}) \in d_3 \mathcal{E}_{2^n} \end{array} \right\}$$

soit

$$\omega_{\mathbf{d}}(2) = 2 \times 4 \lim_{n \to +\infty} 2^{-2n} \# \left\{ \mathbf{x} \in (\mathbb{Z}/2^n\mathbb{Z})^2 \quad \middle| \quad \begin{array}{c} L_i(\mathbf{x}) \in d_i \mathcal{E}_{2^n} \\ Q(\mathbf{x}) \in d_3 \mathcal{E}_{2^n} \end{array} \right\} = 2\sigma_2(\mathbf{d})$$

ce qui est bien ce qu'il fallait démontrer.

1.6.5 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 $s_i > 0$ et $t_i > 0$ pour tout i. On utilise la forme de Leray en paramétrant par les t_i. La forme de Leray est par conséquent ici donnée par

$$(-2^3 t_1 t_2 t_3)^{-1} \mathrm{d}s_1 \mathrm{d}s_2 \mathrm{d}s_3 \mathrm{d}x_1 \mathrm{d}x_2.$$

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

$$f_i(\mathbf{x}, \mathbf{s}, \mathbf{t}) = L_i(\mathbf{x})/d_i - (s_i^2 + t_i^2) \quad \text{et} \quad f_3(\mathbf{x}, \mathbf{s}, \mathbf{t}) = Q(\mathbf{x})/d_3 - (s_3^2 + t_3^2)$$

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 calcul de l'intégrale suivante

$$\int_0^{\sqrt{A}} \frac{\mathrm{d}s}{\sqrt{A - s^2}} = \frac{1}{\sqrt{A}} \int_0^{\sqrt{A}} \frac{\mathrm{d}s}{\sqrt{1 - (s/\sqrt{A})^2}}$$

donc

$$\int_0^{\sqrt{A}} \frac{\mathrm{d}s}{\sqrt{A - s^2}} = \left[\arcsin\left(\frac{x}{\sqrt{A}} \right) \right]_0^{\sqrt{A}} = \frac{\pi}{2}.$$

En substituant $t_i = \sqrt{d_i^{-1} L_i(\mathbf{x}) - s_i^2}$ et $t_3 = \sqrt{d_3^{-1} Q(\mathbf{x}) - s_3^2}$, on obtient finalement

$$\omega_{\mathcal{R}}(\infty) = 2^3 \int_{\mathbf{x} \in \mathcal{R}} \left(\prod_{1 \leqslant i \leqslant 2} \int_0^{\sqrt{d_i^{-1} L_i(\mathbf{x})}} \frac{\mathrm{d}s_i}{\sqrt{d_i^{-1} L_i(\mathbf{x}) - s_i^2}} \int_0^{\sqrt{d_3^{-1} Q(\mathbf{x})}} \frac{\mathrm{d}s_3}{\sqrt{d_3^{-1} Q(\mathbf{x}) - s_3^2}} \right) \mathrm{d}x_1 \mathrm{d}x_2$$

soit

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

Ceci achève la preuve du Théorème 3.

Chapitre 2

Démonstration de la conjecture de Manin

L'objet de cette partie est de démontrer la conjecture de Manin sur les surfaces de Châtelets considérées.

2.1 Passage aux torseurs universels

2.1.1 Un peu de géométrie des surfaces de Châtelet

Ici, comme expliqué dans [7], on peut faire les choses à la main et on n'utilise donc pas la construction des torseurs universels via les anneaux de Cox comme c'est fait par exemple dans [18]. On ne rappelle pas ici les définitions d'un torseur et d'un torseur universel ([34], [7] ou [35]). Commençons par expliciter la norme et la hauteur (pour la définition et les propriétés des hauteurs, voir [36]) avec lesquelles on travaille. On commence par rappeler quelques éléments de la construction des surfaces de Châtelet. On considère ici des surfaces de Châtelet qui peuvent être définies comme modèles mimimaux propres et lisses de variétés affines de la forme

$$y^2 + z^2 = f(x)$$

où f est le produit de deux formes linéaires et d'une forme quadratique dans notre cas (mais ce qui suit est général). On pose alors $F(u,v) = v^4 f\left(\frac{u}{v}\right)$ et on note $X_1 \subset \mathbb{P}^2 \times \mathbb{A}^1$ l'hypersurface

$$y_1^2 + z_1^2 = t_1^2 F(u,1) \quad \text{pour} \quad ([y_1 : z_1 : t_1], u) \in \mathbb{P}^2 \times \mathbb{A}^1$$

et $X_2 \subset \mathbb{P}^2 \times \mathbb{A}^1$ l'hypersurface

$$y_2^2 + z_2^2 = t_2^2 F(1,v) \quad \text{pour} \quad ([y_2 : z_2 : t_2], v) \in \mathbb{P}^2 \times \mathbb{A}^1.$$

On peut alors montrer que les surfaces de Châtelet X considérées sont les surfaces géométriquement intégres, lisses et projectives obtenues par recollement de X_1 et X_2 via l'isomorphisme

$$\begin{array}{ccc} X_1 \setminus \{u=0\} & \longrightarrow & X_2 \setminus \{v=0\} \\ ([y_1 : z_1 : t_1], u) & \longmapsto & ([y_1 : z_1 : u^2 t_1], u^{-1}). \end{array}$$

Puisqu'on a que f a un discriminant non nul, on sait que sur $\overline{\mathbb{Q}}$ on a une factorisation

$$F(u,v) = (\beta_1 u - \alpha_1 v)(\beta_2 u - \alpha_2 v)(\beta_3 u - \alpha_3 v)(\beta_4 u - \alpha_4 v)$$

avec $[\alpha_i : \beta_i] \in \mathbb{P}^1(\overline{\mathbb{Q}})$ distincts. Les morphismes

$$\begin{array}{lcl} X_1 & \longrightarrow & \mathbb{P}^1 \\ ([y_1 : z_1 : t_1], u) & \longmapsto & [u : 1] \end{array}$$

et

$$\begin{array}{lcl} X_2 & \longrightarrow & \mathbb{P}^1 \\ ([y_2 : z_2 : t_2], v) & \longmapsto & [1 : v] \end{array}$$

se recollent pour donner un morphisme $\pi : X \to \mathbb{P}^1$ dont les fibres sont des coniques et on voit qu'on a quatre fibres dégénérées sur $\overline{\mathbb{Q}}$ correspondants aux $p_i = [\alpha_i : \beta_i]$. La fibre géométrique au-dessus de p_i est la sous-variété de $\overline{X} = X \times_{\mathrm{Spec}(\mathbb{Q})} \mathrm{Spec}(\overline{\mathbb{Q}})$ définie par les équations $u = \alpha_i$ et $y_1 \pm i z_1 = 0$, autrement dit c'est l'union de deux diviseurs géométriquement intègres qui s'intersectent transversalement et sont tous les deux isomorphes à $\mathbb{P}^1$ sur $\overline{\mathbb{Q}}$.
On notera $\mathrm{Pic}(X)$ le groupe de Picard de X, qui est un groupe abélien libre sans torsion de rang ρ_X. On a alors le lemme suivant

Lemme 24. *Si on suppose que $f = f_1 ... f_r$ est la factorisation de f en produits d'irréductibles deux à deux non associées sur $\mathbb{Q}$ (le discriminant étant nul, on n'a pas de facteurs multiples). On note pour tout $1 \leqslant i \leqslant r$, $\mathbb{Q}_{f_i} = \mathbb{Q}[X]/(f_i)$ un corps de rupture de f_i. Alors, on a*

$$\rho_X = 2 + \#\{1 \leqslant i \leqslant r \quad | \quad i \in \mathbb{Q}_{f_i}\}.$$

Démonstration.– La preuve se trouve dans [37]. □

On notera dans la suite Z^m l'ensemble des vecteurs de $\mathbb{Z}^m$ premiers entre eux dans leur ensemble (ou primitifs). On définit à présent la hauteur utilisée. On dispose de la hauteur exponentielle sur $\mathbb{P}^4(\mathbb{Q})$ qui est définie par

$$H_4 : \left\{ \begin{array}{lcl} \mathbb{P}^4(\mathbb{Q}) & \longrightarrow & \mathbb{R}_*^+ \\ [x_0 : x_1 : x_2 : x_3 : x_4] & \longmapsto & ||(x_0, x_1, x_2, x_3, x_4)|| \end{array} \right.$$

dès lors qu'on s'est fixé une norme de $\mathbb{R}^5$ et si on choisit comme représentant de $[x_0 : x_1 : x_2 : x_3 : x_4]$ des x_i entiers et premiers entre eux dans leur ensemble. On va alors montrer qu'on a un morphisme $\psi : X \to \mathbb{P}^4(\mathbb{Q})$. En effet, suppsons que $f(x) = c_0 x^4 + ... + c_4$ avec des coefficients c_i entiers. On définit alors les applications suivantes

$$\begin{array}{lcl} X_1 & \longrightarrow & \mathbb{P}^4 \\ ([y_1 : z_1 : t_1], u) & \longmapsto & [t_1 : u t_1 : u^2 t_1 : y_1 : z_1] \end{array}$$

et

$$\begin{array}{lcl} X_2 & \longrightarrow & \mathbb{P}^4 \\ ([y_2 : z_2 : t_2], v) & \longmapsto & [v^2 t_2 : v t_2 : t_2 : y_2 : z_2] \end{array}$$

$$\left\{ \begin{array}{l} x_0 x_2 = x_1^2, \\ x_3^2 + x_4^2 = c_4 x_0^2 + c_3 x_0 x_1 + c_2 x_0 x_2 + c_1 x_1 x_2 + c_0 x_2^2, \end{array} \right.$$

que l'on notera Y et où on posera $Q(x_0, x_1, x_2)$ pour la forme quadratique apparaissant à droite de la seconde égalité. On définit alors notre hauteur $H : X \to \mathbb{R}_*^+$ par $H = H_4 \circ \psi$ et notre problème de comptage est alors l'estimation asymptotique, lorsque B tend vers $+\infty$ de

$$N(B) = \#\{x \in X(\mathbb{Q}) \quad | \quad H(x) \leqslant B\}.$$

On transforme alors notre problème de comptage en un autre problème de comptage sur des coniques (c'est là qu'on tire partie de la fibraton en coniques) grâce au lemme suivant.

Lemme 25. *On a* $N(B) = \frac{1}{4}T(B)$ *où*

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

Démonstration.– Sur chaque droite D de $\mathbb{P}^4(\mathbb{Q})$, il y a exactement deux points à coordonnées entières et primitives (ils sont opposés l'un de l'autre ce qui fait en particulier que la hauteur est bien définie) et

$$N(B) = \frac{1}{2}\#\{\mathbf{x} \in Z^5 \quad | \quad [\mathbf{x}] \in Y, \quad ||\mathbf{x}|| \leqslant B\}.$$

On a alors une 1 : 2 correspondance entre les solutions de $x_0x_2 = x_1^2$ et les (t, u, v) avec (u, v) premiers entre eux donnée par $(x_0, x_1, x_2) = t(v^2, uv, u^2)$ et le caractère primitif de $\mathbf{x}$ est alors équivalent à celui de (t, x_3, x_4) (d'après les expressions ci-dessus de x_0, x_1 et x_2 et le caractère primitif de u et v). En remarquant alors que $Q(v^2, uv, u^2) = F(u, v)$, on obtient bien le lemme annoncé. □

Dans notre cas, on a donc l'égalité

$$N(B) = \frac{1}{4}\#\left\{(y, z, t; u, v) \in Z^3 \times Z^2 \quad \middle| \quad \begin{array}{l} ||(v^2t, uvt, u^2t, y, z))|| \leqslant B, \\ y^2 + z^2 = t^2L_1(u, v)L_2(u, v)Q(u, v) \end{array} \right\}.$$

On choisit désormais la norme avec laquelle on va travailler (ce n'est pas une vraie perte de généralité du fait de l'équivalence des normes puisqu'on travaille en dimension finie). On pose $\delta = \sqrt{(|a_1| + |b_1|)(|a_2| + |b_2|)(|a_3| + |b_3| + |c_3|)}$ et on considère la norme suivante

$$||\mathbf{x}|| = \max(|x_0|, |x_1|, |x_2|, \delta^{-1}|x_3|, \delta^{-1}|x_4|).$$

Grâce à ce choix de norme, on a une expression plus agréable de $||(v^2t, uvt, u^2t, y, z))||$. On considère alors $\mathcal{T} \subset \mathbb{A}^5 = \mathrm{Spec}[y, z, t, u, v]$ la sous-variété définie par l'équation

$$y^2 + z^2 = t^2L_1(u, v)L_2(u, v)Q(u, v)$$

avec les conditions $(y, z, t) \neq 0$ et $(u, v) \neq 0$. Il s'agit d'un $\mathbb{G}_m^2$-torseur sur X grâce à l'action induite par celle de $\mathbb{G}_m^2$ sur $\mathbb{G}_m^5$ donnée par

$$(\lambda, \mu) \mapsto (\lambda, \lambda, \mu^{-2}\lambda, \mu, \mu).$$

Pour les $(y, , t, u, v)$ considérés, on a

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

En effet, il est tout d'abord clair que

$$|u^2t| \leqslant \max(u^2,v^2)|t|, \quad |v^2t| \leqslant \max(u^2,v^2)|t| \quad \text{et} \quad |uvt| \leqslant \frac{1}{2}(u^2+v^2)|t| \leqslant \max(u^2,v^2)|t|.$$

Il reste donc à voir que $|y|$ et $|z| \leqslant \max(u^2,v^2)|t|$. Traitons par exemple le cas de y, celui de z lui étant parfaitement symétrique. On a

$$y^2 + z^2 = t^2 L_1(u,v)L_2(u,v)Q(u,v)$$

donc

$$y^2 \leqslant t^2 L_1(u,v)L_2(u,v)Q(u,v).$$

On a alors

$$L_i(u,v) = a_i u + b_i v \leqslant (|a_i| + |b_i|)\max(|u|,|v|)$$

et de même

$$Q(u,v) \leqslant (|a_3| + |b_3| + |c_3|)\max(u^2,v^2) = (|a_3| + |b_3| + |c_3|)\max(|u|,|v|)^2$$

et ainsi

$$y^2 \leqslant t^2\delta^2 \max(|u|,|v|)^4.$$

D'où,

$$\delta^{-1}|y| \leqslant |t|\max(|u|,|v|)^2 = \max(u^2,v^2)|t|.$$

On en déduit par symétrie sur le signe de t que

$$N(B) = \frac{1}{2}\#\left\{(y,z,t;u,v) \in (Z^3 \times Z^2) \cap \mathcal{T} \quad | \quad 0 < \max(u^2,v^2)t \leqslant B\right\}.$$

On montre alors que la contribution des $(y,z,t;u,v)$ tels que

$$L_1(u,v)L_2(u,v)Q(u,v) = 0$$

est $O(1)$ ce qui convient et permet de supposer que $L_1(u,v)L_2(u,v)Q(u,v) \neq 0$ dans la suite. En effet, si on cherche les (u,v) premiers entre eux tels que

$$a_i u + b_i v = 0$$

alors on obtient que $u = kb_i$ et $v = la_i$ et en réinjectant, on obtient $k = -l$ et pour que la condition de coprimalité soit satisfaite, on voit qu'il n'y a que les solutions $(b_i/(a_i,b_i), -a_i/(a_i,b_i))$ et $(-b_i/(a_i,b_i), a_i/(a_i,b_i)$ ce qui donne bien un $O(1)$. Il reste donc à voir que les (u,v) premiers entre eux tels que $Q(u,v) = 0$ donnent également un $O(1)$. Par irréductibilité, si on avait un tel couple, on aurait $uv \neq 0$ et donc $Q(u/v,1) = 0$ ce qui est absurde.

On pose

$$\mathcal{D} = \{d \in \mathbb{N} \quad | \quad p|d \Rightarrow p \equiv 1[4]\},$$

où on peut remarquer que si $d_0 \in \mathcal{D}$, alors tous les diviseurs de d_0 sont aussi dans l'ensemble $\mathcal{D}$. On introduit ensuite

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

On a alors clairement $r(n;1) = r(n)$ au sens défini précédemment et on peut remarquer que $r(y^2n;y) = 0$ si $y \notin \mathcal{D}$. En effet, soit $y \notin \mathcal{D}$ et supposons qu'il existe deux entiers a et b tels que $(y,a,b) = 1$. Soit alors p un nombre premier divisant y non congru à 1 modulo 4. Si on n'a que $p = 2$ dans ce cas, alors on a $y = 2^\ell y'$ avec $y' \in \mathcal{D}$ et on remarque que les couples (a,b) tels que $y^2n = a^2 + b^2$ sont ceux convenant pour $y'^2n = a'^2 + b'^2$ multipliés par $2^{2\ell}$, $(a,b) = 2^{2\ell}(a',b')$ (on n'a qu'une seule façon d'écrire $2^{2\ell}$ comme somme de deux carrés, 0 plus lui-même, et on a le même nombre de couples et cela réalise la bijection entre les deux ensembles) et donc dans ce cas aucun couple ne vérifie $(y,a,b) = 1$. Si, en revanche, il existe $p \equiv 3[4]$ divisant y, alors modulo p, le fait que $y^2n = a^2 + b^2$ se réécrit

$$a^2 \equiv -b^2[p]$$

et puisque $(y,a,b) = 1$, a ou b est inversible modulo p, ce qui impliquerait que -1 est un carré modulo p, ce qui est exclu puisque $p \equiv -1[4]$. On a donc bien obtenu ce qu'on désirait.
Utilisant une inversion de Möbius pour traiter la condition de coprimalité, on aboutit à la formule suivante

$$r(y^2n;y) = \sum_{\substack{k|y \\ k\in\mathcal{D}}} \mu(k) r\left(\frac{y^2n}{k^2}\right)$$

où on ne considére que les $y \in \mathcal{D}$ d'après ce qui précède et où donc on a automatiquement une somme sur des entiers $k \in \mathcal{D}$.

On voit que pour les $(y,z,t;u,v)$ considérés, on doit avoir

$$L_1(u,v)L_2(u,v)Q(u,v) > 0$$

et donc cela nous invite à considérer pour ε_1, ε_2 et $\varepsilon_3 \in \{-1,+1\}$ et $T \geqslant 1$ la région

$$R^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(T) = \left\{ (u,v) \in \mathbb{R}^2 \quad \middle| \quad \begin{array}{l} |u|,|v| \leqslant \sqrt{T}, \\ \varepsilon_i L_i(u,v) > 0, \quad \varepsilon_3 Q(u,v) > 0 \end{array} \right\}.$$

Puisque le nombre de $(y,z,t;u,v) \in (Z^3 \times Z^2) \cap \mathcal{T}$ s'écrit $r(t^2L_1(u,v)L_2(u,v)Q(u,v);t)$ pour chaque t fixé plus petit que B et dans $\mathcal{D}$ (si on veut un terme non nul), pour chaque couple $(u,v) \in \times Z^2$ tel que $|u|,|v| \leqslant B/t$, $\varepsilon_i L_i(u,v) > 0$, et $\varepsilon_3 Q(u,v) > 0$ pour tous choix de ε_i tels que $\varepsilon_1\varepsilon_2\varepsilon_3 = 1$. En effet, on compte là les couples (y,z) tels que par définition (y,z,t) soient premiers entre eux dans leur ensemble et $(y,z,t;u,v) \in \mathcal{T}$. On en déduit donc l'expression

$$N(B) = \frac{1}{2} \sum_{\substack{t\leqslant B \\ t\in\mathcal{D}}} \sum_{\substack{\varepsilon_i\in\{1,+1\} \\ \varepsilon_1\varepsilon_2\varepsilon_3=1}} \sum_{(u,v)\in Z^2\cap R^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(B/t)} r(t^2L_1(u,v)L_2(u,v)Q(u,v);t)$$

$$= \frac{1}{2} \sum_{\substack{t\leqslant B \\ t\in\mathcal{D}}} \sum_{\substack{\varepsilon_i\in\{-1,+1\} \\ \varepsilon_1\varepsilon_2\varepsilon_3=1}} \sum_{(u,v)\in Z^2\cap R^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(B/t)} r(t^2\varepsilon_1L_1(u,v)\varepsilon_2L_2(u,v)\varepsilon_3Q(u,v);t).$$

On écrit alors

$$r(t^2\varepsilon_1L_1(u,v)\varepsilon_2L_2(u,v)\varepsilon_3Q(u,v);t) = \sum_{k|t} \mu(k) r\left(\frac{t^2}{k^2}L_1^+(u,v)L_2^+(u,v)Q^+(u,v)\right)$$

où on note $L_i^+ = \varepsilon_i L_i$ et $Q^+ = \varepsilon_3 Q$. Écrivant $t = kl$, on obtient

$$N(B) = \frac{1}{2} \sum_{\substack{kl \leqslant B \\ (k,l)\in\mathcal{D}}} \mu(k) \sum_{\substack{\varepsilon_i \in \{-1,+1\} \\ \varepsilon_1\varepsilon_2\varepsilon_3 = 1}} \sum_{(u,v)\in Z^2 \cap R^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(B/kl)} r\left(l^2 L_1^+(u,v) L_2^+(u,v) Q^+(u,v)\right)$$

donc

$$N(B) = \frac{1}{2} \sum_{k\in\mathcal{D}} \mu(k) \sum_{\substack{l \leqslant B/k \\ l\in\mathcal{D}}} \sum_{\substack{\varepsilon_i \in \{-1,+1\} \\ \varepsilon_1\varepsilon_2\varepsilon_3 = 1}} \sum_{(u,v)\in Z^2 \cap R^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(B/kl)} r\left(l^2 L_1^+(u,v) L_2^+(u,v) Q^+(u,v)\right).$$

2.1.2 Passage aux torseurs universels et reformulation du problème de comptage

Dans la suite, on notera pour éviter d'alourdir les notations $\omega(\gcd(a_0, ..., a_n)) = \omega(a_0, ..., a_n)$. L'idée est maintenant de séparer le terme $r\left(l^2 L_1^+(u,v) L_2^+(u,v) Q^+(u,v)\right)$ en un terme faisant intervenir t^2, un faisant intervenir L_1^+, un L_2^+ et un dernier faisant intervenir Q^+, c'est le passage aux torseurs universels. On passe d'un problème de comptage sur $\mathcal{T}$ à un problème de comptage sur des variétés affines de $\mathbb{A}^8$ d'équations de la forme

$$L_i(\mathbf{x}) = d_i(s_i^2 + t_i^2) \quad \text{et} \quad Q(\mathbf{x}) = d_3(s_3^2 + t_3^2), \tag{2.1}$$

On verra qu'il n'y a qu'un nombre fini en fait de torseurs universels pour lesquels on a des points rationnels, qui correspondent à un nombre fini de choix des d_i dans la somme du Théorème 2. Pour faire cela, on a besoin d'établir une formule d'écalement permettant de relier $r(n_1n_2n_3n_4)$ avec des quantités du type $r(n_i/d_i)$ qui pallie la non complète multiplicativité de la fonction r_0. On commence par poser

$$r_0(n) = \frac{r(n)}{4} = \sum_{d|n} \chi(d)$$

qui est multiplicative et c'est pour cette fonction qu'on va établir notre formule d'éclatement. On l'établit pas à pas en établissant d'abord le résultat classique suivant

$$r_0(n_1n_2) = \sum_{d|(n_1,n_2)} \mu(d)\chi(d) r_0\left(\frac{n_1}{d_1}\right) r_0\left(\frac{n_2}{d_2}\right).$$

On peut établir cette relation en constatant que les deux membres de l'égalité sont des fonctions multiplicatives égales sur les couples de puissances de nombres premiers. On regarde selon la congruence de p modulo 4. Si $p = 2$ tout est nul et on a égalité. Si $p \equiv 3[4]$, alors $r_0(p^k) = 0$ si k est pair et 1 sinon ce qui montre bien qu'on va avoir égalité puisque $\chi(p) = -1$. Et si, $p \equiv 1[4]$, on a $\chi(p) = 1$ et $r_0(p^k) = k + 1$ donc on a à nouveau égalité puisque $(n_1 + 1)(n_2 + 1) - n_1n_2 = n_1 + n_2 + 1$ et on a obtenu l'identité souhaitée. On pouvait aussi l'obtenir comme un cas particulier d'une situation plus générale : on a de telles formules d'éclatement pour toute fonction multiplicative qui s'écrit la convolée de deux fonctions strictement multiplicatives comme c'est fait dans [38]. On en déduit alors la formule suivante valable pour trois entiers.

Lemme 26. *Soient n_1, n_2 et n_3 trois entiers naturels. Alors, on a la formule suivante*

$$r_0(n_1n_2n_3) = \sum_{d_id_j|n_k} \frac{\chi(d_1d_2d_3)\mu(d_3)\mu(d_1d_2)}{2^{\omega(d_2,n_2)+\omega(d_1,n_1)}} r_0\left(\frac{n_1}{d_2d_3}\right) r_0\left(\frac{n_2}{d_1d_3}\right) r_0\left(\frac{n_3}{d_1d_2}\right)$$

où on a $\{i,j,k\}$ qui parcourt les permutations de l'ensemble $\{1,2,3\}$.

