Le problème de Tchébychev pour le douzième polynôme cyclotomique

Cécile Dartyge

Le problème de Tchébychev pour le douzième polynôme cyclotomique

Cécile Dartyge (Nancy)

Abstract. Let $P^+(n)$ denote the largest prime factor of the integer n and $\Phi_{12}(n) = n^4 - n^2 + 1$. We prove that for X large enough we have :

$$P^+\Big(\prod_{X<n\leqslant 2X} \Phi_{12}(n)\Big) \geqslant X^{1+c} \text{ with } c = 10^{-26531}.$$

Résumé. On note $P^+(n)$ le plus grand facteur premier de l'entier n et $\Phi_{12}(n) = n^4 - n^2 + 1$. Nous montrons pour X assez grand la minoration :

$$P^+\Big(\prod_{X<n\leqslant 2X} \Phi_{12}(n)\Big) \geqslant X^{1+c} \text{ avec } c = 10^{-26531}.$$

Sommaire

1. Introduction

En 1837, Dirichlet ([38] pp. 315-350), a montré que si a et $q \geqslant 1$ sont deux entiers premiers entre eux, alors il existe une infinité de nombres premiers de la forme $a + nq$.

La conjecture de Bouniakowsky consiste à étendre ce Théorème de Dirichlet à des polynômes de degré supérieur. Plus précisément elle énonce qu'un polynôme f irréductible sans diviseur fixe et de coefficient dominant positif représente une infinité de nombres premiers. Cette conjecture qui est un cas particulier de l'hypothèse H de Schinzel et Sierpiński ([48] ou [23]), est actuellement hors d'atteinte pour des polynômes f de degré supérieur ou égal à 2. Plus le degré de f est grand plus le problème est difficile car la suite $\{f(n)\}_{n\geqslant 1}$ devient de plus en plus éparse.

Cependant ces dernières décennies, des avancées spectaculaires ont été obtenues pour des polynômes en deux variables. Le cas des polynômes de degré 2 en deux variables a été résolu par Iwaniec dans un article paru en 1974 [33]. Friedlander et Iwaniec [20] ont donné en 1998 une formule asymptotique du nombre de nombres premiers de la forme

$a^2 + b^4$, les entiers a et b étant dans un domaine naturel. Peu de temps après Heath-Brown [25] a montré un résultat analogue pour la forme $a^3 + 2b^3$. Ce dernier résultat fut ensuite généralisé aux formes binaires cubiques irréductibles et sans diviseur fixe par Heath-Brown et Moroz [27], [28].

Une autre façon d'approcher la conjecture de Bouniakowski est de rechercher des entiers n tels que $f(n)$ ait une structure multiplicative proche de celle d'un nombre premier. Les recherches engagées dans cette voie ont principalement eu pour objectif de montrer l'existence d'une infinité de valeurs polynomiales de l'un des deux types suivants :

(i) $f(n)$ est un entier presque premier c'est-à-dire avec un nombre de facteurs premiers inférieur à une borne ne dépendant que du polynôme f ;

(ii) $f(n)$ est divisible par un grand nombre premier. On entend par là un nombre premier d'un ordre de grandeur le plus proche possible de n^d, d étant le degré de f, en tous cas supérieur à $nw(n)$ où w est une fonction telle que $\lim_{n\to+\infty} w(n) = +\infty$.

Pour le type (i), Iwaniec [34] a démontré qu'il existait une infinité d'entiers n tels que $n^2 + 1$ soit un P_2 où P_r désigne un entier avec au plus r facteurs premiers. Très récemment, Lemke Oliver [39] a étendu ce résultat aux polynômes irréductibles de degré 2 sans diviseur fixe. Lorsque d, le degré du polynôme f est supérieur ou égal à 3, il est maintenant établi que f représente une infinité de P_{d+1}. On trouvera dans l'introduction de [39] un historique précis sur cette question.

Pour $n \in \mathbb{N}^*$, on note $P^+(n)$ le plus grand facteur premier de n et $P^-(n)$ le plus petit facteur premier avec la convention $P^+(1) = 1$ et $P^-(1) = +\infty$. Le problème de Tchébychev évoqué dans le titre de cet article correspond à la recherche de valeurs polynomiales de type (ii). Nous reprenons ici la dénomination de Nagell [44] et celle de Hooley [31]. Elle fait référence au résultat de Tchébychev suivant qui est la première avancée sur cette question :

$$\lim_{x\to+\infty} \frac{P^+\Big(\prod_{n\leqslant x}(n^2+1)\Big)}{x} = +\infty. \tag{1·1}$$

Cette inégalité a été reconstituée par Markov [42] à partir de manuscrits posthumes de Tchébychev.

En 1917 Pólya [47] a établi une telle formule pour les polynômes cyclotomiques. Quelques années plus tard, Nagell [44] a obtenu pour tout f irréductible de degré supérieur ou égal à 2 et $\vartheta \in [0, 1[$ la minoration :

$$P^+\Big(\prod_{n\leqslant x} f(n)\Big) \gg_{f,\vartheta} x(\log x)^{\vartheta}. \tag{1·2}$$

Erdős [17] a ensuite montré dans un article paru en 1952 qu'il existait $A > 0$ tel que

$$P^+\Big(\prod_{n\leqslant x} f(n)\Big) \gg_f x(\log x)^{A\log\log\log x}. \tag{1·3}$$

Ce résultat fut amélioré une quarantaine d'années plus tard par Erdős et Schinzel [18] qui ont montré que l'on pouvait remplacer le membre de droite de la minoration (1·3) par $x\exp\exp(c(\log\log x)^{2/3})$ pour une constante $c > 0$ absolue. Actuellement, le meilleur résultat valable pour tout polynôme irréductible de degré supérieur à 2 est celui de Tenenbaum [50]. Il a montré pour tout $\alpha \in]0, 2 - \log 4[$, l'inégalité :

$$P^+\Big(\prod_{n\leqslant x} f(n)\Big) > x\exp\{(\log x)^{\alpha}\} \quad (x > x_0(f,\alpha)).$$

Une version de cette inégalité dans certains petits intervalles a été obtenue par Nair et Tenenbaum [46]. Ils ont montré pour tout entier $k \geqslant \deg f \geqslant 2$, $\alpha \in]0, 2 - \log 4[$ et $y = x^{\frac{\deg f}{k}}$ la minoration

$$P^+\Big(\prod_{x<n\leqslant x+y} f(n)\Big) > y \exp\{(\log x)^\alpha\} \quad (x > x_0(f,\alpha)).$$

En 1967 Hooley ([30] ou [31]) a obtenu une avancée importante pour le polynôme n^2+1 (ainsi que pour les polynômes de la forme $n^2 - D$ où D est un entier négatif) :

$$P_x := P^+\Big(\prod_{n\leqslant x}(n^2+1)\Big) \gg x^{1,1}. \tag{1·4}$$

Une partie de la preuve passe par l'étude des quantités

$$\sum_{P<p\leqslant 2P} \log p |\{n \leqslant x : n^2 + 1 \equiv 0 \,(\mathrm{mod}\, p)\}|,$$

avec $x \ll P \ll P_x$. En utilisant des méthodes de sommes d'exponentielles, ce problème revient à majorer en moyenne sur p des sommes de la forme :

$$\sum_{\substack{O\leqslant\Omega<p\\ \Omega^2+1\equiv 0\,(\mathrm{mod}\,p)}} \mathrm{e}\Big(\frac{h\Omega}{p}\Big), \tag{1·5}$$

avec la notation usuelle $\mathrm{e}(t) = \exp(2i\pi t)$. La clé de la preuve est d'exploiter la correspondance bijective établie par Legendre [49] entre les solutions de la congruence $\Omega^2 + 1 \equiv 0 \,(\mathrm{mod}\, m)$ resp. $\Omega^2 - D \equiv 0 \,(\mathrm{mod}\, m)$ et des représentations de m par des formes quadratiques de discriminant -1 resp. D, où D est un entier strictement négatif et sans facteur carré. La difficulté d'établir une majoration de (1·5) en moyenne sur une suite de nombres premiers p dans un intervalle prescrit est réglée en utilisant du crible. Le problème est ramené à des majorations de sommes quasiment du type

$$\sum_{P^{1/2}\ll s\ll P^{1/2}} \Big|\sum_{\substack{|r|<s\\ (r,s)=1}} \mathrm{e}\Big(\frac{k\overline{r}}{s}\Big)\Big|, \tag{1·6}$$

où $\overline{r}$ est un inverse* de r modulo s. La somme sur r est une somme de Kloosterman et est un $O(s^{1/2+\varepsilon}(s,k)^{1/2})$ d'après les travaux de Weil [53]. La dernière avancée relative au polynôme n^2+1 est celle de Deshouillers et Iwaniec [16]. Elle consiste à remplacer dans l'argument de Hooley la majoration de Weil par les majorations en moyenne de sommes de Kloosterman qu'ils ont obtenues dans [15] par le biais de la théorie des formes modulaires. Ils montrent ainsi pour x assez grand la minoration :

$$P_x > x^\vartheta,$$

où ϑ est solution de l'équation $2 - \vartheta - 2\log(2-\vartheta) = \frac{5}{4}$, $\vartheta = 1,202....$

Hooley [32] est également à l'origine d'un progrès fondamental pour un polynôme de degré 3.

---

* Plus généralement les barres dans les écritures du type $\overline{x}$ désigneront les inverses relatifs au dénominateur de la fraction ou au module de la congruence étudiée.

Il montre que sous la condition suivante appelée hypothèse R^*,

$$(R^*) \qquad \sum_{\substack{\zeta_1 \leqslant r \leqslant \zeta_2 \\ (s,r)=1}} \mathrm{e}\Big(\frac{h\overline{r}+kr}{s}\Big) \ll (1+\zeta_2-\zeta_1)^{1/2} s^{\varepsilon}(h,k,s)^{1/2},$$

on a :

$$P^+\Big(\prod_{n\leqslant x}(n^3+2)\Big) \gg x^{31/30}.$$

L'idée directrice de la preuve est tout naturellement d'adapter les arguments de (1·4) au polynôme n^3+2. Hooley parvient effectivement à établir une bijection entre les solutions de $\Omega^3+2 \equiv 0 \pmod m$ et des représentations de m par la forme cubique $\varphi(x,y,z) = x^3+2y^3+4z^3-6xyz$ qui est la norme de $x+y\sqrt[3]{2}+z\sqrt[3]{4}$ sur $\mathbb{Q}(\sqrt[3]{2})$. En simplifiant beaucoup, le passage de (1·5) à (1·6) correspond à la transformation :

$$(1\cdot7) \qquad \sum_{P<m\leqslant 2P} \sum_{\substack{0\leqslant\Omega<m \\ \Omega^3+2\equiv 0 \,(\mathrm{mod}\, m)}} \mathrm{e}\Big(\frac{h\Omega}{m}\Big) \longrightarrow \sum_{b,c\approx P^{1/3}} \sum_{\substack{A<a\leqslant A+P^{1/3} \\ (b^2-ac,b^3-2c^3)=1}} \mathrm{e}\Big(\frac{hc^2\overline{b^2-ac}}{b^3-2c^3}\Big).$$

Le problème est que la somme sur a est de longueur très courte $\approx P^{1/3}$, alors que le dénominateur b^3-2c^3 est en général d'un ordre de grandeur P. Les majorations de Weil donnent alors un résultat moins bon qu'une majoration triviale. C'est la raison pour laquelle l'hypothèse R^* est nécessaire.

En 2001, Heath-Brown [24] a résolu cette difficulté et a montré le résultat inconditionnel suivant : pour tout X assez grand, il existe une proportion positive d'entiers $n \in]X, 2X]$ tels que n^3+2 ait un facteur premier supérieur à $X^{1+10^{-303}}$. En particulier, on a :

$$(1\cdot8) \qquad P^+\Big(\prod_{n\leqslant x}(n^3+2)\Big) > x^{1+10^{-303}}.$$

Dans ce travail Heath-Brown n'a pas vraiment cherché à obtenir la meilleure puissance possible dans le membre de droite de (1·8) et il précise qu'il est fort probable qu'elle puisse être améliorée.

Un des nouveaux ingrédients apportés par Heath-Brown est un résultat de majoration de sommes très courtes d'exponentielles d'argument une fraction rationnelle (rappelé dans le Théorème 12.1 *infra*), c'est-à-dire de la forme :

$$\sum_{\substack{A<n<A+B \\ (g(n),q)=1}} \mathrm{e}\Big(\frac{f(n)\overline{g(n)}}{q}\Big),$$

où $f, g \in \mathbb{Z}[X]$. Le résultat de Heath-Brown fournit une majoration non triviale de cette somme même quand la longueur B est extrêmement petite par rapport à q sous réserve que l'entier q puisse s'écrire sous la forme $q = q_0 q_1 \cdots q_k$ avec des diviseurs q_i de taille pas trop importante.

Une difficulté est que les entiers $q = b^3-2c^3$ de (1·7) n'admettent pas tous une telle décomposition. Il est donc impossible d'insérer directement ces résultats dans l'argument de Hooley. Cela a conduit Heath-Brown à suivre une autre voie que celle communément appelée l'approche de Tchébychev-Hooley.

L'approche de Heath-Brown présente des similitudes avec celles d'Erdős [17], Erdős et Schinzel [18] puis Tenenbaum [50] qui consistaient à obtenir une minoration du nombre

d'entiers $n \leqslant x$ tels que $f(n)$ ait un diviseur compris entre $x/2$ et x. La variante proposée par Heath-Brown vise à montrer qu'il existe une proportion positive d'entiers $n < x$ tels que $f(n)$ possède un diviseur suffisamment friable, dans l'intervalle $]x^{1+\delta}, x^{1+2\delta}]$. Le grand avantage de cette approche réside dans la souplesse dans le choix des diviseurs dans l'intervalle $]x^{1+\delta}, x^{1+2\delta}]$. Il peut alors se restreindre à la recherche des entiers n tels que $f(n)$ soit divisible par un $m \in]x^{1+\delta}, x^{1+2\delta}]$ pour lequel l'entier q associé soit bien factorisable.

Dans cet article nous établissons un résultat analogue à (1·8) pour un polynôme de degré 4. Soit Φ_{12} le douzième polynôme cyclotomique : $\Phi_{12}(X) = X^4 - X^2 + 1$.

Théorème 1.1. *Il existe $c > 0$ tel que pour X assez grand on ait la minoration :*

$$P^+\Big(\prod_{X<n\leqslant 2X} \Phi_{12}(n)\Big) \geqslant X^{1+c}. \tag{1·9}$$

La valeur $c = 10^{-26531}$ est admissible.

Nous n'avons pas cherché à déterminer le meilleur exposant possible dans (1·9). Nous voulions juste obtenir un exposant strictement supérieur à 1 sans rajouter trop de complications lors de certaines étapes. La détermination numérique d'un exposant c admissible n'était cependant pas immédiate. Elle repose sur l'existence de solutions d'un système linéaire d'une trentaine d'inéquations avec 14 inconnues. Bruno Pinçon a fait un programme PARI utilisant la méthode du simplexe qui fournit une solution proche de la meilleure possible.

En modifiant quelques paramètres de la preuve du Théorème 1.1 on peut montrer qu'il existe $c' > 0$ tel que $P^+(\Phi_{12}(n)) \geqslant n^{1+c'}$ pour une proportion positive d'entiers n. L'exposant c' alors obtenu est légèrement plus petit que c.

Le fil rouge de la démonstration du Théorème 1.1 est l'article de Heath-Brown [24] dont nous avons adopté une grande partie des notations. En particulier nous profitons à de nombreuses reprises de la transcription du problème en termes d'idéaux de l'anneau des entiers d'un corps de nombres. Ainsi $n^3 + 2$ est la norme de l'idéal $(n + \sqrt[3]{2})$, et il y a une correspondance entre les facteurs premiers de $n^3 + 2$ et les idéaux premiers intervenant dans la décomposition de $(n + \sqrt[3]{2})$. Cette correspondance rend bien plus commode la présentation et la compréhension de différentes étapes.

Dans [24] Heath-Brown indique que la principale difficulté pour étendre (1·8) à d'autres polynômes irréductibles f de degré supérieur ou égal à 3 est de trouver une correspondance entre des solutions de $f(\Omega) \equiv 0 \,(\mathrm{mod}\, m)$ et des représentations de m comme une norme d'un élément d'un anneau d'entiers.

Cette difficulté est résolue ici pour le polynôme Φ_{12}. Nous nous sommes efforcés de bien expliciter les différentes étapes de cette partie pour ainsi entrevoir comment la généraliser à d'autres polynômes.

Notre méthode est un procédé d'élimination d'une variable. Elle s'adapte assez facilement pour obtenir une transformation du type (1·7) valable pour des polynômes f irréductibles tels que l'anneau des entiers d'un corps de nombres associé à f et le groupe des unités correspondant ne soient pas trop compliqués.

Malheureusement l'entier q obtenu par cette méthode ne peut pas toujours se factoriser sous une forme adaptée aux majorations de sommes d'exponentielles d'Heath-Brown.

Pour des polynômes de degré 4 notre méthode permet d'obtenir pour une assez large famille de polynômes une transformation de type (1·7) avec un membre de droite alors du type

$$\sum_{b,c,d} \sum_{\substack{A_1<a<A_2 \\ (G(a,b,c,d),q(b,c,d))=1}} \mathrm{e}\Big(\frac{F(a,b,c,d)\overline{G(a,b,c,d)}}{q(b,c,d)}\Big),$$

où F, G, q sont des polynômes en 4 ou 3 variables à coefficients entiers.

Pour Φ_{12}, l'entier q que nous obtenons est de la forme

$$q(b,c,d) = (b^2+c^2)(b^2+db+d^2)(-3c^2+(b+2d)^2). \tag{1·10}$$

Nous devons alors montrer qu'il existe une proportion positive de triplets (b,c,d), tels que l'entier $q(b,c,d)$ puisse s'écrire comme un produit de 8 diviseurs de taille bien contrôlée.

Il nous a semblé intéressant d'étudier ce problème dans un cadre plus général. Considérons f_1 et f_2 deux formes binaires irréductibles de degré supérieur ou égal à 2. En utilisant des résultats sur les réseaux de $\mathbb{Z}^3$ nous obtenons une sorte de niveau de distribution pour les suites de couples $(f_1(b,c), f_2(b,d))$ quand les triplets (b,c,d) parcourent un pavé de $\mathbb{Z}^3$. Si les longueurs des arêtes du pavé sont d'un ordre de grandeur M, notre résultat (Théorème 8.1 *infra.*) donne une estimation en moyenne sur $q_1 < Q_1$, $q_2 < Q_2$ du nombre de triplets (b,c,d) tels que $q_1 | f_1(b,c)$ et $q_2 | f_2(b,d)$ pour $Q_1Q_2 < M^{3-\varepsilon}$ et $\max(Q_1,Q_2) < M^{2-\varepsilon}$.

Une variante de ce résultat nous permet de montrer qu'il existe "beaucoup" de triplets (b,c,d) tels que l'entier q donné par (1·10) soit bien factorisable. Nos majorations profitent également des avancées récentes de la Bretèche, Browning, Henriot et Tenenbaum [5], [9], [29] sur des moyennes de fonctions multiplicatives d'argument des valeurs prises par un polynôme de $\mathbb{Z}[X]$ ou par une forme binaire.

Nous énonçons dans cette introduction une version simplifiée du Théorème 8.1.

Théorème 1.2. *Soient $f_1, f_2 \in \mathbb{Z}[x,y]$ deux formes binaires irréductibles de degré supérieur à 2. On considère pour $M \geqslant 1$ les ensembles :*

$$\mathcal{A}(m_1,m_2) = \{(b,c,d) \in [1,M]^3 : m_1 | f_1(b,c),\ m_2 | f_2(b,d) \text{ et } (m_1,b,c) = 1 = (m_2,b,d)\}.$$

Pour $i = 1,2$, on définit $\varrho^*_{f_i}(m) = |\{0 \leqslant u,v < m : m | f_i(u,v) \text{ et } (u,v,m) = 1\}|$, puis

$$E_0 := \sideset{}{^*}\sum_{\substack{m_1<Q_1\\ m_2<Q_2\\ (m_1,m_2)=1}} \Big| |\mathcal{A}(m_1,m_2)| - \frac{M^3 \varrho^*_{f_1}(m_1)\varrho^*_{f_2}(m_2)}{m_1^2 m_2^2} \Big|,$$

où l'astérisque dans la sommation indique que pour $i = 1,2$, $(m_i, f_i(1,0)f_i(0,1)) = 1$. On a alors la majoration :

$$E_0 \ll_{f_1,f_2} M^2 (Q_1Q_2)^{1/3} (\log M)^7 + M^{2+\varepsilon}(\sqrt{Q_1} + \sqrt{Q_2}).$$

Notons $\zeta_{12} = \mathrm{e}^{i\pi/6}$ une des racines de Φ_{12}. Dans un premier temps on adapte plusieurs idées de Heath-Brown pour montrer comment le problème peut se ramener à la minoration du cardinal d'un ensemble de la forme :

$$\mathcal{A}_1 = \{X < n \leqslant 2X : \exists J \in \mathcal{J} \text{ tel que } n + \zeta_{12} \in J\},$$

où $\mathcal{J}$ est une famille d'idéaux vérifiant une série de conditions. La deuxième partie comporte les différentes étapes pour la transformation de type (1·7). La troisième concerne l'énoncé puis la preuve du Théorème 8.1. Après une brève étude de la structure du groupe des unités de $\mathbb{Z}[\zeta_{12}]$, nous sommes enfin en mesure de définir précisément notre ensemble $\mathcal{J}$ d'idéaux. Les 6 derniers paragraphes de cet article sont dévolus à la minoration du cardinal de l'ensemble $\mathcal{A}_1$ correspondant. Là encore on suit la stratégie mise en place

par Heath-Brown. Le fait de travailler avec une variable supplémentaire et une forme q composée de 3 facteurs irréductibles rend certaines étapes assez délicates.

Nous avons choisi de présenter en détail le cas du polynôme Φ_{12} afin d'obtenir un exposant complètement explicite. Il serait intéressant de déterminer précisément l'ensemble des polynômes pour lesquels notre méthode est valable ainsi que ceux pour lesquels on puisse déjà obtenir un résultat conditionnel avec une hypothèse de type R^*. Nous espérons obtenir prochainement des avancées significatives sur ce sujet.

Dans tout cet article la lettre ε désignera un réel strictement positif arbitrairement petit et qui ne sera pas le même à chaque occurrence. La notation $(a_1, \dots, a_n)$ renverra soit à un élément de $\mathbb{R}^n$ ou $\mathbb{C}^n$ soit au pgcd des entiers $a_1, \dots, a_n$. Nous espérons que le contexte sera suffisamment clair pour que le lecteur ne soit pas dérouté par cette ambiguïté.

Remerciements. La réalisation de cet article a énormément bénéficié de l'aide de trois personnes que je tiens à remercier très chaleureusement. Les premières avancées sur ce problème ont été obtenues avec Guillaume Hanrot. Sa collaboration a été cruciale notamment pour le Lemme 6.2. Bruno Pinçon a accepté de faire le travail de programmation qui permet de déterminer l'exposant c et assurer ainsi que tout cet échafaudage ne s'effondre pas. Régis de la Bretèche a relu très attentivement une version préliminaire de cet article. Ses nombreuses remarques et suggestions ont apporté de très fortes améliorations dans plusieurs parties de ce travail.

2. Comment détecter des valeurs polynomiales avec un grand facteur premier ?

Soit $f \in \mathbb{Z}[X]$ un polynôme irréductible de degré d tel que $f(\mathbb{N}) \subset \mathbb{N}$. Il existe alors un réel $k_f > 0$ tel que $f(n) \leqslant k_f n^d$ pour tout $n \in \mathbb{N}$.

Le point de départ de différentes méthodes utilisées pour le problème de Tchébychev est d'évaluer de deux manières différentes la quantité :

$$V_f(X) = \sum_{X < n \leqslant 2X} \log(f(n)).$$

D'une part, lorsque $X < n \leqslant 2X$, $\log(f(n)) = d \log X + O(1)$. On obtient ainsi sans peine

$$V_f(X) = dX \log X + O(X). \tag{2·1}$$

D'autre part on peut aussi évaluer $V_f(X)$ en profitant de l'additivité du logarithme.

Suivant la présentation d'Heath-Brown, on l'exploite sous la forme :

$$\log(f(n)) = \log^{(1)}(f(n)) + \log^{(2)}(f(n)),$$

avec

$$\log^{(1)}(f(n)) = \sum_{\substack{k \geqslant 1,\ p \leqslant DX \\ p^k \| f(n)}} k \log p \quad \text{et} \quad \log^{(2)}(f(n)) = \sum_{\substack{k \geqslant 1,\ p > DX \\ p^k \| f(n)}} k \log p,$$

où $p^k \| n$ signifie que $p^k | f(n)$ et que p^{k+1} ne divise pas $f(n)$ et $D > 0$ est tel que

$$D^{d-1} > k_f 2^d. \tag{2·2}$$

Soit

$$\mathcal{A}(f) = \{X < n \leqslant 2X : \log^{(1)}(f(n)) \geqslant \log X\}. \tag{2·3}$$

Nous proposons ici une légère variante du Théorème 3 de [18] qui ressemble également au Lemme 2 de [24].

Lemme 2.1. *On suppose qu'il existe $\alpha > 0$ tel que pour X assez grand, $|\mathcal{A}(f)| \geqslant \alpha X$. On a alors pour X assez grand*

$$P^+\Big(\prod_{X<n\leqslant 2X} f(n)\Big) \gg_f X^{1+\frac{\alpha}{d-1-\alpha}}. \tag{2·4}$$

Les idées de la démonstration sont déjà présentes sous une forme voisine dans [17] puis dans [18], [50] et [46]. La première partie de la preuve consiste à évaluer la contribution des $\log^{(1)}(f(n))$ à $V_f(X)$.

Lemme 2.2. *On a l'égalité :*

$$\sum_{X<n\leqslant 2X} \log^{(1)}(f(n)) = X\log X + O(X).$$

On part de l'égalité

$$\begin{aligned}\sum_{X<n\leqslant 2X} \log^{(1)}(f(n)) &= \sum_{\substack{p\leqslant DX\\ k\geqslant 1}} \log p \sum_{\substack{X<n\leqslant 2X\\ p^k\mid f(n)}} 1\\ &= \sum_{p\leqslant DX} \log p \sum_{\substack{X<n\leqslant 2X\\ p\mid f(n)}} 1 + \sum_{p\leqslant DX,k\geqslant 2} \log p \sum_{\substack{X<n\leqslant 2X\\ p^k\mid f(n)}} 1.\end{aligned} \tag{2·5}$$

La contribution des $k \geqslant 2$ est négligeable :

$$\sum_{p\leqslant DX,k\geqslant 2} \log p \sum_{\substack{X<n\leqslant 2X\\ p^k\mid f(n)}} 1 = \sum_{\substack{k\geqslant 2\\ p\leqslant DX\\ p^k\leqslant k_f 2^d X^d}} (\log p) r_f(p^k)\Big(\frac{X}{p^k} + O(1)\Big),$$

avec $r_f(m) = |\{0 \leqslant u < m : f(u) \equiv 0 \,(\mathrm{mod}\, m)\}|$. Il existe une constante $C > 0$ absolue telle que $r_f(p^k) \leqslant C$ pour tous p, k (cf. [45]).

On a donc :

$$\begin{aligned}\sum_{\substack{k\geqslant 2\\ p\leqslant DX\\ p^k\leqslant k_f 2^d X^4}} \log p\Big(\frac{X}{p^k} + O(1)\Big) r_f(p^k) &\ll X \sum_{p\leqslant DX} \frac{\log p}{p^2} + \sum_{p\leqslant DX} \log p \left[\frac{\log X}{\log p}\right]\\ &\ll X.\end{aligned}$$

Pour la somme sur p restante de (2·5) on applique le Théorème de Nagell [44]

$$\sum_{p\leqslant DX} (\log p) r_f(p)\big(\frac{X}{p} + O(1)\big) = X\log X + O(X).$$

Cela termine la preuve du Lemme 2.2.