Démonstration.– On part bien entendu de la formule pour deux entiers qu'on vient d'établir pour obtenir que

$$r_0(n_1n_2n_3) = \sum_{d|(n_1n_2,n_3)} \mu(d)\chi(d) r_0\left(\frac{n_1n_2}{d}\right) r_0\left(\frac{n_3}{d}\right).$$

On peut alors, à cause de la présence du $\mu(d)$ se restreindre aux d sans facteurs carrés. Pour de tels d, le nombre de façon d'écrire $d = d_1d_2$ avec $d_1|n_2$ et $d_2|n_1$ est égal à $2^{\omega(d,n_1,n_2)}$. En effet, les premiers intervenant dans les décompositions en produit de facteurs premiers de d_1 et d_2 divisent nécessairement $\gcd(d,n_1,n_2)$ et pour un tel nombre premier p qui divise n_1 et n_2, on a le choix de le mettre dans la décomposition de d_1 ou dans celle de d_2. Pour les autres premiers qui ne divisent que d et n_1 par exemple, on n'a pas d'autre choix que de les mettre dans d_2. On remarque alors que

$$2^{\omega(d,n_1,n_2)} = 2^{\omega(d_1,n_1)+\omega(d_2,n_2)}$$

d'après ce qui précède et car $(d_1,d_2) = 1$ puisqu'on n'a pas de facteurs multiples. On en déduit donc que

$$r_0(n_1n_2n_3) = \sum_{\substack{d_1d_2|n_3 \\ d_1|n_2,d_2|n_1}} \frac{\mu(d_1d_2)\chi(d_1d_2)}{2^{\omega(d_1,n_1)+\omega(d_2,n_2)}} r_0\left(\frac{n_1}{d_2}\frac{n_2}{d_1}\right) r_0\left(\frac{n_3}{d_1d_2}\right).$$

On remplace alors

$$r_0\left(\frac{n_1}{d_2}\frac{n_2}{d_1}\right) = \sum_{d_3|(n_1/d_2,n_2/d_1)} \mu(d_3)\chi(d_3) r_0\left(\frac{n_1}{d_1d_3}\right) r_0\left(\frac{n_2}{d_1d_3}\right)$$

pour obtenir que

$$r_0(n_1n_2n_3) = \sum_{\substack{d_1d_2|n_3 \\ d_1|n_2,d_2|n_1}} \sum_{\substack{d_1d_3|n_2 \\ d_2d_3|n_1}} \frac{\chi(d_1d_2d_3)\mu(d_3)\mu(d_1d_2)}{2^{\omega(d_2,n_2)+\omega(d_1,n_1)}} r_0\left(\frac{n_1}{d_2d_3}\right) r_0\left(\frac{n_2}{d_1d_3}\right) r_0\left(\frac{n_3}{d_1d_2}\right)$$

qui est bien la formule recherchée puisque χ est complétement multiplicative. □

On est alors désormais en mesure d'établir la formule qui nous sera utile avec quatre entiers. On auait aussi pu utiliser uniquement la formule avec deux entiers en écrivant $n_1n_2n_3n_4 = n_1n_2 \times n_3n_4$ et on aurait obtenu une autre formule mais elle est moins adaptée que celle qu'on va établir pour la suite. On a donc le lemme suivant.

Lemme 27. *Soient n_1, n_2, n_3 et n_4 quatre entiers naturels. Alors, on a la formule suivante*

$$r_0(n_1n_2n_3n_4) =$$

$$\sum_{\substack{\mathbf{d},\mathbf{d}'\in\mathbb{N}^3\\ d_1d_2d_3|n_4,d_id'_jd'_k|n_i}} \frac{\mu(d_1d_2d_3)\mu(d'_1d'_2)\mu(d'_3)\chi(d_1d_2d_3d'_1d'_2d'_3)}{3^{\omega(d_1,n_2,n_3)+\omega(d_2,n_1,n_3)+\omega(d_3,n_1,n_2)}2^{\omega(d'_1,n_1/d_1)+\omega(d'_2,n_2/d_2)}\prod_{\substack{\{i,j,k\}=\{1,2,3\}\\ i<j}} 2^{\omega(d_i,n_j)-\omega(d_i,n_j,n_k)+\omega(d_j,n_i)-\omega(d_j,n_i,n_k)}}\times$$

$$r_0\left(\frac{n_1}{d_1d'_2d'_3}\right)r_0\left(\frac{n_2}{d_2d'_1d'_3}\right)r_0\left(\frac{n_3}{d_3d'_1d'_2}\right)r_0\left(\frac{n_4}{d_1d_2d_3}\right)$$

où $\{i,j,k\}$ *parcourt l'ensemble des permutations de* $\{1,2,3\}$.

Démonstration.– Utilisant la formule d'éclatement pour deux entiers, on obtient

$$r_0(n_1n_2n_3n_4)=\sum_{d|(n_1n_2n_3,n_4)}\mu(d)\chi(d)r_0\left(\frac{n_1n_2n_3}{d}\right)r_0\left(\frac{n_4}{d}\right).$$

Comme précédemment, on peut se restreindre aux entiers d sans facteur carré, et on va compter le nombre de décompositions $d=d_1d_2d_3$ avec $d_1|n_1$, $d_2|n_2$ et $d_3|n_3$. Pour les nombres premiers p divisant (d,n_1,n_2,n_3) qui divisent chacun des n_i, on a trois choix ce qui donne un terme

$$3^{\omega(d,n_1,n_2,n_3}=3^{\omega(d_1,n_2,n_3)+\omega(d_2,n_1,n_3)+\omega(d_3,n_1,n_2)}$$

puisque le fait que d soit sans facteur carré implique que les d_i soient premiers entre eux deux à deux. Ensuite, on va traiter les p premiers qui divisent deux des n_i exactement (pour ceux qui en divisent un exactement il n'y a pas de choix). On en a par exemple pour ceux qui divisent exactement n_1 et n_2 :

$$\omega(d,n_1,n_2)-\omega(d,n_1,n_2,n_3)=$$

$$\omega(d_1,n_2)+\omega(d_2,n_1)+\omega(d_3,n_2,n_1)-(\omega(d_1,n_2,n_3)+\omega(d_2,n_1,n_3)+\omega(d_3,n_1,n_2))$$

soit

$$\omega(d,n_1,n_2)-\omega(d,n_1,n_2,n_3)=\omega(d_1,n_2)-\omega(d_1,n_2,n_3))+\omega(d_2,n_1)-\omega(d_2,n_1,n_3).$$

On a alors le choix de mettre ce premier dans d_1 ou dans d_2 et on obient un facteur

$$2^{\omega(d_1,n_2)-\omega(d_1,n_2,n_3)+\omega(d_2,n_1)-\omega(d_2,n_1,n_3)}$$

ce qui donne finalement

$$r_0(n_1n_2n_3n_4)=$$

$$\sum_{\substack{d_1d_2d_3|n_4\\ d_1|n_1,d_2|n_2,d_3|n_3}} \frac{\mu(d_1d_2d_3)\chi(d_1d_2d_3)}{3^{\omega(d_1,n_2,n_3)+\omega(d_2,n_1,n_3)+\omega(d_3,n_1,n_2)}\prod_{\substack{\{i,j,k\}=\{1,2,3\}\\ i<j}} 2^{\omega(d_i,n_j)-\omega(d_i,n_j,n_k))+\omega(d_j,n_i)-\omega(d_j,n_i,n_k)}}\times$$

$$r_0\left(\frac{n_1}{d_1}\frac{n_2}{d_2}\frac{n_3}{d_3}\right)r_0\left(\frac{n_4}{d_1d_2d_3}\right).$$

On remplace alors

$$r_0\left(\frac{n_1}{d_1}\frac{n_2}{d_2}\frac{n_3}{d_3}\right)=\sum_{d'_id'_j|n_k/d_k}\frac{\chi(d'_1d'_2d'_3)\mu(d'_1)\mu(d'_2d'_3)}{2^{\omega(d'_2,n_2/d_2)+\omega(d'_3,n_3/d_3)}}r_0\left(\frac{n_1}{d_1d'_2d'_3}\right)r_0\left(\frac{n_2}{d_2d'_1d'_3}\right)r_0\left(\frac{n_3}{d_3d'_1d'_2}\right),$$

et finalement on obtient bien la formule souhaitée. □

On commence par poser pour alléger les notations

$$c(\mathbf{d},\mathbf{d}',L_1(u,v),L_2(u,v),Q(u,v))=c(\mathbf{d},\mathbf{d}',L_1^+(u,v),L_2^+(u,v),Q^+(u,v))=$$
$$3^{\omega(d_1,L_2(u,v),Q(u,v))+\omega(d_2,L_1(u,v),Q(u,v))+\omega(d_3,L_1(u,v),L_2(u,v))}2^{\omega(d_1',L_1(u,v)/d_1)+\omega(d_2',L_2(u,v)/d_2)}\times$$
$$\prod_{\substack{\{i,j,k\}=\{1,2,3\}\\ i<j}}2^{\omega(d_i,L_j(u,v))-\omega(d_i,L_j(u,v),L_k(u,v))+\omega(d_j,L_i(u,v))-\omega(d_j,L_i(u,v),L_k(u,v))}$$

où on a ici adopté la notation $L_3=Q$ pour simplifier dans le produit. On a donc

$$r\left(l^2L_1^+(u,v)L_2^+(u,v)Q^+(u,v)\right)=\frac{1}{2^6}\sum_{\substack{\mathbf{d},\mathbf{d}'\in\mathbb{N}^3\\ d_1d_2d_3|l^2,d_id_j'd_k'|L_i}}\frac{\mu(d_1d_2d_3)\mu(d_1'd_2')\mu(d_3')\chi(d_1d_2d_3d_1'd_2'd_3')}{c(\mathbf{d},\mathbf{d}',L_1(u,v),L_2(u,v),Q(u,v))}\times$$
$$r\left(\frac{L_1(u,v)}{d_1d_2'd_3'}\right)r\left(\frac{L_2(u,v)}{d_2d_1'd_3'}\right)r\left(\frac{Q(u,v)}{d_3d_1'd_2'}\right)r\left(\frac{l^2}{d_1d_2d_3}\right).$$

On écrit $m=d_1d_2d_3$ qui divise nécessairement l et est dans $\mathcal{D}$. En particulier, $\chi(m)=1$. On écrit $l=ms$ et on obtient

$$N(B)=\frac{1}{2^7}\sum_{\substack{mk\leqslant B\\ k,m\in\mathcal{D}}}\mu(m)\mu(k)\sum_{\substack{s\leqslant\frac{B}{mk}\\ s\in\mathcal{D}}}r(ms^2)\sum_{\substack{\mathbf{d},\mathbf{d}'\in\mathbb{N}^3\\ m=d_1d_2d_3}}\mu(d_1'd_2')\mu(d_3')\chi(d_1'd_2'd_3')\mathcal{S}_{\mathbf{d},\mathbf{d}'}\left(\frac{B}{msk}\right)$$

où

$$\mathcal{S}_{\mathbf{d},\mathbf{d}'}(T)=\sum_{\substack{\varepsilon_i\in\{-1,+1\}\\ \varepsilon_1\varepsilon_2\varepsilon_3=1}}\sum_{\substack{(u,v)\in Z^2\cap R^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(T)\\ d_1d_2'd_3'|L_1(u,v),d_2d_1'd_3'|L_2(u,v),d_3d_1'd_2'|Q(u,v)}}\frac{r\left(\frac{L_1^+(u,v)}{d_1d_2'd_3'}\right)r\left(\frac{L_2^+(u,v)}{d_2d_1'd_3'}\right)r\left(\frac{Q^+(u,v)}{d_3d_1'd_2'}\right)}{c(\mathbf{d},\mathbf{d}',L_1(u,v),L_2(u,v),Q(u,v))}$$

pour $T\geqslant 1$. Puisque par exemple, $d_1'|\gcd(L_2(u,v),Q(u,v))$ pour (u,v) premiers entre eux, on a déjà vu que cela impliquait que $d_1'|\mathrm{Res}(L_2,Q)=\Delta_{23}$ et donc en particulier on en déduit qu'on a un nombre possible de d_i' majoré par $H=\Delta_{12}\Delta_{13}\Delta_{23}$.

Si on pose, pour $d\in\mathbb{N}$ fixé,

$$f_d(n)=\sum_{ab=n}\mu(a)r(db^2)$$

on obtient (écrire $n=ks$)

$$N(B)=\frac{1}{2^7}\sum_{\substack{mn\leqslant B\\ n,m\in\mathcal{D}}}\mu(m)f_m(n)\sum_{\substack{\mathbf{d},\mathbf{d}'\in\mathbb{N}^3\\ m=d_1d_2d_3,\mathbf{d}'|H}}\mu(d_1'd_2')\mu(d_3')\chi(d_1'd_2'd_3')\mathcal{S}_{\mathbf{d},\mathbf{d}'}\left(\frac{B}{msk}\right).$$

On a vu dans la preuve de la formule d'éclatement que

$$c(\mathbf{d},\mathbf{d}',L_1(u,v),L_2(u,v),Q(u,v))=c(m,\mathbf{d}',L_1(u,v),L_2(u,v),Q(u,v))$$
$$3^{\omega(m,L_1(u,v),L_2(u,v),Q(u,v))}2^{\omega(d_1'd_2',L_1(u,v)/d_1,L_2(u,v)/d_2)}2^{\omega(m,L_1(u,v),L_2(u,v))-\omega(m,L_1(u,v),L_2(u,v),Q(u,v))}\times$$

$$2^{\omega(m,L_1(u,v),Q(u,v))-\omega(m,L_1(u,v),L_2(u,v),Q(u,v))}2^{\omega(m,Q(u,v),L_2(u,v))-\omega(m,L_1(u,v),L_2(u,v),Q(u,v))}.$$

On obtient alors en utilisant la remarque précédente sur les diviseurs du pgcd de $L_i(u,v)$ et $L_j(u,v)$ que

$$\mathcal{S}_{\mathbf{d},\mathbf{d}'}(T)=\sum_{\substack{\varepsilon_i\in\{-1,+1\}\\ \varepsilon_1\varepsilon_2\varepsilon_3=1}}\sum_{\substack{k_1|\gcd(\Delta_{23},m)\\ k_2|\gcd(\Delta_{13},m)}}\sum_{\substack{k_3|\gcd(\Delta_{12},m)\\ k_5|\gcd(\Delta_{12},d_1'd_2')\\ k_4|\gcd(\gcd(\Delta_{12},\Delta_{13},\Delta_{23}),m)}}\frac{1}{3^{\omega(k_4)}2^{\omega(k_5)+\omega(k_1)+\omega(k_2)+\omega(k_3)}}\times$$

$$\sum_{\substack{(u,v)\in Z^2\cap R^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(T)\\ d_1d_2'd_3'|L_1(u,v),d_2d_1'd_3'|L_2(u,v),d_3d_1'd_2'|Q(u,v)}}r\left(\frac{L_1^+(u,v)}{d_1d_2'd_3'}\right)r\left(\frac{L_2^+(u,v)}{d_2d_1'd_3'}\right)r\left(\frac{Q^+(u,v)}{d_3d_1'd_2'}\right),$$

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

$$\begin{cases} k_1=\gcd(m,L_2(u,v),Q(u,v))/\gcd(m,L_1(u,v),L_2(u,v),Q(u,v)),\\ k_2=\gcd(m,L_1(u,v),Q(u,v))/\gcd(m,L_1(u,v),L_2(u,v),Q(u,v)),\\ k_3=\gcd(m,L_1(u,v),L_2(u,v))/\gcd(m,L_1(u,v),L_2(u,v),Q(u,v)),\\ k_4=\gcd(m,L_1(u,v),L_2(u,v),Q(u,v)),\\ k_5=\gcd(d_1'd_2',L_1(u,v)/d_1,L_2(u,v)/d_2). \end{cases}\tag{2.2}$$

On utilise alors le raisonnement suivant :

$$\#\{x\in\mathcal{E}\quad|\quad f_i(x)=1\}=\sum_{d_1>0}\mu(d_1)\#\{x\in\mathcal{E}\quad|\quad d_1|f(x),\quad f_i(x)=1\quad(i>1)\}$$

et

$$\#\{x\in\mathcal{E}\quad|\quad d_1|f(x),\quad f_i(x)=1\quad(i>1)\}=$$
$$\sum_{d_2>0}\mu(d_2)\#\{x\in\mathcal{E}\quad|\quad d_1|f(x),\quad d_2|f_2(x),\quad f_i(x)=1\quad(i>2)\}$$

donc en itérant

$$\#\{x\in\mathcal{E}\quad|\quad f_i(x)=1\}=\sum_{d_1>0}\sum_{d_2>0}...\sum_{d_r>0}\mu(d_1)\mu(d_2)...\mu(d_r)\#\{x\in\mathcal{E}\quad|\quad d_i|f_i(x)\}.$$

On applique ce raisonnement à $k_4=\gcd(m,L_1,L_2,Q)$ (on note la nouvelle variable k_4') et à $k_4=\gcd(m,L_1,Q)/k_1$ (on note la nouvelle variable k_1'), etc... On obtient alors

$$\mathcal{S}_{\mathbf{d},\mathbf{d}'}(T)=$$

$$\sum_{\substack{\varepsilon_i\in\{-1,+1\}\\ \varepsilon_1\varepsilon_2\varepsilon_3=1}}\sum_{\substack{k_4k_1k_1'|\gcd(\Delta_{23},m)\\ k_4k_2k_2'|\gcd(\Delta_{13},m)}}\sum_{\substack{k_4k_3k_3'|\gcd(\Delta_{12},m)\\ k_5k_5'|\gcd(\Delta_{12},d_1'd_2')\\ k_4k_4'|\gcd(\gcd(\Delta_{12},\Delta_{13},\Delta_{23}),m)}}\frac{\mu(k_1')\mu(k_2')\mu(k_3')\mu(k_4')\mu(k_5')}{3^{\omega(k_4)}2^{\omega(k_5)+\omega(k_1)+\omega(k_2)+\omega(k_3)}}\times$$

$$\sum_{\substack{(u,v)\in Z^2\cap R^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(T)\\ d_1d_2'd_3'|L_1(u,v),d_2d_1'd_3'|L_2(u,v),d_3d_1'd_2'|Q(u,v)}}r\left(\frac{L_1^+(u,v)}{d_1d_2'd_3'}\right)r\left(\frac{L_2^+(u,v)}{d_2d_1'd_3'}\right)r\left(\frac{Q^+(u,v)}{d_3d_1'd_2'}\right),$$

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

$$\begin{cases} k_4k_1k_1'|\gcd(m,L_2(u,v),Q(u,v)),\\ k_4k_2k_2'|\gcd(m,L_1(u,v),Q(u,v)),\\ k_4k_3k_3'|\gcd(m,L_1(u,v),L_2(u,v)),\\ k_4k_4'|\gcd(m,L_1(u,v),L_2(u,v),Q(u,v)),\\ k_5k_5'|\gcd(d_1'd_2',L_1(u,v)/d_1,L_2(u,v)/d_2). \end{cases} \tag{2.3}$$

On peut alors réécrire cette somme sous la forme (les nouvelles conditions étant équivalentes aux anciennes)

$$\mathcal{S}_{\mathbf{d},\mathbf{d}'}(T)=$$
$$\sum_{\substack{\varepsilon_i\in\{-1,+1\}\\ \varepsilon_1\varepsilon_2\varepsilon_3=1}}\sum_{\substack{k_4k_1k_1'|\gcd(\Delta_{23},m)\\ k_4k_2k_2'|\gcd(\Delta_{13},m)}}\sum_{\substack{k_4k_3k_3'|\gcd(\Delta_{12},m)\\ k_5k_5'|\gcd(\Delta_{12},d_1'd_2')\\ k_4k_4'|\gcd(\gcd(\Delta_{12},\Delta_{13},\Delta_{23}),m)}}\frac{\mu(k_1')\mu(k_2')\mu(k_3')\mu(k_4')\mu(k_5')}{3^{\omega(k_4)}2^{\omega(k_5)+\omega(k_1)+\omega(k_2)+\omega(k_3)}}\times$$
$$\sum_{(u,v)\in Z^2\cap R^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(T)} r\left(\frac{L_1^+(u,v)}{d_1d_2'd_3'}\right)r\left(\frac{L_2^+(u,v)}{d_2d_1'd_3'}\right)r\left(\frac{Q^+(u,v)}{d_3d_1'd_2'}\right),$$

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

$$\begin{cases} [d_1d_2'd_3',k_4k_2k_2',k_4k_3k_3',k_4k_4',d_1k_5k_5']\big|L_1(u,v),\\ [d_2d_1'd_3',k_4k_1k_1',k_4k_3k_3',k_4k_4',d_2k_5k_5']\big|L_2(u,v),\\ [d_3d_1'd_2',k_4k_1k_1',k_4k_2k_2',k_4k_4']\big|Q(u,v). \end{cases} \tag{2.4}$$

Il nous reste encore à enlever la condition de coprimalité sur les couples (u,v) au moyen d'une dernière inversion de Möbius. On notera dans la suite

$$L_{i,e}=eL_i^+=e\varepsilon_iL_i\quad\text{et}\quad Q_e=e^2Q^+=e^2\varepsilon_3Q,$$

pour tout entier naturel e. La somme

$$\sum_{\substack{(u,v)\in Z^2\cap R^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(T)\\ [d_1d_2'd_3',k_4k_2k_2',k_4k_3k_3',k_4k_4',d_1k_5k_5']|L_1\\ [d_2d_1'd_3',k_4k_1k_1',k_4k_3k_3',k_4k_4',d_2k_5k_5']|L_2\\ [d_3d_1'd_3',k_4k_1k_1',k_4k_2k_2',k_4k_4']|Q}} r\left(\frac{L_1^+(u,v)}{d_1d_2'd_3'}\right)r\left(\frac{L_2^+(u,v)}{d_2d_1'd_3'}\right)r\left(\frac{Q^+(u,v)}{d_3d_1'd_2'}\right)$$

(où on note L_i et Q en indice à la place de $L_i(u,v)$ et $Q(u,v)$ pour ne pas alourdir les notations) est alors égale à (on écrit $(u,v)=e(x,y)$ avec $e=\gcd(u,v)$ et donc $x,y\leqslant e^{-2}T$) :

$$\sum_{0<e\leqslant\sqrt{T}}\mu(e)\mathcal{U}(e^{-2}T)=\sum_{e=1}^{+\infty}\mu(e)\mathcal{U}(e^{-2}T)$$

puisque $\mathcal{U}(T)$ est nulle pour $T<1$ étant donné qu'on n'a aucun point dans la région dans laquelle on compte et où

$$\mathcal{U}(T)=\mathcal{U}^{\varepsilon_1,\varepsilon_2,\varepsilon_3}_{\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e}(T)$$

avec

$$\mathcal{U}(T) = \sum_{\substack{(x,y)\in\mathbb{Z}^2\cap R^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(T)\\ [d_1d_2'd_3',k_4k_2k_2',k_4k_3k_3',k_4k_4',d_1k_5k_5']|L_{1,e}\\ [d_2d_1'd_3',k_4k_1k_1',k_4k_3k_3',k_4k_4',d_2k_5k_5']|L_{2,e}\\ [d_3d_1'd_2',k_4k_1k_1',k_4k_2k_2',k_4k_4']|Q_e}} r\left(\frac{L_{1,e}(u,v)}{d_1d_2'd_3'}\right) r\left(\frac{L_{2,e}(u,v)}{d_2d_1'd_3'}\right) r\left(\frac{Q_e(u,v)}{d_3d_1'd_2'}\right). \quad (2.5)$$

On a ainsi démontré le lemme suivant.

Lemme 28. *On a*

$$N(B) = \frac{1}{2^7}\sum_{e=1}^{+\infty}\mu(e)\sum_{m\in\mathcal{D}}\mu(m)\sum_{\substack{n\leqslant N\\ n\in\mathcal{D}}} f_m(n) \sum_{\substack{\varepsilon_i\in\{-1,+1\}\\ \varepsilon_1\varepsilon_2\varepsilon_3=1}} \sum_{\substack{k_4k_1k_1'|\gcd(\Delta_{23},m)\\ k_4k_2k_2'|\gcd(\Delta_{13},m)}}$$

$$\sum_{\substack{k_4k_3k_3'|\gcd(\Delta_{12},m)\\ k_5k_5'|\gcd(\Delta_{12},d_1'd_2')\\ k_4k_4'|\gcd(\gcd(\Delta_{12},\Delta_{13},\Delta_{23}),m)}} \frac{\mu(k_1')\mu(k_2')\mu(k_3')\mu(k_4')\mu(k_5')}{3^{\omega(k_4)}2^{\omega(k_5)+\omega(k_1)+\omega(k_2)+\omega(k_3)}} \sum_{\substack{\mathbf{d},\mathbf{d}'\in\mathbb{N}^3\\ m=d_1d_2d_3,\mathbf{d}'|H}} \mu(d_1'd_2')\mu(d_3')\chi(d_1'd_2'd_3')\mathcal{U}\left(\frac{B}{me^2n}\right)$$

où $\mathcal{U}(T) = \mathcal{U}^{\varepsilon_1,\varepsilon_2,\varepsilon_3}_{\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e}(T)$ *et* $N = \frac{B}{me^2}$.

Démonstration.– En effet, on a $e \leqslant \sqrt{\frac{B}{mn}}$ et donc, quand on intervertit, on a bien e et m qui varient dans $\mathbb{N}\cap\mathcal{D}$ et ensuite $n \leqslant \frac{B}{me^2}$. □

On a alors besoin dans la suite d'un résultat un peu plus fin. En fait, on peut remarquer que $\mathcal{U}(T)$ est nulle si on n'a pas

$$d_1 \leqslant (|a_1|+|b_1|)eT^{1/2}, \quad d_2 \leqslant (|a_2|+|b_2|)eT^{1/2} \quad \text{et} \quad d_3 \leqslant (|a_3|+|b_3|+|c_3|)e^2T$$

puisque par rexemple, on a

$$L_e(x,y) \leqslant (|a_1|+|b_1|)e\max(|x|,|y|) \leqslant (|a_1|+|b_1|)eT^{1/2}$$

dans la région considérée. On a donc en réalité, puisque dans notre somme, $T = \frac{B}{me^2n}$ que

$$m = d_1d_2d_3 \leqslant \delta^2\frac{B^2}{m^2n^2}$$

et donc

$$m^{\frac{3}{2}}n \leqslant B,$$

ce qu'on peut réécrire

$$m^{\frac{3}{4}}n^{\frac{1}{2}} \leqslant \delta B^{\frac{1}{2}}.$$

Mais pour que $\mathcal{U}\left(\frac{B}{me^2n}\right)$ soit non nulle, il faut aussi imposer

$$me^2n \leqslant B$$

et par conséquent,

$$m^{\frac{1}{2}}en^{\frac{1}{2}} \leqslant B^{\frac{1}{2}},$$

ce qui, combiné avec l'inégalité précédente, implique l'inégalité

$$m^{\frac{5}{4}}en \leqslant \delta B$$

et donne lieu au lemme final suivant.

Lemme 29. *On a*

$$N(B)=\frac{1}{2^7}\sum_{e=1}^{+\infty}\mu(e)\sum_{m\in\mathcal{D}}\mu(m)\sum_{\substack{n\leqslant N\\ n\in\mathcal{D}}}f_m(n)\sum_{\substack{\varepsilon_i\in\{-1,+1\}\\ \varepsilon_1\varepsilon_2\varepsilon_3=1}}\sum_{\substack{k_4k_1k_1'|\gcd(\Delta_{23},m)\\ k_4k_2k_2'|\gcd(\Delta_{13},m)}}$$

$$\sum_{\substack{k_4k_3k_3'|\gcd(\Delta_{12},m)\\ k_5k_5'|\gcd(\Delta_{12},d_1'd_2')\\ k_4k_4'|\gcd(\gcd(\Delta_{12},\Delta_{13},\Delta_{23}),m)}}\frac{\mu(k_1')\mu(k_2')\mu(k_3')\mu(k_4')\mu(k_5')}{3^{\omega(k_4)}2^{\omega(k_5)+\omega(k_1)+\omega(k_2)+\omega(k_3)}}\sum_{\substack{\mathbf{d},\mathbf{d}'\in\mathbb{N}^3\\ m=d_1d_2d_3,\mathbf{d}'|H}}\mu(d_1'd_2')\mu(d_3')\chi(d_1'd_2'd_3')\mathcal{U}\left(\frac{B}{me^2n}\right)$$

où $\mathcal{U}(T)=\mathcal{U}^{\varepsilon_1,\varepsilon_2,\varepsilon_3}_{\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e}(T)$ *et* $N=\frac{\delta B}{m^{\frac{5}{4}}e}$.

On a ainsi utilisé une méthode de descente pour passer d'un problème de comptage sur une variété définie par une équation à une variété définie par quatre équations. Autrement dit on est passé d'un problème de comptage sur notre variété de départ à un problème de comptage sur des torseurs universels associés à cette variété.

2.2 Fin de la preuve de la conjecture de Manin

On utilise évidemment le Théorème 2 pour estimer la somme $\mathcal{U}(T)$ définie dans la section précédente en (2.5). Si on pose

$$e_1=d_1d_2'd_3',\quad e_2=d_2d_1'd_3'\quad\text{et}\quad e_3=d_3d_1'd_2'$$

et

$$E_1=[d_1d_2'd_3',k_4k_2k_2',k_4k_3k_3',k_4k_4',d_1k_5k_5'],\quad E_2=[d_2d_1'd_3',k_4k_1k_1',k_4k_3k_3',k_4k_4',d_2k_5k_5']$$

et

$$E_3=[d_3d_1'd_3',k_4k_1k_1',k_4k_2k_2',k_4k_4'],$$

alors les triplets $\mathbf{e}$ et $\mathbf{E}$ vérifient bien les hypothèses d'application du Théorème 2 et on a avec ces notations

$$\mathcal{U}(T)=\sum_{\mathbf{x}\in\Lambda(\mathbf{E};L_{1,e},L_{2,e},Q_e)\cap\sqrt{T}\mathcal{R}}r\left(\frac{L_{1,e}(\mathbf{x})}{e_1}\right)r\left(\frac{L_{2,e}(\mathbf{x})}{e_2}\right)r\left(\frac{Q_e(\mathbf{x})}{e_3}\right),$$

où $\mathcal{R}=R^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(1)$ de sorte que $\sqrt{T}\mathcal{R}=R^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(T)$. On déduit donc du Théorème 2 le lemme suivant.

Lemme 30. *Soit* $\varepsilon>0$ *tel que* $r'(\sqrt{T})^{1-\varepsilon}\geqslant 1$. *On a alors*

$$\mathcal{U}(T)=2\pi^3\mathrm{vol}(\mathrm{R}^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(1))\mathrm{T}\prod_{\mathrm{p}}\sigma_{\mathrm{p}}^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',\mathrm{e})+$$

$$O_\varepsilon\left(\frac{L_\infty(L_{1,e},L_{2,e},Q_e)^\varepsilon E^\varepsilon(r_\infty(R^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(1))r'(L_{1,e},L_{2,e},Q_e,R^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(1))+r_\infty(R^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(1))^2)a'(\mathbf{E},\mathbf{\Delta},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e)T}{\delta(\mathbf{E},L_{1,e},L_{2,e},Q_e)\,(\log(T))^{\eta-\varepsilon}}\right),$$

où

$$\sigma_p^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e)=\left(1-\frac{\chi(p)}{p}\right)^3\sum_{\boldsymbol{\nu}\in\mathbb{Z}^3_{\geqslant 0}}\frac{\chi(p)^{\nu_1+\nu_2+\nu_3}\rho\left(p^{N_1},p^{N_2},p^{N_3}\right)}{p^{2(N_1+N_2+N_3)}}\qquad(2.6)$$

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

$$\sigma_2^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e) = 4\lim_{n\to+\infty} 2^{-2n}\#\left\{\mathbf{x}\in(\mathbb{Z}/2^n\mathbb{Z})^2 \quad \middle| \quad \begin{array}{c} e\varepsilon_i L_i(\mathbf{x}) \in e_i\mathcal{E}_{2^n} \\ e^2\varepsilon_3 Q(\mathbf{x}) \in e_3\mathcal{E}_{2^n}\end{array}\right\}.$$

De plus, on a

$$\prod_p \sigma_p(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e) \ll L_\infty(L_{1,e},L_{2,e},Q_e)^\varepsilon E^\varepsilon a'(\mathbf{E},\mathbf{\Delta},,\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e). \tag{2.7}$$

On peut alors utiliser le fait que $\varepsilon_1\varepsilon_2\varepsilon_3 = 1$ et que $d_1 \equiv d_2 \equiv d_3 \equiv 1[4]$ (car ils sont tous dans $\mathcal{D}$ puisque leur produit m y est) pour réécrire

$$\sigma_2^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e) = 4\lim_{n\to+\infty} 2^{-2n}\#\left\{\mathbf{x}\in(\mathbb{Z}/2^n\mathbb{Z})^2 \quad \middle| \quad \begin{array}{c} eL_i(\mathbf{x}) \in d_j'd_k'\varepsilon_i\mathcal{E}_{2^n} \\ e^2 Q(\mathbf{x}) \in d_1'd_2'\varepsilon_3\mathcal{E}_{2^n}\end{array}\right\}.$$

Puisque $E = E_1E_2E_3$ et par définition des k_i, on peut majorer E par une puissance de L_∞ fois $m^2d_1'd_2'd_3'$ mais puisque $\mathbf{d}'|H$ (où on rappelle que $H = \Delta_{12}\Delta_{13}\Delta_{23}\Delta$), on peut aussi majorer $d_1'd_2'd_3'$ par une puissance de L_∞ et enfin en remarquant que $L_\infty(L_{1,e},L_{2,e},Q_e) \leqslant e^2L_\infty(L_1,L_2,Q)$, on obtient la majoration

$$\prod_p \sigma_p(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e) \ll L_\infty^\varepsilon(me)^\varepsilon a'(\mathbf{E},\mathbf{\Delta},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e),$$

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

En réutilisant l'estimation uniforme de $S(X,\mathbf{e},\mathbf{E})$ obtenue grâce au Lemme 22, on a

$$\mathcal{U}(T) \ll (EL_\infty(L_{1,e},L_{2,e},Q_e))^\varepsilon a'(\mathbf{E},\mathbf{\Delta},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e)\left(r_\infty(R^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(1))^2T + \frac{r_\infty(R^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(1))^{1+\varepsilon}T^{\frac{1}{2}+\varepsilon}}{\delta(\mathbf{E},L_{1,e},L_{2,e},Q_e)}\right).$$

En fait, suivant la même preuve que celle du Lemme 22, on utilise ici une majoration dfférente de $\det(G_f(\mathcal{A}))$. On remarque que (où ici il faut faire attention au fait que les ℓ_i et q correspondent aux contenus des formes $L_{i,e}$ et Q_e)

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

Commençons alors par voir que

$$\frac{E_1}{\gcd(E_1',b)\gcd(E_1,\ell_1)} \geqslant \frac{E_1}{\gcd(E_1,b\ell_1)}.$$

En effet, si $p^{\nu_1+\nu_2}||\gcd(E_1',b)\gcd(E_1,\ell_1)$ avec $p^{\nu_1}||\gcd(E_1,\ell_1)$ et $p^{\nu_2}||\gcd(E_1',b)$, alors on a

$$E_1' = p^{\nu_2}k \quad \text{et} \quad \gcd(E_1,\ell_1) = p^{\nu_1}h$$

donc puisque $E_1 = E_1'\gcd(E_1,\ell_1)$, on en déduit que $p^{\nu_1+\nu_2}|E_1$ et de même $p^{\nu_1+\nu_2}|b\ell_1$ donc

$$\gcd(E_1',b)\gcd(E_1,\ell_1)|\gcd(E_1,b\ell_1)$$

et on en déduit bien que

$$\frac{E_1}{\gcd(E_1', b)\gcd(E_1, \ell_1)} \geqslant \frac{E_1}{\gcd(E_1, b\ell_1)},$$

puis raisonnant de la même façon avec E_2' et E_3', on obtient

$$E'' \geqslant \frac{E}{\gcd(E_1, b\ell_1)\gcd(E_2, b\ell_2)\gcd(E_3, b^2 q)}.$$

On s'intéresse alors pour commencer à la quantité

$$\frac{E_1}{\gcd(E_1, b\ell_1)} = \frac{[d_1 d_2' d_3', k_4 k_2 k_2', k_4 k_3 k_3', k_4 k_4', d_1 k_5 k_5']}{\gcd([d_1 d_2' d_3', k_4 k_2 k_2', k_4 k_3 k_3', k_4 k_4', d_1 k_5 k_5'], b\ell_1)}.$$

On montre tout d'abord l'identité valable pour tout (a, b, c, d) quadruplet d'entiers naturels

$$\min(\max(a+b, c), d) \leqslant \min(\max(b, c), d) + \min(a, d). \tag{2.8}$$

En effet, si $d \leqslant a$, on a

$$\min(\max(a+b, c), d) = d \quad \text{et} \quad \min(\max(b, c), d) + \min(a, d) = \min(\max(b, c), d) + d$$

donc l'inégalité (2.8) est bien vérifiée. Supposons donc désormais $a < d$. Soit $a < d \leqslant b \leqslant a + b$ et $d \leqslant c$ et on a

$$\min(\max(a+b, c), d) = d \quad \text{et} \quad \min(\max(b, c), d) + \min(a, d) = d + a$$

et (2.8) est à nouveau vérifiée. Dans le cas où $a \leqslant b \leqslant a + b \leqslant c \leqslant d$, on a bien

$$c - a \leqslant c$$

tandis que si $a \leqslant b \leqslant c \leqslant a + b \leqslant d$, on a

$$a + b - a = b \leqslant c$$

et si $a \leqslant c \leqslant b \leqslant a + b \leqslant d$, on a

$$a + b - a = b \leqslant b$$

et là encore (2.8) est vraie. Il reste alors les cas $a \leqslant c \leqslant b \leqslant d \leqslant a + b$ qui donne

$$d - a \leqslant b$$

puis $a \leqslant c \leqslant d \leqslant b \leqslant a + b$ qui donne

$$d - a \leqslant d$$

et $a \leqslant b \leqslant c \leqslant d \leqslant a + b$ donne $d - a \leqslant c$ qui est bien vérifiée car $d - a \leqslant b \leqslant c$. On peut alors conclure puisque la position de a par rapport à b et c ne change rien au fait qu'on a bien

$$\min(\max(a+b, c), d) \leqslant \min(\max(b, c), d) + \min(a, d).$$

On utilise cette inégalité (2.8) pour établir que

$$\frac{\gcd([d_1d_2'd_3', k_4k_2k_2', k_4k_3k_3', k_4k_4', d_1k_5k_5'], b\ell_1)}{\gcd(d_1, b\ell_1)} \Bigg| \gcd([d_2'd_3', k_4k_2k_2', k_4k_3k_3', k_4k_4', k_5k_5'], b\ell_1).$$

Pour ce faire, on regarde les valuations p-adiques. Pour établir le résultat il suffit de montrer l'inégalité

$$\min(\max(\nu_p(d_1) + \nu_p(d_2'd_3'), \nu_p(k_4k_2k_2'), \nu_p(k_4k_3k_3'), \nu_p(k_4k_4'), \nu_p(d_1) + \nu_p(k_5k_5')), \nu_p(b\ell_1))$$

$$- \min(\nu_p(d_1), \nu_p(b\ell_1)) \leqslant \min(\max(\nu_p(d_2'd_3'), \nu_p(k_4k_2k_2'), \nu_p(k_4k_3k_3'), \nu_p(k_4k_4'), \nu_p(k_5k_5')), \nu_p(b\ell_1))$$

qui découle bien de (2.8) en remarquant les égalités

$$\max(\nu_p(d_1) + \max(\nu_p(d_2'd_3'), \nu_p(k_4k_2k_2'), \nu_p(k_4k_3k_3'), \nu_p(k_4k_4'), \nu_p(d_1)\nu_p(k_5k_5')) =$$

$$\max(\nu_p(d_1) + \max(\nu_p(d_2'd_3'), \nu_p(k_5k_5')), \max(\nu_p(k_4k_2k_2'), \nu_p(k_4k_3k_3'), \nu_p(k_4k_4')))$$

et

$$\max(\max(\nu_p(d_2'd_3'), \nu_p(k_5k_5')), \max(\nu_p(k_4k_2k_2'), \nu_p(k_4k_3k_3'), \nu_p(k_4k_4'), \nu_p(k_5k_5'))) =$$

$$\max(\nu_p(d_2'd_3'), \nu_p(k_4k_2k_2'), \nu_p(k_4k_3k_3'), \nu_p(k_4k_4'), \nu_p(k_5k_5')).$$

On en déduit, puisqu'on a également

$$[d_1d_2'd_3', k_4k_2k_2', k_4k_3k_3', k_4k_4', k_5k_5'] \geqslant d_1,$$

l'inégalité

$$\frac{E_1}{\gcd(E_1, b\ell_1)} \geqslant \frac{d_1}{\gcd(d_1, b\ell_1)\gcd([d_2'd_3', k_4k_2k_2', k_4k_3k_3', k_4k_4', k_5k_5'], b\ell_1)}.$$

Or, d'après ce qui précède,

$$\gcd([d_2'd_3', k_4k_2k_2', k_4k_3k_3', k_4k_4', k_5k_5'], b\ell_1) | [d_2'd_3', k_4k_2k_2', k_4k_3k_3', k_4k_4', k_5k_5'] | H$$

puisque tous les éléments dont on prend le ppcm divisent H. D'où,

$$\frac{E_1}{\gcd(E_1, b\ell_1)} \geqslant \frac{1}{H}\frac{d_1}{\gcd(d_1, b\ell_1)}.$$

Procèdant au même raisonnement avec les indices 2 et 3, on obtient finalement

$$E'' \geqslant \frac{1}{H^3}\frac{m}{\gcd(d_1, b\ell_1)\gcd(d_2, b\ell_2)\gcd(d_3, b^2q)}.$$

En notant $c(P)$ le contenu d'un polynôme P, on a les relations

$$\ell_i = ec(L_i) \quad \text{et} \quad q = e^2c(Q)$$

où cette fois les $c(L_i)$ et $c(Q)$ sont indépendants des paramètres $\mathbf{d}$, $\mathbf{d}'$, $\mathbf{k}$, $\mathbf{k}'$ et e, ce qui va nous permettre ensuite de pouvoir sommer. On remarque alors qu'on a l'inégalité

$$\min(a + b, c) \leqslant \min(c, a) + \min(c, b).$$

En effet, si $c \leqslant a, b$, alors on a bien $c \leqslant 2c$. Par symétrie entre a et b, on peut supposer sans perte de généralité que $a \leqslant b$. Alors si $a \leqslant b \leqslant a+b \leqslant c$, on a bien $a+b \leqslant a+b$, tandis que si $a \leqslant b \leqslant c \leqslant a+b$, on a également bien $c \leqslant a+b$. Et enfin, si $a \leqslant c \leqslant b \leqslant a+b$, on a toujours bien $c \leqslant a+b$. On en déduit la relation de divisibilité

$$\left.\frac{\gcd(d_1, b\ell_1)}{\gcd(d_1, be)}\right| \gcd(d_1, c(L_1)).$$

Il suffit au niveau des valuations de vérifier

$$\min(\nu_p(d_1), \nu_p(be) + \nu_p(c(L_1))) - \min(\nu_p(d_1), \nu_p(be)) \leqslant \min(\nu_p(d_1), \nu_p(c(L_1)))$$

qui découle de l'inégalité juste ci-dessus. Puisque $\gcd(d_1, c(L_1))|c(L_1)$, on obtient alors

$$E'' \geqslant \frac{1}{c(L_1)c(L_2)c(Q)H^3} \frac{m}{\gcd(d_1, be)\gcd(d_2, be)\gcd(d_3, b^2e^2)}.$$

Étant donné que $m = d_1d_2d_3$ est sans facteur carré, d_3 l'est aussi et donc

$$\gcd(d_3, b^2e^2) = \gcd(d_3, be)$$

et

$$E'' \geqslant \frac{1}{c(L_1)c(L_2)c(Q)H^3} \frac{m}{\gcd(d_1, be)\gcd(d_2, be)\gcd(d_3, be)}.$$

Pour finir, on utilise le fait que

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

En effet, toujours en utilisant le fait que m soit sans facteur carré, on a nécessairement que d_1, d_2 et d_3 sont premiers entre eux deux à deux et donc

$$\gcd(d_1, be)\gcd(d_2, be)\gcd(d_3, be) = \prod_{\substack{p|be \\ p|d_1}} p \prod_{\substack{p|be \\ p|d_2}} p \prod_{\substack{p|be \\ p|d_3}} p$$

tandis que

$$\gcd(d_1d_2d_3, be) = \prod_{\substack{p|be \\ p|d_1d_2d_3}} p = \prod_{\substack{p|be \\ p|d_1}} p \prod_{\substack{p|be \\ p|d_2}} p \prod_{\substack{p|be \\ p|d_3}} p$$

ce qui prouve le résultat. On a finalement obtenu l'inégalité

$$E'' \geqslant \frac{1}{c(L_1)c(L_2)c(Q)H^3} \frac{m}{\gcd(m, be)}$$

ce qui entraîne que

$$\det(G_f(\mathcal{A})) \geqslant \frac{1}{c(L_1)c(L_2)c(Q)H^3} \frac{mf}{\gcd(m, be)}.$$

En reprenant la preuve du Lemme 22 en utilisant cette minoration plutôt que celle utilisant ψ_0, on déduit que

$$\mathcal{U}(T) \ll (EL_\infty(L_{1,e}, L_{2,e}, Q_e))^\varepsilon \sum_{b|\psi(\mathbb{E}')} \#\mathcal{V}(\mathbf{E}'') \times$$

$$\left(r_\infty(R^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(1))^2\frac{T}{b^2\det(G_f(\mathcal{A}))}+\frac{r_\infty(R^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(1))^{1+\varepsilon}T^{\frac12+\varepsilon}}{b\delta(\mathbf{E},L_{1,e},L_{2,e},Q_e)}\right)$$

et on majore alors

$$\frac{1}{b^2\det(G_f(\mathcal{A}))}\ll c(L_1)c(L_2)c(Q)H^3\frac{\gcd(m,be)}{mfb^2}\leqslant c(L_1)c(L_2)c(Q)H^3\frac{\gcd(m,be)}{mb}$$

où on remarque que $\gcd(m,be)\leqslant\gcd(m,b)\gcd(m,e)$ pour obtenir

$$\mathcal{U}(T)\ll c(L_1)c(L_2)c(Q)H^3(EL_\infty(L_{1,e},L_{2,e},Q_e))^\varepsilon\gcd(m,e)\sum_{b|\psi(\mathbb{E}')}\frac{\gcd(m,b)}{b}\#\mathcal{V}(\mathbf{E}'')\times$$

$$\left(r_\infty(R^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(1))^2\frac{T}{m}+\frac{r_\infty(R^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(1))^{1+\varepsilon}T^{\frac12+\varepsilon}}{\delta(\mathbf{E},L_{1,e},L_{2,e},Q_e)}\right).$$

En majorant $\frac{\gcd(m,b)}{b}$ par 1 et en concluant comme dans la preuve du Lemme 22, on aboutit à l'estimation

$$\mathcal{U}(T)\ll c(L_1)c(L_2)c(Q)H^3(meL_\infty)^\varepsilon\gcd(m,e)a'(\mathbf{E},\mathbf{\Delta},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e)\times$$

$$\left(r_\infty(R^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(1))^2\frac{T}{m}+\frac{r_\infty(R^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(1))^{1+\varepsilon}T^{\frac12+\varepsilon}}{\delta(\mathbf{E},L_{1,e},L_{2,e},Q_e)}\right)$$

en recyclant la remarque faite sur le lien entre E et me.

On a ensuite besoin de quelques résultats concernant la fonction f_m définie ci-dessus pour $m\in\mathcal{D}$ et en particulier le suivant est essentiel.