Fin de la preuve du Lemme 2.1.

D'après l'égalité (2·1) et le Lemme 2.2,

$$\sum_{X<n\leqslant 2X} \log^{(2)}(f(n)) = (d-1)X\log X + O(X).$$

On en déduit

$$(d-1)X\log X + O(X) = \sum_{n\in\mathcal{A}(f)} \log^{(2)}(f(n)) + \sum_{\substack{X<n\leqslant 2X\\ n\notin\mathcal{A}(f)}} \log^{(2)}(f(n)). \tag{2·6}$$

Si $n \leqslant 2X$, $f(n) \leqslant k_f 2^d X^d$. Dans ce cas $f(n)$ a au plus $d-1$ facteurs premiers supérieurs à DX car D vérifie (2·2). On a ainsi $\log^{(2)}(f(n)) \leqslant (d-1)\log(P_X)$, où on a noté P_X le membre de gauche de l'inégalité (2·4).

Si $n \in \mathcal{A}(f)$, alors $\prod_{\substack{p^k\| f(n)\\ p\leqslant DX}} p^k \geqslant X$,

$$\prod_{\substack{p^k\| f(n)\\ p>DX}} p^k \leqslant \frac{k_f 2^d X^d}{X} \leqslant k_f 2^d X^{d-1},$$

$f(n)$ a au plus $d-2$ facteurs premiers supérieurs à DX ; $\log^{(2)}(f(n)) \leqslant (d-2)\log(P_X)$.

On note $\mathcal{A}'(f) = \{X < n \leqslant 2X : n \notin \mathcal{A}(f)\}$; l'égalité (2·6) devient :

$$(d-1)X\log X + O(X) \leqslant (d-2)|\mathcal{A}(f)|\log(P_X) + (d-1)\log(P_X)|\mathcal{A}'(f)|.$$

Maintenant $|\mathcal{A}'(f)| = X - |\mathcal{A}(f)|$ on a ainsi

$$\alpha X\log(P_X) \leqslant |\mathcal{A}(f)|\log(P_X) \leqslant (d-1)X\log(P_X/X) + O(X).$$

Cela donne

$$P_X \gg_f X^{1+\frac{\alpha}{d-1-\alpha}},$$

et termine la preuve du Lemme 2.1.

Dans le cas où $f = \Phi_{12}$ on peut prendre $k_f = 1$. Nous choisissons $D = 4$ si bien que les fonctions $\log^{(1)}$ et $\log^{(2)}$ correspondantes sont alors :

$$\log^{(1)}(\Phi_{12}(n)) = \sum_{\substack{k\geqslant 1,\ p\leqslant 4X\\ p^k\|\Phi_{12}(n)}} k\log p \quad \text{et} \quad \log^{(2)}(\Phi_{12}(n)) = \sum_{\substack{k\geqslant 1,\ p>4X\\ p^k\|\Phi_{12}(n)}} k\log p. \tag{2·7}$$

Nous devrons minorer le cardinal de l'ensemble

$$\mathcal{A} := \mathcal{A}(\Phi_{12}) = \{n \in]X, 2X] : \log^{(1)}(\Phi_{12}(n)) \geqslant \log X\}. \tag{2·8}$$

Remarque. Nous avons choisi de reprendre les arguments d'Erdős et de Schinzel car l'exposant de X dans la minoration du Lemme 2.1 est légèrement supérieur à celui fourni par la méthode de Heath-Brown.

Par contre, il faut signaler que la méthode de Heath-Brown a l'avantage de montrer l'existence d'une proportion positive d'entiers n tels que $P^+(f(n)) > n^{1+c'}$ alors que la preuve du Lemme 2.1 ne permet pas de détecter une telle proportion positive.

En reprenant les arguments de Heath-Brown [24] pp. 558-559, on observe que si on est en mesure de trouver deux réels α et $\delta > 0$ tels que

$$|\{n \in]X, 2X] : \log^{(1)}(\Phi_{12}(n)) \geqslant (1+\delta)\log X\}| \geqslant \alpha X \tag{2·9}$$

pour X assez grand alors il existe une proportion positive d'entiers $n \in]X, 2X]$ tels que $P^+(\Phi_{12}(n)) > X^{1+\frac{\alpha\delta}{3}}$.

La méthode de notre article permet d'obtenir des minorations du type (2·9) pour des paramètres $\alpha > 0$ et $\delta > 0$ très petits. On peut ainsi montrer qu'il existe $c' > 0$ tel que $P^+(\Phi_{12}(n)) \geqslant n^{1+c'}$ pour une proportion positive d'entiers n.

L'objet du paragraphe suivant est de reformuler le Lemme 2.1 pour le polynôme Φ_{12} en remplaçant les facteurs premiers par les idéaux premiers d'un anneau des entiers d'un corps de nombres.

3. Passage aux idéaux

Commençons par rappeler quelques propriétés classiques sur le polynôme Φ_{12}.

Ses racines sont $\pm e^{i\pi/6}, \pm e^{-i\pi/6}$. Ce sont les racines primitives 12 èmes de 1.

Le corps $K := \mathbb{Q}[\zeta_{12}] = \mathbb{Q}(\zeta_{12})$ est une extension galoisienne de groupe de Galois isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ avec comme éléments $\sigma_1 = Id$, $\sigma_2 : z \to \bar{z}$, $\sigma_3 : u + \sqrt{3}w \mapsto u - \sqrt{3}w$ où $u, w \in \mathbb{Q}(i)$ et $\sigma_4 = \sigma_2 \circ \sigma_3$.

On a aussi $\Phi_{12}(n) = \prod_{i=1}^{4}(n - \sigma_i(\zeta_{12})) = N(n - \zeta_{12})$, où $N(\alpha)$ est la norme de α, $N(\alpha) = \prod_{i=1}^{4} \sigma_i(\alpha)$.

D'après un théorème général sur les corps cyclotomiques (cf. [52] par exemple), l'anneau des entiers de $\mathbb{Q}(\zeta_{12})$ est $\mathbb{Z}[\zeta_{12}]$.

Soit Δ le discriminant de ce corps de nombres. On a

$$\begin{aligned}\Delta &= N(\Phi'_{12}(\zeta_{12})) = N(4\zeta_{12}^3 - 2\zeta_{12}) \\ &= N(2\sqrt{3}e^{2i\pi/3}) = 16 \times 9 = 144.\end{aligned}$$

On considère la fonction définie sur les idéaux I de $\mathbb{Z}[\zeta_{12}]$ par

$$\varrho(I) = |\{n < N(I) : n \equiv \zeta_{12} \,(\mathrm{mod}\, I)\}|. \tag{3·1}$$

Pour $\alpha \in \mathbb{Z}[\zeta_{12}]$, on écrira $\varrho(\alpha)$ à la place de $\varrho((\alpha))$. On cherche à montrer l'équivalent du Lemme 1 d'Heath-Brown [24].

Lemme 3.1. *Soit I un idéal de $\mathbb{Z}[\zeta_{12}]$. Si l'équation $n \equiv \zeta_{12} \,(\mathrm{mod}\, I)$ admet une solution avec n entier alors I est un produit d'idéaux premiers $\mathcal{P}$ tels que $N(\mathcal{P}) = p$. De plus I ne peut pas être divisible par deux différents idéaux premiers de même norme et ni par les idéaux au dessus de 2 et 3. Réciproquement si I vérifie ces différentes conditions, alors cette congruence admet des solutions et $\varrho(I) = 1$. De plus, si I est un idéal tel que $\varrho(I) = 1$ alors pour tout $m \in \mathbb{Z}$, $I|m \Leftrightarrow N(I)|m$.*

Remarque. Nous avons choisi de présenter ce lemme seulement pour le polynôme Φ_{12}. Cependant les arguments de la preuve ci-dessous s'adaptent vraisemblablement au cas des polynômes unitaires irréductibles de degré 4 tels que si ϑ est une racine de ce polynôme alors $\mathbb{Q}[\vartheta]$ soit une extension galoisienne de $\mathbb{Q}$ dont l'anneau des entiers soit $\mathbb{Z}[\vartheta]$.

Preuve. Soit $\mathcal{P}$ un idéal premier contenant $n - \zeta_{12}$. On a alors $n \equiv \zeta_{12} \,(\mathrm{mod}\, \mathcal{P})$. Tout élément de $\mathbb{Z}[\zeta_{12}]$ est congru à un entier mod $\mathcal{P}$. Or $\mathbb{Z}[\zeta_{12}]/\mathcal{P}$ est un espace vectoriel sur $\mathbb{Z}/p\mathbb{Z}$ avec $1, \zeta_{12}, \zeta_{12}^2, \zeta_{12}^3$ comme partie génératrice. L'élément 1 forme donc une base de $\mathbb{Z}[\zeta_{12}]/\mathcal{P}$. On en déduit que $N(\mathcal{P}) = |\mathbb{Z}[\zeta_{12}]/\mathcal{P}| = p$.

De plus $\mathcal{P}$ ne peut pas être un idéal au dessus de 2 ou de 3 car $\forall n \in \mathbb{Z}$, $N(n - \zeta_{12}) = \Phi_{12}(n)$ est premier avec 6.

Soit p un nombre premier ne divisant pas Δ c'est-à-dire supérieur ou égal à 5. Comme $\mathbb{Q}[\zeta_{12}]/\mathbb{Q}$ est galoisienne, on a trois décompositions possibles :

$$p\mathbb{Z}[\zeta_{12}] = \mathcal{P}_1 \cdots \mathcal{P}_4, \quad N(\mathcal{P}_i) = p \tag{3·2}$$

$$p\mathbb{Z}[\zeta_{12}] = \mathcal{P}_1\mathcal{P}_2 \quad N(\mathcal{P}_i) = p^2$$

$$p\mathbb{Z}[\zeta_{12}] = \mathcal{P}, \quad N(\mathcal{P}) = p^4.$$

Le premier cas correspond à la situation où Φ_{12} se factorise dans $\mathbb{Z}/p\mathbb{Z}[x]$ en 4 facteurs de degré 1, le second au cas de deux facteurs de degré 2 et le troisième au cas où Φ_{12} est irréductible sur $\mathbb{Z}/p\mathbb{Z}$.

Maintenant soient $\mathcal{P}_1$ et $\mathcal{P}_2$ deux idéaux premiers distincts tels que $\mathcal{P}_i|I$ et $N(\mathcal{P}_1) = N(\mathcal{P}_2) = p$. Alors on est dans la configuration $p\mathbb{Z}[\zeta_{12}] = \mathcal{P}_1 \cdots \mathcal{P}_4$ et $\mathcal{P}_i = (p, n_i - \zeta_{12})$ où

n_i décrit les différentes racines modulo p de $\Phi_{12}(n) = 0$. Dans ce cas on a $n_i \equiv n \,(\mathrm{mod}\, \mathcal{P}_i)$ pour $i = 1, 2$ avec $n_1 \not\equiv n_2 \,(\mathrm{mod}\, p)$ puisque $\mathcal{P}_1 \neq \mathcal{P}_2$. Ainsi on peut supposer que $n \not\equiv n_1 \,(\mathrm{mod}\, p)$ (quitte à remplacer n_1 par n_2.) Mais on ne peut avoir à la fois $n_1 \not\equiv n \,(\mathrm{mod}\, p)$ et $n_1 \equiv n \,(\mathrm{mod}\, \mathcal{P}_1)$, cela impliquerait que $N(\mathcal{P}_1) < p$.

Soit I un idéal de la forme $I = \prod_{k=1}^{\ell} \mathcal{P}_k^{\alpha_k}$, où les $\mathcal{P}_k$ sont des idéaux premiers tels que $N(\mathcal{P}_k) = p_k$, les nombres premiers p_k étant $\geqslant 5$, et $p_k \neq p_{k'}$ si $k \neq k'$. Montrons qu'il existe alors $n \in \mathbb{Z}$, $0 \leqslant n < N(I)$ tel que $n - \zeta_{12} \in I$, autrement dit que $\varrho(I) \geqslant 1$. On commence par traiter le cas $I = \mathcal{P}^k$. Alors $N(\mathcal{P})$ est un nombre premier p vérifiant la décomposition (3·2). De plus il existe $a \in \{0, \ldots, p-1\}$ tel que $\mathcal{P} = (p, a - \zeta_{12})$. On a vu que cet entier a est une racine de Φ_{12} modulo p. Par un argument de descente du type lemme de Hensel, on vérifie par récurrence que pour chaque entier $k \geqslant 1$, il existe un unique $a_k \in \{0, \ldots, p^k - 1\}$ tel que $a_k \equiv a \,(\mathrm{mod}\, p)$ et $\Phi_{12}(a_k) \equiv 0 \,(\mathrm{mod}\, p^k)$ (rappelons que p ne divise pas Δ.) Cela implique que $N(a_k - \zeta_{12}) = \Phi_{12}(a_k)$ est divisible par p^k et $\mathcal{P} | (a_k - \zeta_{12})$. Comme $\mathcal{P}$ est le seul idéal premier de norme p qui divise $(a_k - \zeta_{12})$ on peut en conclure que $\mathcal{P}^k$ divise $(a_k - \zeta_{12})$, $\varrho(\mathcal{P}^k) \geqslant 1$.

Dans le cas général $I = \mathcal{P}_1^{\alpha_1} \cdots \mathcal{P}_\ell^{\alpha_\ell}$ on construit de cette manière pour chaque $1 \leqslant k \leqslant \ell$ un entier $a_k \in \{0, \ldots, N(\mathcal{P}_k)^{\alpha_k} - 1\}$ tel que $(a_k - \zeta_{12}) \in \mathcal{P}_k^{\alpha_k}$. On en déduit à l'aide du théorème chinois des restes l'existence d'un entier $n \in \{0, \ldots, N(I) - 1\}$ tel que $n \equiv a_k \,(\mathrm{mod}\, p^{\alpha_k})$ pour tout $1 \leqslant k \leqslant \ell$ et ainsi tel que $n - \zeta_{12} \in I$.

Vérifions maintenant que $\varrho(I) \leqslant 1$. Comme précédemment, si a et b sont deux entiers distincts strictement inférieurs à p^k tels que $a - \zeta_{12} \equiv 0 \,(\mathrm{mod}\, \mathcal{P}^k) \equiv b - \zeta_{12} \,(\mathrm{mod}\, \mathcal{P}^k)$, alors $|\mathbb{Z}[\zeta_{12}]/\mathcal{P}^k| < p^k$, ce qui contredit le fait que $N(\mathcal{P}^k) = N(\mathcal{P})^k = p^k$.

Dans le cas général, s'il existe deux entiers a et b distincts mod $N(I)$ tels que $a - \zeta_{12} \equiv 0 \,(\mathrm{mod}\, I) \equiv b - \zeta_{12} \,(\mathrm{mod}\, I)$, alors cette congruence est réalisée mod $\mathcal{P}^k$ pour tout $\mathcal{P}^k \| I$. Si $a \not\equiv b \,(\mathrm{mod}\, N(I))$, alors il existe $\mathcal{P}^k | I$ tel que $a \not\equiv b \,(\mathrm{mod}\, N(\mathcal{P}^k))$, on est ramené au cas où $I = \mathcal{P}^k$.

Il reste à montrer l'équivalence annoncée à la fin du lemme : $I | m \Leftrightarrow N(I) | m$.

Soient I un idéal tel que $\varrho(I) = 1$ et $m \in \mathbb{Z}$ un multiple de I. Comme les idéaux premiers intervenant dans la décomposition de I sont de norme différente, il suffit de traiter le cas où $I = \mathcal{P}^k$ avec $N(\mathcal{P}) = p$. On procède par récurrence sur k. Pour $k = 1$, $\mathcal{P} | m \Rightarrow N(\mathcal{P}) | N(m)$ avec $N(m) = m^4$. Comme $N(\mathcal{P}) = p$ est un nombre premier, on en déduit que $N(\mathcal{P})$ divise m.

On suppose que la propriété est vérifiée jusqu'au rang $k - 1$ avec $k \geqslant 2$. On écrit $I = \mathcal{P}^k = \mathcal{P}J$. D'après (3·2), p se décompose sous la forme $p = \mathcal{P}\mathcal{P}_2\mathcal{P}_3\mathcal{P}_4$. On en déduit que J divise (m/p) et ensuite que $N(J)$ divise (m/p) avec l'hypothèse de récurrence.

La réciproque est claire puisque $I | (N(I))$. Cela termine la preuve du Lemme 3.1.

Grâce à ce lemme on observe qu'il existe une correspondance bijective entre les facteurs premiers de $\Phi_{12}(n)$ et les idéaux premiers divisant $(n - \zeta_{12})$. On a donc

$$\sum_{\substack{5 \leqslant p \leqslant 4X \\ p | \Phi_{12}(n)}} \log p = \sum_{\substack{5 \leqslant N(\mathcal{P}) \leqslant 4X \\ \mathcal{P} | (n - \zeta_{12})}} \log(N(\mathcal{P})).$$

Suivant la stratégie mise en place par Heath-Brown, nous construirons un sous-ensemble $\mathcal{A}_1 \subset \mathcal{A}$ dont on pourra minorer la densité inférieure. Cet ensemble sera du type

$$\mathcal{A}_1 = \{X < n \leqslant 2X : \exists J \in \mathcal{J} \text{ tel que } J | (n - \zeta_{12})\}, \tag{3·3}$$

où $\mathcal{J}$ est un ensemble d'idéaux de $\mathbb{Z}[\zeta_{12}]$ que nous choisirons au paragraphe 10.

Pour $n \in]X, 2X]$, notons $r_{\mathcal{J}}(n)$ le nombre d'idéaux $J \in \mathcal{J}$ tels que $J | n - \zeta_{12}$. On a alors la minoration

$$|\mathcal{A}_1| \geqslant \Big(\max_{X < n \leqslant 2X} r_{\mathcal{J}}(n)\Big)^{-1} \sum_{J \in \mathcal{J}} |A_J|, \tag{3·4}$$

où

$$A_J = \{n \in]X, 2X] : J | n - \zeta_{12}\}. \tag{3·5}$$

On espère l'approximation

$$|A_J| = X\frac{\varrho(J)}{N(J)} + R_J, \tag{3·6}$$

où R_J est un terme d'erreur qui devra être petit en moyenne sur J.

4. Sur les congruences de $n - \zeta_{12}$

Soit $\alpha = a + b\zeta_{12} + c\zeta_{12}^2 + d\zeta_{12}^3 \in \mathbb{Z}[\zeta_{12}]$. L'objet de ce paragraphe est d'obtenir une expression des solutions de la congruence $n - \zeta_{12} \equiv 0 \,(\mathrm{mod}\,(\alpha))$ en fonction de a, b, c, d. Cette paramétrisation utilise les cofacteurs de m_α la matrice de la multiplication par α dans la base $(1, \zeta_{12}, \zeta_{12}^2, \zeta_{12}^3)$. Il s'agit de la matrice

$$m_\alpha = \begin{pmatrix} a & -d & -c & -b-d \\ b & a & -d & -c \\ c & b+d & a+c & b \\ d & c & b+d & a+c \end{pmatrix}.$$

Le déterminant de cette matrice est $N(\alpha)$:

$$\begin{aligned} N(\alpha) = a^4 + 2a^3c + a^2(2bd + 3c^2 - b^2 + 2d^2) + a(-4bcd - 4b^2c + 2cd^2 + 2c^3) \\ - 4bc^2d + 2db^3 + 3b^2d^2 - b^2c^2 + 2bd^3 - c^2d^2 + b^4 + c^4 + d^4. \end{aligned}$$

Pour $1 \leqslant i, j \leqslant 4$ on note B_{ij} le cofacteur de m_α associé au terme ij de sorte que la matrice inverse de m_α soit

$$m_\alpha^{-1} = \frac{1}{N(\alpha)} \begin{pmatrix} B_{11} & B_{21} & B_{31} & B_{41} \\ B_{12} & B_{22} & B_{32} & B_{42} \\ B_{13} & B_{23} & B_{33} & B_{43} \\ B_{14} & B_{24} & B_{34} & B_{44} \end{pmatrix}. \tag{4·1}$$

Le but de ce paragraphe est de montrer le lemme suivant :

Lemme 4.1. *Soient a, b, c, d des entiers tels que $(B_{14}, N(\alpha)) = 1$ où on a repris la notation $\alpha = a + b\zeta_{12} + c\zeta_{12}^2 + d\zeta_{12}^3$. Posons $J = (\alpha)$. Il existe un entier k_J, $0 \leqslant k_J < N(J)$ tel que l'équivalence suivante soit vérifiée :*

$$n - \zeta_{12} \equiv 0 \,(\mathrm{mod}\, J) \Leftrightarrow n \equiv k_J \,(\mathrm{mod}\, N(J)).$$

De plus, k_J vérifie :

$$k_J \equiv B_{13}\overline{B_{14}} \,(\mathrm{mod}\, N(J)).$$

Preuve. Comme $m_\alpha \circ m_{\alpha^{-1}} = Id$, $m_\alpha^{-1} = m_{\alpha^{-1}}$, on en déduit que

$$\alpha^{-1} = \frac{1}{N(\alpha)}(B_{11} + B_{12}\zeta_{12} + B_{13}\zeta_{12}^2 + B_{14}\zeta_{12}^3),$$

et m_α^{-1} a comme forme :

$$m_\alpha^{-1} = \frac{1}{N(\alpha)} \begin{pmatrix} B_{11} & -B_{14} & -B_{13} & -B_{12} - B_{14} \\ B_{12} & B_{11} & -B_{14} & -B_{13} \\ B_{13} & B_{12} + B_{14} & B_{11} + B_{13} & B_{12} \\ B_{14} & B_{13} & B_{12} + B_{14} & B_{11} + B_{13} \end{pmatrix}. \tag{4·2}$$

Comme $J = (\alpha)$, il est clair que $\zeta_{12}^{\ell}\alpha \equiv 0 \,(\mathrm{mod}\, J)$ pour $\ell = 0, 1, 2, 3$. On obtient ainsi un système linéaire d'équations dont les inconnues sont ζ_{12}, ζ_{12}^2, ζ_{12}^3. On a la congruence matricielle modulo J :

$$\begin{pmatrix} b & c & d \\ a & d+b & c \\ -d & a+c & b+d \\ -c & b & a+c \end{pmatrix} \begin{pmatrix} \zeta_{12} \\ \zeta_{12}^2 \\ \zeta_{12}^3 \end{pmatrix} = \begin{pmatrix} -a \\ d \\ c \\ b+d \end{pmatrix} \mathrm{mod}\, J. \tag{4·3}$$

Les formules de Cramer appliquées aux 3 premières lignes donnent alors :

$$\zeta_{12}\,\mathrm{dét}\begin{pmatrix} b & c & d \\ a & b+d & c \\ -d & a+c & b+d \end{pmatrix} = \mathrm{dét}\begin{pmatrix} -a & c & d \\ d & b+d & c \\ c & a+c & b+d \end{pmatrix} \mathrm{mod}\, J. \tag{4·4}$$

La matrice de gauche de (4·4) est $-B_{14}$. Celle du membre de droite est $-B_{24} = -B_{13}$.

La congruence (4·4) devient

$$B_{14}\zeta_{12} \equiv B_{13} \,(\mathrm{mod}\, J). \tag{4·5}$$

Si $(B_{14}, N(\alpha)) = 1$, et si $m \in \mathbb{Z}$, alors on a la suite d'équivalences :

$$\begin{aligned} m - \zeta_{12} \in J &\Leftrightarrow B_{14}(m - \zeta_{12}) \in J \\ &\Leftrightarrow B_{14}m - B_{13} \equiv 0 \,(\mathrm{mod}\, J) \\ &\Leftrightarrow B_{14}m - B_{13} \equiv 0 \,(\mathrm{mod}\, N(J)), \end{aligned}$$

cette dernière équivalence découlant du Lemme 3.1. Cela prouve l'existence de l'entier k_J et termine la preuve du Lemme 4.1.

Les calculs donnent

$$\begin{aligned} B_{13} &= -a^2c + a(b^2 + 2db - c^2) + c(-c^2 + d^2 + 2db) \\ B_{14} &= -a^2d + 2abc - b^3 - 2b^2d - 2bd^2 + bc^2 + c^2d - d^3. \end{aligned} \tag{4·6}$$

5. Élimination d'une variable

Le Lemme 4.1 fournit une expression explicite de k_J modulo $N(\alpha)$. Afin d'isoler une variable, on souhaite approcher modulo 1 la fraction $\frac{k_J}{N(\alpha)}$ par une fraction dont le dénominateur est un polynôme en seulement 3 variables. Notons R le Résultant de B_{14} et $N(\alpha)$ par rapport à a. Alors $R = q^2$ avec

$$q = (b^2 + c^2)(b^2 + db + d^2)(b^2 - 3c^2 + 4db + 4d^2). \tag{5·1}$$

Ce résultant est de degré trop élevé. On va essayer de trouver une méthode pour éliminer a avec un polynôme en b, c, d de degré moins élevé.

Dans (4·3), si on applique les formules de Cramer au sous-système obtenu en rayant la 3 ème ligne, on trouve :

$$B_{13}\zeta_{12} \equiv -B_{41} \,(\mathrm{mod}\, J).$$

En utilisant les deux expressions de m_α^{-1}, on obtient :

$$B_{13}\zeta_{12} \equiv B_{12} + B_{14} \,(\mathrm{mod}\, J). \tag{5·2}$$

De même en considérant le sous-système donné par les 3 dernières lignes on trouve :

$$\begin{aligned} B_{11}\zeta_{12} &\equiv B_{21} \,(\mathrm{mod}\, J) \\ &\equiv -B_{14} \,(\mathrm{mod}\, J). \end{aligned}$$

En mettant de coté les problèmes de pgcd on obtient 3 congruences pour ζ_{12}.

En profitant de (4·5), (5·2), de l'égalité $B_{24} = B_{13}$ et du Lemme 3.1, on remarque la congruence :

$$B_{14}(B_{12} + B_{14}) - B_{13}^2 \equiv 0 \,(\mathrm{mod}\, N(\alpha)).$$

Effectivement on obtient avec Maple (par exemple) la formule :

$$B_{14}(B_{12} + B_{14}) - B_{13}^2 = (d^2 - c^2 + db)N(\alpha). \tag{5·3}$$

Notons Résultant$(B_{13}, B_{14}\,; a)$ le résultant de B_{13} et B_{14} par rapport à a. On a également *via* Maple :

$$\text{Résultant}(B_{13}, B_{14}\,; a) = (d^2-c^2+db)(b^2+c^2)(d^2+b^2+db)(-3c^2+b^2+4db+4d^2). \tag{5·4}$$

Cela nous amène à définir les formes suivantes :

$$q_1(b,c,d) = q_1(b,c) = b^2 + c^2,\ q_2(b,c,d) = q_2(b,d) = b^2 + db + d^2, \tag{5·5}$$

$$q_3(b,c,d) = (b+2d)^2 - 3c^2,\ q_4(b,c,d) := d^2 - c^2 + db. \tag{5·6}$$

Les facteurs $d^2 - c^2 + db$ apparaissant dans (5·3) et (5·4) se neutraliseront dans la suite. La technique des bases de Gröbner (cf. [21] par exemple) permet après quelques minutes de calculs avec Maple d'obtenir la formule :

$$\begin{aligned} UB_{13} + VB_{14} &= -(d^2 - c^2 + db)(b^2 + c^2)(d^2 + b^2 + db)(-3c^2 + b^2 + 4db + 4d^2) \\ &= -q_4(b,c,d)q(b,c,d), \end{aligned} \tag{5·7}$$

avec

$$U = -2d^4c+ad^2b^2-ad^2c^2-6d^2cb^2+2d^2c^3+4c^3b^2+3c^3db-3dcb^3-4cd^3b-2adc^2b+2ad^3b, \tag{5·8}$$

$$V = 4d^3b^2+2d^3c^2+adc^3-4dc^2b^2-dc^4+4d^2b^3-2ad^2cb-c^2b^3+db^4+2abc^3-adcb^2+c^4b. \tag{5·9}$$

6. Transformations en sommes d'exponentielles

Comme $\mathbb{Z}[\zeta_{12}]$ est principal, les éléments de $\mathcal{J}$ seront des idéaux principaux donc du type $J = (\alpha)$ avec $\alpha = a + b\zeta_{12} + c\zeta_{12}^2 + d\zeta_{12}^3$. Notons $M_{\mathcal{J}} = \max_{X<n\leqslant 2X} r_{\mathcal{J}}(n)$. D'après (3·4) et le Lemme 4.1, on a l'inégalité :

$$|\mathcal{A}_1| \geqslant M_{\mathcal{J}}^{-1} \sum_{J\in\mathcal{J}} \sum_{\substack{X<n\leqslant 2X \\ n\equiv k_J \,(\mathrm{mod}\, N(J))}} 1.$$

En reprenant les transformations d'Heath-Brown ([24] pp. 566-567) pour établir la formule (2.9) du lemme 4 p. 562 de [24], on obtient le lemme suivant

Lemme 6.1. *Soit $\mathcal{E} \subset \mathbb{Z}[\zeta_{12}]$ tel que $(B_{14}, N(\alpha)) = 1\ \forall \alpha \in \mathcal{E}$. Soit $\mathcal{J}(\mathcal{E}) = \{(\alpha) : \alpha \in \mathcal{E}\}$, avec d'éventuelles répétitions, un élément J de $\mathcal{J}(\mathcal{E})$ apparaissant autant de fois qu'il existe de $\alpha \in \mathcal{E}$ tel que $J = (\alpha)$.*

On a alors la majoration :

$$\sum_{J \in \mathcal{J}(\mathcal{E})} R_J = \sum_{\alpha \in \mathcal{E}} R_{(\alpha)} \ll (\log H) H^{-1} |\mathcal{E}| + (\log H) \sum_{h=1}^{H^2} \min(h^{-1}, Hh^{-2}) |S(h)|, \tag{6·1}$$

avec pour $X' = X$ ou $2X$

$$S(h) = \sum_{J \in \mathcal{J}(\mathcal{E})} \mathrm{e}\Big(\frac{h(X' - k_J)}{N(\alpha)}\Big),$$

les R_J étant les termes "restes" définis par (3·6).