Lemme 31. *Soit $m\in\mathcal{D}$ sans facteur carré. Alors on a*

$$\sum_{\substack{n\leqslant x\\ n\in\mathcal{D}}}\frac{f_m(n)}{n}=\frac{r(m)\varphi^\dagger(m)}{\pi}\left(\log(x)+O\left(\log^2(2+\omega(m))\right)\right),$$

où

$$\varphi^\dagger(m)=\prod_{p|m}\left(1+\frac1p\right)^{-1}.$$

Démonstration.– On considére la série de Dirichlet associée

$$F_m(s)=\sum_{n\in\mathcal{D}}\frac{f_m(n)}{n^s}$$

et posant $r_0=\frac14 r$, par définition de f_m, on a

$$F_m(s)=4\sum_{k\in\mathcal{D}}\frac{\mu(k)}{k^s}\sum_{n\in\mathcal{D}}\frac{r_0(mn^2)}{n^s}.$$

On pose alors $\delta = \delta_p = \nu_p(m) \in \{0,1\}$ et $\delta = 1$ si, et seulement si, $p|m$ et $p \equiv 1[4]$. Décomposant en produit eulérien, il vient

$$\sum_{k\in\mathcal{D}} \frac{\mu(k)}{k^s} = \prod_{p\equiv 1[4]} \left(1 + \sum_{\nu\geqslant 1} \frac{\mu(p^\nu}{p^{\nu s}}\right) = \prod_{p\equiv 1[4]} \left(1 - \frac{1}{p^s}\right)$$

et

$$\sum_{n\in\mathcal{D}} \frac{r_0(mn^2)}{n^s} = \prod_{p\equiv 1[4]} \sum_{\nu\geqslant 0} \frac{r_0(p^{2\nu+\delta}}{p^{\nu s}} = \prod_{p\equiv 1[4]} \sum_{\nu\geqslant 0} \frac{1+2\nu+\delta}{p^{\nu s}}.$$

D'où,

$$F_m(s) = 4 \prod_{p\equiv 1[4]} \left(1 - \frac{1}{p^s}\right) \prod_{p\equiv 1[4]} \sum_{\nu\geqslant 0} \frac{1+2\nu+\delta}{p^{\nu s}}.$$

Or,

$$\sum_{\nu\geqslant 0} \frac{1+\delta}{p^{\nu s}} = \frac{1+\delta}{1-p^{-s}}$$

et

$$\sum_{\nu\geqslant 0} \frac{2\nu}{p^{\nu s}} = 2\frac{p^{-s}}{(1-p^{-s})^2}$$

en dérivant la série géométrique. On en déduit l'égalité

$$\sum_{\nu\geqslant 0} \frac{1+2\nu+\delta}{p^{\nu s}} = \frac{(1+\delta)(1-p^{-s}) + 2p^{-s}}{(1-p^{-s})^2}$$

et donc

$$F_m(s) = 4 \prod_{p\equiv 1[4]} (1-p^{-s}) \frac{(1+\delta)(1-p^{-s}) + 2p^{-s}}{(1-p^{-s})^2} = 4 \prod_{p\equiv 1[4]} \left(1 + \delta + 2\frac{p^{-s}}{(1-p^{-s})}\right).$$

Or,

$$\prod_{p\equiv 1[4]} \frac{1+p^{-s}}{1-p^{-s}} \prod_{p\equiv 1[4]} \frac{1+\delta+(1-\delta)p^{-s}}{1+p^{-s}} = \prod_{p\equiv 1[4]} \frac{1+p^{-s}+\delta(1-p^{-s})}{1-p^{-s}}$$

et en écrivant $1+p^{-s} = 1-p^{-s}+2p^{-s}$, on obtient bien

$$F_m(s) = 4 \prod_{p\equiv 1[4]} \frac{1+p^{-s}}{1-p^{-s}} \prod_{p\equiv 1[4]} \frac{1+\delta+(1-\delta)p^{-s}}{1+p^{-s}}.$$

On a alors

$$\frac{\zeta(s)L(s,\chi)}{(1+2^{-s})\zeta(2s)} = \frac{1}{1+2^{-s}} \prod_p \frac{1-p^{-2s}}{(1-p^{-s})(1-\chi(p)p^{-s})}$$

Si $p \equiv 3[4]$,

$$\frac{1-p^{-2s}}{(1-p^{-s})(1-\chi(p)p^{-s})} = \frac{1-p^{-2s}}{(1-p^{-s})(1+p^{-s})} = \frac{1-p^{-2s}}{1-p^{-2s}} = 1$$

et vu que si $p \equiv 1[4]$, $\chi(p) = 1$ et que $\chi(2) = 0$, on a

$$\frac{\zeta(s)L(s,\chi)}{(1+2^{-s})\zeta(2s)} = \prod_{p\equiv 1[4]} \frac{1-p^{-2s}}{(1-p^{-s})^2} = \prod_{p\equiv 1[4]} \frac{1+p^{-s}}{1-p^{-s}}.$$

Ensuite, si p ne divise pas m, alors $\delta = 0$ et

$$\frac{1+\delta+(1-\delta)p^{-s}}{1+p^{-s}} = 1$$

donc

$$F_m(s) = 4\frac{\zeta(s)L(s,\chi)}{(1+2^{-s})\zeta(2s)} H_m(s),$$

où

$$H_m(s) = \prod_{p|m} \frac{1+1+(1-1)p^{-s}}{1+p^{-s}} = \prod_{p|m} \frac{2}{1+p^{-s}} = r_0(m) \prod_{p|m} \left(1+\frac{1}{p^s}\right)^{-1},$$

puisque m est sans facteur carré et donc $r_0(m) = \prod_{p|m} 2$. Le même raisonnement fournit la relation

$$F_1(s) = 4\frac{\zeta(s)L(s,\chi)}{(1+2^{-s})\zeta(2s)}$$

et donc en notant que $H_1(s) = 1$, on en déduit que $F_m(s) = F_1(s)H_m(s)$. La série de Dirichlet F_1 est méromorphe dans le demi-plan $\mathrm{Re}(s) > \frac{1}{2}$ avec un pôle simple en $s = 1$ (quotient de fonctions L et ζ) et on note $h_m(n)$ la fonction arithmétique telle que

$$H_m(s) = \sum_{n\in\mathcal{D}} \frac{h_m(n)}{n^s}.$$

On a en particulier $f_m = f_1 * h_m$. On fait alors appel à un théorème taubérien. En effet, le théorème taubérien de Hardy-Littlewood-Karamata ([39]) permet de relier le comportement de $\sum_{n\geqslant 1} a_n/n^\sigma$ et $\sum_{n\leqslant x} a_n/n$. Ici, en notant $c = 4/\pi$, on a bien

$$F_1(s) = \frac{c+o(1)}{\sigma-1}$$

avec $\omega = 1$ puisqu'on connaît le pôle en 1. Comme $\Gamma(2) = 1! = 1$, on en déduit bien le résultat voulu à condition de vérifier que

$$f_1(n) \geqslant -K,$$

pour une certaine constante K. Or, on sait que $n \in \mathcal{D}$ donc dans ce cas

$$f_1(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \tau(d^2).$$

Calculons alors

$$f_1(p^\nu) = \mu(1)\tau(p^{2\nu}) + \mu(p)\tau(p^{2(\nu-1)})$$

qui donne

$$f_1(p^\nu) = 2\nu + 1 - (2(\nu-1)+1) = 2 = 2^{\omega(p^\nu)}$$

et par multiplicativité, on en déduit

$$f_1(n) = 2^{\omega(n)} \geqslant 0$$

et on peut bien appliquer le théorème taubérien cité plus haut.

On en déduit alors l'estimation souhaitée dans le cas général. On a

$$\sum_{\substack{n\leqslant x\\ n\in\mathcal{D}}} \frac{f_m(n)}{n} = \sum_{\substack{k\leqslant x\\ k\in\mathcal{D}}} \frac{h_m(k)}{k} \sum_{\substack{n\leqslant x/k\\ n\in\mathcal{D}}} \frac{f_1(n)}{n} = \sum_{\substack{k\leqslant x\\ k\in\mathcal{D}}} \frac{h_m(k)}{k} \left(\frac{4\log(x/k)}{\pi} + O(1)\right),$$

soit

$$\sum_{\substack{n\leqslant x\\ n\in\mathcal{D}}} \frac{f_m(n)}{n} = \sum_{\substack{k\leqslant x\\ k\in\mathcal{D}}} \frac{h_m(k)}{k} \left(\frac{4\log(x)}{\pi} + O(\log(2k))\right),$$

où on utilise le fait que $\log(k) \leqslant \log(2k)$. On obtient bien ainsi le bon terme principal et il ne reste plus qu'à vérifier qu'on a un terme d'erreur adéquat. On étudie

$$\sum_{k=1}^{+\infty} \frac{|h_m(k)|\log(2k)}{k}.$$

Le développement en produit eulérien de H_m montre que $h_m(k)$ est éventuellement non nul si, et seulement si, les nombres premiers intervenant dans la décomposition de k interviennent dans celle de m. On a

$$H_m(s) = r_0(m) \prod_{p|m} \sum_{\nu\geqslant 0} \frac{(-1)^\nu}{p^{\nu s}} = \sum_k \frac{h_m(k)}{k^s}.$$

On en déduit donc les relations

$$h_m(p^\nu) = 0 \quad \text{si } p \nmid m$$

et

$$h_m(p^\nu) = 2(-1)^\nu \quad \text{sinon.}$$

On va alors majorer le terme

$$\frac{\log(2k)}{k} = \frac{\log(2p_1^{\nu_1}...p_r^{\nu_r})}{p_1^{\nu_1}...p_r^{\nu_r}}$$

où les p_i sont tous les diviseurs premiers de m et les ν_i des entiers positifs ou nuls. On sait alors qu'on a toujours $k \leqslant 2^{k-1} \leqslant p^{k-1}$, on en déduit donc la série d'inégalités

$$\frac{\nu_{p_i}(p_1^{\nu_1}...p_r^{\nu_r})}{p_1^{\nu_1}...p_r^{\nu_r}} \leqslant \frac{\nu_i}{p_i^{\nu_i}} \leqslant \frac{1}{p_i}$$

et on a donc

$$\frac{\log(2k)}{k} = \frac{\log(2)}{k} + \sum_{p|m} \frac{\nu_p(k)}{k}\log(p) \leqslant 1 + \sum_{p|m} \frac{\log(p)}{p}$$

ce qui entraîne, puisque $H_m(0) = r_0(m)$ et de même $\tilde{H}_m(0) = r_0(m)$, la majoration

$$\sum_k \frac{|h_m(k)|\log(k)}{k} \leqslant r_0(m)\left(1 + \sum_{p|m} \frac{\log(p)}{p}\right)$$

ce qui convient. On a alors

$$\sum_{p|m} \frac{\log(p)}{p} \leqslant \sum_{j\leqslant\omega(m)} \frac{\log(p_i)}{p_i}$$

où p_i désigne le i-ème nombre premier. Le premier théorème de Mertens fournit

$$\sum_{p|m} \frac{\log(p)}{p} \ll \log(\omega(m)) \ll \log(2+\omega(m)).$$

On en déduit donc

$$\sum_k \frac{|h_m(k)|\log(k)}{k} \leqslant r_0(m)\log(2+\omega(m)).$$

On écrit alors $1 = \varphi^\dagger(m)\varphi^\dagger(m)^{-1}$ et on remarque que

$$\varphi^\dagger(m)^{-1} = \prod_{p|m}\left(1+\frac{1}{p}\right) \ll \log(\omega(m)) \ll \log(2+\omega(m)).$$

On en conclut donc que

$$\sum_k \frac{|h_m(k)|\log(k)}{k} \leqslant r_0(m)\varphi^\dagger(m)\log^2(2+\omega(m)),$$

ce qui permet d'achever la preuve du lemme. □

Utilisant le lemme qu'on vient de montrer, on déduit pour $\varepsilon > 0$ et $0 < \theta \leqslant 1$, que

$$\sum_{\substack{n\leqslant x\\ n\in\mathcal{D}}} \frac{|f_m(n)|}{n^\theta} \leqslant x^{1-\theta} \sum_{\substack{n\leqslant x\\ n\in\mathcal{D}}} \frac{|f_m(n)|}{n} \ll m^\varepsilon x^{1-\theta}\log(x).$$

On a utilisé $n \leqslant x$ pour majorer $n^{-\theta}$ par $x^{1-\theta}n^{-1}$ et on a également utilisé le fait que la fonction arithmétique $r_0\varphi^\dagger$ est majorée par m^ε. En effet,

$$r_0(p^\nu) \leqslant \nu + 1$$

et

$$\varphi^\dagger(p^\nu) = 1 + \frac{1}{p}$$

donc

$$\frac{r_0(p^\nu)\varphi^\dagger(p^\nu)}{p^{\varepsilon\nu}} \leqslant \frac{(\nu+1)(1+p)}{p^{1+\varepsilon\nu}} \underset{p^\nu\to+\infty}{\longrightarrow} 0.$$

On en déduit à présent la conjecture de Manin pour les surfaces de Châtelet considérées.

L'idée est bien évidemment d'injecter la formule asymptotique obtenue grâce au Théorème 2 de $\mathcal{U}(T)$ dans l'expression de $N(B)$ que l'on a obtenue dans le Lemme 28. La difficulté réside alors en la non-uniformité de cette formule asymptotique en les paramètres sur lesquels on somme. Pour parer à cette difficulté, on pose

$$S(B) = S^{\varepsilon_1,\varepsilon_2,\varepsilon_3}_{\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e}(B) = \sum_{\substack{n\leqslant N\\ n\in\mathcal{D}}} f_m(n)\mathcal{U}\left(\frac{B}{me^2n}\right),$$

avec $N = \frac{\delta B}{m^{\frac{5}{4}}e}$, de telle sorte que

$$N(B) = \frac{1}{2^7}\sum_{e=1}^{+\infty}\mu(e)\sum_{m\in\mathcal{D}}\mu(m)\sum_{\substack{\varepsilon_i\in\{-1,+1\}\\ \varepsilon_1\varepsilon_2\varepsilon_3=1}}\sum_{\substack{\mathbf{d},\mathbf{d}'\in\mathbb{N}^3\\ m=d_1d_2d_3,\mathbf{d}'|H}}\mu(d_1'd_2')\mu(d_3')\chi(d_1'd_2'd_3')\times$$

$$\sum_{\substack{k_4k_1k_1'|\gcd(\Delta_{23},m)\\ k_4k_2k_2'|\gcd(\Delta_{13},m)}}\sum_{\substack{k_4k_3k_3'|\gcd(\Delta_{12},m)\\ k_5k_5'|\gcd(\Delta_{12},d_1'd_2')\\ k_4k_4'|\gcd(\gcd(\Delta_{12},\Delta_{13},\Delta_{23}),m)}}\frac{\mu(k_1')\mu(k_2')\mu(k_3')\mu(k_4')\mu(k_5')}{3^{\omega(k_4)}2^{\omega(k_5)+\omega(k_1)+\omega(k_2)+\omega(k_3)}}S(B).$$

Posant

$$\sigma^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e) = \prod_p \sigma_p^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e),$$

on voit que le terme principal attendu pour $S(B)$ est donné par

$$2\pi^3\mathrm{vol}(\mathrm{R}^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(1))\sigma^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',\mathrm{e})\frac{\mathrm{B}}{\mathrm{me}^2}\sum_{\substack{\mathrm{n}\leqslant\mathrm{N}\\ \mathrm{n}\in\mathcal{D}}}\frac{\mathrm{f_m(n)}}{\mathrm{n}}$$

soit d'après ce qui précède

$$2\pi^2\mathrm{vol}(\mathrm{R}^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(1))\sigma^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',\mathrm{e})\mathrm{r(m)}\varphi^\dagger(\mathrm{m})\frac{\mathrm{B}\log(\mathrm{B})}{\mathrm{me}^2}.$$

On pose par conséquent

$$E^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e) =$$

$$\frac{1}{B\log(B)}\left|S(B) - 2\pi^2\mathrm{vol}(\mathrm{R}^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(1))\sigma^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',\mathrm{e})\mathrm{r(m)}\varphi^\dagger(\mathrm{m})\frac{\mathrm{B}\log(\mathrm{B})}{\mathrm{me}^2}\right|.$$

Commençons par voir que

$$E^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e) \underset{B\to+\infty}{\longrightarrow} 0,$$

à $\mathbf{e}$, $\mathbf{E}$, $\mathbf{d}$, $\mathbf{d}'$, $\mathbf{k}$, $\mathbf{k}'$ et e fixés. On utilise bien sûr pour cela le Lemme 31 et la formule asymptotique donnée par le Théorème 2. Pour ce faire, on écrit

$$E^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e) \leqslant$$

$$\frac{1}{B\log(B)}\left|S(B) - 2\pi^3\mathrm{vol}(\mathrm{R}^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(1))\sigma^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',\mathrm{e})\frac{\mathrm{B}}{\mathrm{me}^2}\sum_{\substack{\mathrm{n}\leqslant\mathrm{N}\\ \mathrm{n}\in\mathcal{D}}}\frac{\mathrm{f_m(n)}}{\mathrm{n}}\right|$$

$$+\frac{1}{B\log(B)}\left|2\pi^3\mathrm{vol}(\mathrm{R}^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(1))\sigma^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',\mathrm{e})\frac{\mathrm{B}}{\mathrm{me}^2}\sum_{\substack{\mathrm{n}\leqslant N\\ \mathrm{n}\in\mathcal{D}}}\frac{\mathrm{f_m(n)}}{\mathrm{n}}-\right.$$

$$\left.2\pi^2\mathrm{vol}(\mathrm{R}^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(1))\sigma^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',\mathrm{e})\mathrm{r(m)}\varphi^\dagger(\mathrm{m})\frac{\mathrm{B}\log(\mathrm{B})}{\mathrm{me}^2}\right|.$$

Commençons par traiter le premier terme qui est

$$\leqslant\frac{1}{B\log(B)}\sum_{\substack{n\leqslant N\\ n\in\mathcal{D}}}|f_m(n)|\left|\mathcal{U}\left(\frac{B}{me^2n}\right)-2\pi^3\mathrm{vol}(\mathrm{R}^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(1))\sigma^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',\mathrm{e})\frac{\mathrm{B}}{\mathrm{me}^2\mathrm{n}}\right|.$$

Or, l'estimation du Théorème 2 fournit que

$$\left|\mathcal{U}\left(\frac{B}{me^2n}\right)-2\pi^3\mathrm{vol}(\mathrm{R}^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(1))\sigma^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',\mathrm{e})\frac{\mathrm{B}}{\mathrm{me}^2\mathrm{n}}\right|$$

$$\ll\frac{B}{me^2n\log(B)^{\eta-\varepsilon}},$$

où ici on néglige les dépendances de la constante en les formes et en les paramètres $\mathbf{e}$, $\mathbf{E}$, $\mathbf{d}$, $\mathbf{d}'$, $\mathbf{k}$, $\mathbf{k}'$ et e qui sont fixés. On a donc que le premier terme est

$$\ll\frac{1}{\log(B)^{1+\eta-\varepsilon}}\sum_{\substack{n\leqslant N\\ n\in\mathcal{D}}}\frac{|f_m(n)|}{n}.$$

On utilise alors le Lemme 31 pour obtenir

$$\ll\frac{r(m)\varphi^\dagger(m)}{\log(B)^{\eta-\varepsilon}}.$$

Or, m est indépendant de B et on effectue le calcul avec tous les paramètres fixés ici donc on a bien que le premier terme tend vers 0 lorsque B tend vers l'infini. Regardons alors ce qu'il en est du deuxième terme. Pour les mêmes raisons, on a qu'il a une contribution

$$\ll\frac{1}{\log(B)}\left|\sum_{\substack{n\leqslant N\\ n\in\mathcal{D}}}\frac{f_m(n)}{n}-\frac{r(m)\varphi^\dagger(m)}{\pi}\log(B)\right|\ll\frac{r(m)\varphi^\dagger(m)\log^3(2+\omega(m))}{\log(B)}$$

qui, comme ci-dessus, tend vers 0 à m fixé, ce qui permet bien d'obtenir

$$E^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e)\underset{B\to+\infty}{\longrightarrow}0.$$

D'où,

$$S(B)=2\pi^2\mathrm{vol}(\mathrm{R}^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(1))\sigma^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',\mathrm{e})\mathrm{r(m)}\varphi^\dagger(\mathrm{m})\frac{\mathrm{B}\log(\mathrm{B})}{\mathrm{me}^2}+\mathrm{o(B}\log(\mathrm{B})),$$

soit encore

$$S(B)\sim2\pi^2\mathrm{vol}(\mathrm{R}^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(1))\sigma^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',\mathrm{e})\mathrm{r(m)}\varphi^\dagger(\mathrm{m})\frac{\mathrm{B}\log(\mathrm{B})}{\mathrm{me}^2}.$$

On voudrait maintenant remplacer cette estimation de $S(B)$ dans le formule donnant $N(B)$ qu'on a obtenue. On utilise pour cela un théorème de convergence dominée et il suffit donc pour pouvoir conclure de montrer la majoration

$$\sum_{e=1}^{+\infty}\sum_{m\in\mathcal{D}}\sum_{\substack{\varepsilon_i\in\{-1,+1\}\\ \varepsilon_1\varepsilon_2\varepsilon_3=1}}\sum_{\substack{\mathbf{d},\mathbf{d}'\in\mathbb{N}^3\\ m=d_1d_2d_3,\mathbf{d}'|H}}\sum_{\substack{k_4k_1k_1'|\gcd(\Delta_{23},m)\\ k_4k_2k_2'|\gcd(\Delta_{13},m)}}\sum_{\substack{k_4k_3k_3'\\ k_5k_5'|\gcd(\Delta_{12},m)\\ k_4k_4'|\gcd(\gcd(\Delta_{12},\Delta_{13},\Delta_{23}),m)}}\times$$

$$\left|\frac{\mu(k_1')\mu(k_2')\mu(k_3')\mu(k_4')\mu(k_5')}{3^{\omega(k_4)}2^{\omega(k_5)+\omega(k_1)+\omega(k_2)+\omega(k_3)}}\mu(e)\mu(m)\mu(d_1'd_2')\mu(d_3')\chi(d_1'd_2'd_3')E^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e)\right|\ll 1$$

où là encore on n'explicitera pas la constante puisqu'on en n'aura pas besoin. Pour cela, puisque tout les termes apparaissant dans la somme sont inférieurs à 1, il suffit de montrer

$$\sum_{e=1}^{+\infty}\sum_{m\in\mathcal{D}}\sum_{\substack{\varepsilon_i\in\{-1,+1\}\\ \varepsilon_1\varepsilon_2\varepsilon_3=1}}\sum_{\substack{\mathbf{d},\mathbf{d}'\in\mathbb{N}^3\\ m=d_1d_2d_3,\mathbf{d}'|H}}\sum_{\substack{k_4k_1k_1'|\gcd(\Delta_{23},m)\\ k_4k_2k_2'|\gcd(\Delta_{13},m)}}\sum_{\substack{k_4k_3k_3'|\gcd(\Delta_{12},m)\\ k_5k_5'|\gcd(\Delta_{12},d_1'd_2')\\ k_4k_4'|\gcd(\gcd(\Delta_{12},\Delta_{13},\Delta_{23}),m)}}E^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e)\ll 1.$$

Pour établir cela, on va majorer $E^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e)$. On avait obtenu la majoration

$$\mathcal{U}\left(\frac{B}{me^2n}\right)\ll(me)^{\varepsilon}\gcd(m,e)a'(\mathbf{E},\mathbf{\Delta},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e)\left(r_\infty(R^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(1))^2\frac{B}{me^2n}+\frac{r_\infty(R^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(1))^{1+\varepsilon}B^{\frac12+\varepsilon}}{m^{\frac12}en^{\frac12+\varepsilon}}\right)$$

(où on remarque qu'on n'a pas besoin du δ). Mais, puisque la somme sur les ε_i est finie, cela ne pose pas de problème de convergence et on peut donc écrire

$$\mathcal{U}\left(\frac{B}{me^2n}\right)\ll(me)^{\varepsilon}\gcd(m,e)a'(\mathbf{E},\mathbf{\Delta},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e)\left(\frac{B}{m^2e^2n}+\frac{B^{\frac12+\varepsilon}}{m^{\frac12}en^{\frac12+\varepsilon}}\right).$$

Prenant cette fois $N=\frac{\delta B}{m^{\frac54}e}$ (Lemme 29), on obtient grâce au Lemme 31 (δ ne dépend que des formes et d'aucun des paramètres) que

$$S(B)\ll(me)^{\varepsilon}\gcd(m,e)a'(\mathbf{E},\mathbf{\Delta},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e)\left(B\log(B)\frac{1}{m^2e^2}+B^{\frac12-\varepsilon}\log(B)\frac{B^{\frac12+\varepsilon}}{d^{\frac58}e^{\frac12}m^{\frac12}e}\right)$$

soit

$$S(B)\ll(me)^{\varepsilon}\gcd(m,e)a'(\mathbf{E},\mathbf{\Delta},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e)\left(B\log(B)\frac{1}{m^2e^2}+B\log(B)\frac{1}{m^{\frac98}e^{\frac32}}\right).$$

ce qui implique

$$\frac{1}{B\log(B)}|S(B)|\ll(me)^{\varepsilon}\gcd(m,e)a'(\mathbf{E},\mathbf{\Delta},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e)\left(\frac{1}{m^2e^2}+\frac{1}{m^{\frac98}e^{\frac32}}\right).$$

En utilisant à nouveau la remarque que ce qui dépend des ε_i peut passer dans la constante et les faits que

$$r(m)\varphi^{\dagger}(m)\ll m^{\varepsilon}$$

et que

$$\sigma^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e) \ll L_\infty^\varepsilon (me)^\varepsilon$$

où la constante L_∞ est ici indépendante des paramètres sur lesquels on somme, on obtient

$$\left|2\pi^2 \mathrm{vol}(\mathrm{R}^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(1))\sigma^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',\mathrm{e})\mathrm{r}(\mathrm{m})\varphi^\dagger(\mathrm{m})\frac{\mathrm{B}\log(\mathrm{B})}{\mathrm{me}^2}\right| \leqslant (me)^\varepsilon \frac{1}{me^2}.$$

On peut donc en conclure

$$E^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e) \ll (me)^\varepsilon \gcd(m,e) a'(\mathbf{e},\mathbf{\Delta},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e)\left(\frac{1}{m^2e^2}+\frac{1}{m^{\frac{9}{8}}e^{\frac{3}{2}}}+\frac{1}{me^2}\right).$$