Preuve. On applique le Lemme 4.1 à chaque élément de $\mathcal{E}$, puis on fait apparaître des sommes trigonométriques exactement de la même manière que [24] pp. 566-567.

Nous utilisons maintenant le paragraphe précédent pour transformer les sommes $S(h)$ en des sommes d'exponentielles d'argument une fraction rationnelle avec un dénominateur en trois variables (ici b, c, d).

Lemme 6.2. *On suppose que $(q, B_{14}) = 1$. Alors $(N(\alpha), B_{14}) = 1$ et on a l'égalité pour $h \in \mathbb{Z}$:*

$$\mathrm{e}\Big(\frac{-hk_J}{N(\alpha)}\Big) = \mathrm{e}\Big(\frac{-hU\overline{B_{14}}}{q} + hR(a,b,c,d)\Big),$$

$$\text{avec } R(a,b,c,d) = \frac{U}{qB_{14}} - \frac{B_{13}}{N(\alpha)B_{14}}.$$

Preuve. On a vu au paragraphe précédent que $q^2(b,c,d)$ est le résultant par rapport à a des polynômes B_{14} et $N(\alpha)$. On en déduit que si $(q, B_{14}) = 1$, alors $(N(\alpha), B_{14}) = 1$.

D'après le Lemme 4.1, si $J = (\alpha)$ avec $\alpha = a + b\zeta_{12} + c\zeta_{12}^2 + d\zeta_{12}^3$, alors

$$k_J \equiv B_{13}\overline{B_{14}} \,(\mathrm{mod}\, N(\alpha)).$$

On a alors

$$\mathrm{e}\Big(\frac{-hk_J}{N(\alpha)}\Big) = \mathrm{e}\Big(\frac{-hB_{13}\overline{B_{14}}}{N(\alpha)}\Big) = \mathrm{e}\Big(\frac{hB_{13}\overline{N(\alpha)}}{B_{14}} - \frac{hB_{13}}{N(\alpha)B_{14}}\Big), \tag{6·2}$$

où on vient d'utiliser la réécriture de Bézout suivante (pour $(u,v) = 1$) :

$$\frac{\overline{u}}{v} + \frac{\overline{v}}{u} \equiv \frac{1}{uv} \,(\mathrm{mod}\, 1). \tag{6·3}$$

En utilisant à plusieurs reprises (6·3) et en supposant que $(qq_4, B_{13}B_{14}) = 1$, on peut déduire des formules (5·3) et (6·2) l'égalité annoncée dans le Lemme 6.2. Cependant la condition de coprimalité entre q_4 et $B_{13}B_{14}$ ne semble pas absolument nécessaire.

Effectivement si on multiplie (5·3) par U, (5·7) par B_{13} et on somme les 2 formules ainsi obtenues, on arrive à l'égalité :

$$q_4(UN(\alpha) - B_{13}q) = B_{14}(U(B_{12} + B_{14}) + VB_{13}). \tag{6·4}$$

On espère alors que q_4 divise $U(B_{12}+B_{14})+VB_{13}$. C'est en effet le cas. On constate à l'aide par exemple du logiciel SAGE la formule :

$$UN(\alpha)-B_{13}q=-B_{14}Z, \tag{6·5}$$

avec

$$\begin{aligned}Z=&-ab^5-a^2b^3c-2a^3bc^2+2ab^3c^2-3a^2bc^3+5b^3c^3-3abc^4-bc^5+a^3b^2d-5ab^4d\\&-5b^4cd-a^3c^2d-3ab^2c^2d+8b^2c^3d+c^5d+2a^3bd^2-6ab^3d^2-13b^3cd^2-6abc^2d^2\\&+bc^3d^2+ab^2d^3-2a^2cd^3-12b^2cd^3-5ac^2d^3-2c^3d^3+2abd^4-4bcd^4-2cd^5.\end{aligned}$$

La forme précise de Z est juste donnée à titre indicatif, ici on a seulement besoin de savoir que $B_{13}\overline{N(\alpha)}\equiv U\overline{q}\,(\mathrm{mod}\,B_{14})$. On insère alors cette congruence dans (6·2) puis on applique une nouvelle fois (6·3). On obtient la formule annoncée dans le Lemme 6.2.

Nous choisirons a,b,c,d de sorte que les deux fractions $\frac{hU}{qB_{14}}$, $\frac{hB_{13}}{N(\alpha)B_{14}}$ soient d'un ordre de grandeur négligeable.

Comme le dénominateur de la fraction $\frac{hU\overline{B_{14}}}{q}$ ne dépend plus de a, on pourra majorer non trivialement la somme

$$\sum_{A<a\leqslant A+B}\mathrm{e}\Big(\frac{-hU\overline{B_{14}}}{q}\Big),$$

grâce au Théorème 2 de l'article de Heath-Brown [24].

Cependant pour appliquer ce théorème il faut que q soit bien friable et sans facteur carré.

7. Sur les solutions dans $\mathbb{Z}/m\mathbb{Z}$ d'une équation du type $f=0$

7·1. Cas des formes binaires irréductibles

Soit $f\in\mathbb{Z}[x,y]$ une forme binaire irréductible à coefficients entiers. On note

$$\varrho_f(m)=|\{0\leqslant u,v<m : f(u,v)\equiv 0\,(\mathrm{mod}\,m)\}| \tag{7·1}$$

et

$$\varrho_f^*(m)=|\{0\leqslant u,v<m : f(u,v)\equiv 0\,(\mathrm{mod}\,m),\ (u,v,m)=1\}|. \tag{7·2}$$

Nous utiliserons également la fonction

$$\tilde{\varrho}_f(m)=|\{0\leqslant u<m : f(1,u)\equiv 0\,(\mathrm{mod}\,m),\ (u,m)=1\}|. \tag{7·3}$$

Lorsque p ne divise pas le coefficient dominant de $f(1,v)$, on a :

$$\tilde{\varrho}_f(p^k)=\frac{\varrho_f^*(p^k)}{\varphi(p^k)}.$$

Dans ce paragraphe on rappelle des résultats classiques sur les valeurs de ces fonctions puis on établit des estimations en moyenne relatives à ces fonctions qui nous serviront dans la suite.

Les résultats du lemme suivant se trouvent respectivement dans [22] formula (2.3.1), [9] formule (2.6) et les formules (3.3), (3.6) de [12].

Lemme 7.1. *Soit $f \in \mathbb{Z}[x,y]$ une forme binaire primitive et irréductible de degré $d \geqslant 2$.*
(i) On a uniformément pour $Q \geqslant 2$:

$$\sum_{p<Q} \frac{\varrho_f(p)\log p}{p^2} = \log Q + O(1).$$

(ii) Si p ne divise pas le discriminant de f, alors

$$\varrho_f(p^\nu) \leqslant \begin{cases} 2dp^\nu \frac{p^{(d-2)\lceil \nu/d\rceil}-1}{p^{d-2}-1} + p^{2(\nu-\lceil \nu/d\rceil)} & \text{si } d \geqslant 3 \\ 4p^\nu \lceil \nu/2\rceil (1-1/p) + p^{(\nu-\lceil \nu/2\rceil)} & \text{si } d = 2 \end{cases} \tag{7·4}$$

(iii) On a uniformément pour $Q \geqslant 1$:

$$\sum_{q\leqslant Q} \frac{\varrho_f^*(q)}{\varphi(q)} \ll Q \text{ et } \sum_{q\leqslant Q} \frac{\varrho_f(q)}{q^2} = C_f \log Q + O(1),$$

où $C_f = Res_{s=2} \sum_{q=1}^\infty \frac{\varrho_f(q)}{q^s}$ est un réel strictement positif.

On utilisera aussi la majoration valable pour tout p, issue de la formule (2.3) du lemme 2.2 de [9]

$$\varrho_f(p^\nu) \leqslant (2d+1)p^{\min(2\nu-1, \lfloor (2-1/d)\nu\rfloor)}. \tag{7·5}$$

Lemme 7.2. *Soient $f \in \mathbb{Z}[x,y]$ une forme binaire primitive et irréductible de degré $d \geqslant 2$ et $i \in \mathbb{N}$. On a uniformément pour $X \geqslant 2$:*

$$\sum_{n\leqslant X} \frac{\tau^i(n)\varrho_f(n)}{n} \ll_{f,i} X(\log X)^{2^i-1}.$$

On applique le Théorème III 3.5 de [51] à la fonction multiplicative $h(n) = \tau^i(n)\varrho_f(n)/n$. Les conditions (i) et (ii)* de ce théorème se vérifient facilement à l'aide du Lemme 7.1. On a ainsi en profitant du Lemme 7.1 (ii) :

$$\sum_{n\leqslant X} \frac{\tau^i(n)\varrho_f(n)}{n} \ll \frac{X}{\log X} \sum_{n\leqslant X} \frac{h(n)}{n} \ll \frac{X}{\log X}\Big(\prod_{p\leqslant X} \sum_{\nu\geqslant 0} \frac{(\nu+1)^i \varrho_f(p^\nu)}{p^{2\nu}}\Big).$$

Pour évaluer les sommes sur ν dans les produits eulériens, on écrit ν sous la forme $\nu = u + \lambda d$ avec $1 \leqslant u \leqslant d$ pour contrôler les exposants en $\lceil \nu/d\rceil$ puis on applique (7·4) :

$$\sum_{n\leqslant X} \frac{\tau^i(n)\varrho_f(n)}{n} \ll \frac{X}{\log X} \prod_{p\leqslant X} \Big(1 + \frac{2^i\varrho_f(p)}{p^2} + O\Big(\frac{1}{p^2}\Big)\Big) \ll X(\log X)^{2^i-1}.$$

Le lemme suivant nous servira dans le paragraphe sur les niveaux de distribution des couples $(f_1(b,c), f_2(b,d))$.

---

* Il s'agit de montrer l'existence de deux réels positifs A, B tels que : (i) pour tous $y \geqslant 2$, $\sum_{p\leqslant y} h(p)\log p \leqslant Ay$; (ii) $\sum_p \sum_{\nu\geqslant 2} \frac{h(p^\nu)\log p^\nu}{p^\nu} \leqslant B$.

Lemme 7.3. *Soit $f \in \mathbb{Z}[x,y]$ une forme binaire primitive et irréductible de degré $d \geqslant 2$. Soient $\alpha \in]0,1]$ et $\beta \in]0,1[$.*

(i) On a alors uniformément pour tous B, C, M_1, M_2 tels que $B^\alpha \leqslant M_1 \leqslant B$, $C^\alpha \leqslant M_2 \leqslant C$:

$$\sum_{\substack{B<b\leqslant B+M_1\\ C<c\leqslant C+M_2}} \tau^2(f(b,c)) \ll M_1M_2(\log(B+C))^3.$$

(ii) Sous les hypothèses de (i) et pour ξ sans facteur carré tel que $\xi^\beta \leqslant \min(M_1,M_2)$ on a l'inégalité :

$$\sum_{\substack{B\leqslant b\leqslant B+M_1\\ C\leqslant c\leqslant C+M_2}} \tau(f(\xi b,c)) \ll M_1M_2\log(B+C)^2 H_{1,d}(\xi),$$

$$\text{avec } H_{1,d}(\xi) = \prod_{\substack{p\mid\xi\\ p>d}} \Big(1-\frac{1}{p}\Big)\Big(1-\frac{\varrho_f(p)}{p^2}\Big)^{-1}\Big(1+\frac{d(d+3)}{6p}\Big).$$

(iii) Sous les hypothèses de (ii), on a :

$$\sum_{\substack{B\leqslant b\leqslant B+M_1\\ C\leqslant c\leqslant C+M_2}} \tau^2(f(\xi b,c)) \ll M_1M_2\log(B+C)^3 H_{2,d}(\xi),$$

$$\text{avec } H_{2,d}(\xi) = \prod_{\substack{p\mid\xi\\ p>d}} \Big(1-\frac{1}{p}\Big)\Big(1-\frac{\varrho_f(p)}{p^2}\Big)^{-1}\Big(1+\frac{d(2d^2+9d+13)}{6p}\Big).$$

Les constantes implicites dépendent au plus de f, α, β.

Preuve. (i) On applique le Théorème 1.1 de l'article [9] de La Bretèche et Tenenbaum sur les valeurs moyennes de fonctions arithmétiques de formes binaires (on peut consulter également les articles [5] et [10]) :

$$\sum_{\substack{B\leqslant b\leqslant B+M_1\\ C\leqslant c\leqslant C+M_2}} \tau^2(f(b,c)) \ll M_1M_2E_f,$$

avec

$$E_f = \prod_{d<p\leqslant B+C+M_1+M_2} \Big(1-\frac{\varrho_f(p)}{p^2}\Big) \sum_{1\leqslant s\leqslant B+C+M_1+M_2} \tau^2(s)\frac{\varrho_f(s)}{s^2}. \tag{7·6}$$

On utilise alors le Lemme 7.1 (i). Pour tout $M > d$, on a :

$$\prod_{d<p\leqslant M}\Big(1-\frac{\varrho_f(p)}{p^2}\Big) \leqslant \exp\Big(-\sum_{d<p\leqslant M}\frac{\varrho_f(p)}{p^2}\Big) \ll (\log M)^{-1},$$

puis le Lemme 7.2 avec une sommation par parties :

$$\sum_{1\leqslant s\leqslant M} \tau^2(s)\frac{\varrho_f(s)}{s^2} \ll (\log M)^4.$$

On en déduit que $E_f \ll (\log(B+C))^3$ en prenant $M = B+C+M_1+M_2$. Cela termine la preuve du point (i) du Lemme 7.3.

Pour les points (ii) et (iii) on applique à nouveau le Théorème 1.1 de [9] mais avec le polynôme $g(b,c) = f(\xi b, c)$. Nous ne donnons ici que la preuve de (iii), celle de (ii) étant similaire. Dans ce cas $\|g\|$, la somme des coefficients de g, est un $O(\xi^d)$ et la condition (1.8) du Théorème 1.1 de [9] relative à $\|g\|$ est bien réalisée.

La variable ξ amène cependant des complications. Pour étudier les valeurs de ϱ_g, nous écrivons $f(x,y) = \sum_{i=0}^{d} \alpha_i x^i y^{d-i}$. Soit $u_0 = (\xi, \alpha_0)$. On associe à chaque $p|u_0$ l'entier k_p tel que p^{k_p} soit la plus grande puissance de p divisant tous les coefficients $\alpha_i \xi^i$, $(0 \leqslant i \leqslant d)$. En d'autres termes $k_p = \min_{0\leqslant i\leqslant d}(v_p(\alpha_i \xi^i))$, v_p étant la valuation p-adique. Comme les coefficients de f sont premiers entre eux dans leur ensemble et ξ est sans facteur carré, $k_p \leqslant d$. Alors $u := \prod_{p|u_0} p^{k_p}$ divise $f(\xi x, y)$, $\forall (x,y) \in \mathbb{Z}^2$.

On a alors $\tau^2(f(\xi b, c)) = \tau^2(u g_1(b,c)) \leqslant \tau^2(u)\tau^2(g_1(b,c))$ où on a posé $g_1(b,c) = u^{-1} f(\xi b, c)$. Remarquons que $\tau(u) \leqslant \tau(\alpha_0)$. Le polynôme g_1 est maintenant primitif. Le Théorème 1.1 de [9] donne alors

$$\sum_{\substack{B\leqslant b\leqslant B+M_1\\ C\leqslant c\leqslant C+M_2}} \tau^2(f(\xi b, c)) \ll M_1 M_2 E_{g_1},$$

où E_{g_1} est défini par la formule (7·6) en remplaçant f par g_1.

Pour évaluer cette quantité nous devons étudier les valeurs de la fonction ϱ_{g_1}.

Si $(p,\xi) = 1$, alors $\varrho_{g_1}(p^k) = \varrho_f(p^k)$.

Si $p|\xi$ mais $(p,u) = 1$ alors $\varrho_{g_1}(p^k) = \varrho_g(p^k)$. Et dans ce cas, si $(p,y) = 1$ alors $f(\xi x, y) \not\equiv 0 \pmod p$. Si $p|y$ alors $f(\xi x, y) = p^d f\big(x\frac{\xi}{p}, \frac{y}{p}\big)$. On en déduit que si $k \leqslant d$, $\varrho_{g_1}(p^k) = p^{2k-1}$. Il reste à déterminer $\varrho_{g_1}(p^k)$ pour $k > d$. Là encore pour que $p^k | f(\xi x, y)$, il faut que $p|y$. Auquel cas, $p^k | g_1(x,y)$ si et seulement si $p^{k-d} | f\big(\frac{\xi}{p}x, \frac{y}{p}\big)$. Ainsi $\varrho_{g_1}(p^k) = p^{2d-1}\varrho_f(p^{k-d})$ vu que $\big(\frac{\xi}{p}, p\big) = 1$ lorsque ξ est sans facteur carré. Si $p|u_0$ et est strictement supérieur à d, on a bien $\varrho_{g_1}(p) < p^2$ vu que le polynôme g_1 est primitif. Puis à l'aide de (7·5), on vérifie que

$$\sum_{k=0}^{+\infty} \frac{\varrho_{g_1}(p^k)}{p^{2k}} < +\infty.$$

Cette majoration est suffisante car il n'y a qu'un nombre fini de nombres premiers p divisant u_0.

Le produit eulérien de $E_{g_1}(M)$ est alors

$$\prod_{d<p\leqslant B+C+M_1+M_2} \Big(1 - \frac{\varrho_{g_1}(p)}{p^2}\Big) \ll \prod_{p|\xi}\Big(1-\frac{1}{p}\Big) \prod_{\substack{d<p\leqslant M\\ (p,\xi)=1}} \Big(1 - \frac{\varrho_f(p)}{p^2}\Big).$$

On majore la série de E_{g_1} de la même façon que pour f :

$$\sum_{s\leqslant M} \tau^2(s)\frac{\varrho_{g_1}(s)}{s^2} \ll \prod_{\substack{(p,\xi)=1\\ d\leqslant p<M}} \Big(1 + \sum_{k=1}^{+\infty} \frac{(k+1)^2 \varrho_f(p^k)}{p^{2k}}\Big)$$
$$\times \prod_{p|\xi}\Big(1 + \sum_{k=1}^{d}\frac{(k+1)^2}{p} + \sum_{k=d+1}^{+\infty}\frac{(k+1)^2\varrho_f(p^{k-d})}{p^{2k-2d+1}}\Big).$$

En utilisant de nouveau le Lemme 7.1, on vérifie que le deuxième produit eulérien est

$$\ll \prod_{p|\xi}\Big(1 + \frac{d(2d^2+9d+13)}{6p}\Big).$$

On en déduit que

$$E_{g_1}(M) \ll (\log M)^3 \prod_{p|\xi} \Big(1 + \frac{d(2d^2+9d+13)}{6p}\Big).$$

7·2. Cas des facteurs de q

Dans ce paragraphe nous déterminons le nombre de solutions des congruences $q(b,c,d) \equiv 0 \,(\mathrm{mod}\, p^\alpha)$, pour $\alpha = 1$ ou 2, $q = q_1q_2q_3$ et q_1, q_2, q_3 sont les formes en deux ou trois variables définies par (5·5), (5·6). Nous avons choisi de ne traiter que ces deux valeurs de α car ce sont les seules qui nous serviront dans la suite. On évite ainsi des considérations de pgcd plus longues. On associe aux formes binaires q_1 et q_2 les fonctions $\tilde{\varrho}_{q_i}$ définies suivant (7·3) :

$$\tilde{\varrho}_{q_1}(m) = |\{0 \leqslant v^2 < m : v^2 + 1 \equiv 0 \,(\mathrm{mod}\, m)\}|,$$

$$\tilde{\varrho}_{q_2}(m) = |\{0 \leqslant v < m : v^2 + v + 1 \equiv 0 \,(\mathrm{mod}\, m)\}|.$$

Les valeurs de ces fonctions sont données par le lemme suivant :

Lemme 7.4. *Les fonctions $\tilde{\varrho}_{q_1}$ et $\tilde{\varrho}_{q_2}$ sont multiplicatives et prennent les valeurs suivantes*

$$\tilde{\varrho}_{q_1}(p^\nu) = \begin{cases} 2 & \text{si } p \equiv 1 \,(\mathrm{mod}\, 4) \\ 0 & \text{si } p \equiv -1 \,(\mathrm{mod}\, 4) \\ 1 & \text{si } p^\nu = 2 \\ 0 & \text{si } p = 2 \text{ et } \nu \geqslant 2, \end{cases} \qquad \tilde{\varrho}_{q_2}(p^\nu) = \begin{cases} 2 & \text{si } p \equiv 1 \,(\mathrm{mod}\, 3) \\ 0 & \text{si } p \equiv 2 \,(\mathrm{mod}\, 3) \\ 1 & \text{si } p^\nu = 3 \\ 0 & \text{si } p = 3 \text{ et } \nu \geqslant 2. \end{cases}$$

Comme $q_3 = 4q_2 - 3q_1$, on remarque que si un entier m premier à 6 divise $q_i(b,c,d)$ et $q_j(b,c,d)$ pour deux entiers $i \neq j$ alors $m|(q_1(b,c,d), q_2(b,c,d), q_3(b,c,d))$.

Soit $\tilde{\Phi}_{12}$ la forme binaire associée à Φ_{12} :

$$\tilde{\Phi}_{12}(c,d) = d^4 \Phi_{12}\Big(\frac{c}{d}\Big) = c^4 - c^2d^2 + d^4. \tag{7·7}$$

Lemme 7.5. *Soient c et d deux entiers, $p > 3$ un nombre premier tel que $(p, cd) = 1$ et $1 \leqslant i < j \leqslant 3$. Le système de congruences $\begin{cases} q_i(b,c,d) \equiv 0 \,(\mathrm{mod}\, p) \\ q_j(b,c,d) \equiv 0 \,(\mathrm{mod}\, p) \end{cases}$ admet une solution b si et seulement si $p|\tilde{\Phi}_{12}(c,d)$. Dans ce cas cette solution b est déterminée de manière unique modulo p.*

Preuve. D'après la remarque précédent l'énoncé de ce lemme, il suffit de considérer le cas $i = 1$, $j = 2$. On commence par vérifier le sens direct. Si p divise $q_1(b,c,d)$ et $q_2(b,c,d)$ alors $(b,p) = 1$. Il existe deux entiers $0 \leqslant \Omega_1, \Omega_2 < p$ tels que $\Omega_1^2 + 1 \equiv 0 \,(\mathrm{mod}\, p)$, $\Omega_2^2 + \Omega_2 + 1 \equiv 0 \,(\mathrm{mod}\, p)$, $b \equiv \Omega_1 c \,(\mathrm{mod}\, p)$, $b \equiv \Omega_2 d \,(\mathrm{mod}\, p)$. Ainsi $c \equiv -\Omega_1\Omega_2 d \,(\mathrm{mod}\, p)$ (puisque $-\Omega_1$ est l'inverse de Ω_1 modulo p). On vérifie ensuite que $-\Omega_1\Omega_2$ est une racine primitive douzième de l'unité. On en déduit que $\tilde{\Phi}_{12}(c,d) \equiv 0 \,(\mathrm{mod}\, p)$.

Réciproquement, si $p|\tilde{\Phi}_{12}(c,d)$ avec $(p,cd) = 1$, alors il existe $0 \leqslant w < p$ tel que $c \equiv wd \,(\mathrm{mod}\, p)$ et $\Phi_{12}(w) = 0$. On observe ensuite que $\Omega_1 := w^3$ est une racine primitive quatrième de 1, $\Omega_2 := w^4$ est une racine cubique de 1 et $w \equiv w^4 w^{-3} \,(\mathrm{mod}\, p) \equiv -\Omega_1\Omega_2 \,(\mathrm{mod}\, p)$. On choisit alors b tel que $b \equiv \Omega_1 c \,(\mathrm{mod}\, p)$ de sorte que $q_1(b,c,d) \equiv 0 \,(\mathrm{mod}\, p)$. Ce choix de b est pertinent puisque $b \equiv \Omega_1 wd \,(\mathrm{mod}\, p) \equiv \Omega_2 d \,(\mathrm{mod}\, p)$, $q_2(b,c,d) \equiv 0 \,(\mathrm{mod}\, p)$. De plus cette solution est la seule possible car $q_2(b, -\Omega_1 c) \not\equiv 0 \,(\mathrm{mod}\, p)$.

Remarque. Si $p \equiv 1 \pmod{12}$ et $(p, cd) = 1$ alors le résultant des polynômes modulo p $q_1(*, c)$ et $q_2(*, d)$ est

$$\prod_{\substack{\Omega_1^2+1\equiv 0 \pmod p \\ \Omega_2^2+\Omega_2+1\equiv 0 \pmod p}} (\Omega_1 c - \Omega_2 d) \equiv \tilde{\Phi}_{12}(c, d) \pmod p.$$

Ce résultant s'annule si et seulement s'il existe Ω_1, Ω_2 tels que $c \equiv -\Omega_1\Omega_2 d \pmod p$ c'est-à-dire pour $\tilde{\Phi}_{12}(c, d) \equiv 0 \pmod p$.

On généralise la fonction ϱ_f^* aux formes en trois variables. Le souci est qu'il sera parfois commode d'interpréter les formes q_1 et q_2 comme des formes en trois variables (avec une variable muette). Pour lever toute ambiguïté nous utilisons la lettre σ pour des congruences liées à des formes en trois variables. Si f est un polynôme en trois variables, on définit

$$\sigma_f(m) = |\{0 \leqslant b, c, d < m : m | f(b, c, d)\}|,$$

$$\sigma_f^*(m) = |\{0 \leqslant b, c, d < m : m | f(b, c, d),\ (m, bcd) = 1\}.$$

Lemme 7.6. *On a les égalités suivantes pour $\alpha = 1, 2$:*

$$\sigma_{q_1}^*(p^\alpha) = \begin{cases} 2\varphi(p^\alpha)^2 & \text{si } p \equiv 1 \pmod 4 \\ 0 & \text{si } p \equiv -1 \pmod 4 \\ 1 & \text{si } p^\alpha = 2 \\ 0 & \text{si } p^\alpha = 4 \end{cases}, \quad \sigma_{q_2}^*(p^\alpha) = \begin{cases} 2\varphi(p^\alpha)^2 & \text{si } p \equiv 1 \pmod 3 \\ 0 & \text{si } p \equiv -1 \pmod 3 \\ 4 & \text{si } p^\alpha = 3 \\ 0 & \text{si } p^\alpha = 9 \end{cases}$$

$$\sigma_{q_3}^*(p^\alpha) = \begin{cases} 2\varphi(p^\alpha)(p-2)p^{\alpha-1} & \text{si } p \equiv \pm 1 \pmod{12} \\ 0 & \text{si } p \equiv \pm 5 \pmod{12} \\ 1 & \text{si } p^\alpha = 2 \\ 4 & \text{si } p^\alpha = 3 \\ 0 & \text{si } p^\alpha = 4, 9 \end{cases}.$$

Preuve. Les valeurs de $\sigma_{q_1}^*$, $\sigma_{q_2}^*$ s'obtiennent avec le Lemme 7.4. Pour q_3, des solutions existent si et seulement si 3 est un carré modulo p, c'est-à-dire si et seulement si $p \equiv \pm 1 \pmod{12}$ ou $p^\alpha = 2$ ou 3. Les cas $p^\alpha = 2$ ou 3 s'évaluent par un comptage direct. Lorsque $p \equiv \pm 1 \pmod{12}$ et $p \geqslant 5$, les triplets (b, c, d) comptés dans $\sigma_{q_3}^*(p^\alpha)$ sont de la forme $(b, \pm\overline{\Omega}_3(b + 2d), d)$ où $(bd(b + 2d), p) = 1$ et Ω_3 est une solution de $\Omega_3^2 \equiv 3 \pmod{p^\alpha}$. Pour chaque d premier avec p donné on compte $(p-2)p^{\alpha-1}$ entiers b tels que $(b(b + 2d), p) = 1$. On en déduit les valeurs de $\sigma_{q_3}^*(p^\alpha)$ annoncées dans dans le Lemme 7.6.

Nous passons maintenant à l'étude des valeurs de $\sigma_q(p^\alpha)$ pour $\alpha = 1, 2$. On commence par étudier le cas où $(p, bcd) = 1$.

Lemme 7.7. *Pour $\alpha = 1, 2$ les deux assertions suivantes sont vérifiées.*
(i) Si $p \not\equiv 1 \pmod{12}$ et si $p \geqslant 5$ alors

$$\sigma_q^*(p^\alpha) = \begin{cases} 2\varphi(p^\alpha)^2 & \text{si } p \equiv \pm 5 \pmod{12} \\ 2\varphi(p^\alpha)(p-2)p^{\alpha-1} & \text{si } p \equiv -1 \pmod{12}. \end{cases}$$

(ii) Si $p \equiv 1 \pmod{12}$, alors

$$\sigma_q^*(p^\alpha) = \varphi(p^\alpha)p^{\alpha-1}(4p^{\alpha-1} + 6p - 20). \tag{7·8}$$

Preuve. Dans le cas (i), les polynômes q_i n'ont pas de solution commune modulo p et $\sigma_q^*(p^\alpha) = \sum_{i=1}^3 \sigma_{q_i}^*(p^\alpha)$. On applique alors le Lemme 7.6.

Dans le cas (ii) on commence par étudier le nombre de (b,c,d) comptés dans $\sigma_q^*(p^\alpha)$ tels que $p|\tilde{\Phi}_{12}(c,d)$. Cela concerne $4\varphi(p)p^{2(\alpha-1)}$ tels couples (c,d). On a vu au Lemme 7.5 que pour de tels (c,d) il existait un entier b déterminé de manière unique modulo p tel que $p|q_i(b,c,d)$ pour tous $i=1,2,3$. Ces triplets (b,c,d) fournissent alors $4\varphi(p)p^{3(\alpha-1)}$ solutions.

On compte maintenant les (b,c,d) tels que $\tilde{\Phi}_{12}(c,d) \equiv 0 \,(\mathrm{mod}\, p)$, $q_i(b,c,d) \equiv 0 \,(\mathrm{mod}\, p^\alpha)$ pour un $i \in \{1,2,3\}$ mais $q_j(b,c,d) \not\equiv 0 \,(\mathrm{mod}\, p)$ pour $j \neq i$. Pour $i=1,2$ et c,d donnés on obtient une seule solution b supplémentaire telle $q_i(b,c,d) \equiv 0 \,(\mathrm{mod}\, p^\alpha)$. Pour $i=3$ il faut s'assurer que le b obtenu soit premier avec p. Cela ne peut arriver que si $-3c^2+4d^2 \equiv 0 \,(\mathrm{mod}\, p)$, ou encore $\overline{c^2}\,\mathrm{d}^2 \equiv 3 \times \overline{4} \,(\mathrm{mod}\, p)$. Or $\overline{c}d$ est une racine de Φ_{12} modulo p. Cela implique $(3\times\overline{4})^2 - 3\times\overline{4}+1 \equiv 0 \,(\mathrm{mod}\, p)$. En multipliant cette congruence par 16 on constate que cela n'arrive que dans le cas où $p=13$. Effectivement les racines de Φ_{12} modulo 13 sont congrues à $-2,2,6,-6$. Si $d \equiv \pm 2c \,(\mathrm{mod}\, 13)$ alors le b que l'on cherchait est bien divisible par p, mais ce n'est pas le cas si $d \equiv \pm 6c \,(\mathrm{mod}\, 13)$.

Ainsi le nombre de triplets (b,c,d) tels que $q(b,c,d) \equiv 0 \,(\mathrm{mod}\, p^\alpha)$ et $\tilde{\Phi}_{12}(c,d) \equiv 0 \,(\mathrm{mod}\, p)$ est

$$\begin{cases} 4\varphi(p)p^{3(\alpha-1)} + 12\varphi(p)p^{2(\alpha-1)} & \text{si } p \neq 13 \\ 4\varphi(p)p^{3(\alpha-1)} + 10\varphi(p)p^{2(\alpha-1)} & \text{si } p = 13. \end{cases} \tag{7·9}$$

Il reste maintenant à déterminer les triplets solutions tels que $\tilde{\Phi}_{12}(c,d) \not\equiv 0 \,(\mathrm{mod}\, p)$. Pour de tels c,d donnés on obtient 6 solutions b telles que $p^\alpha|q(b,c,d)$. Il faut retirer celles telles que $p|bcd$. Cela ne peut arriver que si $4d^2-3c^2 \equiv 0 \,(\mathrm{mod}\, p)$. Ce n'est jamais le cas si $p=13$. Lorsque $p \neq 13$, et c,d sont donnés tels que $p|4d^2-3c^2$, on obtient 5 racines b de $q(b,c,d)$ (une seule pour q_3 et deux pour chaque q_i, $i=1,2$.)

Le nombre de (b,c,d) tels que $p^\alpha|q(b,c,d)$ et $(p, bcd\tilde{\Phi}_{12}(c,d)) = 1$ est ainsi :

$$\begin{cases} 6\varphi(p^\alpha)(p-7)p^{\alpha-1} + 10\varphi(p^\alpha)p^{\alpha-1} & \text{si } p \neq 13 \\ 6\varphi(p^\alpha)(p-5)p^{\alpha-1} & \text{si } p = 13. \end{cases} \tag{7·10}$$

Le premier terme du cas $p \neq 13$ dans la ligne précédente correspond aux triplets (b,c,d) tels que $(bcd\tilde{\Phi}_{12}(c,d)(4d^2-3c^2), p) = 1$, le deuxième aux triplets (b,c,d) d'entiers premiers avec p tels que $4d^2-3c^2 \equiv 0 \,(\mathrm{mod}\, p)$. Finalement, on obtient (7·8) en additionnant (7·9) et (7·10).

On termine ce paragraphe en donnant les valeurs de $\sigma_q(p)$ et de $\sigma_q(p^2)$ pour $p \geqslant 5$. Pour $p=2,3$ on obtient avec un calcul direct : $\sigma_q(2)=5$, $\sigma_q(3)=11$.

Lemme 7.8. *La fonction σ_q prend les valeurs suivantes pour $p \geqslant 5$:*

$$\sigma_q(p) = \begin{cases} 6p^2-11p+6 & \textit{si } p \equiv 1 \,(\mathrm{mod}\, 12) \\ 2p^2+p-2 & \textit{si } p \not\equiv 1 \,(\mathrm{mod}\, 12) \end{cases},$$

$$\sigma_q(p^2) = \begin{cases} 13p^4-24p^3+12p^2 & \textit{si } p \equiv 1 \,(\mathrm{mod}\, 12) \\ 5p^4-4p^3 & \textit{si } p \not\equiv 1 \,(\mathrm{mod}\, 12). \end{cases}$$

Pour établir ce lemme il ne nous reste plus qu'à compter le nombre de triplets (b,c,d) tels que $p|bcd$ et $p^\alpha|q(b,c,d)$ avec $\alpha=1$ ou 2.

• Si $p|b$ et $p|cd$ alors $p^2|q$; cela donne $2p^{2(\alpha-1)}p^\alpha - p^{3(\alpha-1)}$ triplets (b,c,d).

• Si $p|b$ mais $p \nmid cd$ alors $p|q$ si et seulement si $p|(-3c^2+4d^2)$. Cela fait $2(p-1)$ triplets (b,c,d) modulo p si $p \equiv \pm 1 \,(\mathrm{mod}\, 12)$ et 0 triplets si $p \equiv \pm 5 \,(\mathrm{mod}\, 12)$.

Puis $p^2|q$ si et seulement si $p^2|(-3c^2+4d^2+4db)$. En écrivant $b=pb_1$, $c=c_0+pc_1$, $d=d_0+pd_1$, on remarque que $-3c_0^2+4d_0^2\equiv 0\,(\mathrm{mod}\,p)$ puis que deux variables parmi les (b_1,c_1,d_1) peuvent être arbitraires. On trouve alors $2(p-1)p^2$ ou 0 triplets suivant que $p\equiv\pm1\,(\mathrm{mod}\,12)$ ou $p\equiv\pm5\,(\mathrm{mod}\,12)$.

On a donc dans cette situation $2(p-1)p^{2(\alpha-1)}$ ou 0 triplets.

• Si $p\nmid b$, mais divise le pgcd (c,d) alors $q\equiv b^6\,(\mathrm{mod}\,p)$.

• Si $p\nmid bc$ mais divise d, alors $p|q\Leftrightarrow p|q_1(b,c)(-3c^2+b^2)$. Comme précédemment, on vérifie que si $p\geqslant 5$ est tel que $p|q$ alors p divise soit q_1 soit q_3 mais ne peut pas diviser à la fois q_1 et q_3. On en déduit que si $p^2|q$ alors ou bien $p^2|q_1$, ou bien $p^2|(-3c^2+b^2+4bpd')$ où on a écrit $d=pd'$. Si $p\equiv 1\,(\mathrm{mod}\,12)$ alors on obtient $4\varphi(p^\alpha)p^{\alpha-1}$ triplets (b,c,d), si $p\equiv 5,-1\,(\mathrm{mod}\,12)$ on trouve $2\varphi(p^\alpha)p^{\alpha-1}$ triplets (b,c,d).

• Si $p\nmid bd$ mais divise c alors $p|q\Rightarrow p|q_2(b,d)(b+2d)^2$. Si $p|q_2$, alors il existe $1\leqslant\Omega_2<p$ tel que $\Omega_2^2+\Omega_2+1\equiv 0\,(\mathrm{mod}\,p)$ et $b\equiv\Omega_2 d\,(\mathrm{mod}\,p)$. Mais si p divise aussi $b+2d$, alors $\Omega_2\equiv -2\,(\mathrm{mod}\,p)$, $p|(4-2+1)$ ce qui contredit le fait que $p\geqslant 5$.

Ainsi dans ce dernier cas, on obtient $p^{\alpha-1}\varrho^*_{q_2}(p^\alpha)+p^{3\alpha-3}(p-1)$ triplets.

On rassemble ces remarques dans deux tableaux. Le premier sert à calculer les valeurs de $\sigma_q(p)$. Dans chaque case on compte le nombre de triplets (b,c,d), $0\leqslant b,c,d<p$, tels que $p|q(b,c,d)$, p et b,c,d devant vérifier les contraintes données par la première ligne et la première colonne.

	$p\equiv 1\,(\mathrm{mod}\,12)$	$p\equiv -1\,(\mathrm{mod}\,12)$	$p\equiv 5\,(\mathrm{mod}\,12)$	$p\equiv -5\,(\mathrm{mod}\,12)$
$p\nmid bcd$	$6p^2-22p+16$	$2p^2-6p+4$	$2p^2-4p+2$	$2p^2-4p+2$
$p\|b$ et $p\|cd$	$2p-1$	$2p-1$	$2p-1$	$2p-1$
$p\|b$ et $p\nmid cd$	$2p-2$	$2p-2$	0	0
$p\nmid b$ et $p\|(c,d)$	0	0	0	0
$p\|d,\ p\nmid bc$	$4p-4$	$2p-2$	$2p-2$	0
$p\|c,\ p\nmid cd$	$3p-3$	$p-1$	$p-1$	$3p-3$
$\sigma_q(p)$	$6p^2-11p+6$	$2p^2+p-2$	$2p^2+p-2$	$2p^2+p-2$

On effectue un tableau analogue pour déterminer le nombre de triplets (b,c,d), $0\leqslant b,c,d<p^2$, $p^2|q(b,c,d)$.

	$p \equiv 1 \pmod{12}$	$p \equiv -1 \pmod{12}$	$p \equiv 5 \pmod{12}$	$p \equiv -5 \pmod{12}$
$p \nmid bcd$	$10p^4 - 30p^3 + 20p^2$	$2p^4 - 6p^3 + 4p^2$	$2p^4 - 4p^3 + 2p^2$	$2p^4 - 4p^3 + 2p^2$
$p\|b$ et $p\|cd$	$2p^4 - p^3$	$2p^4 - p^3$	$2p^4 - p^3$	$2p^4 - p^3$
$p\|b$ et $p \nmid cd$	$2p^3 - 2p^2$	$2p^3 - 2p^2$	0	0
$p \nmid b$ et $p\|(c,d)$	0	0	0	0
$p\|d,\ p \nmid bc$	$4p^3 - 4p^2$	$2p^3 - 2p^2$	$2p^3 - 2p^2$	0
$p\|c,\ p \nmid bd$	$p^4 + p^3 - 2p^2$	$p^4 - p^3$	$p^4 - p^3$	$p^4 + p^3 - 2p^2$
$\sigma_q(p^2)$	$13p^4 - 24p^3 + 12p^2$	$5p^4 - 4p^3$	$5p^4 - 4p^3$	$5p^4 - 4p^3$

Dans la suite de ce travail nous utiliserons ces deux tableaux pour évaluer les cardinaux $|\{0 \leqslant b, c, d < p^\alpha : p|cd \text{ et } p^\alpha|q\}|$ avec $\alpha = 1, 2$.

8. Le niveau de distribution de q : une approche avec des réseaux de $\mathbb{Z}^3$

8·1. Énoncé du résultat

Soient f_1, f_2 deux formes binaires irréductibles et $P =]B, B+M] \times]C, C+M] \times]D, D+M]$ un cube de $\mathbb{R}^3$. On suppose qu'il existe $\vartheta > 0$ tel que

$$M \geqslant \max(|B|, |C|, |D|)^\vartheta. \tag{8·1}$$

Pour $\mathbf{u}, \mathbf{v} \in \mathbb{Z}^3$, $\mathbf{u} = (u_1, u_2, u_3), \mathbf{v} = (v_1, v_2, v_3)$, on écrira $\mathbf{u} \equiv \mathbf{v} \pmod{m}$ pour indiquer que $u_i \equiv v_i \pmod{m}$ pour $i = 1, 2, 3$. On s'intéresse aux ensembles

$$\mathcal{A}(m_1, m_2, m_3, \mathbf{u}) = \{(b, c, d) \in P : m_1|f_1(b, c),\ m_2|f_2(b, d), (b, c, m_1) = 1 = (b, d, m_2), \\ (b, c, d) \equiv \mathbf{u} \pmod{m_3}\}.$$

Le but de ce paragraphe est d'obtenir une estimation en moyenne des cardinaux des ensembles $\mathcal{A}(m_1, m_2, m_3, \mathbf{u})$, autrement dit une majoration des quantités

$$E = E(m_3) := \sideset{}{^*}\sum_{\substack{m_1 < Q_1 \\ (m_1, m_3) = 1}} \sideset{}{^*}\sum_{\substack{m_2 < Q_2 \\ (m_2, m_1 m_3) = 1}} \left| |\mathcal{A}(m_1, m_2, m_3, \mathbf{u})| - \frac{M^3 \varrho^*_{f_1}(m_1) \varrho^*_{f_2}(m_2)}{m_1^2 m_2^2 m_3^3} \right|, \tag{8·2}$$

où les étoiles dans les symboles de sommation indiquent ici que les entiers m_1, m_2 vérifient la condition :

$$(m_i, f_i(1, 0) f_i(0, 1)) = 1 \quad (i = 1, 2).$$

Théorème 8.1. *Soient f_1, $f_2 \in \mathbb{Z}[x,y]$ deux formes binaires primitives et irréductibles de degré supérieur ou égal à 2. Soient $\varepsilon > 0$ et P un cube de $\mathbb{R}^3$, $P =]B, B+M] \times]C, C+M] \times]D, D+M]$ vérifiant (8·1) pour un certain $\vartheta > 0$. Pour tous $\mathbf{u} \in \mathbb{Z}^3$, $m_3 \geqslant 1$ on a :*

$$E \underset{\varepsilon,\vartheta}{\ll_{f_1,f_2,}} (\log M)^7 \Big(Q_1Q_2 + \frac{(Q_1Q_2)^{1/2}M^{3/2}}{m_3^{3/4}} + \frac{(Q_1Q_2)^{1/3}M^2}{m_3^2} \Big) + M^{1+\varepsilon}(Q_1+Q_2) + M^{2+\varepsilon} + \frac{M^{2+\varepsilon}}{m_3^2}(\sqrt{Q_1}+\sqrt{Q_2}). \tag{8·3}$$

Remarques. (1) Les puissances de $\log M$ dans (8·3) ne dépendent pas des degrés de f_1 et de f_2. Cela est dû aux travaux récents de La Bretèche, Browning et Tenenbaum [5], [9] sur les majorations de moyennes de fonctions arithmétiques sur les formes binaires. Il est probable que l'on puisse améliorer les puissances de log dans (8·3) et remplacer certains M^ε par des puissances de $\log M$ notamment en utilisant l'article récent d'Henriot [29] sur les moyennes de fonctions arithmétiques sur des suites polynomiales.

Cependant, le résultat que nous obtenons est largement suffisant pour l'utilisation que nous en ferons dans cet article. En fait une majoration avec un M^ε à la place de $(\log M)^7$ dans (8·3) aurait suffi ici. Nous avons essayé de donner dans (8·3) une majoration de E sous une forme assez compacte. On trouvera à la fin de la preuve de ce théorème une majoration de E plus précise mais avec un paramètre à choisir.

(2) Ce théorème nous permet de prendre des niveaux Q_1, Q_2 tels que Q_1Q_2 soit très proche de M^3. Nous appliquerons ce résultat aux formes quadratiques $f_1 = q_1$ et $f_2 = q_2$. Pour de telles formes quadratiques nous aurions pu adopter une autre approche qui repose sur l'équirépartition des racines d'un polynôme irréductible de degré 2. En utilisant les travaux de Hooley ([30] ou [31]) on peut obtenir en surmontant des problèmes de pgcd (à l'aide par exemple de [13]), une estimation asymptotique de quantités de la forme pour b donné :

$$\sum_{\substack{m_1<Q_1 \\ m_0|m_1}} \sum_{\substack{C<c\leqslant C+M \\ b^2+c^2\equiv 0 \,(\mathrm{mod}\, m_1) \\ c\equiv v \,(\mathrm{mod}\, m_3)}} 1, \tag{8·4}$$

pour un niveau $Q_1 = M^{1+\vartheta_1}$ avec un certain $\vartheta_1 > 0$. En reprenant les travaux de Fouvry et Iwaniec [19] sur les nombres premiers de Gauss, et en y insérant la généralisation de Balog, Blomer, Dartyge et Tenenbaum [1] de l'inégalité de type grand crible pour toutes les formes binaires quadratiques irréductibles on obtient une majoration de quantités de la forme :

$$\sum_{m_2<Q_2} \Big| \sum_b \sum_{\substack{D<d\leqslant D+M \\ d\equiv 0 \,(\mathrm{mod}\, m_3) \\ b^2+bd+d^2\equiv 0 \,(\mathrm{mod}\, m_2)}} \lambda_b - \frac{(D_2-D_1)}{m_2} \sum_b \lambda_b \varrho(b,m_2) \Big|, \tag{8·5}$$

où (λ_b) est une suite de nombres complexes nulle pour $b \notin [B, B+M]$. En appliquant ensuite (8·4) puis (8·5) avec des suites (λ_b) adéquates, on devrait obtenir un résultat du type le Théorème 8.1 valable pour un produit $Q_1Q_2 < M^{3+\vartheta}$ mais avec un $\vartheta > 0$ probablement petit. Ce domaine en m_1, m_2 est ainsi meilleur que celui du Théorème 8.1 mais la contribution en m_3 est moins bien contrôlée. Si on adopte cette approche, on rencontre de nombreux problèmes de pgcd qui rendent la progression laborieuse malgré toutes les astuces mises au point dans [19] pour régler ce type de difficulté. Cette deuxième approche présente aussi l'inconvénient de fournir une majoration de la forme

$$\sum_{m_2<Q_2} \Big| \sum_{\substack{m_1<Q_1 \\ m_0|m_1}} |\mathcal{A}(m_1,m_2,m_3,u)| - .... \Big|, \tag{8·6}$$

autrement dit elle ne s'applique qu'avec des suites $\{m_0m_1\}_{m_1}$ de multiples consécutifs d'un entier m_0. Dans notre application l'entier m_1 est un produit de deux nombres premiers. Le gain que l'on obtient sur la taille Q_1Q_2 est perdu par l'utilisation de cribles alors nécessaires pour appliquer (8·6) à une suite d'entiers criblés m_1. Cependant cette méthode peut s'avérer plus pertinente dans d'autres circonstances.

(3) Dans [12], [41], [10], les résultats sont valables pour des couples (b, c) dans des domaines du plan dont le bord vérifient des conditions assez générales tandis que le Théorème 8.1 n'aborde que le cas où (b, c, d) appartient à un cube de $\mathbb{R}^3$. Cela est dû au fait qu'en dimension 2, le nombre de points d'un domaine dont le bord est assez régulier est proche de la mesure de Lebesgue de ce domaine, l'erreur de cette approximation étant d'un ordre de grandeur inférieur au périmètre de ce domaine. En dimension supérieure à 3, ce principe de Lipschitz n'est pas toujours vérifié (cf [14]). Cependant Davenport ([14]) a établi un résultat très général qui s'applique aux pavés mais également à bien d'autres domaines comme par exemple les ensembles semi-algébriques. Il est donc possible d'établir des estimations de type le Théorème 8.1 valables pour une large gamme de régions $\mathcal{R} \subset \mathbb{R}^3$.

8·2. Partition des ensembles $\mathcal{A}(m_1, m_2, m_3, \mathbf{u})$

On effectue une partition de $\mathcal{A}(m_1, m_2, m_3, \mathbf{u})$ à l'aide des racines modulo m_1 et m_2 des polynômes $f_1(1, Y)$, $f_2(1, Y)$. Notons $\mathbf{u} = (u, v, w)$.

On considère les ensembles suivants :

$$\Lambda^*(m_1, m_2) = \{(b, c, d) \in \mathbb{Z}^3 : (m_1, b, c) = 1 = (m_2, b, d),\ m_1 | f_1(b, c),\ m_2 | f_2(b, d)\},$$

$$\Psi_{m_3} = \Psi_{m_3}(\mathbf{u}) = \{(b, c, d) \in \mathbb{Z}^3 : (b, c, d) \equiv (u, v, w) \,(\mathrm{mod}\, m_3)\}.$$

Dans la ligne précédente, (b, c, d) et (u, v, w) désignent des triplets d'entiers et non des pgcd. Avec ces notations (qui reprennent celles de Marasingha [41]),

$$\mathcal{A}(m_1, m_2, m_3, \mathbf{u}) = \Lambda^*(m_1, m_2) \cap P \cap \Psi_{m_3}.$$

Soit $(b, c, d) \in \Lambda^*(m_1, m_2)$. Si $p | (b, m_1)$, alors $f_1(b, c) \equiv \alpha_{d_1} c^{d_1} \,(\mathrm{mod}\, p)$, $\alpha_{d_1} = f_1(0, 1)$ étant le coefficient dominant de $f_1(1, c)$. D'après la condition $*$ de (8·2) et la contrainte $(m_1, b, c) = 1$, p ne peut pas diviser $\alpha_{d_1} c$. On en déduit que si $(b, c, d) \in \Lambda^*(m_1, m_2)$ alors $(b, m_1) = 1$. On vérifie de la même manière que $(b, m_2) = 1$.

On peut donc écrire que $f_1(1, \overline{b}c) \equiv 0 \,(\mathrm{mod}\, m_1)$, $f_2(1, \overline{b}d) \equiv 0 \,(\mathrm{mod}\, m_2)$. On en déduit qu'il existe un unique couple d'entiers $(\Omega_1, \Omega_2) \in [0, m_1[\times [0, m_2[$ tel que pour $i = 1, 2$, $f_i(1, \Omega_i) \equiv 0 \,(\mathrm{mod}\, m_i)$, $(\Omega_i, m_i) = 1$ et $c \equiv \Omega_1 b \,(\mathrm{mod}\, m_1)$, $d \equiv \Omega_2 b \,(\mathrm{mod}\, m_2)$. On peut donc faire une partition de $\Lambda^*(m_1, m_2)$ de la manière suivante :

$$\Lambda^*(m_1, m_2) = \bigcup_{\substack{0 \leqslant \Omega_1 < m_1 \\ (\Omega_1, m_1) = 1 \\ f_1(1, \Omega_1) \equiv 0 \,(\mathrm{mod}\, m_1)}} \ \bigcup_{\substack{0 \leqslant \Omega_2 < m_2 \\ (\Omega_2, m_2) = 1 \\ f_2(1, \Omega_2) \equiv 0 \,(\mathrm{mod}\, m_2)}} G^*(\Omega_1, \Omega_2),$$

où $G^*(\Omega_1, \Omega_2)$ est l'ensemble des $(b, c, d) \in \mathbb{Z}^3$ tels que

$$\begin{cases} c \equiv \Omega_1 b \,(\mathrm{mod}\, m_1),\ d \equiv \Omega_2 b \,(\mathrm{mod}\, m_2) \\ (m_1, b, c) = (m_2, b, d) = 1. \end{cases}$$

Ainsi $G^*(\Omega_1, \Omega_2) \subset G(\Omega_1, \Omega_2)$ où $G(\Omega_1, \Omega_2)$ est le réseau de $\mathbb{Z}^3$ défini par :

$$G(\Omega_1, \Omega_2) = \{(b, c, d) \in \mathbb{Z}^3 : c \equiv \Omega_1 b \,(\mathrm{mod}\, m_1),\ d \equiv \Omega_2 b \,(\mathrm{mod}\, m_2)\}.$$

8·3. On enlève des conditions de coprimalité

On traite les conditions de coprimalité apparaissant dans les ensembles $G^*(\Omega_1,\Omega_2)$ à l'aide de la formule d'inversion de Möbius. Signalons que ces conditions imposent que les entiers b soient différents de 0. Dans tout ce paragraphe, nous conserverons cette contrainte sur les entiers b. On commence par le pgcd (b,c,m_1) :

$$|G^*(\Omega_1,\Omega_2)\cap P\cap\Psi_{m_3}| = \sum_{\substack{(b,c,d)\in G(\Omega_1,\Omega_2)\cap P\cap\Psi_{m_3}\\ (b,d,m_2)=1}} \sum_{\xi_1|(b,c,m_1)} \mu(\xi_1). \tag{8·7}$$

Soit $\xi_1|(b,c,m_1)$ donné. Si on remplace b,c par $b'\xi_1, c'\xi_1$, on observe que

$$c\equiv\Omega_1 b\,(\mathrm{mod}\,m_1)\Leftrightarrow c'\equiv\Omega_1 b'\,(\mathrm{mod}\,m_1/\xi_1).$$

Soit $E_1 = E_1(m_1,m_2,\Omega_1,\Omega_2)$ la contribution à (8·7) des $\xi_1>\Delta$ où Δ sera choisi ultérieurement. Nous cherchons maintenant à obtenir une majoration de cette contribution. Dans les deux lignes de (8·8) les entiers m_1 changent de rôle. Dans la première ligne chaque m_1 est un multiple d'un entier $\xi_1>\Delta$ ainsi $m_1=\xi_1 m_1'$; dans la deuxième ligne nous avons interverti certaines sommations puis renommé m_1 les entiers m_1' correspondants :

$$\begin{aligned} E_1^* &:= \sum_{\substack{m_1<Q_1\\ m_2<Q_2\\ (m_1,m_2)=1}} \sum_{\Omega_1,\Omega_2} E_1 \\ &\ll \sum_{\Delta<\xi_1<Q_1} \sum_{\substack{\xi_1 m_1<Q_1\\ m_2<Q_2}} \sum_{\substack{1\leqslant\Omega_1<\xi_1 m_1\\ (\Omega_1,\xi_1 m_1)=1\\ f_1(1,\Omega_1)\equiv 0\,(\mathrm{mod}\,\xi_1 m_1)}} \sum_{\substack{1\leqslant\Omega_2<m_2\\ (m_2,\Omega_2)=1\\ f_2(1,\Omega_2)\equiv 0\,(\mathrm{mod}\,m_2)}} \sum_{\substack{(\xi_1 b,\xi_1 c,d)\in P\\ c\equiv\Omega_1 b\,(\mathrm{mod}\,m_1)\\ d\equiv\Omega_2\xi_1 b\,(\mathrm{mod}\,m_2)\\ (b,d,m_2)=1}} \mu^2(\xi_1). \end{aligned} \tag{8·8}$$

Nous ferons à d'autres reprises ces types de changements de rôles des variables de sommation.