On l'a vu, la somme sur les ε_i ne pose pas de problème puisqu'elle est finie, de même les sommes sur les $\mathbf{k}$, $\mathbf{k}'$ et $\mathbf{d}'$ sont finies donc ne posent pas de problème. Passons à la somme sur les $\mathbf{d}$. On somme sur les triplets vérifiant $m = d_1d_2d_3$ et à m fixé, on a un nombre de tels triplets $\ll m^\varepsilon$. Commençons par le remarquer pour les couples tels que $m = d_1d_2$. On en a exactement $\tau(m) = 2^{\omega(m)}$ (m sans facteur carré) car en effet, il suffit de se fixer un diviseur d_1 de m quelconque et alors d_2 est automatiquement fixé. Pour trois entiers, on se fixe un diviseur de m et pour chaque diviseur, on a autant de couples tels que $m/d_1 = d_2d_3$, on obtient donc

$$\sum_{k|m}\tau(m/k) = \sum_{k|m} 2^{\omega(m)-\omega(k)}$$

puisqu'on est sans facteur carré. On a en fait $\tau * \mathbf{1}$ triplets $\mathbf{d}$ et

$$\tau * \mathbf{1}(p^\nu) = \sum_{k=0}^{\nu}(k+1) = \nu + 1 + \frac{\nu(\nu+1)}{2}$$

et donc $\tau * \mathbf{1}(m) \ll m^\varepsilon$. Pour conclure à l'application du théorème de convergence dominée, il ne reste alors plus qu'à voir que

$$\sum_{e=1}^{+\infty}\sum_{m\in\mathcal{D}}(me)^\varepsilon \gcd(m,e) a'(\mathbf{E},\mathbf{\Delta},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e)\left(\frac{1}{m^2e^2}+\frac{1}{m^{\frac{9}{8}}e^{\frac{3}{2}}}+\frac{1}{me^2}\right)$$

converge. Cependant, on a pour l'instant

$$(me)^\varepsilon \gcd(m,e) a'(\mathbf{e},\mathbf{\Delta},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e)\left(\frac{1}{m^2e^2}+\frac{1}{m^{\frac{9}{8}}e^{\frac{3}{2}}}+\frac{1}{me^2}\right) \ll (me)^\varepsilon \gcd(m,e) a'(\mathbf{e},\mathbf{\Delta},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e)\frac{1}{me^2}$$

ce qui n'est pas assez bon pour obtenir une convergence. On améliore donc l'estimation qu'on a utilisé de $\sigma^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e)$. On a clairement que

$$\prod_{p\nmid m}\left|\sigma_p^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e)\right| \ll \sigma^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e) \ll (L_\infty me)^\varepsilon.$$

On améliore en revanche notre estimation de

$$\prod_{p|m}\left|\sigma_p^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e)\right|.$$

Si $p=2$, on a vu qu'il n'y avait pas de problèmes puisqu'on peut majorer par 4 et faire rentrer ça dans la constante. Pour les p impairs, on utilise la majoration donnée par le point f) du Lemme 3 :

$$\rho(p^{N_1},p^{N_2},p^{N_3}) \ll (N_3+1)p^{\min\left(2(N_1+N_2)+\frac{3N_3}{2},2(N_1+N_3)+N_2,2(N_2+N_3)+N_1\right)}. \tag{2.9}$$

On a alors

$$\left|\sigma_p^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e)\right| \leqslant \sum_{\boldsymbol{\nu}\in\mathbb{N}^3}\frac{\rho(p^{N_1},p^{N_2},p^{N_3})}{p^{2(N_1+N_2+N_3)}}$$

où les $N_i=\max(\nu_p(E_i),\nu_i+\nu_p(e_i))$ ont été définis plus haut. On a donc

$$\left|\sigma_p^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e)\right| \ll \sum_{\boldsymbol{\nu}\in\mathbb{N}^3}(N_3+1)\frac{1}{p^{\frac{N_1}{3}+\frac{N_2}{3}+\frac{N_3}{6}}}.$$

En effet, on utilise la majoration (2.9) et dans le cas où

$$2(N_1+N_2)+\frac{3N_3}{2} \leqslant 2(N_1+N_3)+N_2 \quad \text{et} \quad 2(N_1+N_2)+\frac{3N_3}{2} \leqslant 2(N_2+N_3)+N_1$$

ou de manière équivalente

$$N_1 \leqslant \frac{N_3}{2} \quad \text{et} \quad N_2 \leqslant \frac{N_3}{2},$$

on obtient la majoration

$$\ll \frac{p^{2(N_1+N_2)+\frac{3N_3}{2}}}{p^{2(N_1+N_2+N_3)}} = \frac{1}{p^{\frac{N_3}{2}}}$$

et en écrivant

$$\frac{N_3}{2}=\frac{N_3}{6}+\frac{N_3}{6}+\frac{N_3}{6} \geqslant \frac{N_3}{6}+\frac{N_1}{3}+\frac{N_2}{3},$$

on obtient bien la conclusion souhaitée. Dans le cas où

$$2(N_1+N_3)+N_2 \leqslant 2(N_2+N_3)+N_1 \quad \text{et} \quad 2(N_1+N_3)+N_2 \leqslant 2(N_1+N_2)+\frac{3N_3}{2}$$

ou de manière équivalente

$$N_1 \leqslant N_2 \quad \text{et} \quad \frac{N_3}{2} \leqslant N_2,$$

on obtient la majoration

$$\ll \frac{p^{2(N_1+N_3)+N_2}}{p^{2(N_1+N_2+N_3)}} = \frac{1}{p^{N_2}}$$

et on écrit

$$N_2=\frac{N_2}{3}+\frac{N_2}{3}+\frac{N_2}{3} \geqslant \frac{N_3}{6}+\frac{N_1}{3}+\frac{N_2}{3}$$

pour conclure. Le dernier cas étant parfaitement symétrique avec ce dernier, on a bien obtenue la majoration annoncée. On tire alors partie du fait que m soit sans facteur carré. On note $m=d_1d_2d_3$ et $\delta_i=\nu_p(d_i)$ de sorte qu'on peut supposer $\delta_1+\delta_2+\delta_3=1$ lorsque $p|m$. De plus, par définition de E_i et N_i, on voit que $N_i \leqslant \nu_i+\delta_i$ et donc on a

$$\prod_{p|m}\left|\sigma_p^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e)\right| \ll \prod_{p|m}p^{-\frac{\delta_1+\delta_2+\delta_3}{6}}\prod_{p|m}\sum_{\boldsymbol{\nu}\in\mathbb{N}^3}(N_3+1)\frac{1}{p^{\frac{\nu_1}{3}+\frac{\nu_2}{3}+\frac{\nu_3}{6}}}.$$

On a alors

$$\prod_{p|m} p^{-\frac{\delta_1+\delta_2+\delta_3}{6}} = \prod_{p|m} p^{-\frac{1}{6}} = m^{-\frac{1}{6}}$$

toujours puisque m est sans facteur carré. D'autre part,

$$\sum_{\boldsymbol{\nu}\in\mathbb{N}^3} (N_3+1)\frac{1}{p^{\frac{\nu_1}{3}+\frac{\nu_2}{3}+\frac{\nu_3}{6}}} \leqslant \sum_{\boldsymbol{\nu}\in\mathbb{N}^3} (\nu_3+\nu_p(e_3)+1)\frac{1}{p^{\frac{\nu_1}{3}+\frac{\nu_2}{3}+\frac{\nu_3}{6}}}.$$

Or,

$$\sum_{\boldsymbol{\nu}\in\mathbb{N}^3} (\nu_3+1)\frac{1}{p^{\frac{\nu_1}{3}+\frac{\nu_2}{3}+\frac{\nu_3}{6}}} \ll 1$$

et

$$\nu_p(e_3)\sum_{\boldsymbol{\nu}\in\mathbb{N}^3} \frac{1}{p^{\frac{\nu_1}{3}+\frac{\nu_2}{3}+\frac{\nu_3}{6}}} \ll \nu_p(e_3).$$

Or, $\nu_p(e_3) \ll \nu_p(m)$ puisque les $\mathbf{d}'$ sont bornées uniformément en les paramètres sur lesquels on somme. On a donc les majorations

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

et finalement

$$\prod_{p|m}\left|\sigma_p^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e)\right| \ll m^{-\frac{1}{6}+\varepsilon}.$$

On a par conséquent

$$|\sigma^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e)| \ll m^{-\frac{1}{6}+\varepsilon}e^{\varepsilon},$$

et en utilisant plutôt cette estimation, on obtient finalement

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

où on a bien au dénominateur uniquement des exposants strictement supérieurs à 1, si on choisit ε assez petit, qui vont permettre d'obtenir la convergence souhaitée. Ensuite, on remarque que

$$a'(\mathbf{E},\boldsymbol{\Delta},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e)$$

concerne les formes primitives, donc en fait on n'a pas de dépendance en e et on a plutôt

$$a'(\mathbf{E},\boldsymbol{\Delta},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e) = a'(\mathbf{E},\boldsymbol{\Delta},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}').$$

Par définition de cette quantité en (1.20), on obtient que

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

où la constante est une puissance de L_∞ et donc en particulier est indépendante des paramètres de sommation. On en déduit alors qu'on peut appliquer le théorème de convergence dominée si

$$\sum_{e=1}^{+\infty}\sum_{m\in\mathcal{D}}(me)^{\varepsilon}\gcd(m,e)\frac{1}{m^{\frac{9}{8}}e^{\frac{3}{2}}} \ll 1.$$

On peut choisir ε de façon à ce que les exposants au dénominateur restent strictement supérieurs à 1 et donc il suffit par exemple de prouver la convergence de

$$\sum_{e=1}^{+\infty}\sum_{m\in\mathcal{D}}\gcd(m,e)\frac{1}{m^{\frac{9}{8}}e^{\frac{3}{2}}}.$$

Pour le voir, on tire partie de la multiplicativité et on regarde le comportement des facteurs eulériens qui sont donnés par

$$F_p=\sum_{a,b=0}^{\infty}\frac{p^{\min(a,b)}}{p^{\frac{9a}{8}+\frac{3b}{2}}}=1+\sum_{\substack{a,b=0\\ab\neq 0}}^{\infty}\frac{p^{\min(a,b)}}{p^{\frac{9a}{8}+\frac{3b}{2}}}.$$

On sépare donc la somme selon les positions relatives de a et b. On a donc

$$F_p=1+\sum_{a=1}^{+\infty}\sum_{b=0}^{a-1}\frac{p^{\min(a,b)}}{p^{\frac{9a}{8}+\frac{3b}{2}}}+\sum_{a=0}^{+\infty}\sum_{b=0}^{a}\frac{p^{\min(a,b)}}{p^{\frac{9a}{8}+\frac{3b}{2}}}.$$

La première somme donne

$$\sum_{a=1}^{+\infty}\sum_{b=0}^{a-1}\frac{1}{p^{\frac{9a}{8}+\frac{b}{2}}}=\sum_{a=1}^{+\infty}\frac{1}{p^{\frac{9a}{8}}}\sum_{b=0}^{a-1}\frac{1}{p^{\frac{b}{2}}}\leqslant\sum_{a=1}^{+\infty}\frac{a}{p^{\frac{9a}{8}}}\ll p^{-\frac{9}{8}}.$$

La deuxième somme donne

$$\sum_{a=0}^{+\infty}\sum_{b=0}^{a}\frac{1}{p^{\frac{a}{8}+\frac{3b}{2}}}=\sum_{b=1}^{+\infty}\sum_{a=0}^{b}\frac{1}{p^{\frac{a}{8}+\frac{3b}{2}}}\leqslant\sum_{b=1}^{+\infty}\frac{b}{p^{\frac{3b}{2}}}\ll p^{-\frac{3}{2}}.$$

On en déduit que

$$F_p\ll 1+p^{-\frac{9}{8}}=1+p^{-1-\frac{1}{8}}$$

et donc que

$$\sum_{e=1}^{+\infty}\sum_{m\in\mathcal{D}}\gcd(m,e)\frac{1}{m^{\frac{9}{8}}e^{\frac{3}{2}}}=\prod_p F_p\ll 1.$$

On peut donc appliquer le théorème de convergence dominée pour obtenir :

Théorème 6. *Posant $r_0=\frac{1}{4}r$, on a*

$$N(B)\underset{B\to+\infty}{\sim}c_0B\log(B),$$

avec

$$c_0=\frac{\pi^2}{2^4}\sum_{e=1}^{+\infty}\frac{\mu(e)}{e^2}\sum_{m\in\mathcal{D}}\frac{\mu(m)r_0(m)\varphi^\dagger(m)}{m}\sum_{\substack{\varepsilon_i\in\{-1,+1\}\\ \varepsilon_1\varepsilon_2\varepsilon_3=1}}\mathrm{vol}\left(\mathrm{R}^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(1)\right)\sum_{\substack{\mathbf{d},\mathbf{d}'\in\mathbb{N}^3\\ m=d_1d_2d_3,\mathbf{d}'|H}}\mu(\mathrm{d}_1'\mathrm{d}_2')\mu(\mathrm{d}_3')\chi(\mathrm{d}_1'\mathrm{d}_2'\mathrm{d}_3')\times$$

$$\sum_{\substack{k_4k_1k_1'|\gcd(\Delta_{23},m)\\ k_4k_2k_2'|\gcd(\Delta_{13},m)}}\ \sum_{\substack{k_4k_3k_3'|\gcd(\Delta_{12},m)\\ k_5k_5'|\gcd(\Delta_{12},d_1'd_2')\\ k_4k_4'|\gcd(\gcd(\Delta_{12},\Delta_{13},\Delta_{23}),m)}}\frac{\mu(k_1')\mu(k_2')\mu(k_3')\mu(k_4')\mu(k_5')}{3^{\omega(k_4)}2^{\omega(k_5)+\omega(k_1)+\omega(k_2)+\omega(k_3)}}\sigma^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}',e).$$

Ceci démontre donc la conjecture de Manin dans le cas des surfaces de Châtelet considérées.

Chapitre 3

La conjecture de Peyre

Pour conclure le traitement de ces surfaces de Châtelet, il reste à montrer que la constante c_0 obtenue dans le Théorème 6 est en accord avec la conjecture de Peyre. On va noter c_X la constante conjecturée par Peyre.

3.1 La constante de Peyre

3.1.1 Généralités

Si on note $C^1_{\text{eff}}(X)$ le cône de $\text{Pic}(X) \otimes_{\mathbb{Z}} \mathbb{C}$ engendré par les classes de diviseurs effectifs et $C^1_{\text{eff}}(X)^\vee$ le cône dual défini par

$$C^1_{\text{eff}}(X)^\vee = \{y \in \text{Pic}(X) \otimes_{\mathbb{Z}} \mathbb{R}^\vee \quad | \quad \forall x \in C^1_{\text{eff}}(X), \quad \langle x, y\rangle \geqslant 0\},$$

où $\langle ., .\rangle$ désigne la forme d'intersection. Si ω_X^{-1} désigne l'inverse du faisceau canonique sur X, alors $\alpha(X)$ est le volume du polytope $P(X)$ suivant

$$P(X) = \{y \in C^1_{\text{eff}}(X)^\vee \quad | \quad \langle y, \omega_X^{-1}\rangle = 1\}$$

où l'hyperplan $\langle y, \omega_X^{-1}\rangle = 1$ est muni d'une mesure adéquate ([3]). Ensuite on a

$$\beta(X) = \#H^1(\text{Gal}(\overline{\mathbb{Q}}, \mathbb{Q}), \text{Pic}(\overline{X})) = \text{Coker}\left(\text{Br}(\mathbb{Q}) \to \text{Br}(X)\right),$$

où $\overline{X} = X \times_{\text{Spec}(\mathbb{Q})} \text{Spec}(\overline{\mathbb{Q}})$. On rappelle alors que conjecturalement, on a

$$c_X = \alpha(X)\beta(X)\omega_H(\overline{X(\mathbb{Q})}),$$

où $\omega_H(\overline{X(\mathbb{Q})})$ est un nombre de Tamagawa que l'on explicitera plus tard.

3.1.2 La constante de Peyre dans le cas des surfaces de Châtelet considérées

Dans le cas des surfaces de Châtelet, on peut montrer qu'on a toujours $\alpha(X) = 1$ et pour calculer $\beta(X)$, on utilise le résultat suivant tiré de [34] dont on ne donne pas la preuve ici.

Proposition 1. *Soit k un coprs parfait et X la compactification naturelle et lisse de la surface donnée par*

$$y^2 - bz^2 = aP(x),$$

avec $P \in k[x]$ un polynôme de degré pair et a et b dans k^*. Soit $\overline{d_1}$,...,$\overline{d_m}$ les classes modulo 2 des degrés des facteurs irréductibles de P, alors le groupe $H^1(k, Pic(\overline{X}))$ est isomorphe au quotient de l'orthogonal de $\langle(\overline{d_1}, ..., \overline{d_m})\rangle$ dans $(\mathbb{Z}/2\mathbb{Z})^m$ pour la forme diagonale classique par $\langle(1, ..., 1)\rangle$.

En particulier, ici $b = -1$, $a = 1$ et $k = \mathbb{Q}$ et P est de degré 4. Si P est irréductible, on a $(\overline{d_1}, ..., \overline{d_m}) = (0)$ et donc l'orthogonal de $\{0\}$ dans $\mathbb{Z}/2\mathbb{Z}$ est tout l'espace et lorsqu'on quotiente par un sous-espace e dimension 1, on va obtenir $\{0\}$ et donc

$$\#H^1(\mathrm{Gal}(\overline{\mathbb{Q}}, \mathbb{Q}), \mathrm{Pic}(\overline{X})) = 0.$$

De même, lorsque $P = LC$, on a $(\overline{d_1}, ..., \overline{d_m}) = (1, 1)$ et l'orthogonal dans $(\mathbb{Z}/2\mathbb{Z})^2$ est de dimension 1 donc le quotient est nul et on a toujours

$$\#H^1(\mathrm{Gal}(\overline{\mathbb{Q}}, \mathbb{Q}), \mathrm{Pic}(\overline{X})) = 0.$$

Dans le cas $P = L_1L_2L_3L_4$, on a $(\overline{d_1}, ..., \overline{d_m}) = (1, 1, 1, 1)$ et l'orthogonal dans $(\mathbb{Z}/2\mathbb{Z})^4$ est de dimension 3 donc le quotient est de dimension 2 donc isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$ et on a bien

$$\#H^1(\mathrm{Gal}(\overline{\mathbb{Q}}, \mathbb{Q}), \mathrm{Pic}(\overline{X})) = 4,$$

tout ceci étant conforme aux cas précédemment étudiés. Enfin, dans notre cas, on a $P = L_1L_2Q$ donc $(\overline{d_1}, ..., \overline{d_m}) = (1, 1, 0)$ et l'orthogonal dans $(\mathbb{Z}/2\mathbb{Z})^3$ est de dimension 2 donc le quotient est de dimension 1 donc isomorphe à $(\mathbb{Z}/2\mathbb{Z})$ et on a alors

$$\#H^1(\mathrm{Gal}(\overline{\mathbb{Q}}, \mathbb{Q}), \mathrm{Pic}(\overline{X})) = 2.$$

D'après [35] et [7], on déduit que l'ensemble des classes d'isomorphismes de torseurs universels au-dessus de X possédant au moins un point rationnel est fini, ce qui permet d'exhiber une partition finie de l'ensemble des points rationnels de X, indexée par toute famille de représentants de ces classes d'isomorphismes. La constante de Peyre s'écrit alors comme la somme des constantes relatives à chaque élément de la partition. Considérons un point rationnel $Q = (y, z, t, u, v)$ tel que $(y, z, t) = (u, v) = 1$ et

$$t^2L_1(u, v)L_2(u, v)Q(u, v) = y^2 + z^2.$$

Alors, on peut déjà déduire l'existence d'un unique triplet $(\varepsilon_1, \varepsilon_2, \varepsilon_3) \in \{-1, +1\}$ (le signe de $L_i(u, v)$ et $Q(u, v)$) tels que $\varepsilon_1\varepsilon_2\varepsilon_3 = 1$ et

$$\varepsilon_i L_i(u, v) > 0 \quad \text{et} \quad \varepsilon_3 Q(u, v) > 0,$$

puisqu'on avait vu que la contribution des termes tels que $L_1(u, v)L_2(u, v)Q(u, v) = 0$ était $O(1)$. Puis, on pose

$$\Delta_{i,j}^{sc} = \prod_{\substack{p|\Delta_{i,j} \\ p\equiv 1[4]}} p \quad \text{et} \quad \Delta_{i,j}^{nsc} = \prod_{\substack{p|\Delta_{i,j} \\ p\equiv 3[4]}} p.$$

Le fait que $L_1(u,v)L_2(u,v)Q(u,v)$ soit une somme de deux carrés ($t \neq 0$ car sinon $y = z = 0$ et on a une contradiction sur la coprimalité) implique que si $p \equiv 3[4]$, on ait

$$\nu_p(L_1(u,v)L_2(u,v)Q(u,v)) = \nu_p(L_1(u,v)) + \nu_p(L_2(u,v)) + \nu_p(Q(u,v)) \equiv 0[2].$$

On pose alors

$$m_1 = \prod_{\substack{p\equiv 3[4] \\ \nu_p(L_1(u,v))\equiv 1[2]}} p, \quad m_2 = \prod_{\substack{p\equiv 3[4] \\ \nu_p(L_2(u,v))\equiv 1[2]}} p \quad \text{et} \quad m_3 = \prod_{\substack{p\equiv 3[4] \\ \nu_p(Q(u,v))\equiv 1[2]}} p,$$

de sorte que $m_i | L_i(u,v)$ et $m_3 | Q(u,v)$. Mais on a mieux, si $p|m_1$, alors puisque $\nu_p(L_1(u,v) \geq 1$, $p|L_1(u,v)$ et

$$\nu_p(L_1(u,v)L_2(u,v)Q(u,v)) = \nu_p(L_1(u,v)) + \nu_p(L_2(u,v)) + \nu_p(Q(u,v)) \equiv 0[2],$$

il existe un et un seul des deux indices $\{2,3\}$ tel que $\nu_p(L_2(u,v))$ ou $\nu_p(Q(u,v))$ soit impair (et l'autre est donc pair). On a donc que $p|m_1$ et $p|m_2$ par exemple et puisque $(u,v) = 1$ comme on l'a vu précédemment, cela implique que $p|\Delta_{12}^{nsc}$, si bien qu'on en déduit les relations

$$m_1 | [\Delta_{12}^{nsc}, \Delta_{13}^{nsc}], \quad m_2 | [\Delta_{12}^{nsc}, \Delta_{23}^{nsc}] \quad \text{et} \quad m_3 | [\Delta_{13}^{nsc}, \Delta_{23}^{nsc}],$$

et

$$\nu_p\left(\frac{L_i(u,v)}{m_i}\right) \equiv \nu_p\left(\frac{Q(u,v)}{m_3}\right) \equiv 0[2],$$

pour tous les nombres premiers $p \equiv 3[4]$. De plus, $m_1m_2m_3$ est un carré car on a pour chaque premier p qui le divise, $p^2||m_1m_2m_3$ d'après ce qui précède. On montre alors de manière analogue à la proposition 4.9 de [18] qu'on obtient ainsi un système de représentants des classes d'isomorphie de torseurs universels (tout point rationnel de X apartient à un et un seul torseur) indexée par les tels triplets $\boldsymbol{\varepsilon}$ et $\mathbf{m}$. On a donc en particulier

$$X(\mathbb{Q}) = \bigsqcup_{\substack{\boldsymbol{\varepsilon}\in\Sigma \\ \mathbf{m}\in M}} X_{\boldsymbol{\varepsilon},\mathbf{m}}(\mathbb{Q}),$$

où

$$\Sigma = \{\boldsymbol{\varepsilon} \in \{-1,+1\}^3 \quad | \quad \varepsilon_1\varepsilon_2\varepsilon_3 = 1\}$$

et

$$M = \{\mathbf{m} \in \mathbb{N}^3 \quad | \quad m_i | [\Delta_{12}^{nsc}, \Delta_{i3}^{nsc}], \quad m_3 | [\Delta_{13}^{nsc}, \Delta_{23}^{nsc}], \quad \sqrt{m_1m_2m_3} \in \mathbb{N}, \quad (m_1,m_2,m_3) = 1\}.$$

Si on suppose l'abscence d'obstruction de Brauer-Manin, alors un résultat de [19] montre que si X a des points rationnels dns chaque complété de $\mathbb{Q}$, alors il existe un torseur $\mathcal{T}_{\boldsymbol{\varepsilon},\mathbf{m}}$ pour lequel il en est de même. Or, un des intérêts des torseurs est qu'ils sont géomériquement plus simples et en particulier, ils vérifient le principe de Hasse. On peut donc en déduire l'existence d'un point rationnel de $\mathcal{T}_{\boldsymbol{\varepsilon},\mathbf{m}}(\mathbb{Q})$ et donc de $X(\mathbb{Q})$ et donc de X, ce qui montre que X vérifie la principe de Hasse sous l'hypothèse précédente.

On déduit de la décomposition

$$X(\mathbb{Q}) = \bigsqcup_{\substack{\boldsymbol{\varepsilon}\in\Sigma \\ \mathbf{m}\in M}} X_{\boldsymbol{\varepsilon},\mathbf{m}}(\mathbb{Q})$$

que la constante de Peyre ([26]) s'écrit

$$c_X = 2 \sum_{\substack{\boldsymbol{\varepsilon}\in\Sigma \\ \mathbf{m}\in M}} \omega_H(\overline{X_{\boldsymbol{\varepsilon},\mathbf{m}}(\mathbb{Q})}),$$

où par définition de la mesure de Tamagawa,

$$\omega_H(\overline{X_{\boldsymbol{\varepsilon},\mathbf{m}}(\mathbb{Q})}) = \omega_\infty(\boldsymbol{\varepsilon},\mathbf{m}) \prod_p \omega_p(\boldsymbol{\varepsilon},\mathbf{m}),$$

où $\omega_\infty(\boldsymbol{\varepsilon},\mathbf{m})$ et $\omega_p(\boldsymbol{\varepsilon},\mathbf{m})$ sont respectivement les densités archimédiennes et $p-$adiques ssociées à la partie $X_{\boldsymbol{\varepsilon},\mathbf{m}}(\mathbb{Q})$ de $X(\mathbb{Q})$. Cette formule découle de la vérificaton du principe de Hasse sur les torseurs universels, la densité de points rationnels est alors un produit de densités.

On donne alors des expressions pour les $\omega_\infty(\boldsymbol{\varepsilon},\mathbf{m})$ et $\omega_p(\boldsymbol{\varepsilon},\mathbf{m})$. Supposons dans un premier temps que $p \nmid 2\Delta_{12}^{nsc}\Delta_{13}^{nsc}\Delta_{23}^{nsc}$. Alors dans ce cas là, on a

$$\omega_p(\boldsymbol{\varepsilon},\mathbf{m}) = \lim_{n\to+\infty} p^{-4n} \# \left\{ (u,v,y,z,t) \in (\mathbb{Z}/p^n\mathbb{Z})^5 \quad \middle| \quad \begin{array}{l} t^2 L_1(u,v)L_2(u,v)Q(u,v) = y^2+z^2 \\ p\nmid (u,v), \quad p\nmid (y,z,t) \end{array} \right\}.$$

On utilise l'expression de $S(A;p^n)$ donnée dans le Lemme 23 pour calculer ce terme. On commence par traiter le cas $p \equiv 3[4]$. Dans ce cas, on a nécessairement $(t,p)=1$ car sinon on obtiendrait

$$y^2+z^2 \equiv 0[p]$$

ce qui impliquerait que -1 serait un carré dans $\mathbb{F}_p$. On a donc

$$p \nmid (y,z,t) \Longleftrightarrow p \not| t$$

de sorte que le cardinal

$$\# \left\{ (u,v,y,z,t) \in (\mathbb{Z}/p^n\mathbb{Z})^5 \quad \middle| \quad \begin{array}{l} t^2 L_1(u,v)L_2(u,v)Q(u,v) = y^2+z^2 \\ p\nmid (u,v), \quad p\nmid (y,z,t) \end{array} \right\}$$

est donné par

$$\varphi(p^n) \times \# \left\{ (u,v,y,z) \in (\mathbb{Z}/p^n\mathbb{Z})^4 \quad \middle| \quad \begin{array}{l} L_1(u,v)L_2(u,v)Q(u,v) = y^2+z^2 \\ p\nmid (u,v) \end{array} \right\}.$$

En effet, on choisit un t inversible et ensuite on a

$$L_1(u,v)L_2(u,v)Q(u,v) = (y/t)^2 + (z/t)^2.$$

Utilisant que $\varphi(p^n) = p^n\left(1-\frac{1}{p}\right)$, on obtient l'égalité

$$\omega_p(\boldsymbol{\varepsilon},\mathbf{m}) = \lim_{n\to+\infty} \frac{1-\frac{1}{p}}{p^{3n}} \# \left\{ (u,v,y,z) \in (\mathbb{Z}/p^n\mathbb{Z})^4 \quad \middle| \quad \begin{array}{l} L_1(u,v)L_2(u,v)Q(u,v) = y^2+z^2 \\ p\nmid (u,v) \end{array} \right\}.$$

On suit alors le même raisonnement que dans la section 1.6 en séparant selon la valuation $p-$adique de $L_1(u,v)L_2(u,v)Q(u,v)$ pour obtenir

$$\omega_p(\boldsymbol{\varepsilon},\mathbf{m}) = \lim_{n\to+\infty} \frac{1-\frac{1}{p^2}}{p^{2n}} \sum_{\substack{0\leq k<n\\ 2|k}} \#\left\{(u,v)\in(\mathbb{Z}/p^n\mathbb{Z})^2 \quad \middle| \quad \begin{array}{l}\nu_p(L_1(u,v)L_2(u,v)Q(u,v))=k\\ p\nmid(u,v)\end{array}\right\},$$

puisque $S_0(L_1(u,v)L_2(u,v)Q(u,v),p^n)=p^n(1+\frac{1}{p})$ si $k<n$ et $2|k$. Or, pour $k\geq 1$, on a

$$\#\left\{(u,v)\in(\mathbb{Z}/p^n\mathbb{Z})^2 \quad \middle| \quad \begin{array}{l}\nu_p(L_1(u,v)L_2(u,v)Q(u,v))=k\\ p\nmid(u,v)\end{array}\right\} =$$

$$p^{2n}\left(\frac{\rho^*(p^k;L_1L_2Q)}{p^{2k}} - \frac{\rho^*(p^{k+1};L_1L_2Q)}{p^{2(k+1)}}\right),$$

où

$$\rho^*(p^k;L_1L_2Q) = \#\{\mathbf{x}\in\left(\mathbb{Z}/p^k\mathbb{Z}\right)^2 \quad | \quad p^k|L_1(\mathbf{x})L_2(\mathbf{x})Q(\mathbf{x}), \quad (x_1,x_2,p)=1\}.$$

En effet, on compte les couples tels que la valuation p-adique soit plus grande que k et on enlève ceux de valuation strictement plus grande que k. Et enfin, le facteur p^{2n} vient du fait qu'on a

$$p^{2n}\frac{\rho^*(p^k;L_1L_2Q)}{p^{2k}} = \#\{\mathbf{x}\in(\mathbb{Z}/p^n\mathbb{Z})^2 \quad | \quad p^k|L_1(\mathbf{x})L_2(\mathbf{x})Q(\mathbf{x}), \quad (x_1,x_2,p)=1\},$$

puisque tout ne dépend que de la classe de $\mathbf{x}$ modulo p^k. Dans le cas où $k=0$, on prend tous les couples (u,v) tels que $p\nmid(u,v)$. On a

$$\varphi(p^n)p^N + p^n\varphi(p^n) - \varphi(p^n)^2 = p^{2n}\left(1-\frac{1}{p^2}\right)$$

tels couples et on obtient donc

$$p^{2n}\left(1-\frac{1}{p^2}-\frac{\rho^*(p;L_1L_2Q)}{p^2}\right).$$

Finalement

$$\omega_p(\boldsymbol{\varepsilon},\mathbf{m}) = \left(1-\frac{1}{p^2}\right)\left(1-\frac{1}{p^2}-\frac{\rho^*(p;L_1L_2Q)}{p^2}+\sum_{\substack{1\leq k\\ 2|k}}\frac{\rho^*(p^k;L_1L_2Q)}{p^{2k}}-\frac{\rho^*(p^{k+1};L_1L_2Q)}{p^{2(k+1)}}\right).$$

Puisque dans ce cas, on a $\chi(p^\nu)=(-1)^\nu$, on en déduit que (grâce à la condition $k|2$ qui implique qu'on n'a pas de simplification) que

$$\omega_p(\boldsymbol{\varepsilon},\mathbf{m}) = \left(1-\frac{1}{p^2}\right)\left(1-\frac{1}{p^2}+\sum_{1\leq\nu}\frac{\chi(p^\nu)\rho^*(p^\nu;L_1L_2Q)}{p^{2\nu}}\right).$$

Passons désormais au cas $p\equiv 1[4]$. On ne peut plus effectuer la simplification par t comme précédemment. On raisonne donc selon la valuation p-adique de t. Commençons par traiter

le cas $\nu_p(t) = 0$. Dans ce cas, t est inversible modulo p et donc on peut faire comme précédemment mais en utilisant cette fois la formule $S_0((L_1(u,v)L_2(u,v)Q(u,v), p^n) = p^n(1+k)(1-\frac{1}{p})$ si $k < n$ de façon à obtenir, si on note $\omega_p(\boldsymbol{\varepsilon}, \mathbf{m})(l)$ la contribution de $\omega_p(\boldsymbol{\varepsilon}, \mathbf{m})$ des termes tels que $\nu_p(t) = l \geq 0$, l'expression

$$\omega_p(\boldsymbol{\varepsilon}, \mathbf{m})(0) = \left(1 - \frac{1}{p}\right)^2 \left(1 - \frac{1}{p^2} - \frac{\rho^*(p; L_1L_2Q)}{p^2} + \sum_{1 \leq k} (k+1) \left(\frac{\rho^*(p^k; L_1L_2Q)}{p^{2k}} - \frac{\rho^*(p^{k+1}; L_1L_2Q)}{p^{2(k+1)}}\right)\right)$$

Par téléscopage, on en déduit

$$\omega_p(\boldsymbol{\varepsilon}, \mathbf{m})(0) = \left(1 - \frac{1}{p}\right)^2 \left(1 - \frac{1}{p^2} + \sum_{1 \leq \nu} \frac{\chi(p^\nu)\rho^*(p^\nu; L_1L_2Q)}{p^{2\nu}}\right).$$

Il reste alors à traiter les cas $l \geq 1$. Dans ce cas $p|t$ et donc

$$p \nmid (y, z, t) \Longleftrightarrow p \nmid (y, z)$$

et on sépare à nouveau suivant $k = \nu_p(L_1(u,v)L_2(u,v)Q(u,v))$. Cette fois, on utilise la formule $S_0(t^2L_1(u,v)L_2(u,v)Q(u,v), p^n) = p^n(1+k+2l)\left(1-\frac{1}{p}\right)$ pour $k + 2l < n$ pour obtenir l'égalité

$$\omega_p(\boldsymbol{\varepsilon}, \mathbf{m})(l) = \lim_{n \to +\infty} \frac{p^{n-l}}{p^{4n}} \sum_{0 \leq k+2l < n} \times$$

$$\#\left\{(u,v,y,z) \in (\mathbb{Z}/p^n\mathbb{Z})^4 \quad \middle| \quad \begin{array}{l} \nu_p(L_1(u,v)L_2(u,v)Q(u,v)) = k \\ t^2L_1(u,v)L_2(u,v)Q(u,v) = y^2 + z^2 \\ p \nmid (u,v), \quad p \nmid (y,z) \end{array}\right\}.$$

On choisit t de valuation l dans $\mathbb{Z}/p^n\mathbb{Z}$ et ensuite il reste le choix de (y,z,u,v), donc on a p^{n-l} choix pour t en particulier. Puis on va choisir les (u,v) selon la valuation $p-$adique et ensuite le $S(A;p^n)$ donne les (y,z), le reste donnant une limite nulle. On a alors

$$\#\left\{(u,v,y,z) \in (\mathbb{Z}/p^n\mathbb{Z})^4 \quad \middle| \quad \begin{array}{l} \nu_p(L_1(u,v)L_2(u,v)Q(u,v)) = k \\ t^2L_1(u,v)L_2(u,v)Q(u,v) = y^2 + z^2 \\ p \nmid (u,v) \end{array}\right\} = p^n\left(1 - \frac{1}{p}\right)(k+1+2l)\times$$

$$\#\left\{(u,v) \in (\mathbb{Z}/p^n\mathbb{Z})^2 \quad \middle| \quad \begin{array}{l} \nu_p(L_1(u,v)L_2(u,v)Q(u,v)) = k \\ p \nmid (u,v), \end{array}\right\}$$

où

$$\#\left\{(u,v) \in (\mathbb{Z}/p^n\mathbb{Z})^2 \quad \middle| \quad \begin{array}{l} \nu_p(L_1(u,v)L_2(u,v)Q(u,v)) = k \\ p \nmid (u,v), \end{array}\right\} =$$

$$p^{2n}\left(\frac{\rho^*(p^k; L_1L_2Q)}{p^{2k}} - \frac{\rho^*(p^{k+1}; L_1L_2Q)}{p^{2(k+1)}}\right)$$

lorsque $k \geq 1$ et

$$\#\left\{(u,v) \in (\mathbb{Z}/p^n\mathbb{Z})^2 \quad \middle| \quad \begin{array}{l} \nu_p(L_1(u,v)L_2(u,v)Q(u,v)) = 0 \\ p \nmid (u,v), \end{array}\right\} = p^{2n}\left(1 - \frac{1}{p^2} - \frac{\rho^*(p; L_1L_2Q)}{p^2}\right).$$

Cependant, jusqu'à présent, on a compté tout le monde et pas seulement les couples tels que $p \nmid (y,z)$. Il faut donc retrancher à ces quantités ceux qui s'écrivent $y = py'$ et $z = pz'$ et on veut donc compter les $(y,z) \in (\mathbb{Z}/p^n\mathbb{Z})^2$ tels que

$$\left(\frac{t}{p}\right)^2 L_1(u,v)L_2(u,v)Q(u,v) = (y')^2 + (z')^2[p^{n-2}].$$

On paut appliquer la formule dès que $2(l-1)+k < n-2$ soit $2l+k < n$ donc exactement pour les mêmes indices que dans la somme ci-dessus. De plus, pour pour (u,v) tels que $\nu_p(L_1(u,v)L_2(u,v)Q(u,v)) = k$ avec k vérifiant cette inégalité, on obtient

$$S_0(L_1(u,v)L_2(u,v)Q(u,v), p^{n-2}) = p^{n-2}\left(1-\frac{1}{p}\right)(k+1+2(l-1)).$$

Or, $px' = px''$ si, et seulement si, x' et x'' sont égaux modulo p^{n-1} donc les solutions (x',y') se remontent en p^2 couples modulo p^{n-1} qui, multipliés par p, donnent tous les (x,y) divisibles par p. On obtient par conséquent

$$p^{n-2}p^2\left(1-\frac{1}{p}\right)(k+1+2(l-1))\#\left\{(u,v)\in(\mathbb{Z}/p^n\mathbb{Z})^2 \;\middle|\; \begin{array}{l}\nu_p(L_1(u,v)L_2(u,v)Q(u,v))=k\\ p\nmid(u,v),\end{array}\right\}$$

et en réexploitant les formules précédentes, on en déduit finalement l'expression

$$\omega_p(\boldsymbol{\varepsilon},\mathbf{m})(l) = \frac{\left(1-\frac{1}{p}\right)^2}{p^l}\left((2l+1)\left(1-\frac{1}{p^2}-\frac{\rho^*(p;L_1L_2Q)}{p^2}\right)+\right.$$

$$\sum_{0\le k}(k+1+2l)\left(\frac{\rho^*(p^k;L_1L_2Q)}{p^{2k}}-\frac{\rho^*(p^{k+1};L_1L_2Q)}{p^{2(k+1)}}\right)-(2(l-1)+1)\left(1-\frac{1}{p^2}-\frac{\rho^*(p;L_1L_2Q)}{p^2}\right)-$$

$$\left.\sum_{0\le k}(k+1+2(l-1))\left(\frac{\rho^*(p^k;L_1L_2Q)}{p^{2k}}-\frac{\rho^*(p^{k+1};L_1L_2Q)}{p^{2(k+1)}}\right)\right).$$

Ainsi, on a

$$\omega_p(\boldsymbol{\varepsilon},\mathbf{m})(l) = 2\frac{\left(1-\frac{1}{p}\right)^2}{p^l}\left(1-\frac{1}{p^2}-\frac{\rho^*(p;L_1L_2Q)}{p^2}+\sum_{0\le k}\left(\frac{\rho^*(p^k;L_1L_2Q)}{p^{2k}}-\frac{\rho^*(p^{k+1};L_1L_2Q)}{p^{2(k+1)}}\right)\right),$$

soit

$$\omega_p(\boldsymbol{\varepsilon},\mathbf{m})(l) = 2\frac{\left(1-\frac{1}{p}\right)^2}{p^l}\left(1-\frac{1}{p^2}\right)$$

par téléscopage. Or,

$$\omega_p(\boldsymbol{\varepsilon},\mathbf{m}) = \sum_{l\ge 0}\omega_p(\boldsymbol{\varepsilon},\mathbf{m})(l)$$

et donc d'après ce qui précède, on a

$$\omega_p(\boldsymbol{\varepsilon},\mathbf{m}) = \left(1-\frac{1}{p}\right)^2\left(1-\frac{1}{p^2}+\sum_{1\le\nu}\frac{\chi(p^\nu)\rho^*(p^\nu;L_1L_2Q)}{p^{2\nu}}\right)+2\left(1-\frac{1}{p}\right)^2\left(1-\frac{1}{p^2}\right)\sum_{l\ge 1}p^{-l}.$$

On calcule alors

$$2\left(1-\frac{1}{p}\right)^2\left(1-\frac{1}{p^2}\right)\sum_{l\geq 1}p^{-l}=2\left(1-\frac{1}{p}\right)^2\left(1-\frac{1}{p^2}\right)\frac{\frac{1}{p}}{1-\frac{1}{p}}$$

et donc

$$\omega_p(\boldsymbol{\varepsilon},\mathbf{m})=\left(1-\frac{1}{p}\right)^2\sum_{1\leq\nu}\left(\frac{\chi(p^\nu)\rho^*(p^\nu;L_1L_2Q)}{p^{2\nu}}\right)+\left(1-\frac{1}{p}\right)^2\left(1-\frac{1}{p^2}\right)\left(1+\frac{\frac{2}{p}}{1-\frac{1}{p}}\right),$$

où

$$1+\frac{\frac{2}{p}}{1-\frac{1}{p}}=\frac{1+\frac{1}{p}}{1-\frac{1}{p}}$$

donc

$$\omega_p(\boldsymbol{\varepsilon},\mathbf{m})=\left(1-\frac{1}{p}\right)^2\sum_{1\leq\nu}\frac{\chi(p^\nu)\rho^*(p^\nu;L_1L_2Q)}{p^{2\nu}}+\left(1-\frac{1}{p^2}\right)^2.$$

En particulier, on remarque que dans ces cas $\omega_p(\boldsymbol{\varepsilon},\mathbf{m})=\omega_p$ ne dépend ni de $\boldsymbol{\varepsilon}$ ni de $\mathbf{m}$.

Examinons alors le cas où $p|2\Delta_{12}^{nsc}\Delta_{13}^{nsc}\Delta_{23}^{nsc}$ et commençons par le cas p impair. Alors dans ce cas, si on note $\mu_i=\nu_p(m_i)$, on doit rajouter la condition $2|\nu_p(L_i(u,v))-\mu_i$ et $2|\nu_p(Q(u,v))-\mu_3$, de sorte qu'on a

$$\omega_p(\boldsymbol{\varepsilon},\mathbf{m})=\lim_{n\to+\infty}p^{-4n}\#\left\{(u,v,z,y,t)\in(\mathbb{Z}/p^n\mathbb{Z})^5\;\middle|\;\begin{array}{l}t^2L_1(u,v)L_2(u,v)Q(u,v)\equiv y^2+z^2[p^n]\\ p\nmid(u,v),\quad p\not| (y,z,t)\\ 2|\nu_p(L_i(u,v))-\mu_i,\quad 2|\nu_p(Q(u,v))-\mu_3\end{array}\right\}$$

$$=\lim_{n\to+\infty}\frac{1-\frac{1}{p}}{p^{3n}}\#\left\{(u,v,z,y)\in(\mathbb{Z}/p^n\mathbb{Z})^4\;\middle|\;\begin{array}{l}L_1(u,v)L_2(u,v)Q(u,v)\equiv y^2+z^2[p^n]\\ p\nmid(u,v)\\ 2|\nu_p(L_i(u,v))-\mu_i,\quad 2|\nu_p(Q(u,v))-\mu_3\end{array}\right\}$$

comme ci-dessus puisque nécessairement $p\equiv 3[4]$, qui ne dépend ici que de $\mathbf{m}$ et pas de $\boldsymbol{\varepsilon}$. Passons alors au cas $p=2$. Les choix des m_i impliquent que

$$\frac{L_i(u,v)}{m_i}\quad\text{et}\quad\frac{Q(u,v)}{m_3}$$

s'écrivent comme sommes de deux carrés étant donné qu'on a rendu les valuations des premiers congrus à 3 modulo 4 paires. Les conditions

$$L_i(u,v)\in\varepsilon_i m_i\mathcal{E}_{2^n}\quad\text{et}\quad Q(u,v)\in\varepsilon_3 m_3\mathcal{E}_{2^n}$$

sont donc nécessairement remplies pour tout entier naturel n. On en déduit l'expression

$$\omega_2(\boldsymbol{\varepsilon},\mathbf{m})=\lim_{n\to+\infty}2^{-4n}\#\left\{(u,v,z,y,t)\in(\mathbb{Z}/2^n\mathbb{Z})^5\;\middle|\;\begin{array}{l}t^2L_1(u,v)L_2(u,v)Q(u,v)\equiv y^2+z^2[2^n]\\ 2\nmid(u,v),\quad 2\not| (y,z,t)\\ L_i(u,v)\in\varepsilon_i m_i\mathcal{E}_{2^n},\quad Q(u,v)\in\varepsilon_3 m_3\mathcal{E}_{2^n}\end{array}\right\}.$$

On sait que $2\not| t$ car sinon on aurait $y^2+z^2\equiv 0[2]$ mais puisque $2\nmid(y,z,t)$, alors 2 ne pourrait dviser (y,z) et donc y^2+z^2 serait congru à 2 et non 0 modulo 2. On a donc

$$\omega_2(\boldsymbol{\varepsilon},\mathbf{m})=\lim_{n\to+\infty}2^{-3n-1}\#\left\{(u,v,z,y)\in(\mathbb{Z}/2^n\mathbb{Z})^4\;\middle|\;\begin{array}{l}L_1(u,v)L_2(u,v)Q(u,v)\equiv y^2+z^2[2^n]\\ 2\nmid(u,v)\\ L_i(u,v)\in\varepsilon_i m_i\mathcal{E}_{2^n},\quad Q(u,v)\in\varepsilon_3 m_3\mathcal{E}_{2^n}\end{array}\right\}.$$

comme ci-dessus car $\varphi(2^n) = 2^{n-1}$. Et en utilisant $S_0(A, 2^n) = 2^{n+1}$ sous les bonnes conditions, on obtient comme ci-dessus

$$\omega_2(\boldsymbol{\varepsilon}, \mathbf{m}) = \lim_{n\to+\infty} 2^{-2n} \# \left\{ (u,v) \in (\mathbb{Z}/2^n\mathbb{Z})^2 \quad \middle| \quad \begin{array}{l} 2 \nmid (u,v) \\ L_i(u,v) \in \varepsilon_i m_i \mathcal{E}_{2^n}, \quad Q(u,v) \in \varepsilon_3 m_3 \mathcal{E}_{2^n} \end{array} \right\}.$$

Noter ici qu'il n'y a pas besoin d'extraire selon la valuation p-adique et qu'on a une dépendance en les deux variables $\boldsymbol{\varepsilon}$ et $\mathbf{m}$.

Intéressons-nous à présent à la densité archimédienne. Grâce à la symétrie du problème, on peut se restreindre à $y > 0$ et $z > 0$ et donc

$$\omega_\infty(\boldsymbol{\varepsilon}, \mathbf{m}) = 2 \lim_{B\to+\infty} \frac{1}{B\log(B)} \int_D \frac{\mathrm{d}u\mathrm{d}v\mathrm{d}t\mathrm{d}y}{2\sqrt{t^2 L_1(u,v)L_2(u,v)Q(u,v) - y^2}}$$

où on a utilisé une forme de Leray en paramétrant en z de sorte que l'inverse du jacobien soit $(2z)^{-1}$ car

$$z^2 = t^2 L_1(u,v)L_2(u,v)Q(u,v) - y^2,$$

et où

$$D = \{(u,v,y,t) \in \mathbb{R}^4 \quad | \quad (u,v) \in \sqrt{B/t}\mathcal{R}_{\boldsymbol{\varepsilon}}, \quad 0 < y < t\sqrt{L_1(u,v)L_2(u,v)Q(u,v)}, \quad 1 < t < B\},$$

où

$$\mathcal{R}_{\boldsymbol{\varepsilon}} = \{\mathbf{x} \in \mathbb{R}^2 \quad | \quad \max(|x_1|, |x_2|) \leq 1 \quad \text{et} \quad \varepsilon_1 L_1(\mathbf{x}) > 0, \quad \varepsilon_2 L_2(\mathbf{x}) > 0, \quad \varepsilon_3 Q(\mathbf{x}) > 0\}.$$

En utilisant la formule

$$\int_0^{\sqrt{A}} \frac{\mathrm{d}x}{\sqrt{A - x^2}} = \frac{\pi}{2},$$

on obtient

$$\omega_\infty(\boldsymbol{\varepsilon}, \mathbf{m}) = \frac{\pi}{2} \lim_{B\to+\infty} \frac{1}{B\log(B)} \int_1^B \mathrm{d}t \int_{\sqrt{B/t}\mathcal{R}_{\boldsymbol{\varepsilon}}} \mathrm{d}u\mathrm{d}v.$$

Or,

$$\int_{\sqrt{B/t}\mathcal{R}_{\boldsymbol{\varepsilon}}} \mathrm{d}u\mathrm{d}v = \frac{B}{t}\mathrm{vol}(\mathcal{R}_{\boldsymbol{\varepsilon}})$$

donc

$$\omega_\infty(\boldsymbol{\varepsilon}, \mathbf{m}) = \frac{\pi}{2}\mathrm{vol}(\mathcal{R}_{\boldsymbol{\varepsilon}}),$$

qui ne dépend que de $\boldsymbol{\varepsilon}$ et pas de $\mathbf{m}$. Réinjectant cette expression, on obtient l'égalité

$$c_X = \sum_{\substack{\boldsymbol{\varepsilon}\in\Sigma \\ \mathbf{m}\in M}} \mathrm{vol}(\mathcal{R}_{\boldsymbol{\varepsilon}}) \times \pi \prod_p \omega_p(\boldsymbol{\varepsilon}, \mathbf{m}), \tag{3.1}$$

où on a $\mathcal{R}_{\boldsymbol{\varepsilon}} = R^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(1)$.