On a pour b, d, m_1, ξ_1 donnés la majoration :

$$\sum_{\substack{m_2<Q_2\\ (m_2,\xi_1 m_1)=1\\ (m_2,b,d)=1}} \sum_{\substack{1\leqslant\Omega_2<m_2,\ (\Omega_2,m_2)=1\\ f_2(1,\Omega_2)\equiv 0\,(\mathrm{mod}\,m_2)\\ d\equiv\Omega_2\xi_1 b\,(\mathrm{mod}\,m_2)}} 1\leqslant\tau(f_2(\xi_1 b,d)). \tag{8·9}$$

Pour les variables d'indice 1, comme la condition $(b,c,m_1)=1$ a disparu, on n'a plus l'équivalence

$$m_1|f_1(b,c)\Leftrightarrow\exists!\Omega_1\in\{1,\dots,m_1\} : f_1(1,\Omega_1)\equiv 0\,(\mathrm{mod}\,m_1)\text{ et }c\equiv\Omega_1 b\,(\mathrm{mod}\,m_1). \tag{8·10}$$

On traite cette difficulté en écrivant les entiers m_1 sous la forme $m_1=m_0m_1'$ avec $m_0|(b,c)$ et $(m_1',\frac{b}{m_0},\frac{c}{m_0})=1$. Cela nous permettra de profiter d'une équivalence du type (8·10) avec m_1' à la place de m_1.

On découpe alors E_1^* en deux sommes $E_{11}^*+E_{12}^*$ telles que dans E_{11}^*, $\xi_1 m_0\leqslant M^{1-\varepsilon}$ et dans E_{12}^*, $\xi_1 m_0>M^{1-\varepsilon}$.

Commençons par majorer E_{11}^*. Pour b, c, ξ_1 donnés, on a :

(8·11)
$$\sum_{m_1<Q_1/\xi_1} \sum_{\substack{1\leqslant\Omega_1<\xi_1 m_1\\(\Omega_1,\xi_1 m_1)=1\\ f_1(1,\Omega_1)\equiv 0 \,(\mathrm{mod}\, m_1\xi_1)\\ c\equiv\Omega_1 b \,(\mathrm{mod}\, m_1)}} 1 = \sum_{\substack{m_0<Q_1/\xi_1\\ m_0|(b,c)}} \sum_{\substack{m_1'<Q_1/\xi_1 m_0\\ (m_1',\frac{b}{m_0},\frac{c}{m_0})=1}} \sum_{\substack{1\leqslant\Omega_1<\xi_1 m_0 m_1'\\(\Omega_1,\xi_1 m_0 m_1')=1\\ f_1(1,\Omega_1)\equiv 0 \,(\mathrm{mod}\, m_0 m_1'\xi_1)\\ \frac{c}{m_0}\equiv\frac{b}{m_0}\Omega_1 \,(\mathrm{mod}\, m_1')}} 1$$
$$\leqslant \sum_{\substack{m_0<Q_1/\xi_1\\ m_0|(b,c)}} \tilde{\varrho}_{f_1}(m_0\xi_1)\tau\Big(f_1\Big(\frac{b}{m_0},\frac{c}{m_0}\Big)\Big).$$

En profitant de (8·9), (8·11) on a pour E_{11}^* :

$$E_{11}^* \ll \sum_{\Delta<\xi_1\leqslant M^{1-\varepsilon}} \mu^2(\xi_1) \sum_{m_0<M^{1-\varepsilon}/\xi_1} \tilde{\varrho}_{f_1}(\xi_1 m_0) \sum_{\substack{(\xi_1 b,\xi_1 c,d)\in P\\ m_0|(b,c)}} \tau\Big(f_1\Big(\frac{b}{m_0},\frac{c}{m_0}\Big)\Big)\tau(f_2(\xi_1 b,d)).$$

Soit $P(\xi_1) =]B\xi_1^{-1},(B+M)\xi_1^{-1}]\times]C\xi_1^{-1},(C+M)\xi_1^{-1}]\times]D,D+M]$. On sépare ensuite les variables c et d :

(8·12)
$$E_{11}^* \ll \sum_{\substack{\Delta<\xi_1<M^{1-\varepsilon}\\ m_0\xi_1<M^{1-\varepsilon}}} \mu^2(\xi_1)\tilde{\varrho}_{f1}(m_0\xi_1) \sum_{\substack{(b,c,d)\in P(\xi_1)\\ m_0|(b,c)}} \Big(\tau^2\Big(f_1\Big(\frac{b}{m_0},\frac{c}{m_0}\Big)\Big)+\tau^2(f_2(\xi_1 b,d))\Big).$$

Pour m_0 donné, nous majorons les sommes sur b, c, d correspondantes à l'aide du Lemme 7.3 :

$$\sum_{\substack{(b,c,d)\in P(\xi_1)\\ m_0|(b,c)}} \tau^2\Big(f_1\Big(\frac{b}{m_0},\frac{c}{m_0}\Big)\Big) \ll \frac{M^3}{\xi_1^2 m_0^2}(\log M)^3,$$

tandis que pour estimer la somme relative à $\tau^2(f_2(\xi_1 b,d))$ nous oublions la condition $m_0|b$ car m_0 n'est pas toujours sans facteur carré. Cela nous coûtera un facteur $\log M$:

$$\sum_{\substack{(b,c,d)\in P(\xi_1)\\ m_0|(b,c)}} \tau^2(f_2(\xi_1 b,d)) \ll \frac{M^3}{\xi_1^2 m_0}(\log M)^3 H_{2,d_2}(\xi_1).$$

En reportant cela dans E_{11}^* et en profitant de l'inégalité $\tilde{\varrho}_f(k\ell) \leqslant \tilde{\varrho}_f(k)\tilde{\varrho}_f(\ell)$, on en déduit :

(8·13)
$$\begin{aligned} E_{11}^* &\ll M^3(\log M)^3 \sum_{m_0<M^{1-\varepsilon}} \frac{\tilde{\varrho}_{f_1}(m_0)}{m_0} \sum_{\Delta<\xi_1\leqslant M^{1-\varepsilon}} \frac{\mu^2(\xi_1)H_{2,d_2}(\xi)}{\xi_1^2}\\ &\ll \frac{M^3(\log M)^4}{\Delta}\prod_{p<M}\Big(1+\frac{H_{2,d_2}(p)}{p}\Big)\\ &\ll M^3\Delta^{-1}(\log M)^5. \end{aligned}$$

Il reste à majorer E_{12}^*. Lorsque $Q_1 > \xi_1 m_0 > M^{1-\varepsilon}$, le Lemme 7.3 ne s'applique plus car les intervalles sur b et c sont de longueur trop petite. Nous ignorons alors la condition $m_1'|f_1(\xi_1 b,\xi_1 c)$. Cependant d parcourt toujours un intervalle de longueur M. On majore la fonction $\tau(f_2(\xi_1 b,d))$ par un $O(M^\varepsilon)$:

$$
\begin{aligned}
E_{12}^* &\ll M^\varepsilon \sum_{\substack{\xi_1>\Delta\\ M^{1-\varepsilon}\leqslant m_0\xi_1\leqslant Q_1}} \mu^2(\xi_1)\tilde\varrho_{f_1}(m_0\xi_1) \sum_{m_1'<Q_1/m_0\xi_1} \tilde\varrho_{f_1}(m_1') \sum_{\substack{(b,c,d)\in P(\xi_1)\\ m_0|(b,c)}} 1\\
&\ll M^\varepsilon \sum_{\substack{\xi_1>\Delta\\ M^{1-\varepsilon}\leqslant m_0\xi_1\leqslant Q_1}} \mu^2(\xi_1)\tilde\varrho_{f_1}(m_0\xi_1)\frac{Q_1}{\xi_1 m_0}\Big(1+\frac{M^2}{m_0^2\xi_1^2}\Big)M \ll Q_1M^{1+\varepsilon}.
\end{aligned}
\tag{8·14}
$$

Il se peut qu'avec plus d'attention on puisse remplacer le terme M^ε par une puissance de log notamment en utilisant les travaux d'Henriot [29] qui fournissent des majorations de valeurs moyennes de fonctions arithmétiques d'argument polynomial avec un contrôle explicite du discriminant du polynôme considéré.

On obtient finalement grâce à (8·13) et (8·14)

$$E_1^* \ll M^3(\log M)^5\Delta^{-1} + Q_1M^{1+\varepsilon}.$$

On élimine de la même manière la condition $(b,d,m_2)=1$:

$$
|G^*(\Omega_1,\Omega_2)\cap P\cap\Psi_{m_3}| = \sum_{(b,c,d)\in G(\Omega_1,\Omega_2)\cap P\cap\Psi_3} \sum_{\substack{\xi_1|(b,c,m_1)\\ \xi_2|(b,d,m_2)\\ \xi_1<\Delta}} \mu(\xi_1)\mu(\xi_2)+E_1(m_1,m_2).
\tag{8·15}
$$

Comme $(m_1,m_2)=1$, $(\xi_1,\xi_2)=1$ également. Soit E_2^* la contribution des $\xi_2>\Delta$. On montre avec les mêmes arguments que ceux utilisés pour la majoration de E_1^* :

$$E_2^* \ll M^3(\log M)^7\Delta^{-1} + Q_2M^{1+\varepsilon}.
\tag{8·16}$$

Il faut cependant signaler que la preuve de (8·16) est un peu plus longue car il y a deux variables supplémentaires : ξ_2 et disons m_0' le pgcd $(b\xi_2^{-1}, c\xi_2^{-1}, m_2\xi_2^{-1})$. On rencontrera au paragraphe 8.5 une situation similaire.

8·4. Utilisation de réseaux de $\mathbb{Z}^3$

Dans la suite nous supposons donc que $\xi_i\leqslant\Delta$ pour $i=1,2$. On a ainsi :

$$
\begin{aligned}
|G^*(\Omega_1,\Omega_2)\cap P\cap\Psi_{m_3}| =& \sum_{\substack{\xi_1|m_1\\ \xi_1\leqslant\Delta}}\sum_{\substack{\xi_2|m_2\\ \xi_2\leqslant\Delta}} \mu(\xi_1\xi_2)|\{(\xi_1\xi_2b,\xi_1c,\xi_2d)\in G(\Omega_1,\Omega_2)\cap P\cap\Psi_{m_3}\}|\\
&+ O(E_1^*(m_1,m_2)+E_2^*(m_1,m_2)),
\end{aligned}
$$

par définition ; on vient de voir que la contribution des termes $E_1^*(m_1,m_2)$, $E_2^*(m_1,m_2)$ est assez petite. Cependant dans la ligne ci-dessus, l'entier b peut maintenant être nul. La contribution issue de $b=0$ est négligeable. On peut la majorer par :

$$
\sum_{\xi_1,\xi_2\leqslant\Delta}\sum_{\substack{m_1<Q_1/\xi_1\\ m_2<Q_2/\xi_2}} \mu^2(\xi_1\xi_2)\prod_{i=1,2}\tilde\varrho_{f_i}(m_i\xi_i)\Big(1+\frac{M}{\xi_im_i}\Big) \ll (M+Q_1)(M+Q_2)(\log M)^4.
\tag{8·17}
$$

Comme $(m_1,m_2)=1=(m_3,m_1m_2)$, on a :

$$
\begin{aligned}
|G^*(\Omega_1,\Omega_2)\cap P\cap\Psi_{m_3}| =& \sum_{\substack{\xi_1|m_1\\ \xi_1\leqslant\Delta}}\sum_{\substack{\xi_2|m_2\\ \xi_2\leqslant\Delta}} \mu(\xi_1\xi_2)|\{(b,c,d)\in P(\xi_1,\xi_2)\cap\Psi'_{m_3}:\\
&c\equiv\Omega_1\xi_2b\,(\mathrm{mod}\,m_1/\xi_1),\ d\equiv\Omega_2\xi_1b\,(\mathrm{mod}\,m_2/\xi_2)\}|\\
&+ O(E_1^*(m_1,m_2)+E_2^*(m_1,m_2)),
\end{aligned}
$$

où $\Psi'_{m_3} = \{(b,c,d) \in \mathbb{Z}^3 : b \equiv \overline{\xi_1\xi_2}u \,(\mathrm{mod}\, m_3),\ c \equiv \overline{\xi}_1 v \,(\mathrm{mod}\, m_3),\ d \equiv \overline{\xi}_2 w \,(\mathrm{mod}\, m_3)\}$ et $P(\xi_1,\xi_2)$ est le pavé

$$P(\xi_1,\xi_2) =]B(\xi_1\xi_2)^{-1}, (B+M)(\xi_1\xi_2)^{-1}]\times]C\xi_1^{-1}, (C+M)\xi_1^{-1}]\times]D\xi_2^{-1}, (D+M)\xi_2^{-1}].$$

Pour (b,c,d) tel que $(\xi_1\xi_2 b, \xi_1 c, \xi_2 d) \in G(\Omega_1,\Omega_2) \cap P \cap \Psi_{m_3}$, il existe deux entiers λ_1 et λ_2 tels que

$$\xi_1 c = \Omega_1\xi_1\xi_2 b + \lambda_1 m_1 \text{ et } \xi_2 d = \Omega_2\xi_1\xi_2 b + \lambda_2 m_2. \tag{8·18}$$

Soient u', v', w' compris entre 1 et m_3 tels que $u' \equiv \overline{\xi_1\xi_2}u \,(\mathrm{mod}\, m_3)$, $v' \equiv \overline{\xi}_1 v \,(\mathrm{mod}\, m_3)$, et $w' \equiv \overline{\xi}_2 w \,(\mathrm{mod}\, m_3)$. On écrit alors $b = u' + \beta m_3$, $c = v' + \gamma m_3$, $d = w' + \delta m_3$. Nos contraintes sur b,c,d deviennent à l'aide de (8·18) :

$$v' + \gamma m_3 = \Omega_1\xi_2(u' + \beta m_3) + \lambda_1\frac{m_1}{\xi_1},\ w' + \delta m_3 = \Omega_2\xi_1(u' + \beta m_3) + \lambda_2\frac{m_2}{\xi_2}.$$

On représente cela de la manière suivante :

$$m_3\begin{pmatrix}\beta\\ \gamma\\ \delta\end{pmatrix} \in P(\xi_1,\xi_2) - \begin{pmatrix}u'\\ v'\\ w'\end{pmatrix}$$

avec

$$m_3\begin{pmatrix}\beta\\ \gamma\\ \delta\end{pmatrix} = \begin{pmatrix}0\\ \Omega_1\xi_2 u' - v'\\ \Omega_2\xi_1 u' - w'\end{pmatrix} + \beta m_3\begin{pmatrix}1\\ \Omega_1\xi_2\\ \Omega_2\xi_1\end{pmatrix} + \lambda_1\begin{pmatrix}0\\ \frac{m_1}{\xi_1}\\ 0\end{pmatrix} + \lambda_2\begin{pmatrix}0\\ 0\\ \frac{m_2}{\xi_2}\end{pmatrix}.$$

Cela impose alors

$$\lambda_1\frac{m_1}{\xi_1} \equiv v' - \Omega_1\xi_2 u' \,(\mathrm{mod}\, m_3) \text{ et } \lambda_2\frac{m_2}{\xi_2} \equiv w' - \Omega_2\xi_1 \,(\mathrm{mod}\, m_3).$$

Cela nous amène à poser pour $i = 1, 2$, $\lambda_i = \nu_i + \mu_i m_3$ avec $0 \leqslant \nu_1, \nu_2 < m_3$ et

$$\nu_1\frac{m_1}{\xi_1} \equiv v' - \Omega_1\xi_2 u' \,(\mathrm{mod}\, m_3) \text{ et } \nu_2\frac{m_2}{\xi_2} \equiv w' - \Omega_2\xi_1 \,(\mathrm{mod}\, m_3).$$

Il existe ainsi deux entiers t_1 et t_2 tels que

$$t_1 m_3 = \nu_1\frac{m_1}{\xi_1} + \Omega_1\xi_2 u' - v' \text{ et } t_2 m_3 = \nu_2\frac{m_2}{\xi_2} + \Omega_2\xi_1 - w'.$$

On obtient alors

$$m_3\begin{pmatrix}\beta\\ \gamma\\ \delta\end{pmatrix} \in P(\xi_1,\xi_2) - \begin{pmatrix}u'\\ v'\\ w'\end{pmatrix}$$

pour

$$m_3\begin{pmatrix}\beta\\ \gamma\\ \delta\end{pmatrix} = \begin{pmatrix}0\\ t_1 m_3\\ t_2 m_3\end{pmatrix} + \beta m_3\begin{pmatrix}1\\ \Omega_1\xi_2\\ \Omega_2\xi_1\end{pmatrix} + \mu_1 m_3\begin{pmatrix}0\\ \frac{m_1}{\xi_1}\\ 0\end{pmatrix} + \mu_2 m_3\begin{pmatrix}0\\ 0\\ \frac{m_2}{\xi_2}\end{pmatrix}.$$

En divisant par m_3 on arrive à

$$\beta\begin{pmatrix}1\\ \Omega_1\xi_2\\ \Omega_2\xi_1\end{pmatrix}+\mu_1\begin{pmatrix}0\\ \frac{m_1}{\xi_1}\\ 0\end{pmatrix}+\mu_2\begin{pmatrix}0\\ 0\\ \frac{m_2}{\xi_2}\end{pmatrix}\in P''(\xi_1,\xi_2), \tag{8·19}$$

avec

$$P''(\xi_1,\xi_2)=]B_1'',B_2''[\times]C_1'',C_2''[\times]D_1'',D_2''[$$

où

$$]B_1'',B_2''[=\Big]\frac{B}{m_3\xi_1\xi_2}-\frac{u'}{m_3},\frac{(B+M)}{m_3\xi_1\xi_2}-\frac{u'}{m_3}\Big[, \tag{8·20}$$

$$]C_1'',C_2''[=\Big]\frac{C}{m_3\xi_1}-\frac{v'}{m_3}-t_1,\frac{(C+M)}{m_3\xi_1}-\frac{v'}{m_3}-t_1\Big[, \tag{8·21}$$

$$]D_1'',D_2''[=\Big]\frac{D}{m_3\xi_2}-\frac{w'}{m_3}-t_2,\frac{(D+M)}{m_3\xi_2}-\frac{w'}{m_3}-t_2\Big[. \tag{8·22}$$

La correspondance entre les triplets (b,c,d) tels que $(\xi_1\xi_2 b,\xi_1 c,\xi_2 d)\in G(\Omega_1,\Omega_2)\cap P\cap\Psi_3$ et les (β,μ_1,μ_2) que nous venons de construire est bijective. On a donc :

$$1=|\Lambda\cap P''(\xi_1,\xi_2)|, \tag{8·23}$$

$$\sum_{\substack{(b,c,d)\in P(\xi_1,\xi_2)\cap\Psi'_{m_3}\\ c\equiv\Omega_1\xi_2 b\,(\mathrm{mod}\,m_1\xi_1^{-1})\\ d\equiv\Omega_2\xi_1 b\,(\mathrm{mod}\,m_2\xi_2^{-1})}}$$

où Λ est le réseau (ou sous-réseau) de $\mathbb{Z}^3$ dont une base est

$$\begin{pmatrix}1\\ \Omega_1\xi_2\\ \Omega_2\xi_1\end{pmatrix},\ \begin{pmatrix}0\\ m_1/\xi_1\\ 0\end{pmatrix},\ \begin{pmatrix}0\\ 0\\ m_2/\xi_2\end{pmatrix}.$$

Le déterminant de ce réseau est $m_1m_2/(\xi_1\xi_2)$. Il admet une base (e_1,e_2,e_3) formée des minima successifs pour ce réseau. C'est-à-dire : pour $i=1,2,3$, $\|e_i\|=\lambda_i$ où λ_i est la borne inférieure des λ positifs tels qu'il existe i vecteurs du réseau Λ indépendants et de norme inférieure ou égale à λ. (Cette propriété est vérifiée par tous les réseaux de dimension $\leqslant 4$ cf. [43]).

Lemme 8.2(Minkowski). *Les minima successifs λ_i d'un réseau de dimension n vérifient*

$$\lambda_1\cdots\lambda_r\leqslant(\gamma_n^r)\,\mathrm{dét}(\Lambda)^{r/n}\qquad(1\leqslant i\leqslant n),$$

où γ_n est la constante d'Hermite.

On trouvera une définition de la constante d'Hermite et une présentation de ce théorème dans de nombreux ouvrages sur les réseaux comme par exemple dans le livre de Martinet [43] à la page 44 pour la constante d'Hermite et page 50 pour le théorème de Minkowski. On peut également consulter le chapitre VIII du livre de Cassels [11]. Pour $n=3$, $\gamma_3^3=2$, ainsi les vecteurs de notre base vérifient :

(8·24)

$$\|e_1\|\leqslant\Big(\frac{2m_1m_2}{\xi_1\xi_2}\Big)^{1/3},\ \|e_1\|\|e_2\|\leqslant\Big(\frac{2m_1m_2}{\xi_1\xi_2}\Big)^{2/3},\ \Big(\frac{m_1m_2}{\xi_1\xi_2}\Big)\leqslant\|e_1\|\|e_2\|\|e_3\|\leqslant 2\Big(\frac{m_1m_2}{\xi_1\xi_2}\Big).$$

La minoration de $\|e_1\|\|e_2\|\|e_3\|$ résulte de l'inégalité de Hadamard (cf. par exemple [43] p. 40) : le produit des normes des vecteurs d'une base d'un réseau est supérieur ou égal au déterminant de ce réseau.

Le lemme suivant est une sorte de généralisation du Lemme 2.1 de [12] et est probablement un résultat classique sur les réseaux. Il ne servira finalement pas vraiment dans cet article mais pourra peut-être être utile dans d'autres situations.

Lemme 8.3. *Soit $(e_1, \dots, e_n)$ un base d'un réseau de $\mathbb{Z}^n$ formée de vecteurs minimaux. On note $\langle\ ,\ \rangle$ le produit scalaire euclidien. On a l'inégalité :*

$$\max_{1 \leqslant i < j \leqslant n} \frac{|\langle e_i, e_j \rangle|}{\|e_i\| \|e_j\|} \leqslant \frac{1}{2}. \tag{8·25}$$

Preuve. Soient $1 \leqslant i < j \leqslant n$ donnés.

Notons $c = \frac{1}{\|e_i\|}\langle e_i, e_j \rangle$. Il existe $k \in \mathbb{Z}$ tel que $|c - k\|e_i\|| \leqslant \frac{\|e_i\|}{2}$. Si $k = 0$ convient, alors

$$\frac{|\langle e_i, e_j \rangle|}{\|e_i\| \|e_j\|} = \frac{|c|}{\|e_j\|} \leqslant \frac{\|e_i\|}{2\|e_j\|} \leqslant \frac{1}{2},$$

puisque $\|e_i\| \leqslant \|e_j\|$. L'inégalité (8·25) est bien vérifiée dans ce cas. Si k ne peut pas être nul, alors soit $e'_j = e_j - ke_i$. On peut écrire e_j sous la forme $e_j = c\frac{e_i}{\|e_i\|} + w_j$ avec $\langle w_j, e_i \rangle = 0$. On a alors $e'_j = (c - k\|e_i\|)\frac{e_i}{\|e_i\|} + w_j$. On en déduit que

$$\|e'_j\|^2 = \big|c - k\|e_i\|\big|^2 + \|w_j\|^2 \leqslant \frac{\|e_i\|^2}{4} + \|w_j\|^2 < c^2 + \|w_j\|^2 = \|e_j\|^2.$$

Le système $(e_1, \dots, e_{j-1}, e'_j, e_{j+1}, \dots, e_n)$ est une base du réseau avec un vecteur e'_j de norme strictement inférieure à $\|e_j\|$ ce qui contredit le fait que $(e_1, \dots, e_n)$ soit une base formée de vecteurs minimaux. Cela termine la preuve du Lemme 8.3.

Il est naturel d'approcher le cardinal de (8·23) par la mesure de Lebesgue du volume associé à ce cardinal. En dimension 2 l'erreur ainsi créée est un O du périmètre. En dimension supérieure à 3 on dispose du résultat de Davenport suivant :

Théorème 8.4(Davenport [14]). *Soit $\mathcal{R}$ un sous-ensemble compact de $\mathbb{R}^n$. Notons $N(\mathcal{R})$ le nombre de points de $\mathcal{R}$ à coordonnées entières et $V(\mathcal{R})$ le volume de $\mathcal{R}$. On suppose que $\mathcal{R}$ vérifie les deux conditions suivantes :*

(i) Toute droite parallèle à l'un des n axes de coordonnées a une intersection avec $\mathcal{R}$ soit vide soit composée d'au plus h intervalles.

(ii) Pour tout $1 \leqslant m \leqslant n-1$, la propriété (i) reste vraie (avec $m \leqslant n$) pour toute région de $\mathbb{R}^n$ obtenue en projetant $\mathcal{R}$ sur un sous-espace défini en prenant $n - m$ coordonnées égales à 0.

On a alors

$$|N(\mathcal{R}) - V(\mathcal{R})| \leqslant \sum_{m=0}^{n-1} h^{n-m} V_m,$$

où V_m est la somme des volumes de dimension m formés par les projections de $\mathcal{R}$ sur les différents sous espaces obtenus en imposant $m - n$ coordonnées égales à 0, et $V_0 = 1$ par convention.

Nous nous inspirons de l'application de ce théorème donnée dans l'article de Belabas [2] (voir également [3]) pour un volume bien plus complexe que le notre. Dans notre cas $h = 1$ est admissible. Signalons que dans le cas de volumes plus compliqués, Belabas et Fouvry ([2], [3]) règlent cette difficulté en rappelant si $\mathcal{R}$ est un compact défini par un nombre fini d'inégalités polynomiales alors le nombre h vérifiant les conditions (i) et (ii) du Théorème 8.4 est borné par une constante ne dépendant que des polynômes définissant $\mathcal{R}$. (voir par exemple [1, Théorème 2.3.4 et Proposition 4.4.5]).