3.2 Vers la validation de la conjecture de Peyre

3.2.1 Transformation de la constante c_0

On revient dans cette section à l'expression de la constante c_0 obtenue grâce au Théorème 6 que l'on met sous une forme similaire à celle de c_X en (3.1). On réécrit cette constante c_0 sous la forme

$$c_0 = \frac{\pi^2}{2^4} \sum_{m \in \mathcal{D}} \frac{\mu(m) r_0(m) \varphi^\dagger(m)}{m} \sum_{\substack{\varepsilon_i \in \{-1,+1\} \\ \varepsilon_1\varepsilon_2\varepsilon_3 = 1}} \mathrm{vol}\left(R^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(1)\right) \sum_{\substack{\mathbf{d},\mathbf{d}' \in \mathbb{N}^3 \\ m = d_1 d_2 d_3, \mathbf{d}' | H}} \mu(d_1' d_2') \mu(d_3') \chi(d_1' d_2' d_3') \times$$

$$\sum_{\substack{k_4 k_1' | \gcd(\Delta_{23}, m) \\ k_4 k_2' | \gcd(\Delta_{13}, m)}} \sum_{\substack{k_4 k_3' | \gcd(\Delta_{12}, m) \\ k_5 k_5' | \gcd(\Delta_{12}, d_1' d_2') \\ k_4 k_4' | \gcd(\gcd(\Delta_{12}, \Delta_{13}, \Delta_{23}), m)}} \frac{\mu(k_1') \mu(k_2') \mu(k_3') \mu(k_4') \mu(k_5')}{3^{\omega(k_4)} 2^{\omega(k_5) + \omega(k_1) + \omega(k_2) + \omega(k_3)}} \sigma_*^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e}, \mathbf{E}, \mathbf{d}, \mathbf{d}', \mathbf{k}, \mathbf{k}'),$$

où

$$\sigma_*^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e}, \mathbf{E}, \mathbf{d}, \mathbf{d}', \mathbf{k}, \mathbf{k}') = \sum_{e=1}^{+\infty} \frac{\mu(e)}{e^2} \sigma^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e}, \mathbf{E}, \mathbf{d}, \mathbf{d}', \mathbf{k}, \mathbf{k}', e).$$

On rappelle qu'on a

$$\sigma^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e}, \mathbf{E}, \mathbf{d}, \mathbf{d}', \mathbf{k}, \mathbf{k}', e) = \prod_p \sigma_p^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e}, \mathbf{E}, \mathbf{d}, \mathbf{d}', \mathbf{k}, \mathbf{k}', e)$$

avec

$$\sigma_p^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e}, \mathbf{E}, \mathbf{d}, \mathbf{d}', \mathbf{k}, \mathbf{k}', e) = \left(1 - \frac{\chi(p)}{p}\right)^3 \sum_{\boldsymbol{\nu} \in \mathbb{N}^3} \frac{\chi(p)^{\nu_1+\nu_2+\nu_3} \rho(p^{N_1}, p^{N_2}, p^{N_3}; L_{1,e}, L_{2,e}, Q_e)}{p^{2(N_1+N_2+N_3)}}$$

où $N_i = \max(\nu_p(e_i) + \nu_i, \nu_p(E_i))$ si $p > 2$ et

$$\sigma_2^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e}, \mathbf{E}, \mathbf{d}, \mathbf{d}', \mathbf{k}, \mathbf{k}', e) = 4 \lim_{n \to +\infty} 2^{-2n} \# \left\{ \mathbf{x} \in (\mathbb{Z}/2^n\mathbb{Z})^2 \quad \middle| \quad \begin{array}{l} eL_i(\mathbf{x}) \in e_i \varepsilon_i \mathcal{E}_{2^n} \\ e^2 Q(\mathbf{x}) \in e_3 \varepsilon_3 \mathcal{E}_{2^n} \end{array} \right\}.$$

Puisque chaque terme $\sigma_p^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e}, \mathbf{E}, \mathbf{d}, \mathbf{d}', \mathbf{k}, \mathbf{k}', e)$ ne dépend que de $\nu_p(e)$ car dans $\rho(p^{N_1}, p^{N_2}, p^{N_3}; L_{1,e}, L_{2,}$ on a des conditions du type $p^{N_i} | p^{\nu_p(e)} L_i$ et de même pour Q avec du $p^{2\nu_p(e)}$, on peut écrire

$$\sigma_*^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e}, \mathbf{E}, \mathbf{d}, \mathbf{d}', \mathbf{k}, \mathbf{k}') = \prod_p \sigma_{*,p}^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e}, \mathbf{E}, \mathbf{d}, \mathbf{d}', \mathbf{k}, \mathbf{k}').$$

Soit dans un premier temps $p > 2$. On a alors un facteur eulérien donné par

$$\sum_{0 \leq k \leq 1} \frac{(-1)^k}{p^{2k}} \left(1 - \frac{\chi(p)}{p}\right)^3 \sum_{\boldsymbol{\nu} \in \mathbb{N}^3} \frac{\chi(p)^{\nu_1+\nu_2+\nu_3} \rho(p^{N_1}, p^{N_2}, p^{N_3}; L_{1,e}, L_{2,e}, Q_e)}{p^{2(N_1+N_2+N_3)}}$$

ce qui donne

$$\left(1 - \frac{\chi(p)}{p}\right)^3 \left(\sum_{\boldsymbol{\nu} \in \mathbb{N}^3} \frac{\chi(p)^{\nu_1+\nu_2+\nu_3} \rho(p^{N_1}, p^{N_2}, p^{N_3}; L_1, L_2, Q)}{p^{2(N_1+N_2+N_3)}} - \sum_{\boldsymbol{\nu} \in \mathbb{N}^3} \frac{\chi(p)^{\nu_1+\nu_2+\nu_3} \rho(p^{N_1}, p^{N_2}, p^{N_3}; L_{1,p}, L_{2,p}, Q_p)}{p^{2(N_1+N_2+N_3+1)}} \right).$$

On a vu que pour $k \leq N_1 + N_2 + N_3$, les conditions ne dépendant que la congruence modulo $p^{N_1+N_2+N_3}$ (cf preuve du Théorème 2), on a

$$\frac{\rho(p^{N_1}, p^{N_2}, p^{N_3}; L_1, L_2, Q)}{p^{2(N_1+N_2+N_3)}} = p^{-2(N_1+N_2+N_3+1)} \#\{\mathbf{x} \in \left(\mathbb{Z}/p^{N_1+N_2+N_3+1}\mathbb{Z}\right)^2 \quad | \quad p^{N_i} | L_i(\mathbf{x}), \quad p^{N_3} | Q(\mathbf{x})\}.$$

Et enfin, en effectuant le changement de variable $\mathbf{x}' = p\mathbf{x}$ dans

$$\rho(p^{N_1}, p^{N_2}, p^{N_3}; L_{1,p}, L_{2,p}, Q_p) = \#\{\mathbf{x} \in \left(\mathbb{Z}/p^{N_1+N_2+N_3}\mathbb{Z}\right)^2 \quad | \quad p^{N_i} | L_i(p\mathbf{x}), \quad p^{N_3} | Q(p\mathbf{x})\},$$

on obtient

$$\rho(p^{N_1}, p^{N_2}, p^{N_3}; L_{1,p}, L_{2,p}, Q_p) = \#\{\mathbf{x} \in \left(\mathbb{Z}/p^{N_1+N_2+N_3+1}\mathbb{Z}\right)^2 \quad | \quad p^{N_i} | L_i(\mathbf{x}), \quad p^{N_3} | Q(\mathbf{x}), \quad p | \mathbf{x}\}.$$

Finalement, on aboutit à l'expression suivante

$$\sigma_{*,p}^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e}, \mathbf{E}, \mathbf{d}, \mathbf{d}', \mathbf{k}, \mathbf{k}') = \left(1 - \frac{\chi(p)}{p}\right)^3 \sum_{\boldsymbol{\nu} \in \mathbb{N}^3} \frac{\chi(p)^{\nu_1+\nu_2+\nu_3} \tilde{\rho}(p^{N_1}, p^{N_2}, p^{N_3}; L_1, L_2, Q)}{p^{2(N_1+N_2+N_3+1)}}$$

où

$$\tilde{\rho}(p^{N_1}, p^{N_2}, p^{N_3}; L_1, L_2, Q) = \#\{\mathbf{x} \in \left(\mathbb{Z}/p^{N_1+N_2+N_3+1}\mathbb{Z}\right)^2 \quad | \quad p^{N_i} | L_i(\mathbf{x}), \quad p^{N_3} | Q(\mathbf{x}), \quad p \not| \mathbf{x}\}.$$

Traitons alors le cas $p = 2$. On obtient un facteur eulérien

$$4 \lim_{n \to +\infty} \left(2^{-2n} \# \left\{ \mathbf{x} \in (\mathbb{Z}/2^n\mathbb{Z})^2 \quad \middle| \quad \begin{array}{c} L_i(\mathbf{x}) \in e_i \varepsilon_i \mathcal{E}_{2^n} \\ Q(\mathbf{x}) \in e_3 \varepsilon_3 \mathcal{E}_{2^n} \end{array} \right\} - 2^{-2(n+1)} \# \left\{ \mathbf{x} \in (\mathbb{Z}/2^n\mathbb{Z})^2 \quad \middle| \quad \begin{array}{c} 2L_i(\mathbf{x}) \in e_i \varepsilon_i \mathcal{E}_{2^n} \\ 2^2 Q(\mathbf{x}) \in e_3 \varepsilon_3 \mathcal{E}_{2^n} \end{array} \right\} \right)$$

et ensuite

$$\sigma_{*,2}^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e}, \mathbf{E}, \mathbf{d}, \mathbf{d}', \mathbf{k}, \mathbf{k}') = 4 \lim_{n \to +\infty} 2^{-2n} \# \left\{ \mathbf{x} \in (\mathbb{Z}/2^n\mathbb{Z})^2 \quad \middle| \quad \begin{array}{l} L_i(\mathbf{x}) \in e_i \varepsilon_i \mathcal{E}_{2^n} \\ Q(\mathbf{x}) \in e_3 \varepsilon_3 \mathcal{E}_{2^n} \\ 2 \not| \mathbf{x} \end{array} \right\}$$

par le même raisonnement.

On écrit alors c_0 sous la forme

$$c_0 = \sum_{\substack{\boldsymbol{\varepsilon} \in \Sigma \\ \mathbf{m} \in M}} \mathrm{vol}(\mathcal{R}_{\boldsymbol{\varepsilon}}) c_0(\boldsymbol{\varepsilon}, \mathbf{m}).$$

On décompose la somme sur $\mathbf{d}'$ en une somme sur $\mathbf{m} \in M$ et une somme sur $\mathbf{c}$ dans un ensemble que l'on va préciser dans un instant. Tout d'abord, la présence du terme $\mu(d_1'd_2')\mu(d_3')$ implique qu'on peut restreindre la somme aux d_i' sans facteur carré et tels que $(d_1', d_2') = 1$. De plus, si on examine attentivement comment on a obtenu l'expression de $N(B)$ dans la section 2.1.2, on a exprimé

$$r(l^2 L_1^+(u,v) L_2^+(u,v) Q^+(u,v))$$

à l'aide de la formule d'éclatement avec quatre entiers donnée par le Lemme 27. On peut donc supposer que

$$r(l^2 L_1^+(u,v) L_2^+(u,v) Q^+(u,v)) \neq 0$$

sinon on a une contribution nulle à la somme et donc à la constante. On a donc comme ci-dessus que pour les nombres premiers $p \equiv 3[4]$, on a nécessairement

$$\nu_p(L_1^+(u,v)) + \nu_p(L_2^+(u,v)) + \nu_p(Q^+(u,v)) \equiv 0[2].$$

De plus, la formule nous fournissait

$$r\left(l^2 L_1^+(u,v)L_2^+(u,v)Q^+(u,v)\right) = \frac{1}{2^6} \sum_{\substack{\mathbf{d},\mathbf{d}'\in\mathbb{N}^3 \\ d_1d_2d_3|n_4, d_i d_j' d_k'|n_i}} \frac{\mu(d_1d_2d_3)\mu(d_1'd_2')\mu(d_3')\chi(d_1d_2d_3d_1'd_2'd_3')}{c(\mathbf{d},\mathbf{d}', L_1(u,v), L_2(u,v), Q(u,v))} \times$$

$$r\left(\frac{L_1^+(u,v)}{d_1d_2'd_3'}\right) r\left(\frac{L_2^+(u,v)}{d_2d_1'd_3'}\right) r\left(\frac{Q^+(u,v)}{d_3d_1'd_2'}\right) r\left(\frac{l^2}{d_1d_2d_3}\right).$$

On peut également restreindre la sommation aux $\mathbf{d}'$ tels que

$$r\left(\frac{L_1^+(u,v)}{d_1d_2'd_3'}\right) r\left(\frac{L_2^+(u,v)}{d_2d_1'd_3'}\right) r\left(\frac{Q^+(u,v)}{d_3d_1'd_2'}\right) \neq 0.$$

Dans un tel cas, on a nécessairement, puisque $d_i \in \mathcal{D}$ (et donc tous ses facteurs premiers sont congrus à 1 modulo 4), que

$$\nu_p(L_1^+(u,v)) \equiv \nu_p(d_2'd_3')[2], \quad \nu_p(L_2^+(u,v)) \equiv \nu_p(d_1'd_3')[2] \quad \text{et} \quad \nu_p(Q^+(u,v)) \equiv \nu_p(d_1'd_2')[2].$$

Le fait que d_2' et d_3' soient sans facteurs carrés donne que $\nu_p(d_2'd_3') \in \{0,1,2\}$ et le fait que $d_i'|\Delta_{j,k}$ avec $\{i,j,k\} = \{1,2,3\}$ implique que $d_2'd_3'|\Delta_{12}\Delta_{13}$. O peut alors écrire $d_2'd_3'$ sous la forme $d_2'd_3' = c_1m_1$ avec

$$c_1 = \prod_{p|d_2'd_3', p\equiv 1[4]} p^{\nu_p(d_2'd_3')} \prod_{p|d_2'd_3', p\equiv 3[4], \nu_p(d_2'd_3')\equiv 0[2]} p^2$$

car $\nu_p(d_2'd_3') \equiv 0[2]$ implique que $\nu_p(d_2'd_3') = 0$ ou 2 et où pour $p \equiv 1[4]$, on a $\nu_p(d_2'd_3') = 1$ ou 2, et

$$m_1 = \prod_{p|d_2'd_3', p\equiv 3[4], \nu_p(d_2'd_3')\equiv 1[2]} p|[\Delta_{1,2}^{nsc}, \Delta_{1,3}^{nsc}]$$

puisque la condition $\nu_p(d_2'd_3') \equiv 1[2]$ implique ici que $\nu_p(d_2'd_3') = 1$. De même, on peut écrire $d_1'd_3' = c_2m_2$ avec

$$c_2 = \prod_{p|d_1'd_3', p\equiv 1[4]} p^{\nu_p(d_1'd_3')} \prod_{p|d_1'd_3', p\equiv 3[4], \nu_p(d_1'd_3')\equiv 0[2]} p^2$$

et

$$m_2 = \prod_{p|d_1'd_3', p\equiv 3[4], \nu_p(d_1'd_3')\equiv 1[2]} p|[\Delta_{1,2}^{nsc}, \Delta_{2,3}^{nsc}].$$

Enfin, le fait que $(d_1', d_2') = 1$ implique que $d_1'd_2'$ est sans facteur carré et donc on peut écrire $d_1'd_2' = c_3m_3$ avec

$$c_3 = \prod_{p|d_1'd_2', p\equiv 1,2[4]} p|[\Delta_{1,3}^{sc}, \Delta_{2,3}^{sc}]$$

et

$$m_3 = \prod_{p|d_1'd_2', p\equiv 3[4], \nu_p(d_1'd_3')\equiv 1[2]} p|[\Delta_{1,3}^{nsc}, \Delta_{2,3}^{nsc}].$$

La condition

$$\nu_p(L_1^+(u,v)) + \nu_p(L_2^+(u,v)) + \nu_p(Q^+(u,v)) \equiv 0[2]$$

implique comme précédemment que si $p|m_i$, il existe un unique indice i_0 parmi j et k tel que $p|m_{i_0}$. On a donc bien que $(m_1,m_2,m_3)=1$ et que $m_1m_2m_3$ est un carré, ainsi $\mathbf{m}\in M$. À tout $\mathbf{d}'$ qui donne une somme non nulle et donc une constante non nulle, on peut associer $\mathbf{m}\in M$ et $\mathbf{c}$ comme ci-dessus. Les (c_1,c_2,c_3) ne sont pas nécessairement premiers entre eux mais $c_3|[\Delta_{1,3}^{sc},\Delta_{2,3}^{sc}]$, ensuite $c_2=c_{2,1}c_{2,2}^2$ avec $c_{2,1}|\Delta_{1,2}^{sc}\Delta_{2,3}^{sc}$ et $c_{2,2}|[\Delta_{1,2}^{nsc},\Delta_{2,3}^{nsc}]$, tandis que $c_1=c_{1,1}c_{1,2}^2$ avec

$$c_{1,1}|2\Delta_{1,2}^{sc}\Delta_{1,3}^{sc} \quad \text{et} \quad c_{1,2}|[\Delta_{1,2}^{nsc},\Delta_{1,3}^{nsc}].$$

De plus, on doit avoir $c_3|c_1c_2$. On voit également que

$$\frac{m_1m_2}{m_3}=(m_1,m_2)^2$$

car

$$m_i=\prod_{p|(m_i,m_j)} p \prod_{p|(m_i,m_k)} p.$$

Enfin, on pose $c_3=c_{3,1}$ ce qui est cohérent puisque $(d_1',d_2')=1$, et on a bien $c_{3,2}=1$. On examine à présent les propriétés vérifiées par les $\mathbf{c}_1=(c_{1,1},c_{2,1},c_{3,1})$. On a les relations de divisibilités explicitées ci-dessus et on a vu qu'ils n'étaient pas nécessairement premier entre eux dans leur ensemble. En revanche, on a que $c_{1,1}c_{2,1}c_{3,1}$ est un carré. En effet, on a

$$c_{1,1}c_{2,1}c_{3,1}=\prod_{\substack{p|d_1'd_2'd_3'\\ p\equiv 1,2[4]}} p^{2(\nu_p(d_1')+\nu_p(d_2')+\nu_p(d_3'))}.$$

On pose donc

$$C=\{\mathbf{c}_1\in\mathbb{N}^3 \quad | \quad c_{1,1}|2\Delta_{1,2}^{sc}\Delta_{1,3}^{sc}, \quad c_{2,1}|2\Delta_{1,2}^{sc}\Delta_{2,3}^{sc}, \quad c_{3,1}|2[\Delta_{1,3}^{sc},\Delta_{2,3}^{sc}], \quad \sqrt{c_{1,1}c_{2,1}c_{3,1}}\in\mathbb{N}\},$$

et la discussion qui précède montre que $\mathbf{c}_1\in C$. Passons à une conséquence de ces conditions. Montrons que nécessairement $c_{3,1}|c_{1,1}c_{2,1}$ (en fait le résultat est vrai pour toute permutation des indices sous ces hypothèses) et même que

$$\frac{c_{1,1}c_{2,1}}{c_{3,1}}=(c_{1,1},c_{2,1})^2.$$

On démontre le résultat pour trois entiers a, b et c dont le produit est un carré et dont les valuations p-adiques ne dépassent pas 2 pour a et b et pas 1 pour c comme c'est le cas pour un triplet $\mathbf{c}_1\in C$. On écrit alors

$$a=\prod_{p_i} p_i^{\alpha_i}, \quad b=\prod_{p_i} p_i^{\beta_i} \quad \text{et} \quad b=\prod_{p_i} p_i^{\gamma_i},$$

avec $\alpha_i,\beta_i\leq 2$ et $\gamma_i\leq 1$. On a $\alpha_i+\beta_i+\gamma_i\equiv 0[2]$ par hypothèse et on peut se restreindre aux premiers p_i tels que $\alpha_i+\beta_i+\gamma_i\geq 2$. Ainsi

$$\alpha_i+\beta_i-\gamma_i\geq 2(1-\gamma_i)\geq 0$$

ce qui montre bien que $c|ab$. Si $\gamma_i=0$, alors la valuation du quotient est de $\alpha_i+\beta_i$ mais $\alpha_i+\beta_i\geq 2$ et sous les hypothèses, $\alpha_i+\beta_i+\gamma_i\leq 4$ donc $\alpha_i+\beta_i+\gamma_i=2$ ou 4. Dans le

premier cas, on a nécessairement $\alpha_i = \beta_i = 1$ (en fait on a nécessairement que si $p|c_i$ il divise au moins un des autres c_j donc $(0,2)$ ou $(2,0)$ est exclu) et donc

$$\alpha_i + \beta_i - \gamma_i = 2 = 2\min(\alpha_i, \beta_i),$$

et de même dans le second cas $\alpha_i = \beta_i = 2$ et

$$\alpha_i + \beta_i - \gamma_i = 4 = 2\min(\alpha_i, \beta_i).$$

Supposons alors $\gamma_i = 1$, dans ce cas les conditions donnent que $\alpha_i + \beta_i = 1$ ou 3. Dans le premier cas, on a par exemple, $\alpha_i = 0$ et $\beta_i = 1$ et

$$\alpha_i + \beta_i - \gamma_i = 0 = 2\min(\alpha_i, \beta_i),$$

et enfin lorsque $\alpha_i + \beta_i = 3$, on a par exemple $\alpha_i = 1$ et $\beta_i = 2$ et

$$\alpha_i + \beta_i - \gamma_i = 2 = 2\min(\alpha_i, \beta_i)$$

ce qui achève bien de montrer que $(ab)/c = (a,b)^2$. Notons que ce résultat s'applique également aux $\mathbf{m} \in M$. Intéressons-nous maintenant aux $\mathbf{c}_2 = (c_{1,2}, c_{2,2})$. Soit p divisant $c_{1,2}$ où on rappelle que

$$c_{1,2} = \prod_{\substack{p|(d'_2,d'_3)\\ p\equiv 3[4]}} p.$$

Alors, par définition $c_{1,2}|(m_2, m_3)$ et de même $c_{2,2}|(m_1, m_3)$ où il n'y a pas égalité en général. De plus, par construction $(c_{1,2}, m_1) = 1$ et $(c_{2,2}, m_2) = 1$ et en particulier $(c_{1,2}, c_{2,2}) = 1$. De la relation

$$c_{3,1} m_3 {d'_3}^2 = c_{1,1} c_{2,1} c_{1,2}^2 c_{2,2}^2 m_1 m_2,$$

on tire d'après ce qui précède l'égalité

$$d'_3 = (m_1, m_2)(c_{1,1}, c_{2,1}) c_{1,2} c_{2,2}.$$

On déduit alors de $d'_1 d'_3$ et $d'_2 d'_3$ l'expression

$$d'_1 = \frac{m_2}{c_{1,2}(m_1, m_2)} \frac{c_{2,1}}{(c_{1,1}, c_{2,1})}$$

où le fait que $(c_{1,2}, m_1) = 1$ implique bien que $c_{1,2}(m_1, m_2)|m_2$ et de manière analogue

$$d'_2 = \frac{m_1}{c_{2,2}(m_1, m_2)} \frac{c_{1,1}}{(c_{1,1}, c_{2,1})}.$$

On a donc que réciproquement, la donnée de $\mathbf{m} \in M$, $\mathbf{c}_1 \in C$ et de $\mathbf{c}_2 \in \mathcal{D}((m_2, m_3)) \times \mathcal{D}((m_1, m_3))$ donne un triplet $\mathbf{d}'$ qui convient. La correspondance étant univoque, puisque par exemple si

$$d'_3 = (m_1, m_2)(c_{1,1}, c_{2,1}) c_{1,2} c_{2,2} = (m'_1, m'_2)(c'_{1,1}, c'_{2,1}) c'_{1,2} c'_{2,2}$$

on a en regardant les décompositions en facteurs premiers les égalités $(c'_{1,1}, c'_{2,1}) = (c_{1,1}, c_{2,1})$ et $(m'_1, m'_2) = (m_1, m_2)$, $c'_{1,2} = c_{1,2}$ et $c_{2,2} = c'_{2,2}$. Les égalités de d'_1 et d'_2 donnent alors que

$c_{1,1} = c'_{1,1}$ et $c'_{2,1} = c_{2,1}$ et donc $c'_3 = c_3$ grâce à l'expression de c_3 en fonction du produit de $c_{1,1}$ et $c_{2,1}$ et de leur pgcd. On a alors

$$\frac{m_1}{c_{2,2}(m_1, m_2)} = \frac{m'_1}{c'_{2,2}(m'_1, m'_2)}$$

mais on déduit de $(m'_1, m'_2)c'_{1,2}c'_{2,2} = (m_1, m_2)c_{1,2}c_{2,2}$ que cela implique l'égalité

$$\frac{m_1}{c_{1,2}} = \frac{m'_1}{c'_{1,2}}$$

et de même

$$\frac{m_2}{c_{2,2}} = \frac{m'_2}{c'_{2,2}}.$$

On a donc $m'_1 = m_1$ et $m'_2 = m_2$ et on en déduit $m_3 = m'_3$. On a donc montré

$$\sum_{\mathbf{d}'} = \sum_{\mathbf{m}\in M} \sum_{\mathbf{c}_1\in C} \sum_{\mathbf{c}_2\in\mathcal{D}((m_2,m_3))\times\mathcal{D}((m_1,m_3))}.$$

Il est à noter qu'on aura peut être des termes nuls parce que les hypothèses sur les sommes de droite ne permettent pas de déduire a priori que $d'_i|\Delta_{j,k}$. On remplace ainsi les dépendances en $\mathbf{d}'$ dans la constante

$$\sigma_*^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e}, \mathbf{E}, \mathbf{d}, \mathbf{d}', \mathbf{k}, \mathbf{k}')$$

en remplaçant les $d'_i d'_j$ par leurs expressions en fonction des $\mathbf{m}$, $\mathbf{c}_1$ et $\mathbf{c}_2$, et on remplace de même dans

$$\mu(d'_1 d'_2) = \mu(c_{3,1})\mu(m_3)$$

et

$$\mu(d'_3) = \mu((m_1, m_2))\mu((c_{1,1}, c_{2,1}))\mu(c_{1,2})\mu(c_{2,2})$$

et

$$\chi(d'_1 d'_2 \times d'_3) = \chi(m_3)\chi((m_1, m_2))\chi(c_{1,2})\chi(c_{2,2})$$

puisque $\chi((c_{1,1}, c_{2,1})) = \chi(c_3) = 1$. Cela permet donc d'écrire

$$c_0 = \sum_{\substack{\boldsymbol{\varepsilon}\in\Sigma\\ \mathbf{m}\in M}} \mathrm{vol}(\mathcal{R}_{\boldsymbol{\varepsilon}}) \times c_0(\boldsymbol{\varepsilon}, \mathbf{m})$$

avec

$$c_0(\boldsymbol{\varepsilon}, \mathbf{m}) = \frac{\pi^2}{2^4} \sum_{m\in\mathcal{D}} \frac{\mu(m) r_0(m) \varphi^\dagger(m)}{m} \sum_{\substack{\mathbf{d}\in\mathbb{N}^3\\ m=d_1d_2d_3}} \times$$

$$\sum_{\mathbf{c}_1\in C} \sum_{\mathbf{c}_2\in\mathcal{D}((m_2,m_3))\times\mathcal{D}((m_1,m_3))} \mu(c_{3,1})\mu(m_3)\mu((m_1, m_2))\mu((c_{1,1}, c_{2,1}))\mu(c_{1,2})\mu(c_{2,2})\chi(m_3)\chi((m_1, m_2))\chi(c_{1,2})\chi(c_{2,2})\times$$

$$\sum_{\substack{k_4k_1k'_1|\gcd(\Delta_{2,3},m)\\ k_4k_2k'_2|\gcd(\Delta_{1,3},m)}} \sum_{\substack{k_4k_3k'_3|\gcd(\Delta_{1,2},m)\\ k_5k'_5|\gcd(\Delta_{12},d'_1d'_2)\\ k_4k'_4|\gcd(\gcd(\Delta_{1,2},\Delta_{1,3},\Delta_{2,3}),m)}} \frac{\mu(k'_1)\mu(k'_2)\mu(k'_3)\mu(k'_4)\mu(k'_5)}{3^{\omega(k_4)}2^{\omega(k_5)+\omega(k_1)+\omega(k_2)+\omega(k_3)}} \sigma_*^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e}, \mathbf{E}, \mathbf{d}, \mathbf{d}', \mathbf{k}, \mathbf{k}').$$

Intéressons-nous alors à

$$\sigma_{*,p}^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}')$$

lorsque $p \equiv 1[4]$. On rappelle qu'on a

$$\sigma_{*,p}^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}') = \left(1-\frac{\chi(p)}{p}\right)^3 \sum_{\boldsymbol{\nu}\in\mathbb{N}^3} \frac{\chi(p)^{\nu_1+\nu_2+\nu_3}\tilde{\rho}(p^{N_1},p^{N_2},p^{N_3};L_1,L_2,Q)}{p^{2(N_1+N_2+N_3+1)}}$$

avec $N_i = \max(\nu_p(e_i)+\nu_i, \nu_p(E_i))$ où

$$e_1 = d_1d_2'd_3', \quad e_2 = d_2d_1'd_3' \quad \text{et} \quad e_3 = d_3d_1'd_2'$$

et

$$E_1 = [d_1d_2'd_3', k_4k_2k_2', k_4k_3k_3', k_4k_4', d_1k_5k_5'], \quad E_2 = [d_2d_1'd_3', k_4k_1k_1', k_4k_3k_3', k_4k_4', d_2k_5k_5']$$

et

$$E_3 = [d_3d_1'd_3', k_4k_1k_1', k_4k_2k_2', k_4k_4'].$$

Avec la somme sur $\succcurlyeq$, $_1$ et $_2$, on va avoir

$$e_1 = d_1c_{1,1}c_{1,2}^2m_1, \quad e_2 = d_2c_{2,1}c_{2,2}^2m_2 \quad \text{et} \quad e_3 = d_3c_{3,1}m_3$$

et

$$E_1 = [e_1, k_4k_2k_2', k_4k_3k_3', k_4k_4', d_1k_5k_5'], \quad E_2 = [e_2, k_4k_1k_1', k_4k_3k_3', k_4k_4', d_2k_5k_5']$$

et

$$E_3 = [e_3, k_4k_1k_1', k_4k_2k_2', k_4k_4'].$$

D'après notre choix des p considérés, on va avoir

$$\sigma_{*,p}^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}') = \sigma_{*,p}^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e}',\mathbf{E}',\mathbf{d},\mathbf{m},\mathbf{c}_1,\mathbf{c}_2,\mathbf{k},\mathbf{k}')$$

où

$$e_1' = d_1c_{1,1} \quad e_2' = d_2c_{2,1} \quad \text{et} \quad e_3' = d_3c_{3,1}$$

et

$$E_1' = [e_1', k_4k_2k_2', k_4k_3k_3', k_4k_4', d_1k_5k_5'], \quad E_2' = [e_2', k_4k_1k_1', k_4k_3k_3', k_4k_4', d_2k_5k_5']$$

et

$$E_3' = [e_3', k_4k_1k_1', k_4k_2k_2', k_4k_4'],$$

puisque $\nu_p(e_i) = \nu_p(e_i')$ et $\nu_p(E_i) = \nu_p(E_i')$. En enlevant les dépendances inutiles, on obtient

$$\sigma_{*,p}^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e},\mathbf{E},\mathbf{d},\mathbf{d}',\mathbf{k},\mathbf{k}') = \sigma_{*,p}(\mathbf{e}',\mathbf{d},\mathbf{E}',\mathbf{c}_1,\mathbf{k},\mathbf{k}') =$$

$$\left(1-\frac{\chi(p)}{p}\right)^3 \sum_{\boldsymbol{\nu}\in\mathbb{N}^3} \frac{\chi(p)^{\nu_1+\nu_2+\nu_3}\tilde{\rho}(p^{N_1},p^{N_2},p^{N_3};L_1,L_2,Q)}{p^{2(N_1+N_2+N_3+1)}}$$

avec $N_i = \max(\nu_p(e_i')+\nu_i, \nu_p(E_i'))$.

On passe désormais à l'étude analogue pour les nombres premiers $p \equiv 3[4]$. De la même façon on pose

$$e_1'' = d_1 c_{1,2}^2 m_1 \quad e_2'' = d_2 c_{2,2}^2 m_2 \quad \text{et} \quad e_3'' = d_3 m_3$$

et

$$E_1'' = [e_1'', k_4 k_2 k_2', k_4 k_3 k_3', k_4 k_4', k_5 k_5'], \quad E_2'' = [e_2'', k_4 k_1 k_1', k_4 k_3 k_3', k_4 k_4', k_5 k_5']$$

et

$$E_3'' = [e_3'', k_4 k_1 k_1', k_4 k_2 k_2', k_4 k_4'],$$

de sorte que $\nu_p(e_i'') = \nu_p(e_i)$ et $\nu_p(E_i'') = \nu_p(E_i)$. Mais, on sait que les k_i', k_i pour $i \leqslant 4$ et d_i divisent $m \in \mathcal{D}$ donc les facteurs premiers qui interviennent dans leurs décomposition sont congrus à 1 modulo 4 tandis que $k_5 k_5' | c_3 m_3 = d_1' d_2'$ de sorte que l'on peut remplacer les e_i'' et les E_i'' par

$$e_1'' = c_{1,2}^2 m_1 \quad e_2'' = c_{2,2}^2 m_2 \quad \text{et} \quad e_3'' = m_3$$

et

$$E_1'' = [e_1'', k_5 k_5'], \quad E_2'' = [e_2'', k_5 k_5'] \quad \text{et} \quad E_3'' = e_3''$$

puisqu'on a toujours $\nu_p(e_i'') = \nu_p(e_i)$ et $\nu_p(E_i'') = \nu_p(E_i)$. Ainsi, en supprimant à nouveau les dépendances inutiles, on obtient

$$\sigma_{*,p}^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e}, \mathbf{E}, \mathbf{d}, \mathbf{d}', \mathbf{k}, \mathbf{k}') = \sigma_{*,p}(\mathbf{e}'', \mathbf{E}'', \mathbf{c}_2, \mathbf{m}, (k_5, k_5')) =$$

$$\left(1 - \frac{\chi(p)}{p}\right)^3 \sum_{\boldsymbol{\nu} \in \mathbb{N}^3} \frac{\chi(p)^{\nu_1+\nu_2+\nu_3} \tilde{\rho}(p^{N_1}, p^{N_2}, p^{N_3}; L_1, L_2, Q)}{p^{2(N_1+N_2+N_3+1)}}$$

avec $N_i = \max(\nu_p(e_i'') + \nu_i, \nu_p(E_i''))$ ce qui est indépendant des $\mathbf{k}$, $\mathbf{k}'$ et $\mathbf{d}$.

De la même façon, on obtient que (la condition $\equiv 2^\ell [2^{\ell+2}]$ ou $\times 2^{-\nu_p} \equiv 1[4]$ ne dépend que des premiers congrus à 3 modulo 4 et de ceux qui ne sont pas au carré) donc

$$\sigma_{*,2}^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e}, \mathbf{E}, \mathbf{d}, \mathbf{d}', \mathbf{k}, \mathbf{k}') = \sigma_{*,2}^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{m})$$

avec

$$\sigma_{*,2}^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{m}) = 4 \lim_{n \to +\infty} 2^{-2n} \# \left\{ \mathbf{x} \in (\mathbb{Z}/2^n\mathbb{Z})^2 \quad \middle| \quad \begin{array}{l} L_i(\mathbf{x}) \in m_i \varepsilon_i \mathcal{E}_{2^n} \\ Q(\mathbf{x}) \in m_3 \varepsilon_3 \mathcal{E}_{2^n} \\ 2 \not| \mathbf{x} \end{array} \right\}.$$

3.2.2 Stratégie pour valider la conjecture de Peyre

On pose alors

$$V_1(\mathbf{d}, \mathbf{c}_1) = \sum_{\substack{k_4 k_1' | \gcd(\Delta_{23}, m) \\ k_4 k_2' | \gcd(\Delta_{13}, m)}} \sum_{\substack{k_4 k_3' | \gcd(\Delta_{12}, m) \\ k_5 k_5' | \gcd(\Delta_{12}, c_3) \\ k_4 k_4' | \gcd(\gcd(\Delta_{12}, \Delta_{13}, \Delta_{23}), m)}} \frac{\mu(k_1')\mu(k_2')\mu(k_3')\mu(k_4')\mu(k_5')}{3^{\omega(k_4)} 2^{\omega(k_5)+\omega(k_1)+\omega(k_2)+\omega(k_3)}} \prod_{p \equiv 1[4]} \sigma_{*,p}(\mathbf{e}', \mathbf{d}, \mathbf{E}', \mathbf{c}_1, \mathbf{k}, \mathbf{k}'),$$

puis

$$V_3(\mathbf{m}, \mathbf{c}_2) = \sum_{k_5 k_5' | \gcd(\Delta_{12}, m_3)} \prod_{p \equiv 3[4]} \sigma_{*,p}(\mathbf{e}'', \mathbf{E}'', \mathbf{c}_2, \mathbf{m}, (k_5, k_5'))$$

et enfin

$$V_2(\boldsymbol{\varepsilon}, \mathbf{m}, \mathbf{c}_2) = \frac{1}{4} \sigma_{*,p}^{\varepsilon_1,\varepsilon_2,\varepsilon_3}(\mathbf{e}'', \mathbf{c}_2, \mathbf{m})$$

de sorte qu'on ait

$$c_0(\boldsymbol{\varepsilon},\mathbf{m}) = \mu(m_3)\mu((m_1,m_2))\chi(m_3)\chi((m_1,m_2))\frac{\pi^2}{4}\sum_{\mathbf{c}_2\in\mathcal{D}((m_2,m_3))\times\mathcal{D}((m_1,m_3))}\mu(c_{1,2})\mu(c_{2,2})\chi(c_{1,2})\times$$

$$\chi(c_{2,2})V_2(\boldsymbol{\varepsilon},\mathbf{m})V_3(\mathbf{m},\mathbf{c}_2)\sum_{m\in\mathcal{D}}\frac{\mu(m)r(m)\varphi^\dagger(m)}{4m}\sum_{\substack{\mathbf{d}\in\mathbb{N}^3\\ m=d_1d_2d_3}}\sum_{\mathbf{c}_1\in C}\mu(c_{3,1})\mu((c_{1,1},c_{2,1}))V_1(\mathbf{d},\mathbf{c}_1).$$

Mais m_3 est sans facteur carré et tous ses diviseurs premiers sont congrus à 3 modulo 4 donc

$$\chi(m_3)\mu(m_3) = (-1)^{2\omega(m_3)} = 1$$

et de même

$$\mu((m_1,m_2))\chi((m_1,m_2)) = 1$$

et

$$\mu(c_{1,2})\chi(c_{1,2}) = \mu(c_{2,2})\chi(c_{2,2}) = 1.$$

Par conséquent, on a

$$c_0(\boldsymbol{\varepsilon},\mathbf{m}) = \frac{\pi^2}{4}V_2(\boldsymbol{\varepsilon},\mathbf{m})\sum_{\mathbf{c}_2\in\mathcal{D}((m_2,m_3))\times\mathcal{D}((m_1,m_3))}V_3(\mathbf{m},\mathbf{c}_2)\times$$

$$\sum_{m\in\mathcal{D}}\frac{\mu(m)r(m)\varphi^\dagger(m)}{4m}\sum_{\substack{\mathbf{d}\in\mathbb{N}^3\\ m=d_1d_2d_3}}\sum_{\mathbf{c}_1\in C}\mu(c_{3,1})\mu((c_{1,1},c_{2,1}))V_1(\mathbf{d},\mathbf{c}_1).$$

La stratégie pour conclure à la validation de la conjecture de Peyre est alors, suivant [18] et [26], de décomposer $c_0(\boldsymbol{\varepsilon},\mathbf{m})$ sous la forme

$$c_0(\boldsymbol{\varepsilon},\mathbf{m}) = \pi\prod_p c_p(\boldsymbol{\varepsilon},\mathbf{m})$$

et d'établir que pour tout nombre premier p, on a $c_p(\boldsymbol{\varepsilon},\mathbf{m}) = \omega_p(\boldsymbol{\varepsilon},\mathbf{m})$. Cependant, à l'heure actuelle, il reste un certain nombre de complications techniques à régler du fait que la formule d'éclatement en quatre entiers, et par conséquent le système de représentants des classes d'isomorphie de torseurs universels choisis, soient plus compliqué. Il est à noter qu'on aurait probablement facilité cette partie du travail si on avait fait le passage aux torseurs de manière plus théorique comme dans [18].

Conclusion

Pour conclure, on rappelle que le traitement de la conjecture de Manin sur les surfaces de Châtelet $Y^2 + Z^2 = f(X)$ dépend du type de factorisation du polynôme et que tous les cas possibles sont listés ci-dessous.

(i) $P = L_1L_2L_3L_4$, où les L_j sont des formes linéaires de $\mathbb{Q}[X]$;

(ii) $P = L_1L_2Q$ où les L_j sont des formes linéaires, et Q une forme quadratique irréductible sur $\mathbb{Q}$ mais réductible sur $\mathbb{Q}[i]$;

(iii) $P = L_1L_2Q$ où les L_j sont des formes linéaires, et Q une forme quadratique irréductible sur $\mathbb{Q}[i]$;

(iv) $P = LC$, où L est une forme linéaire, et C est une forme cubique irréductible sur $\mathbb{Q}$;

(v) $P = Q_1Q_2$, où les Q_j sont des formes quadratiques irréductibles sur $\mathbb{Q}$, mais dont l'une au moins est réductible sur $\mathbb{Q}[i]$;

(vi) $P = Q_1Q_2$ où les Q_j sont des formes quadratiques irréductibles sur $\mathbb{Q}[i]$;

(vii) P est irréductible sur $\mathbb{Q}$, mais est réductible sur $\mathbb{Q}[i]$;

(viii) P est une forme irréductible sur $\mathbb{Q}[i]$.

La méthode générale par les torseurs universel et l'utilisation de la géométrie des nombres à travers le Lemme 8 est commune à tous les types de factorisation. Ce sont les outils de théorie analytique des nombres qui varient d'un cas sur l'autre. Ensuite, tous les cas pour lesquels une forme linéaire apparaît dans la factorisation de f donnent lieu à des méthodes similaires à celles développées dans ce rapport, même si chaque cas donne évidemment lieu à des spécificités et des complications techniques particulières. Ils sont traités dans [21], [24], [18] et dans ce rapport. Les cas vi) et vii) sont traités dans [26] et font appel à des outils assez différents et notamment à la fonction $\mathbf{\Delta}$ de Hooley tordue par un caractère ([25] et [40]). Dans chacun des cas, mis à part le cas iii) traité dans ce rapport, la conjecture de Peyre a été vérifiée. Pour terminer le programme de recherche sur les conjectures de Manin, puisque les cas ii), v) et vii) peuvent être considérés comme dégénérés, il reste à l'auteur à terminer les investigations en cours afin de valider la conjecture de Peyre dans ce dernier cas également.

Enfin, on peut citer que la question de la conjecture de Manin sur les surfaces de Châtelet $Y^2 - aZ^2 = f(X)$ avec $a > 0$ ou encore une tentative de généralisation des méthodes utilisées ici à des variétés fibrées en coniques pourraient ultérieurement constituer des pistes de recherche très intéressantes.

Bibliographie

[1] Y.I.Manin. Cubic forms. *volume 4 of North-Holland Mathematical Library. North-Holland Publishing Co., Amsterdam, second edition, translated from the russian by M.Hazewinkel*, (1986).

[2] Y.Tschinkel J.Franke, Y.I.Manin. Rational points of bounded height on Fano varieties. *Invent. Math.* **95(2)**, 421-435, (1989).

[3] E. Peyre. Hauteurs et mesures de Tamagawa sur les variétés de Fano. *Duke Math. J.* **79**, (1995), 101-218.

[4] B.J.Birch. Forms in many variables. *Proc. Roy. Soc. Ser.*, 245-263, (1962).

[5] Y.Tschinkel V.V.Batyrev. Manin's conjecture for toric varieties. *Algebraic Geom.* **7(1)**, 15-53, (1998).

[6] Y.Tschinkel A.Chambert-Loir. On the distribution of points of bounded height on equivariant compactifications of vector groups. *Invent Math.* **148(2)**, 421-452, (2002).

[7] U. Derenthal. Geometry of universal torsors. *PhD Thesis*, (2006).

[8] T. Browning R. de la Bretèche. On Manin's conjecture for singular del Pezzo surfaces of degree four, I. *Michigan Mathematical Journal,* **55**, (2007), 51–80.

[9] T. Browning R. de la Bretèche. On Manin's conjecture for singular del Pezzo surfaces of degree four, II. *Math. Proc. Camb. Phil. Soc.* **143**, (2007), 579–605.

[10] P. Le Boudec. Manin's conjecture for a cubic surface with 2A2+A1 singularity type. *Math. Proc. Cambridge Philos. Soc.*, (2012).

[11] E. Fouvry R. de la Bretèche. L'éclaté du plan projectif en quatre points dont deux conjugués. *J. Reine. Angew. Math.*, (2004), 63–122.

[12] J.J. Sansuc J-L. Colliot-Thélène. 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.J. Sansuc J-L. Colliot-Thélène. La descente sur les variétés rationnelles. *Journées de géométrie algébrique d'Angers*, (1979), 223–237.

[14] J.J. Sansuc J-L. Colliot-Thélène. La descente sur les variétés rationnelles II. *Duke Math. J.* **54**, (1987), 375–492.

[15] R. de la Bretèche. Nombre de points rationnels sur la cubique de Segre. *Proceedings of the London Mathematical Society, (1)* **95**, (2007), 69–155 (doi : 10.1112/plms/pdm001).

[16] P. Salberger V. Blomer, J. Brüdern. On a certain senary cubic form. *arXiv :1205.0190v1*, (2012).

[17] V.A.Iskovskikh. Minimal models of rational surfaces over arbitrary fields. *Math. USSR Izv.* **14**, (1980), 17–39.

[18] E. Peyre R. de la Bretèche, T. Browning. On Manin's conjecture for a family of Châtelet surfaces. *Annals of Mathematics,* **175**, (2012), 1-47.Une version plus longue est aussi disponible à l'adresse http ://arxiv.org/abs/1002. 0255.

[19] H.P.F. Swinnerton-Dyer J-L. Colliot-Thélène, J.J. Sansuc. Intersections of two quadrics and Châtelet surfaces I. *J. reine angew. Math.* **373**, (1987), 37–101.

[20] H.P.F. Swinnerton-Dyer J-L. Colliot-Thélène, J.J. Sansuc. Intersections of two quadrics and Châtelet surfaces II. *J. reine angew. Math.* **374**, (1987), 72–168.

[21] T. Browning R. de la Bretèche. Binary forms as sums of two squares and Châtelet surfaces. *Israel Journal of Math.* **191**, (2012).

[22] S. Daniel. On the divisor-sum problem for binary forms. *J. reine angew. Math.* **507**, (1999), 107–129.

[23] D. R. Heath-Brown. Linear relations amongst sums of two squares. *Number theory and algebraic geometry, 133–176, London Math. Soc. Lecture Note Ser.* **303**, CUP, 2003.

[24] T. Browning R. de la Bretèche. Binary linear forms as sums of two squares. *Compositio Mathematica,* **144 (6)**, (2008), 1375-1402.

[25] G. Tenenbaum R. de la Bretèche. Oscillations localisées sur les diviseurs. *Journal of London Math. Soc. (2012)* **85 (3)**, 669-693, disponible au doi : 10.1112/jlms/jdr058.

[26] G. Tenenbaum R. de la Bretèche. Conjecture de Manin pour certaines surfaces de Châtelet. *à paraître au Journal de l'Institut de Jussieu*, 2013.

[27] T. Browning R. de la Bretèche. Le problème des diviseurs pour des formes binaires de degré 4. *J. reine angew. Math.,* **646**, (2010), 1–44.

[28] T. Browning R. de la Bretèche. Sums of arithmetic functions over values of binary forms. *Acta Arith.* **125**, (2007), 291–304.

[29] G. Marasingha. On the representation of almost primes by pairs of quadratic forms. *Acta Arith.* **124**, (2008), 327–355.

[30] G. Marasingha. Almost primes represented by binary forms. *J. Lond. Math. Soc.*, (2010).

[31] J.-P. Serre. *Cours d'arithmétique.*

[32] H. Davenport. Cubic forms in 16 variables. *Proc. Roy. Soc. A* **272**, (1963), 285–303.

[33] H. Heilbronn. Zeta functions and L-functions. *Algebraic Number Theory*, (1967), 204–230.

[34] A. Skorobogatov. *Torsors and rational points.*

[35] E. Peyre. Counting points on varieties using universal torsors. *Annals of Mathematics,* **175**, (2012).

[36] J.H. Silverman M. Hindry. *Diophantine geometry. An introduction.*

[37] T.D. Browning. Linear growth for Châtelet surfaces. *Math. Annalen* **646**, (2010), 1–44.

[38] Mac Carthy. *Introduction to arithmetical functions.*

[39] G. Tenenbaum. *Introduction à la théorie analytique et probabiliste des nombres.*

[40] G. Tenenbaum R. de la Bretèche. Moyennes de fonctions arithmétiques de formes binaires. *Mathematika* **58**, (2012), 290-304.

[41] P. Le Boudec. Répartition des points rationnels sur certaines surfaces de del pezzo. *Thèse*, (2012).

[42] T. Browning R. de la Bretèche. Manin's conjecture for quartic del Pezzo surfaces with a conic fibration. *Duke Mathematical Journal (2011),* **160**, 1-69.

[43] R. Hartshorne. *Algebraic geometry.*