Nous appliquons le Théorème 8.4 à

$$\mathcal{R} = \{(x_1, x_2, x_3) \in \mathbb{R}^3 : x_1e_1 + x_2e_2 + x_3e_3 \in P''(\xi_1, \xi_2)\}.$$

Notons Φ l'application de $\mathbb{R}^3$ dans lui même qui envoie la base canonique de $\mathbb{R}^3$ sur la base (e_1, e_2, e_3). On approche alors $N(\mathcal{R})$ par

$$\begin{aligned} V(\mathcal{R}) &= \iiint_{\mathbb{R}^3} \mathbf{1}_{(P''(\xi_1,\xi_2))}(\Phi(x_1,x_2,x_3))\,\mathrm{d}x_1\,\mathrm{d}x_2\,\mathrm{d}x_3 = \frac{\xi_1\xi_2\mathrm{vol}(P''(\xi_1,\xi_2))}{m_1m_2} \\ &= \frac{M^3}{m_1m_2m_3^3\xi_1\xi_2}. \end{aligned} \tag{8·26}$$

Pour obtenir le terme principal de (8·2), on somme sur Ω_1, Ω_2, puis sur ξ_1 et sur ξ_2 le terme principal de (8·26). En remarquant que le nombre de Ω_i vaut $\varrho^*_{f_i}(m_i)/\varphi(m_i)$, on obtient pour ce terme lorsque $(m_1, m_2) = 1$:

$$\frac{M^3}{m_1m_2m_3^3}\sum_{\substack{\xi_1|m_1\\ \xi_2|m_2}} \frac{\mu(\xi_1)\mu(\xi_2)}{\xi_1\xi_2}\frac{\varrho^*_{f_1}(m_1)\varrho^*_{f_2}(m_2)}{\varphi(m_1)\varphi(m_2)} = M^3\frac{\varrho^*_{f_1}(m_1)\varrho^*_{f_2}(m_2)}{m_1^2m_2^2m_3^3},$$

ce qui correspond au terme annoncé dans (8·2). Dans ce calcul, on a oublié la contrainte $\xi_1, \xi_2 \leqslant \Delta$. L'erreur faite ainsi a une contribution globale (c'est-à-dire en la sommant sur m_1 et sur m_2) en $O(M^3m_3^{-3}\Delta^{-1}(\log M)^4)$ puisque

$$\sum_{m_1<Q_1}\frac{\varrho^*_{f_1}(m_1)}{m_1\varphi(m_1)}\sum_{\substack{\xi_1>\Delta\\ \xi_1|m_1}}\frac{\mu^2(\xi_1)}{\xi_1} \ll \Delta^{-1}\sum_{m_1<Q_1}\frac{\tau(m_1)\varrho^*_{f_1}(m_1)}{m_1\varphi(m_1)} \ll \Delta^{-1}(\log Q_1)^2,$$

la dernière égalité pouvant se déduire par exemple du Corollaire III.3.6 p. 436 du livre de Tenenbaum [51] combiné avec le résultat de Nagell sur les moyennes de fonctions $\tilde{\varrho}_{f_i}$ ([44]).

8·5. Majorations des volumes V_m

Maintenant on évalue la contribution des termes V_m issus du Théorème 8.4. Pour $i = 0, 1, 2$ on définit ainsi :

$$\Xi_i := \sum_{m_1,m_2,\xi_1,\xi_2,\Omega_1,\Omega_2} V_i. \tag{8·27}$$

Pour $i = 0$, $V_0 = 1$. En utilisant le Lemme 7.2 on obtient

$$\Xi_0 = \sum_{m_1,m_2,\xi_1,\xi_2,\Omega_1,\Omega_2} V_0 \ll Q_1Q_2(\log M)^4. \tag{8·28}$$

Pour Ξ_1 et Ξ_2 nous profitons du fait que notre volume $\mathcal{R}$ soit un parallélépipède et nous nous inspirons des travaux de [12], ou [26], [40], [41], [6], [7], [8], [10]. Notons $\{u_1, u_2, u_3\}$ la base canonique de $\mathbb{R}^3$ puis $f_i = \Phi^{(-1)}(u_i)$ pour $i = 1, 2, 3$. Avec ces notations on a :

$$\begin{aligned} \mathcal{R} &= \Phi^{(-1)}(P''(\xi_1,\xi_2)) \\ &= \{\lambda_1f_1 + \lambda_2f_2 + \lambda_3f_3 : (\lambda_1,\lambda_2,\lambda_3) \in P''(\xi_1,\xi_2)\}. \end{aligned}$$

Pour Ξ_1, $V_1 = |\cup_{i=1}^3 \mathcal{V}_i|$, où $\mathcal{V}_i$ est la projection de $\mathcal{R}$ sur la droite engendrée par u_i. Si on note $|\mathcal{V}_i|$ la mesure de Lebesgue de $\mathcal{V}_i$ et $\delta(\mathcal{R})$ le diamètre de $\mathcal{R}$ on a

$$|\mathcal{V}_i| \leqslant \delta(\mathcal{R}).$$

Comme le diamètre de $\mathcal{R}$ est du même ordre de grandeur que la longueur de la plus longue arête de $\mathcal{R}$ on a :

$$\begin{aligned} V_1 &\ll \max((B_2''-B_1'')\|f_1\|,(C_2''-C_1'')\|f_2\|,(D_2''-D_1'')\|f_3\|) \\ &\ll \frac{M}{m_3\min(\xi_1,\xi_2)}\max(\|f_1\|,\|f_2\|,\|f_3\|). \end{aligned} \tag{8·29}$$

Pour $i=1,2,3$, les coordonnées de f_i dans la base canonique sont données par la i ème colonne de la matrice de $\Phi^{(-1)}$ dans la base canonique. Par exemple pour f_1, si on note (e_{1i},e_{2i},e_{3i}) les coordonnées de e_i dans la base canonique on a :

$$f_1=\frac{1}{\det\Phi}\begin{pmatrix}\begin{vmatrix}e_{22}&e_{23}\\e_{32}&e_{33}\end{vmatrix}\\ -\begin{vmatrix}e_{21}&e_{23}\\e_{31}&e_{33}\end{vmatrix}\\ \begin{vmatrix}e_{21}&e_{22}\\e_{31}&e_{32}\end{vmatrix}\end{pmatrix}.$$

Ainsi,

$$\|f_i\|\ll\frac{1}{\det\Phi}\max_{(j,k)\in\{1,2,3\}^2}\|e_j\wedge e_k\|\ll\frac{1}{\|e_1\|},$$

puisque $\det\Phi\gg\|e_1\|\|e_2\|\|e_3\|$ et $\|e_1\|\leqslant\|e_2\|\leqslant\|e_3\|$. On en déduit :

$$V_1\ll\frac{M}{\|e_1\|m_3\min(\xi_1,\xi_2)}. \tag{8·30}$$

On commence par évaluer la contribution à Ξ_1 des réseaux avec $e_{11}\neq 0$. Notons Ξ_1^* cette quantité :

$$\Xi_1^*=\sum_{\substack{m_1<Q_1\\m_2<Q_2\\(m_1,m_2)=1}}\sum_{\substack{\xi_1|m_1\\\xi_1\leqslant\Delta}}\sum_{\substack{\xi_2|m_2\\\xi_2\leqslant\Delta}}\mu^2(\xi_1)\mu^2(\xi_2)\sum_{\substack{\Omega_1,\Omega_2\\e_{11}\neq0}}\frac{M}{\|e_1\|m_3\min(\xi_1,\xi_2)}.$$

Pour chaque ξ_1,ξ_2, on définit

$$Z(\xi_1,\xi_2):=\sum_{\substack{m_1<Q_1,\ m_2<Q_2\\\xi_1|m_1,\ \xi_2|m_2\\(m_1,m_2)=1}}\sum_{\substack{\Omega_1,\Omega_2\\e_{11}\neq0}}\frac{1}{\|e_1\|},$$

les entiers Ω_1,Ω_1 sont ceux tels que pour $i=1,2$, $0\leqslant\Omega_i<m_i$, $(\Omega_i,m_i)=1$, $f_i(1,\Omega_i)\equiv 0\,(\mathrm{mod}\,m_i)$ et e_1 soit un vecteur (court) du réseau associé à (Ω_1,Ω_2). Rappelons que chaque réseau de $\mathbb{Z}^n$ possède au plus 3^n vecteurs minimaux. Cela nous permettra d'intervertir certaines sommations sans perte substantielle.

Si $e_1=(e_{11},e_{21},e_{31})\in\mathbb{Z}^3$, alors les $m_1,m_2,\Omega_1,\Omega_2$, tels que e_1 soit un vecteur du réseau Λ associé, sont liés par

$$\Omega_1\xi_2e_{11}\equiv e_{21}\,(\mathrm{mod}\,m_1/\xi_1)\text{ et }\Omega_2\xi_1e_{11}\equiv e_{31}\,(\mathrm{mod}\,m_2/\xi_2). \tag{8·31}$$

On effectue ensuite un découpage dyadique suivant la taille de $\|e_1\|$:

$$Z(\xi_1,\xi_2)\leqslant\sum_{k:2^k\leqslant\left(\frac{2Q_1Q_2}{\xi_1\xi_2}\right)^{1/3}}\frac{Z_k(\xi_1,\xi_2)}{2^k},$$

avec

$$Z_k(\xi_1,\xi_2)=\sum_{\substack{e_1\in\mathbb{Z}^3\\e_{11}\neq0\\2^k<\|e_1\|\leqslant2^{k+1}}}\sum_{\substack{m_1<Q_1\\m_2<Q_2\\\xi_1|m_1,\ \xi_2|m_2}}\prod_{i=1}^{2}\sum_{\substack{1\leqslant\Omega_i<m_i\\(\Omega_i,m_i)=1\\f_i(1,\Omega_i)\equiv0\,(\mathrm{mod}\,m_i)\\e_{(i+1)1}\equiv\xi_{3-i}\Omega_ie_{11}\,(\mathrm{mod}\,m_i/\xi_i)}}1.$$

On montre ensuite le lemme

Lemme 8.5. *Pour tout $\varepsilon > 0$, on l'inégalité*

$$Z_k(\xi_1,\xi_2) \ll 2^{3k}(\log M)^4 \tilde{\varrho}_{f_1}(\xi_1)\tilde{\varrho}_{f_2}(\xi_2)\big(H_{2,d_1}(\xi_2)+H_{2,d_2}(\xi_1)\big)+M^{\varepsilon}2^{2k},$$

où les fonctions $H_{2,d}$ sont celles définies au Lemme 7.3

Preuve du Lemme 8.5.

Pour évaluer ces quantités nous devons tenir compte des pgcd $(e_{11},e_{21},m_1/\xi_1)$ et $(e_{11},e_{31},m_2/\xi_2)$ que nous noterons m_{01}, m_{02} respectivement.

Ainsi pour chaque ξ_1,ξ_2, on a la majoration :

(8·32)

$$Z_k(\xi_1,\xi_2) \leqslant \sum_{\substack{e_1\in\mathbb{Z}^3\\ e_{11}\neq 0\\ 2^k<\|e_1\|\leqslant 2^{k+1}}} \sum_{\substack{m_{01}|(e_{11},e_{21})\\ m_{02}|(e_{11},e_{31})}} \sum_{\substack{m_1'\leqslant \frac{Q_1}{\xi_1 m_{01}}\\ m_2'\leqslant \frac{Q_2}{\xi_2 m_{02}}\\ (m_1',\frac{e_{11}}{m_{01}},\frac{e_{21}}{m_{01}})=1\\ (m_2',\frac{e_{11}}{m_{02}},\frac{e_{31}}{m_{02}})=1}} \prod_{i=1}^{2} \sum_{\substack{1\leqslant\Omega_i<m_{0i}m_i'\xi_i\\ (\Omega_i,m_{0i}m_i'\xi_i)=1\\ f_i(1,\Omega_i)\equiv 0\,(\mathrm{mod}\, m_i'm_{0i}\xi_i)\\ e_{(i+1)1}\equiv\xi_{3-i}\Omega_i e_{11}\,(\mathrm{mod}\, m_i')}} 1.$$

Comme au paragraphe 8.3, on observe que pour e_1,m_{01},ξ_1,ξ_2 donnés, le nombre de couples $(m_1',\,\Omega_1)$ intervenant dans (8·32) est inférieur à

$$\tilde{\varrho}_{f_1}(\xi_1 m_{01})\tau(f_1(\xi_2 e_{11}m_{01}^{-1},e_{21}m_{01}^{-1}).$$

On a une majoration analogue pour les couples (m_2',Ω_2). On en déduit :

$$Z_k(\xi_1,\xi_2) \leqslant \sum_{\substack{2^k<\|e_1\|\leqslant 2^{k+1}\\ e_{11}\neq 0}} \sum_{\substack{m_{01}|(e_{11},e_{21})\\ m_{02}|(e_{11},e_{31})}} \prod_{i=1}^{2} \tilde{\varrho}_{f_i}(\xi_i m_{0i})\tau(f_i(e_{11}\xi_{3-i}m_{0i}^{-1},e_{(i+1)1}m_{0i}^{-1})).$$

On procède ensuite de la même façon qu'au paragraphe 8.3. On note $Z_k^{(1)}(\xi_1,\xi_2)$ la contribution à $Z_k(\xi_1,\xi_2)$ apportée par les $m_{01},m_{02}<2^{k(1-\varepsilon)}$ et $Z_k^{(2)}(\xi_1,\xi_2)$ celle par les m_{01},m_{02} tels que $\max(m_{01},m_{02})\geqslant 2^{k(1-\varepsilon)}$. On majore $Z_k^{(1)}(\xi_1,\xi_2)$ à l'aide du Lemme 7.3 en profitant du fait que le produit des deux fonctions diviseurs est inférieur à la somme des carrés de ces fonctions :

$$\begin{aligned} Z_k^{(1)}(\xi_1,\xi_2) &\ll \sum_{\substack{m_{01}<2^{k(1-\varepsilon)}\\ m_{02}<2^{k(1-\varepsilon)}}} 2^{3k}(\log M)^3 \frac{\tilde{\varrho}_{f_1}(\xi_1 m_{01})\tilde{\varrho}_{f_2}(\xi_2 m_{02})}{m_{01}m_{02}}\Big(\frac{H_{2,d_1}(\xi_2)}{m_{01}}+\frac{H_{2,d_2}(\xi_1))}{m_{02}}\Big)\\ &\ll 2^{3k}(\log M)^4\tilde{\varrho}_{f1}(\xi_1)\tilde{\varrho}_{f_2}(\xi_2)(H_{2,d_1}(\xi_2)+H_{2,d_2}(\xi_1)). \end{aligned}$$

Pour $Z_k^{(2)}(\xi_1,\xi_2)$, on remarque que pour $\varepsilon<1/2$:

$$\min(m_{01},m_{02}) \ll 2^{k/2} < 2^{k(1-\varepsilon)} \leqslant \max(m_{01},m_{02}).$$

Cela est dû au fait que m_{01} et m_{02} sont deux entiers premiers entre eux qui divisent e_{11} avec $e_{11}\ll 2^k$. On majore les produits de différentes fonctions multiplicatives rencontrées par $O(M^{\varepsilon})$ avec $\varepsilon>0$ arbitrairement petit :

$$Z_k^{(2)}(\xi_1,\xi_2) \ll M^{\varepsilon} \sum_{m_{01}<2^{k(1-\varepsilon)}\leqslant m_{02}} \frac{2^{2k}}{m_{01}m_{02}}\Big(1+\frac{2^k}{m_{01}m_{02}}\Big) \ll M^{\varepsilon}2^{2k}.$$

Cela termine la preuve du Lemme 8.5.
En reportant cela dans $Z(\xi_1,\xi_2)$ puis dans Ξ_1^* et en sommant sur les différentes variables, on obtient

$$\Xi_1^* \ll M m_3^{-1} (\log M)^6 (Q_1Q_2)^{2/3}\Delta^{1/3} + M^{1+\varepsilon}(Q_1Q_2)^{1/3}\Delta^{2/3} m_3^{-1}. \tag{8·33}$$

C'est cette étape qui a rendu nécessaire l'introduction du paramètre Δ.

Avant d'examiner la contribution à Ξ_1 des réseaux tels que $e_{11}=0$, nous commençons l'étude de celle des termes V_2 issus du Théorème 8.4 : $V_2 = |\cup_{i=1}^3 \mathcal{W}_i|$ où maintenant $\mathcal{W}_i$ est la projection de $\mathcal{R}$ sur le plan engendré par u_j, u_k avec $\{i,j,k\}=\{1,2,3\}$. Notons p_i cette projection. Pour tout $\Omega \in \mathcal{R}$ il existe un point Ω' du bord de $\mathcal{R}$ tel que $p_i(\Omega)=p_i(\Omega')$. On en déduit qu'il suffit d'étudier les images par p_i des faces de $\mathcal{R}$. Notons F_{12} l'une des faces parallèles au plan engendré par f_1 et f_2 :

$$F_{12} = \{\lambda_1 f_1 + \lambda_2 f_2 + D_1'' f_3 : (\lambda_1,\lambda_2) \in [B_1'', B_2''] \times [C_1'', C_2'']\}.$$

Pour l'autre face, on remplace D_1'' par D_2''. Les éléments de $p_1(F_{12})$ ont des coordonnées de la forme :

$$\lambda_1 \begin{pmatrix} 0 \\ f_{21} \\ f_{31} \end{pmatrix} + \lambda_2 \begin{pmatrix} 0 \\ f_{22} \\ f_{32} \end{pmatrix} + D_1'' \begin{pmatrix} 0 \\ f_{23} \\ f_{33} \end{pmatrix}, \quad (\lambda_1,\lambda_2) \in [B_1'', B_2''] \times [C_1'', C_2''].$$

On en déduit que $s_{1,12}$ la surface de $p_1(F_{12})$ vaut :

$$(B_2''-B_1'')(C_2''-C_1'')|f_{21}f_{32}-f_{31}f_{22}|.$$

En profitant des liens entre les coordonnées des vecteurs e_i et f_j puis de (8·24), on observe que

$$\begin{aligned} s_{1,12} &= (B_2''-B_1'')(C_2''-C_1'')\frac{|e_{31}|}{\det \Phi} \\ &\ll \frac{(B_2''-B_1'')(C_2''-C_1'')}{\|e_2\|\|e_3\|} \leqslant \frac{(B_2''-B_1'')(C_2''-C_1'')}{\|e_1\|\|e_2\|}. \end{aligned}$$

On obtient des majorations analogues pour toutes les projections des différentes faces de $\mathcal{R}$ et on a finalement :

$$V_2 \ll \frac{M^2}{m_3^2 \xi_1\xi_2 \|e_1\|\|e_2\|}. \tag{8·34}$$

On règle maintenant la contribution à Ξ_2 des réseaux dont le vecteur associé e_1 a sa première coordonnée e_{11} non nulle. On effectue un découpage dyadique sur les normes des vecteurs e_1 et e_2. En utilisant (8·24) et en notant Ξ_2^* la somme portant sur les $e_{11}\neq 0$, on a :

$$\Xi_2^* \ll \sum_{\xi_1,\xi_2} \frac{\mu^2(\xi_1\xi_2)}{\xi_1\xi_2} \sum_{\substack{k_1,k_2\in\mathbb{N},\ k_1\leqslant k_2 \\ 2^{k_1}\leqslant \left(\frac{2Q_1Q_2}{\xi_1\xi_2}\right)^{1/3} \\ 2^{k_1+k_2}\leqslant \left(\frac{2Q_1Q_2}{\xi_1\xi_2}\right)^{2/3}}} \frac{M^2}{m_3^2 2^{k_1+k_2}} \sum_{m_1,m_2} \sum_{\Omega_1,\Omega_2} \mathbf{1}_{]2^{k_1},2^{k_1+1}]}(\|e_1\|)\mathbf{1}_{]2^{k_2},2^{k_2+1}]}(\|e_2\|),$$

où e_1 avec $e_{11} \neq 0$, e_2 sont les deux premiers vecteurs minimaux d'une base de Λ.

On majore cela en utilisant les sommes $Z_k(\xi_1, \xi_2)$:

$$\Xi_2^* \ll \sum_{\substack{\xi_1 \leqslant \Delta \\ \xi_2 \leqslant \Delta}} \sum_{\substack{k_1,k_2 \in \mathbb{N},\ k_1 \leqslant k_2 \\ 2^{k_1} \leqslant \left(\frac{2Q_1Q_2}{\xi_1\xi_2}\right)^{1/3} \\ 2^{k_1+k_2} \leqslant \left(\frac{2Q_1Q_2}{\xi_1\xi_2}\right)^{2/3}}} \frac{M^2\mu^2(\xi_1\xi_2)Z_{k_1}(\xi_1,\xi_2)}{m_3^2\xi_1\xi_2 2^{k_1+k_2}}.$$

On applique ensuite le Lemme 8.5 :

$$\Xi_2^* \ll M^2(Q_1Q_2)^{1/3}(\log M)^4 m_3^{-2} + M^{2+\varepsilon}m_3^{-2}.$$

Il reste à étudier les contributions à Ξ_1 et Ξ_2 des réseaux dont le premier vecteur e_1 a sa première coordonnée e_{11} nulle. Notons Ξ_i' ces contributions. Nous devons être plus soigneux pour Ξ_1' que pour Ξ_2' car dans Ξ_1' l'une des variables ξ_1 ou ξ_2 a un poids plus important : la majoration de Ξ_1' fera intervenir Δ contrairement à celle de Ξ_2'.

Si $e_{11} = 0$ alors on a :

$$e_{21} \equiv 0 \,(\mathrm{mod}\, \frac{m_1}{\xi_1}),\ e_{31} \equiv 0 \,(\mathrm{mod}\, \frac{m_2}{\xi_2}).$$

Or $\|e_1\| \leqslant (2m_1m_2/(\xi_1\xi_2))^{1/3}$. Le vecteur e_1 a donc une seule coordonnée non nulle. Comme sa norme est minimale, il n'y a que quatre possibilités pour e_1 :

$$e_1 \in \Big\{\big(0, \pm\frac{m_1}{\xi_1}, 0\big), \big(0, 0, \pm\frac{m_2}{\xi_2}\big)\Big\}.$$

Nous choisissons de ne traiter que le cas $e_1 = (0, m_1/\xi_1, 0)$, les cas restants étant similaires.

Comme e_2 est un vecteur court, $|e_{22}| < \frac{m_1}{\xi_1} = \|e_1\|$. Les conditions sur e_1, e_2, e_3 entraînent encore :

$$\|e_2\|^2 \leqslant \|e_2\|\|e_3\| \leqslant \frac{2m_2}{\xi_2} \leqslant \frac{2Q_2}{\xi_2}. \tag{8·35}$$

Cette inégalité ne servira que pour Ξ_2'. Commençons par majorer Ξ_1'.

La majoration (8·30) n'est pas tout à fait suffisante dans le cas où $\min(\xi_1, \xi_2) = \xi_2$. On utilise plutôt la première inégalité de (8·29). Comme

$$f_3 = \frac{\xi_1\xi_2}{m_1m_2}\begin{pmatrix} e_{12}e_{23} - e_{22}e_{13} \\ \frac{e_{13}m_1}{\xi_1} \\ -\frac{e_{12}m_1}{\xi_1} \end{pmatrix},$$

on en déduit que $\|f_3\| \ll \frac{\xi_1\xi_2}{m_1m_2}\|e_1\|\|e_3\| \ll \frac{1}{\|e_2\|}$. En insérant cela dans la première inégalité de (8·29), on obtient

$$V_1 \ll \frac{M}{m_3\xi_1\|e_1\|} + \frac{M}{m_3\xi_2\|e_2\|}. \tag{8·36}$$

La contribution à Ξ_1' des termes en $\frac{M}{m_3\xi_1\|e_1\|}$ est inférieure à

$$\sum_{\substack{\xi_1,\xi_2 \leqslant \Delta \\ \mu^2(\xi_1\xi_2)=1}} \sum_{\substack{m_2 < Q_2 \\ \xi_2 | m_2}} \tilde{\varrho}_{f_2}(m_2) \sum_{\substack{m_1 < Q_1 \\ \xi_1 | m_1}} \frac{M\tilde{\varrho}_{f_1}(m_1)}{m_3m_1} \ll \frac{MQ_2(\log M)^3}{m_3}. \tag{8·37}$$

Nous évaluons maintenant celle des termes en $\frac{M}{m_3\xi_2\|e_2\|}$.

Comme précédemment nous faisons un découpage dyadique de $\|e_1\|$ et $\|e_2\|$. Rappelons que $|e_{22}| < \|e_1\|$.

On doit alors majorer :

$$Y := \sum_{\xi_1,\xi_2\leqslant\Delta} \mu^2(\xi_1\xi_2) \sum_{\substack{k_1,k_2\in\mathbb{N},\ k_1\leqslant k_2\\ 2^{k_1+k_2}\leqslant\left(\frac{2Q_1Q_2}{\xi_1\xi_2}\right)^{2/3}\\ 2^{k_1}\leqslant\left(\frac{2Q_1Q_2}{\xi_1\xi_2}\right)^{1/3}}} \frac{M}{m_3 2^{k_2}\xi_2} \sum_{\substack{e_2=(e_{12},e_{22},e_{32})\\ |e_{22}|\ll 2^{k_1}\\ \max(|e_{12}|,|e_{32}|)\ll 2^{k_2}}} u(e_2), \tag{8·38}$$

où $u(e_2)$ est le nombre de quadruplets $(m_1, m_2, \Omega_1, \Omega_2)$ tels que $\xi|m_i$, $m_i < Q_i$ pour $i = 1, 2$ et

$$0 \leqslant \Omega_i < m_i,\ (\Omega_i, m_i) = 1,\ f_i(1, \Omega_i) \equiv 0 \,(\mathrm{mod}\, m_i),$$

$\|e_1\| = m_1/\xi_1 \in]2^{k_1}, 2^{k_1+1}]$, et satisfaisant les congruences :

$$e_{22} \equiv \xi_2 e_{12}\Omega_1 \,(\mathrm{mod}\, m_1/\xi_1),\ e_{32} \equiv \xi_1 e_{12}\Omega_2 \,(\mathrm{mod}\, m_2/\xi_2).$$

Les entiers m_1/ξ_1, m_2/ξ_2 divisent respectivement $f_1(\xi_2 e_{12}, e_{22})$ et $f_2(\xi_1 e_{12}, e_{32})$. Il y en a au plus $O(M^\varepsilon)$. Une fois que les entiers m_1, m_2 sont fixés, il y a au plus $O(M^\varepsilon)$ couples (Ω_1, Ω_2). Ainsi

$$u(e_2) \ll M^\varepsilon. \tag{8·39}$$

Cependant pour avoir un résultat du type (8·33), il faut être un peu plus précis. En suivant la preuve du Lemme 8.5 avec le vecteur e_2 à la place de e_1, on arrive à

$$\sum_{e_2} u(e_2) \ll 2^{k_1+2k_2}(\log M)^4 \tilde{\varrho}_{f_1}(\xi_1)\tilde{\varrho}_{f_2}(\xi_2)(H_{2,d_1}(\xi_2) + H_{2,d_2}(\xi_1)) + M^\varepsilon 2^{k_1+k_2}.$$

En reportant cela dans (8·38), on obtient une majoration analogue de Y analogue à (8·33).

Passons maintenant à Ξ_2'. On a :

$$\Xi_2' \ll \sum_{\xi_1,\xi_2<\Delta} \frac{\mu^2(\xi_1\xi_2)}{\xi_1\xi_2} \sum_{\substack{m_1<Q_1\\ m_2<Q_2\\ \xi_i|m_i}} \frac{M^2}{m_3^2\|e_1\|\|e_2\|} \sum_{\Omega_1,\Omega_2} 1,$$

où les Ω_1, Ω_2 vérifient les conditions décrites précédemment.

On effectue de nouveau des découpages dyadiques $\|e_2\|$ et sur $\|e_1\| = m_1/\xi_1$ mais cette fois-ci on utilise (8·35) :

$$\Xi_2' \ll \frac{M^{2+\varepsilon}}{m_3^2} \sum_{\xi_1,\ \xi_2<\Delta} \frac{\mu^2(\xi_1\xi_2)}{\xi_1\xi_2} \sum_{k_1\leqslant k_2\leqslant\frac{\log(2Q_2/\xi_2)}{2\log 2}} \frac{1}{2^{k_1+k_2}} \sum_{\substack{e_{12},\ e_{32}\ll 2^{k_2}\\ e_{22}\ll 2^{k_1}}} u(e_2),$$

où on a repris la notation $u(e_2)$ de (8·38). Ici la majoration (8·39) est suffisante et on obtient

$$\Xi_2' \ll \frac{M^{2+\varepsilon}}{m_3^2} \sum_{\xi_1,\xi_2<\Delta} \frac{\mu^2(\xi_1\xi_2)}{\xi_1\xi_2} \sum_{k_1\leqslant k_2\leqslant\frac{\log(2Q_2)/(\xi_2)}{2\log 2}} \frac{1}{2^{k_1+k_2}} \sum_{\substack{e_{12},e_{22}\ll 2^k\\ e_{32}\leqslant 2^\mu}} 1 \ll \frac{M^{2+\varepsilon}\sqrt{Q_1}}{m_3^2}. \tag{8·40}$$

En tenant compte des différents termes d'erreurs obtenus, on trouve pour $\Delta < M^{1-\varepsilon}$:

(8·41)
$$E \ll M^3\Big(\frac{(\log M)^7}{\Delta}\Big) + M^{1+\varepsilon}(Q_1+Q_2) + Q_1Q_2(\log M)^4 + \frac{M^2(\log M)^5(Q_1Q_2)^{1/3}}{m_3^2}$$
$$+ \frac{M(Q_1Q_2)^{2/3}\Delta^{1/3}(\log M)^6}{m_3} + \frac{M^{1+\varepsilon}(Q_1Q_2)^{1/3}\Delta^{2/3}}{m_3}$$
$$+ M^{2+\varepsilon} + \frac{M^{2+\varepsilon}}{m_3^2}(\sqrt{Q_1}+\sqrt{Q_2}).$$

On termine la preuve du Théorème 8.1 en prenant

$$\Delta = \min(M^{3/2}(Q_1Q_2)^{-1/2}m_3^{3/4}, M^{1-\varepsilon}).$$

9. Les unités de $\mathbb{Q}(\zeta_{12})$.

Notons E le groupe de unités de $\mathbb{Q}(\zeta_{12})$. Il est de rang 1 et ainsi isomorphe à $\mathbb{Z}\times W$ où $W = \{\zeta_{12}^j : 0 \leqslant j < 12\}$ est le groupe des racines de l'unité contenues dans $\mathbb{Q}(\zeta_{12})$. Il reste à trouver une unité fondamentale. L'élément $1+\zeta_{12}$ semble être un bon candidat. Le plus grand sous-corps réel contenu dans $\mathbb{Q}(\zeta_{12})$ est $\mathbb{Q}(\sqrt{3})$ dont une unité fondamentale est $\sqrt{3}+2$. (On pourra remarquer que $\sqrt{3}+2 = (1+\zeta_{12})(1+\zeta_{12}^{-1}) = \zeta_{12}^{-1}(1+\zeta_{12})^2$.) Soit E^+ le groupe des unités de $\mathbb{Q}(\sqrt{3})$ et $WE^+ = \{wu : w \in W \text{ et } u \in E^+\}$. Alors $[E : WE^+] = 1$ ou 2 (cf. Theorem 4.12 p. 39 de [52]). En fait ici, $[E : WE^+] = 2$ ([52] Corollary 4.13. p. 39). On en déduit que $E = WE^+ \cup \varepsilon WE^+$, cette union étant disjointe et $\varepsilon \in E \smallsetminus WE^+$. On choisit $\varepsilon = 1+\zeta_{12}$, cela prouve que $1+\zeta_{12}$ est une unité fondamentale.

Comme $\mathbb{Q}(\zeta_{12}) = \mathbb{Q}(i)(\sqrt{3})$, $N(\alpha) = N_{\mathbb{Q}(i)/\mathbb{Q}} \circ N_{\mathbb{Q}(\zeta_{12})/\mathbb{Q}(i)}(\alpha) = |N_{\mathbb{Q}(\zeta_{12})/\mathbb{Q}(i)}(\alpha)|^2 \geqslant 0$.

Nous considérerons dans la suite les idéaux J ayant un générateur $J = (u)$, $u = u_1 + u_2\zeta_{12} + u_3\zeta_{12}^2 + u_4\zeta_{12}^3$ vérifiant :

$$1 \leqslant \frac{|u|^2}{N(u)^{1/2}} < 2+\sqrt{3}. \tag{9·1}$$

Lemme 9.1. *Soit $\alpha \in \mathbb{Z}[\zeta_{12}]$ vérifiant* (9·1)*. Il y a alors au plus 12 éléments $\alpha' \in \mathbb{Z}[\zeta_{12}]$ vérifiant* (9·1) *tels que $(\alpha) = (\alpha')$.*

Preuve. On suppose qu'il existe $\alpha = a+b\zeta_{12}+c\zeta_{12}^2+d\zeta_{12}^3$ et $\alpha' = a'+b'\zeta_{12}+c'\zeta_{12}^2+d'\zeta_{12}^3$ deux éléments de $\mathbb{Z}[\zeta_{12}]$ vérifiant (9·1) tels que $(\alpha) = (\alpha')$. Il existe alors deux entiers k, ℓ tels que $\alpha = \zeta_{12}^k(1+\zeta_{12})^\ell\alpha'$.

On en déduit que $|\alpha^2| = (\sqrt{3}+2)^\ell|\alpha'|^2$.

Comme α, α' vérifient (9·1), cela entraîne que $\ell = 0$. Ainsi $\alpha' = \zeta_{12}^{-k}\alpha$ ce qui fait au plus 12 possibilités pour α'.

Remarque : $|\alpha|^2 = a^2+b^2+c^2+d^2+ac+bd+\sqrt{3}(ab+bc+cd)$.

10. L'ensemble $\mathcal{J}$ des idéaux

Nous sommes maintenant en mesure de décrire l'ensemble $\mathcal{A}_1$ évoqué dans (3·3). Soit $\mathcal{J}$ l'ensemble des idéaux (α), $\alpha = a + b\zeta_{12} + c\zeta_{12}^2 + d\zeta_{12}^3$ où a, b, c, d sont des entiers vérifiant la série de conditions suivantes. La première est relative à la fonction ϱ définie par (3·1) :

$$\varrho(\alpha) = 1. \tag{10·1}$$

Pour contrôler le nombre d'entiers $\alpha \in \mathbb{Z}[\zeta_{12}]$ engendrant le même idéal, on impose :

$$1 \leqslant \frac{|\alpha|^2}{N(\alpha)^{1/2}} < 2 + \sqrt{3}. \tag{10·2}$$

On suppose que $(b, c, d) \in \mathcal{C}$, où $\mathcal{C}$ est le sous-ensemble des triplets de $\mathbb{Z}^3$ défini par les contraintes suivantes. Tout d'abord les entiers $q = q(b, c, d) = \prod_{i=1}^{3} q_i(b, c, d)$, (on rappelle que q_1, q_2, q_3 sont les formes définies par (5·5) et (5·6)) vérifient*

$$P^-(q) > 256 \text{ et } (q, B_{13}B_{14}) = 1. \tag{10·3}$$

La deuxième condition est que q soit un entier sans facteur carré. La troisième est que $q = q_1(b, c)q_2(b, d)q_3(b, c, d)$ peut se factoriser sous la forme

$$q_1(b, c) = q_{11}q_{12}q_{13},\ q_2(b, d) = q_{21}q_{22}q_{23},\ q_3(b, c, d) = q_{31}q_{32},$$

où q_{11}, q_{12}, q_{21}, q_{22}, q_{31} sont des nombres premiers tels que pour $(i, j) \in \{1, 2, 3\} \times \{1, 2\} \setminus \{(3, 2)\}$ on ait :

$$q_{ij} \in [X^{\vartheta_{ij}}, X^{\vartheta_{ij}+\tau_{ij}}],$$

ϑ_{ij} et τ_{ij} étant des réels strictement positifs qui seront précisés dans la suite. Signalons déjà que nous choisirons ces paramètres de sorte que les intervalles $[X^{\vartheta_{ij}}, X^{\vartheta'_{ij}}]$ avec $\vartheta'_{ij} = \vartheta_{ij} + \tau_{ij}$ soient deux à deux disjoints.

Reprenant les notations de [24] nous posons pour un paramètre $\alpha_0 > 0$ qui sera choisi à la fin :

$$M = X^{1/4} \text{ et } N = X^{\frac{1+\alpha_0}{4}}. \tag{10·4}$$

On suppose alors que les coordonnées de α vérifient pour un paramètre $\beta_0 > 0$ que l'on précisera également ultérieurement :

$$|B_{14}| \geqslant M^3 X^{-2\beta_0},\ q \geqslant M^6 X^{-\beta_0}. \tag{10·5}$$

Nous ajoutons une condition sur c, d, q qui n'est pas absolument nécessaire mais simplifiera certaines étapes :

$$(c, d) = (cd, q) = 1. \tag{10·6}$$

On suppose que les idéaux de $\mathcal{J}$ peuvent se factoriser sous la forme $(\alpha) = KL$ avec (cf. [24] p. 559)

$$X < N(KL) \leqslant X^{1+\alpha_0}, \tag{10·7}$$

* La condition $(q, B_{14}) = 1$ est nécessaire à l'application du Lemme 6.2. On a rajouté la condition $(q, B_{13}) = 1$ uniquement pour simplifier l'évaluation du terme S_0 défini à la fin de ce paragraphe.

où K est un idéal premier vérifiant

$$X^{4\alpha_0} < N(K) \leqslant X^{5\alpha_0}. \tag{10·8}$$

Conformément aux notations de [24], nous notons $\mathcal{K}$ l'ensemble de tels idéaux K, puis pour $K \in \mathcal{K}$ donné, $\mathcal{L}(K)$ la famille formée par les idéaux L qui conviennent c'est-à-dire les idéaux $KL = (\alpha)$ vérifiant toutes les conditions précédentes. La famille (ou suite) $\mathcal{L}(K)$ peut alors contenir des répétitions, ce nombre de répétitions étant le nombre de générateurs α d'un KL, vérifiant (10·1), (10·2) et les conditions relatives aux entiers q correspondants (il y en a au plus 12 d'après le Lemme 9.1). On notera aussi $\mathcal{I}(K)$ la famille avec d'éventuelles répétitions formée par les idéaux KL avec $L \in \mathcal{L}(K)$.

Nous imposons une condition supplémentaire pour les idéaux L. Il faut que L soit un idéal tel que $P^-(N(L)) \geqslant z := X^{\vartheta_0}$ avec $\vartheta_0 > 0$ que nous choisirons plus tard. Cette dernière condition assure qu'un élément de $\mathbb{Q}[\zeta_{12}]$ de la forme $n - \zeta_{12}$, $X < n \leqslant 2X$, appartient à au plus $[\alpha_0^{-1}]2^{[4\vartheta_0^{-1}]}$ idéaux de type KL.

Avec ces deux conditions, $P^+(N(KL)) \leqslant \max(X^{1-3\alpha_0}, X^{5\alpha_0}) \leqslant X$ si $\alpha_0 \leqslant 1/5$. Cela entraîne que pour $n - \zeta_{12} \in (\alpha)$,

$$\log^{(1)}(\Phi_{12}(n)) = \log^{(1)}(N((n-\zeta_{12})) \geqslant \log(N(KL)) \geqslant \log X,$$

et ainsi $n \in \mathcal{A}$.

Notre ensemble $\mathcal{A}_1$ est alors :

$$\mathcal{A}_1 = \{n \in]X, 2X] : \exists J \in \mathcal{J},\ n - \zeta_{12} \in J\}.$$

Il s'agit maintenant de minorer le cardinal de cet ensemble. D'après le Lemme 9.1 et en vertu de nos différentes conditions sur les facteurs premiers des idéaux KL, on a la minoration suivant les notations (3·5) et (3·6)

$$|\mathcal{A}_1| \geqslant \frac{\alpha_0 2^{-[4/\vartheta_0]}}{12} \sum_{J \in \mathcal{J}} |A_J|. \tag{10·9}$$

On rappelle l'approximation :

$$|A_J| = X\frac{\varrho(J)}{N(J)} + R_J.$$

La condition $P^-(N(L)) \geqslant X^{\vartheta_0}$ se détecte avec un crible linéaire. On reprend les poids $\{\lambda_d^-\}$ du crible linéaire de Rosser-Iwaniec pour un crible de niveau $X^{3\vartheta_0}$ (voir [35] ou [36] par exemple). Rappelons que si $\lambda_d^- \neq 0$ alors $d \leqslant X^{3\vartheta_0}$ et $d | \prod_{p<X^{\vartheta_0}} p$. En prenant

$$\alpha_0 > 3\vartheta_0/4, \tag{10·10}$$

on s'assure que $(N(K), d) = 1$ lorsque $\lambda_d^- \neq 0$.

Pour $z \geqslant 2$, on définit $P(z) = \prod_{p<z} p$. On obtient alors

$$|\mathcal{A}_1| \geqslant \frac{\alpha_0 2^{-[4/\vartheta_0]}}{12}(XS_0 + S_1),$$

avec

$$S_0 = \sum_{K\in\mathcal{K}} \sum_{L\in\mathcal{L}(K)} \Big(\sum_{\substack{d|N(L)\\ d|P(X^{\vartheta_0})}} \lambda_d^- \Big) \frac{\varrho(KL)}{N(KL)} \text{ et } S_1 = \sum_{K\in\mathcal{K}} \sum_{L\in\mathcal{L}(K)} \Big(\sum_{\substack{d|N(L)\\ d|P(X^{\vartheta_0})}} \lambda_d^- \Big) R_{KL}.$$

Nous devons montrer que $S_1 = o(X)$ et trouver un réel $\kappa > 0$ tel que $S_0 \geqslant \kappa$.

On termine ce paragraphe par un lemme assurant que les coordonnées des α tels que $(\alpha) \in \mathcal{J}$ ne peuvent être de taille trop grande.

Lemme 10.1. *Soit $\alpha = a + b\zeta_{12} + c\zeta_{12}^2 + d\zeta_{12}^3$ vérifiant* (10·2) *et* (10·7). *Alors en utilisant les notation de* (10·4) *on a :*

$$\max(|a|, |b|, |c|, |d|) \ll N.$$

Preuve. Pour $\alpha = a + b\zeta_{12} + c\zeta_{12}^2 + d\zeta_{12}^3$, on a

$$\alpha = a + b\frac{\sqrt{3}}{2} + \frac{c}{2} + i\Big(\frac{b + c\sqrt{3}}{2} + d\Big)$$

et

$$|\alpha|^2 = \Big(a + \frac{b\sqrt{3} + c}{2}\Big)^2 + \Big(\frac{b + c\sqrt{3}}{2} + d\Big)^2. \tag{10·11}$$

Soit $\alpha_3 = \sigma_3(\alpha)$ où σ_3 est le plongement $\sigma_3 : u + \sqrt{3}w \mapsto u - \sqrt{3}w$ avec $u, w \in \mathbb{Z}[i]$. Ainsi,

$$\alpha_3 = a + \frac{c - b\sqrt{3}}{2} + i\Big(d + \frac{b - c\sqrt{3}}{2}\Big) \text{ et } |\alpha_3|^2 = \Big(a + \frac{c - \sqrt{3}b}{2}\Big)^2 + \Big(d + \frac{b - c\sqrt{3}}{2}\Big)^2. \tag{10·12}$$

Or $N(\alpha) = |\alpha|^2|\alpha_3|^2$, ainsi (10·2) devient

$$|\alpha_3|^2 \leqslant |\alpha|^2 \leqslant (2 + \sqrt{3})^2|\alpha_3|^2.$$

En reportant cela dans la contrainte $N(\alpha) \leqslant X^{1+\alpha_0}$, cela implique que

$$\max(|\alpha_3|^4, |\alpha|^4) \leqslant (2 + \sqrt{3})^2 X^{1+\alpha_0}.$$

On en déduit à l'aide de (10·11) et (10·12) que

$$\max(|a + \frac{c}{2}|, |b|, |d + \frac{b}{2}|, |c|) \ll N,$$

puis le lemme.

Remarque. Les arguments de la preuve de ce lemme permettent de montrer que si (a, b, c, d) vérifient (10·2) alors

$$\max(|a|, |b|, |c|, |d|) \ll N(\alpha)^{1/4}. \tag{10·13}$$

Notation. On notera $\mathcal{R} \subset \mathbb{R}^4$ la région définie par les différentes conditions "non arithmétiques" sur α : $\mathcal{R}$ est ainsi l'ensemble des $(a, b, c, d) \in \mathbb{R}^4$ vérifiant (10·2), (10·5) et

$$M^4 \leqslant N(\alpha) < N^4. \tag{10·14}$$

11. Premières transformations de S_0 et S_1

Dans cette partie nous adaptons les manipulations faites au paragraphe 4 de [24]. En reprenant pas à pas les arguments de Heath-Brown [24] page 568, on vérifie alors que le terme S_0 devient

$$S_0 = \sum_{K\in\mathcal{K}} \sum_{L\in\mathcal{L}(K)} \sum_{A|L} \lambda^-_{N(A)} \frac{\varrho(KL)}{N(KL)}. \tag{11·1}$$

La somme sur A ci-dessus porte sur les idéaux A non divisibles par deux idéaux premiers de même norme et dont tous les idéaux premiers sont de norme un nombre premier appartenant à $]3, X^{\vartheta_0}[$. Rappelons que $\lambda^-_{N(A)} = 0$ si $N(A) > X^{3\vartheta_0}$.

On procède de la même manière pour S_1 :

$$S_1 = \sum_{K\in\mathcal{K}} \sum_{A} \lambda^-_{N(A)} \sum_{\substack{L\in\mathcal{L}(K)\\ A|L}} R_{KL}\varrho(KL).$$

On applique ensuite le Lemme 6.1 avec pour K et A fixés tels que $\varrho(KA) = 1$, $\mathcal{E} = \{\alpha : (\alpha) \in \mathcal{I}(K) \text{ et } A|(\alpha)\}$. Ainsi, en profitant également du Lemme 6.2 et en utilisant le fait que $|\mathcal{L}(K)| = |\mathcal{I}(K)|$ on a :

$$S_1 \ll \sum_{K\in\mathcal{K}} \sum_{A} |\lambda^-_{N(A)}| \varrho(KA)(\log H)\Big\{\frac{|\mathcal{L}(K)|}{H} + \sum_{h=1}^{H^2} \min(h^{-1}, Hh^{-2})|S_2(h)|\Big\},$$

avec

$$S_2(h) = \sum_{\substack{(\alpha)\in\mathcal{I}(K)\\ A|(\alpha)}} \mathrm{e}\Big(\frac{-hU\overline{B_{14}}}{q} + \frac{hX'}{N(\alpha)}\Big)\mathrm{e}(hR(a,b,c,d)), \tag{11·2}$$

$R(a,b,c,d)$ étant la fraction rationnelle définie au Lemme 6.2 et $X' = X$ ou $2X$. La contribution du terme en $|\mathcal{L}(K)|/H$ dans le membre de droite de (11·2) est alors $O(X^{1+\alpha_0+3\vartheta_0}H^{-1}\log H)$. Si on écrit $H = X^{\eta_0}$, cela impose

$$\eta_0 > \alpha_0 + 3\vartheta_0. \tag{11·3}$$

D'après nos hypothèses sur a, b, c, d, on a les majorations suivantes :

$$U \ll N^5,\ M^6X^{-\beta_0} \ll |q| \ll N^6,\ B_{13} \ll N^3,\ N(\alpha) \gg M^4 \text{ et} |B_{14}| \gg M^3X^{-2\beta_0}.$$

On en déduit l'approximation :

$$\begin{aligned}\mathrm{e}(hR(a,b,c,d)) &= 1 + O\Big(\Big|\frac{hU}{qB_{14}}\Big| + \Big|\frac{hB_{13}}{N(\alpha)B_{14}}\Big|\Big)\\ &= 1 + O(|h|N^5M^{-9}X^{3\beta_0} + |h|N^3M^{-7}X^{2\beta_0}) = 1 + O(|h|X^{-1+\frac{5\alpha_0}{4}+3\beta_0}).\end{aligned}$$

La contribution de ce terme d'erreur à S_1 est alors inférieure à une constante près à

$$\sum_{K\in\mathcal{K}} \sum_{A:N(A)<X^{3\vartheta_0}} H(\log H)^2|\mathcal{L}(K)|X^{-1+\frac{5\alpha_0}{4}+3\beta_0} \ll H(\log H)^2X^{\frac{9\alpha_0}{4}+3\beta_0+3\vartheta_0},$$

puisque $\sum_{K\in\mathcal{K}} |\mathcal{L}(K)| \ll X^{1+\alpha_0}$. On imposera alors :

$$\frac{9\alpha_0}{4} + 3\beta_0 + \eta_0 + 3\vartheta_0 < 1. \tag{11·4}$$

Comme $\varrho(KA) = 1$, il existe un entier j tel que $\zeta_{12} \equiv j \,(\mathrm{mod}\, KA)$. Cet entier j ne dépend que de KA. La condition $KA|(\alpha)$ est alors équivalente à (on s'inspire de [24] page 570) :

$$\begin{aligned}a &\equiv -bj - cj^2 - dj^3 \,(\mathrm{mod}\, N(KA))\\ &\equiv a(b,c,d,KA) \,(\mathrm{mod}\, N(KA)).\end{aligned}$$

12. Majoration de sommes d'exponentielles très courtes

Dans ce paragraphe on obtient une majoration de S_1 en fonction des paramètres $\alpha_0, \beta_0, \eta_0, \vartheta_0, \vartheta_{ij}, \vartheta'_{ij}$ $(i,j) \in \{(1,2)\}^2 \cup \{(3,1)\}$. À la fin de cet article ces paramètres seront choisis de sorte que

$$S_1 = o(X).$$

Pour $(b,c,d) \in \mathbb{R}^3$ donné, on note $\mathcal{D}(b,c,d) = \{a \in \mathbb{R} : (a,b,c,d) \in \mathcal{R}\}$. Ces ensembles $\mathcal{D}(b,c,d)$ sont des unions finies d'intervalles de longueur $O(N)$. Ce nombre d'intervalles est borné par une constante indépendante de (b,c,d). En reprenant les observations du paragraphe précédent on a sous les conditions (11·3) et (11·4) :

$$|S_1| \ll \log H \sum_{h=1}^{H^2} \min\Big(\frac{1}{h}, \frac{H}{h^2}\Big) \sum_{K\in\mathcal{K}} \sum_{A} |\lambda^-_{N(A)}| |\varrho(KA)| |S(h,A,K)| + o(X), \tag{12·1}$$

avec

$$S(h,A,K) = \sum_{(b,c,d)\in\mathcal{C}} \sum_{\substack{a\in\mathcal{D}(b,c,d)\\ a\equiv a(b,c,d,K,A) \,(\mathrm{mod}\, N(KA))\\ (B_{13}B_{14},q)=1}} \mathrm{e}\Big(\frac{-hU\overline{B_{14}}}{q} + \frac{hX'}{N(\alpha)}\Big).$$

On traite la condition $(B_{13},q)=1$ en appliquant la formule d'inversion de Möbius (il faut conserver la condition $(B_{14},q)=1$ pour que l'exponentielle soit définie) :

$$\begin{aligned} |S_1| \leqslant \sum_{K\in\mathcal{K},\ A} |\lambda^-_{N(A)}| \log H \sum_{h=1}^{H^2} \min\Big(\frac{1}{h}, \frac{H}{h^2}\Big) \sum_{(b,c,d)\in\mathcal{C}} \sum_{t|q} |\mu(t)| \\ \times \Big| \sum_{\substack{a\in\mathcal{D}(b,c,d)\\ a\equiv a(b,c,d,KA) \,(\mathrm{mod}\, N(KA))\\ t|B_{13}}} \mathrm{e}\Big(\frac{-hU\overline{B_{14}}}{q} + \frac{hX'}{N(\alpha)}\Big)\Big| + o(X). \end{aligned}$$

On vérifie que pour tout $p|t$, B_{13} est un polynôme en a qui n'est pas identiquement nul modulo p. En effet au vu de (4·6), cela n'arrive pour un tel p que si p divise $(c, b^2+2db-c^2, -c^2+d^2+2db)$. Cela entraîne que p divise c et $b(b+2d)$. Donc p^2 divise b^2+c^2 ou $q_3(b,c,d)$ ce qui contredit le fait que q soit sans facteur carré.

Comme B_{13} est un polynôme en a de degré au plus 2, la contrainte $t|B_{13}$ peut se traduire en au plus $2^{\omega(t)}$ congruences de la forme $a \equiv a' \,(\mathrm{mod}\, t)$.

On a ainsi :

$$\sum_{\substack{a\in\mathcal{D}(b,c,d)\\ a\equiv a(b,c,d,KA) \,(\mathrm{mod}\, N(KA))\\ t|B_{13}}} \mathrm{e}\Big(\frac{-hU\overline{B_{14}}}{q} + \frac{hX'}{N(\alpha)}\Big) = \sum_{\sigma\in\mathcal{S}} \sum_{\substack{a\in\mathcal{D}(b,c,d)\\ a\equiv\sigma \,(\mathrm{mod}\, t'N(KA))}} \mathrm{e}\Big(\frac{-hU\overline{B_{14}}}{q} + \frac{hX'}{N(\alpha)}\Big), \tag{12·2}$$

où t' est un diviseur de t et $\mathcal{S}$ un ensemble de classes de congruences modulo $t'N(KA) := [t, N(KA)]$ avec au plus $O(X^{\varepsilon})$ éléments.

On a vu que pour b,c,d donnés, $\mathcal{D}(b,c,d)$ est une union finie d'intervalles de longueur un $O(N)$. Lorsque t' est "grand" disons $t' \geqslant X^{\alpha_0+\varepsilon_1}$, avec $\varepsilon_1 > 0$, on observe que si a,b,c,d sont donnés, il n'y a qu'un nombre fini d'idéaux K divisant $N(\alpha)$. On peut alors majorer

les sommes sur K de (12·2) par un $O\Big(X^{\varepsilon}\Big(1+\frac{N}{t'N(A)}\Big)\Big)$. On vérifie ensuite facilement que la contribution de tels t' est un $o(X)$ si

$$\frac{3\alpha_0}{4}+3\vartheta_0<1/4. \tag{12·3}$$

Dans la suite de ce paragraphe on peut donc supposer que

$$t'\leqslant X^{\alpha_0+\varepsilon_1}, \tag{12·4}$$

pour un $\varepsilon_1>0$ arbitrairement petit. Nous allons nous arranger pour majorer ces sommes à l'aide du résultat fondamental de Heath-Brown ([24], Theorem 2) sur les sommes très courtes d'exponentielles :

Théorème 12.1(Heath-Brown). *Soit $q=q_0q_1\cdots q_k$ un entier positif sans facteur carré. Soient $f(x),g(x)\in\mathbb{Z}[x]$ tels que $\max(\deg(f(x)),\deg(g(x)))\leqslant D$. On suppose que tous les facteurs premiers de q sont supérieurs à 2^kD. De plus pour tout $p|q$, on suppose qu'il n'existe pas de polynôme $h(x)$ de degré inférieur à $k+1$ tel que $f(x)\equiv g(x)h(x)\,(\mathrm{mod}\,p)$. Alors pour tout $\varepsilon>0$, on a :*

$$\sum_{\substack{A<n\leqslant A+B\\(g(n),q)=1}}\mathrm{e}\Big(\frac{wf(n)\overline{g(n)}}{q}\Big)\ll_{k,D,\varepsilon}q^{\varepsilon}\Big(B\Big(\frac{\Delta}{q_0}\Big)^{1/2^{k+1}}+B^{1-\frac{1}{2^k}}\Big(\frac{q_0}{\Delta}\Big)^{\frac{1}{2^{k+1}}}+\sum_{j=1}^{k}B^{1-\frac{1}{2^j}}q_{k+1-j}^{\frac{1}{2^j}}\Big),$$

avec $\Delta=(q_0,w)$.

Cette majoration est pertinente s'il existe $\lambda>0$ tel que $B^{\lambda}<q_0<B^{2-\lambda},q_i<B^{1-\lambda}$ pour $k\geqslant i\geqslant 1$.

Pour $\sigma\in\mathcal{S}$ fixé, on écrit $a=\sigma+mt'N(KA)$ où m appartient maintenant à un ensemble d'au plus $O(X^{\varepsilon})$ intervalles de longueur d'un ordre de grandeur inférieur à $1+N/(t'N(KA))$. Nous appliquons le Théorème 12.1 avec $f(m)=-U(\sigma+mt'N(KA),b,c,d)$ et $g(m)=B_{14}(\sigma+mt'N(KA),b,c,d)$ et $k=7$. Le degré D correspondant est inférieur à 2, il faut donc que $P^-(q)>2^kD=2^8=256$ ce qui est conforme à (10·3). Vérifions maintenant que lorsque $P^-(q)>256$, il n'y a pas de $p|q$ pour lequel il existe un polynôme h de degré au plus 8 tel que

$$U\equiv B_{14}h\,(\mathrm{mod}\,p). \tag{12·5}$$

Lemme 12.2. *On suppose que q est sans facteur carré, $P^-(q)>256$ et que* (10·6) *a lieu. Il n'existe alors pas de polynôme h de degré inférieur à 8 vérifiant* (12·5).

Preuve. Le polynôme U est de degré au plus 1 en a :

$$U=ad(db^2-dc^2-2c^2b+2d^2b)+c(d(-2d^3-6db^2+2dc^2+3c^2b-3b^3-4d^2b)+4c^2b^2)=:a\mu_1+\mu_2.$$

Nous commençons par vérifier que

$$(\mu_1,q)=1. \tag{12·6}$$

Soit $p|q$. D'après (10·6) on a $(p,d)=1$. Observons que $\mu_1=d(2bq_2-(d+2b)q_1)$.

Si $p|q_1$, alors

$$\mu_1 \equiv 2bdq_2 \,(\mathrm{mod}\, p)$$
$$\not\equiv 0 \,(\mathrm{mod}\, p)$$

puisque q est sans facteur carré.

Si $p|q_2$ alors $\mu_1 \equiv -d(d+2b)q_1 \,(\mathrm{mod}\, p)$. Si p divise $d+2b$ alors $q_2 \equiv 3b^2 \,(\mathrm{mod}\, p) \equiv 0 \,(\mathrm{mod}\, p)$, ce qui n'est pas possible. On en déduit que $\mu_1 \not\equiv 0 \,(\mathrm{mod}\, p)$.

Il reste à traiter le cas $p|q_3$. Comme $q_3 = 4q_2 - 3q_1$, $2\mu_1 \equiv dq_1(-b-2d) \,(\mathrm{mod}\, p)$. Or p ne peut pas diviser $b+2d$ (sinon p^2 diviserait q_3), on peut donc également en déduire que $2\mu_1 \not\equiv 0 \,(\mathrm{mod}\, p)$.

Cela termine la preuve de (12·6)

Il reste à vérifier qu'il n'existe pas de polynôme h non nul et de degré inférieur à 8 satisfaisant (12·5) pour un facteur premier p de q.

Soit $p|q$ donné. Comme p ne divise pas d, B_{14} est un polynôme en a de degré 2 tandis que U est de degré inférieur à 1. Comme $p > 256$, il n'existe pas de polynôme non nul h de degré inférieur à 8 tel que $hB_{14} - U$ soit identiquement nul modulo p. Cela termine la preuve du Lemme 12.2.

Soit $t'' = (t'N(KA), q)$. Comme $(B_{14}, q) = 1$, on a $(t'', B_{14}) = 1$. Pour alléger l'écriture nous écrivons U ou $U(a)$ et B_{14} ou $B_{14}(a)$ à la place de $U(a,b,c,d)$ et $B_{14}(a,b,c,d)$ respectivement. Comme q est sans facteur carré, $(t'', q/t'') = 1$. Grâce à (6·3), on a :

$$\mathrm{e}\Big(\frac{hU\overline{B_{14}}}{q}\Big) = \mathrm{e}\Big(\frac{hU\overline{t''B_{14}}}{q/t''} + \frac{hU.\overline{(q/t'')B_{14}}}{t''}\Big).$$

Mais

$$U(\sigma + mt'N(KA))\overline{B_{14}(\sigma + mt'N(KA))} \equiv U(\sigma)\overline{B_{14}(\sigma)} \,(\mathrm{mod}\, t'').$$

Dans cette congruence ci-dessus, le membre de droite ne dépend plus de m. On en déduit pour $\sigma \in \mathcal{S}$ donné l'égalité :

$$\sum_{\substack{a\in\mathcal{D}(b,c,d)\\ a\equiv\sigma \,(\mathrm{mod}\, t'N(KA))}} \mathrm{e}\Big(\frac{-hU\overline{B_{14}}}{q} + \frac{hX'}{N(\alpha)}\Big) = e\Big(\frac{-hU(\sigma)\overline{(q/t'')B_{14}(\sigma)}}{t''}\Big)$$
$$\times \sum_{m\in\mathcal{D}'(b,c,d)} \mathrm{e}\Big(\frac{hf(m)\overline{t''g(m)}}{q/t''} + \frac{hX'}{N(\alpha)}\Big),$$

où f et g sont les polynômes choisis juste après l'énoncé du Théorème 12.1 et $\mathcal{D}'(b,c,d)$ est une union finie d'intervalles de longueur $\ll \frac{N}{N(KA)t'}$. Comme $(t'N(KA), q/t'') = 1$ les polynômes f et g vérifient bien les conditions du Théorème 12.1. L'étape suivante consiste à éliminer le terme $\mathrm{e}\Big(\frac{hX'}{N(\alpha)}\Big)$ à l'aide d'une sommation d'Abel.

D'après (10·13), $\frac{\partial N^{-1}(\alpha)}{\partial a} \ll N(\alpha)^{-5/4} \ll M^{-5}$. La somme sur m ci-dessus est ainsi majorée par un nombre fini de sommes de la forme

(12·7)

$$\sum_{M_1<m\leqslant M_2} \mathrm{e}\Big(\frac{hf(m)\overline{t''g(m)}}{q/t''} + \frac{hX'}{N(\alpha)}\Big) \ll (1 + NXM^{-5}h)$$
$$\times \max_{M_2'\in]M_1,M_2]} \Big|\sum_{M_1<m\leqslant M_2'} \mathrm{e}\Big(\frac{hf(m)\overline{t''g(m)}}{q/t''}\Big)\Big|,$$

avec $M_2 \ll N$ et $M_2 - M_1 \ll 1 + N/(t'N(KA))$. Remarquons déjà que $NXM^{-5} \ll X^{\alpha_0/4}$ et ainsi que $(1 + NXM^{-5}h) \ll X^{\alpha_0/4}h$.

On rappelle que les entiers q sont de la forme $q = q_1(b,c,d)q_2(b,c,d)q_3(b,c,d)$ avec $q_i(b,c,d) = q_{i1}q_{i2}q_{i3}$ pour $i = 1,2$ et $q_3(b,c,d) = q_{31}q_{32}$. Posons $q'_{ij} = q_{ij}/(t'', q_{ij})$. Comme q est sans facteur carré, $q/t'' = \prod_{\substack{1\leqslant i,j\leqslant 3\\(i,j)\neq(3,3)}} q'_{ij}$. Nous appliquons maintenant le Théorème 12.1 avec $k = 7$, et le 8-uplet $(q_0,q_1,q_2,q_3,q_4,q_5,q_6,q_7)$ correspond à $(q'_{32},q'_{31},q'_{11},q'_{21},q'_{22},q'_{12},q'_{13},q'_{23})$. Pour M_1 et M'_2 donnés, notons $M_3 = M'_2 - M_1$. Alors

(12·8)
$$\begin{aligned}\sum_{M_1<m\leqslant M'_2} \mathrm{e}\Big(\frac{hf(m)\overline{t''g(m)}}{q/t''}\Big) \ll X^{\varepsilon}\Big[&M_3\Big(\frac{(h,q'_{32})}{q'_{32}}\Big)^{1/256} + M_3^{127/128}\Big(\frac{q'_{32}}{(q'_{32},h)}\Big)^{1/256}\\ &+ M_3^{1/2}(q'_{23})^{1/2} + M_3^{3/4}(q'_{13})^{1/4} + M_3^{7/8}(q'_{12})^{1/8}\\ &+ M_3^{15/16}(q'_{22})^{1/16} + M_3^{31/32}(q'_{21})^{1/32} + M_3^{63/64}(q'_{11})^{1/64}\\ &+ M_3^{127/128}(q'_{31})^{1/128}\Big].\end{aligned}$$

Notons $W(h)$ le membre de gauche de (12·7). On somme alors sur h ces différents termes. En utilisant la majoration standard (cf. par exemple [24] p. 572) valable pour tout $\ell \in \mathbb{N}^*$:

$$\sum_{h=1}^{H^2} \min\Big(1, \frac{H}{h}\Big)(h,\ell) \ll X^{\varepsilon}H,$$

on obtient :

$$\begin{aligned}\sum_{h=1}^{H^2} \min\Big(\frac{1}{h}, \frac{H}{h^2}\Big)|W(h)| &\ll X^{\alpha_0/4+\varepsilon}H\Big[\frac{M_3}{(q'_{32})^{1/256}} + M_3^{127/128}(q'_{32})^{1/256}\\ &\quad + M_3^{1/2}(q'_{23})^{1/2} + M_3^{3/4}(q'_{13})^{1/4} + M_3^{7/8}(q'_{12})^{1/8}\\ &\quad + M_3^{15/16}(q'_{22})^{1/16} + M_3^{31/32}(q'_{21})^{1/32} + M_3^{63/64}(q'_{11})^{1/64}\\ &\quad + M_3^{127/128}(q'_{31})^{1/128}\Big]\\ &\ll \sum_{i=1}^{9} E_i,\end{aligned}$$

par définition. On note ensuite pour $1 \leqslant i \leqslant 9$, R_i la contribution des E_i pour la majoration de S_1 de sorte que $S_1 \ll \sum_{i=1}^{9} R_i + o(X)$.

En utilisant (10·5) et le fait que $q_1q_2 \ll N^4$, on a avec nos choix de paramètres (on rappelle la notation $\vartheta'_{31} = \vartheta_{31} + \tau_{31}$) :

$$(q'_{32})^{-1/256} \leqslant \Big(\frac{t''}{q_{32}}\Big)^{1/256} \ll \Big(\frac{t''}{M^2X^{-\vartheta'_{31}-\alpha_0-\beta_0}}\Big)^{1/256}.$$

Or $t'' \leqslant t'N(KA) \leqslant X^{\alpha_0+\varepsilon_1}N(KA)$ d'après (12·4). En imposant

$$7\alpha_0 + \beta_0 + 3\vartheta_0 < 1/2, \tag{12·9}$$

on peut utiliser l'encadrement pour t' : $1 \leqslant t' \leqslant M^2X^{-6\alpha_0-\beta_0-3\vartheta_0}$ et en déduire :

$$\frac{M_3}{(q'_{32})^{1/256}} \ll \Big(1 + \frac{N}{t'N(KA)}\Big)\Big(\frac{t'N(KA)}{M^2X^{-\vartheta'_{31}-\alpha_0-\beta_0}}\Big)^{1/256} \ll X^{\frac{\vartheta'_{31}}{256}} + \frac{NX^{\frac{(\vartheta'_{31}+\alpha_0+\beta_0)}{256}}}{M^{\frac{1}{128}}N(KA)^{1-\frac{1}{256}}}.$$

Le nombre total de t', t'' est majoré par une puissance de $\tau(q)$ donc par une puissance de X arbitrairement petite. Les sommes sur b, c, d apportent une contribution inférieure à $O(N^3)$. Comme $N \gg X^{3\vartheta_0+5\alpha_0}$, la contribution sur les idéaux K et A dans les différents R_i est de la forme pour $\varphi \in [0,1[$:

$$\sum_{K\in\mathcal{K}} \sum_{N(A)<X^{3\vartheta_0}} |\lambda^-_{N(A)}| \Big(1+\frac{N}{N(KA)}\Big)^{\varphi} \ll N^{\varphi} X^{(5\alpha_0+3\vartheta_0)(1-\varphi)}, \tag{12·10}$$

(cf. [24] p. 573 pour une situation analogue). En tenant compte de tout cela on obtient

$$R_1 \ll X^{\frac{3}{4}+6\alpha_0+\frac{\vartheta'_{31}}{256}+3\vartheta_0+\eta_0+\varepsilon} + X^{\frac{511}{512}+\frac{5\alpha_0}{4}+\frac{\vartheta'_{31}+6\alpha_0+\beta_0+3\vartheta_0}{256}+\eta_0+\varepsilon}. \tag{12·11}$$

Pour les autres termes nous majorons q'_{ij} par q_{ij} puis (en posant $\vartheta'_{ij} = \vartheta_{ij} + \tau_{ij}$)

$$q_{ij} \ll \begin{cases} X^{\vartheta'_{ij}} & \text{pour } (i,j) \in \{1,2\}^2 \cup \{(3,1)\} \\ N^2 X^{-\vartheta_{i1}-\vartheta_{i2}} & \text{pour } (i,j) \in \{(1,3),(2,3)\} \\ N^2 X^{-\vartheta_{31}} & \text{pour } (i,j) = (3,2). \end{cases} \tag{12·12}$$

Nos termes R_i vérifient alors des majorations de la forme lorsque $i \geqslant 3$:

$$N^3 X^{\varepsilon+\alpha_0/4+\eta_0} N^{\varphi} X^{(5\alpha_0+3\vartheta_0)(1-\varphi)} X^{\vartheta(1-\varphi)} = X^{\varepsilon+\frac{3+\varphi}{4}+\alpha_0(6-\frac{19\varphi}{4})+(3\vartheta_0+\vartheta)(1-\varphi)+\eta_0}, \tag{12·13}$$

avec ϑ tel que le $q_{k\ell}$ associé à R_i vérifie $q_{k\ell} < X^{\vartheta}$. Pour $i = 2$ on a une majoration identique mis à part que le dernier terme du membre de gauche de (12·13) est remplacé par $X^{\vartheta(1-\varphi)/2}$. Dans ce dernier cas, $\varphi = 127/128$ et on peut prendre $\vartheta = \frac{1+\alpha_0}{2} - \vartheta_{31}$ et on obtient :

$$R_2 \ll X^{1+\varepsilon+\frac{165\alpha_0}{128}+\frac{3\vartheta_0}{128}-\frac{\vartheta_{31}}{256}+\eta_0}. \tag{12·14}$$

Pour les termes R_i, $i \geqslant 3$, on prend $\varphi = 1 - 1/2^{i-2}$ et les ϑ sont obtenus avec (12·12). Pour de tels φ, (12·13) est majoré par :

$$X^{1-\frac{1}{2^i}+\varepsilon+\frac{\alpha_0(5.2^{i-2}+19)}{2^i}+\frac{3\vartheta_0}{2^{i-2}}+\eta_0+\frac{\vartheta}{2^{i-2}}}. \tag{12·15}$$

Après une série de calculs, on obtient :

$$\begin{aligned} R_3 &\ll X^{\varepsilon+9/8+31\alpha_0/8+3\vartheta_0/2-(\vartheta_{21}+\vartheta_{22})/2+\eta_0} \\ R_4 &\ll X^{\varepsilon+17/16+41\alpha_0/16+3\vartheta_0/4-(\vartheta_{11}+\vartheta_{12})/4+\eta_0} \\ R_5 &\ll X^{\varepsilon+31/32+59\alpha_0/32+3\vartheta_0/8+\vartheta'_{12}/8+\eta_0} \\ R_6 &\ll X^{\varepsilon+63/64+99\alpha_0/64+3\vartheta_0/16+\vartheta'_{22}/16+\eta_0} \\ R_7 &\ll X^{\varepsilon+127/128+179\alpha_0/128+3\vartheta_0/32+\vartheta'_{21}/32+\eta_0} \\ R_8 &\ll X^{\varepsilon+255/256+339\alpha_0/256+3\vartheta_0/64+\vartheta'_{11}/64+\eta_0} \\ R_9 &\ll X^{\varepsilon+511/512+659\alpha_0/512+3\vartheta_0/128+\vartheta'_{31}/128+\eta_0}. \end{aligned} \tag{12·16}$$

On choisira ces paramètres $\alpha_0, etc.$, de sorte que $R_i = o(X)$ pour $1 \leqslant i \leqslant 9$.

13. Le terme principal S_0 : la somme sur la variable a

Dans ce paragraphe on établit un lemme équivalent au lemme 6 p. 563 de [24]. On rappelle que $\mathcal{R}$ est le domaine de $\mathbb{R}^4$ défini par les conditions (10·2), (10·5) et (10·14). Pour (b,c,d) donnés on considère l'intégrale :

$$I(b,c,d)=\int_{(t,b,c,d)\in\mathcal{R}}\frac{\mathrm{d}t}{N(t,b,c,d)}. \tag{13·1}$$

Lemme 13.1. *Soient g la fonction multiplicative à support sur les entiers sans facteur carré et définie sur les nombres premiers par :*

$$g(p):=|\{P:N(P)=p\}|,$$

et h la fonction définie par :

$$h(n)=\begin{cases}\prod_{p|n}\left(\frac{1-2/p}{1-g(p)/p}\right) & \text{si } n \text{ est sans facteur carré et si } P^-(n)>256\\ 0 & \text{sinon.}\end{cases}$$

On a alors la minoration pour $6\alpha_0+3\vartheta_0<1/4$:

$$S_0\geqslant(C_0+o(1))(\log\frac{5}{4})\prod_{p<X^{\vartheta_0}}\Big(1-\frac{g(p)}{p}\Big)\sum_{(b,c,d)\in\mathcal{C}}I(b,c,d)h(q),$$

avec $C_0=\frac{2}{3}\mathrm{e}^{\gamma}\log 2$.

Remarque. Pour $p\geqslant 5$, on a $g(p)=\begin{cases}4 & \text{si } p\equiv 1\,(\mathrm{mod}\,12)\\ 0 & \text{sinon}\end{cases}$ tandis que $g(2)=g(3)=0$.

Démonstration. On reprend la dernière expression de S_0 donnée par (11·1) :

$$S_0=\sum_{K\in\mathcal{K}}\sum_{L\in\mathcal{L}(K)}\sum_{A|L}\lambda^-_{N(A)}\frac{\varrho(KL)}{N(KL)}.$$

Ensuite on traite la condition $(B_{13}B_{14},q)=1$ à l'aide d'une sommation de Möbius :

$$S_0=\sum_{K\in\mathcal{K}}\sum_{A}\lambda^-_{N(A)}\sum_{(b,c,d)\in\mathcal{C}}\sum_{r|q}\mu(r)\sum_{\substack{a\in\mathcal{D}(b,c,d)\\ r|B_{13}B_{14}\\ KA|(\alpha)}}\frac{1}{N(\alpha)}. \tag{13·2}$$

On note $r=r_1r_2$, avec $r_1=(r,N(KA))$ et $(r_2,N(KA))=1$. Le système de congruences sur a est alors modulo $r_2N(KA)$.

Lemme 13.2. *Soient b,c,d tels que q soit un entier sans facteur carré et premier avec 6. Pour tout p divisant q,*

$$|\{0\leqslant a<p:B_{13}B_{14}\equiv 0\,(\mathrm{mod}\,p)\}|=2. \tag{13·3}$$

Preuve. Notons Δ_{13} et Δ_{14} les discriminants respectifs par rapport à a des polynômes B_{13}, B_{14}. On a alors

$$\Delta_{13}=(b^2+2db-c^2)^2+4c^2(-c^2+d^2+2db)=q_1(b,c)q_3(b,c,d), \tag{13·4}$$

$$(13\cdot5)\quad \Delta'_{14}=\frac{\Delta_{14}}{4}=b^2c^2+d(-b^3-2b^2d-2bd^2+bc^2+dc^2-d^3)=-q_2(b,d)q_4(b,c,d).$$

• On suppose que $p|(b^2+c^2)$. Dans ce cas $\Delta_{13}\equiv 0\,(\mathrm{mod}\,p)$. Effectivement, B_{13} a une racine double modulo p : $\overline{2c}(b^2+2db-c^2)$ qui est une racine de B_{14}. Cependant ce n'est qu'une racine simple de B_{14}, sinon p^2 diviserait $\Delta'_{14}=q_2q_4$. Or d'une part $p\nmid q_2$ car q est sans facteur carré mais il ne divise pas non plus q_4 puisque s'il divise q_1 et $q_4=q_2-q_1$ alors il divise en fait q_2 aussi. Ainsi l'équation par rapport à la variable a, $B_{14}\equiv 0\,(\mathrm{mod}\,p)$ a deux solutions distinctes et on a prouvé (13·3) dans le cas où $p|(b^2+c^2)$.

• Cas où $p|(b^2+db+d^2)$. Dans ce cas $\Delta'_{14}\equiv 0\,(\mathrm{mod}\,p)$. On vérifie ensuite que la racine double de B_{14} est une racine simple de B_{13} et on termine comme dans le premier cas.

• Cas où $p|q_3(b,c,d)$. Alors B_{13} a une racine double et on termine comme dans le premier cas en profitant du fait que $q_3=4q_2-3q_1$. Cela termine la preuve du Lemme 13.2.

Lemme 13.3. *Soit $p\equiv 1\,(\mathrm{mod}\,12)$ et divisant $(q,B_{13}B_{14})$. On a alors :*

$$p|(B_{13},B_{14})\Leftrightarrow p|N(\alpha).$$

Preuve. On suppose que $p|(B_{13},B_{14})$. Rappelons la formule (5.3) :

$$B_{14}(B_{12}+B_{14})-B_{13}^2=(d^2-c^2+db)N(\alpha)=q_4N(\alpha).$$

Cette égalité entraîne que $p|q_4N(\alpha)$. Si $p|q$, il existe $i\in\{1,2,3\}$ tel que $p|q_i$. Comme $q_4=q_2-q_1$ et $q_3=4q_2-3q_1$, si $p|q_4$ alors il existe $j\neq i$ tel que $p|q_j$. Cela n'est pas possible car q est sans facteur carré. Donc p divise $N(\alpha)$.

On vérifie maintenant la réciproque. Soit $p|(q,B_{13}B_{14},N(\alpha))$. On a vu au paragraphe 4 (formule (4.5)) que

$$B_{14}\zeta_{12}\equiv B_{13}\,(\mathrm{mod}\,(\alpha)).$$

Si $p|N(\alpha)$, il existe un idéal $\mathcal{P}$ divisant (α) de norme une puissance de p. La condition $p\equiv 1\,(\mathrm{mod}\,12)$ impose en fait que $N(\mathcal{P})=p$. On a alors :

$$B_{14}\zeta_{12}\equiv B_{13}\,(\mathrm{mod}\,\mathcal{P}).$$

Si $p|B_{13}B_{14}$, $\mathcal{P}$ divise aussi ce produit et donc en fait à la fois B_{13} et B_{14}. On en déduit que $p|(B_{13},B_{14})$. Cela termine la preuve du Lemme 13.3.

Remarque. Si $p\not\equiv 1\,(\mathrm{mod}\,12)$ et divise $(q,B_{13}B_{14})$ alors $p\nmid(B_{13},B_{14})N(\alpha)$.

On retourne à la somme sur a. D'après le théorème des restes chinois, on a :

$$|\{0\leqslant a<r_2N(KA):r|(q,B_{13}B_{14}),\ KA|(\alpha)\}|=\prod_{p|r_2N(KA)}t(p),$$

avec

$$t(p)=\begin{cases}|\{0\leqslant a<p:p|(q,B_{13}B_{14},N(\alpha))\}| & \text{si } p|r_1,\\ |\{0\leqslant a<p:p|(q,B_{13}B_{14})\}| & \text{si } p|r_2,\\ |\{0\leqslant a<p:p|N(\alpha)\}| & \text{si } p|N(KA)/r_1.\end{cases}$$

Comme $\varrho(KA)=1$, tous les facteurs premiers de $N(KA)$ sont congrus à 1 modulo 12. On détermine les valeurs $t(p)$ en utilisant le Lemme 13.2 et le Lemme 13.3 mais aussi les arguments de la preuve du Lemme 13.2 :

$$t(p)=\begin{cases}2 & \text{si } p|r_2,\\ 1 & \text{si } p|N(KA).\end{cases}$$

On en déduit que la somme sur a de (13·2) se ramène à $2^{\omega(r_2)}$ sommes de la forme

$$\sum_{\substack{a\in\mathcal{D}(b,c,d)\\ a\equiv a_0 \,(\mathrm{mod}\, r_2N(KA))}} \frac{1}{N(\alpha)},$$

où a_0 dépend de b, c, d, r, K, A.

D'après la structure de $\mathcal{D}(b,c,d)$, la somme sur a peut alors s'écrire comme un nombre fini de sommes de la forme :

$$\sum_{\substack{a\in[u,v]\\ a\equiv a_0 \,(\mathrm{mod}\, r_2N(KA))}} \frac{1}{N(\alpha)} = \sum_{\lambda\in\left[\frac{u-a_0}{r_2N(KA)},\frac{v-a_0}{r_2N(KA)}\right]} \frac{1}{N(a_0+\lambda r_2N(KA),b,c,d))}.$$

Dans la formule ci-dessus, $N(a_0+\lambda r_2N(KA),b,c,d)$ est la norme de $a+r_2N(KA)\lambda+\zeta_{12}b+\zeta_{12}^2c+\zeta_{12}^3d$. Quitte à découper l'intervalle sur λ en un nombre fini d'intervalles sur lesquels la fonction $\lambda\mapsto N(a_0+\lambda r_2N(KA),b,c,d)$ est monotone, on peut approcher ces sommes par des intégrales en utilisant par exemple le Théorème I.0.4 p. 21 de [51] :

$$\sum_{\substack{a\in[u,v]\\ a\equiv a_0 \,(\mathrm{mod}\, r_2N(KA))}} \frac{1}{N(\alpha)} = \int_{\frac{u-a_0}{r_2N(KA)}}^{\frac{v-a_0}{r_2N(KA)}} \frac{\mathrm{d}\lambda}{N(a_0+\lambda r_2N(KA),b,c,d)} + O\Big((v-u)\max_{u\leqslant t\leqslant v}\Big|\frac{\partial}{\partial t}\frac{1}{N(t,b,c,d)}\Big|\Big).$$

Le terme d'erreur ci-dessus est un $O(NM^{-5})$ puisque $|\frac{\partial}{\partial t}\frac{1}{N(t,b,c,d)}|\ll N(t,b,c,d)^{-5/4}$.

On a alors en reprenant la notation (13·1) :

$$\begin{aligned} S_0 = \sum_{K\in\mathcal{K}}\sum_{A}\lambda^-_{N(A)} \sum_{(b,c,d)\in\mathcal{C}} \sum_{\substack{r_1\mid N(KA)\\ r_1\mid q}} \mu(r_1) \\ \times \sum_{\substack{r_2\mid q\\ (r_2,N(KA))=1}} \mu(r_2)2^{\omega(r_2)}\Big(\frac{I(b,c,d)}{r_2N(AK)}+O(NM^{-5})\Big). \end{aligned} \tag{13·6}$$

La contribution du terme d'erreur de (13·6) est $O(X^{\varepsilon+6\alpha_0+3\vartheta_0-1/4})$ ce qui nous obligera à choisir α_0 et ϑ_0 tels que

$$6\alpha_0+3\vartheta_0<1/4. \tag{13·7}$$

La somme sur r_1 vaut 1 si $(q,N(KA))=1$ sinon elle est nulle :

$$S_0 = \sum_{K\in\mathcal{K}}\sum_{A}\lambda^-_{N(A)} \sum_{\substack{(b,c,d)\in\mathcal{C}\\ (q,N(KA))=1}} \sum_{r_2\mid q}\mu(r_2)2^{\omega(r_2)}\frac{I(b,c,d)}{r_2N(A)N(K)}+o(1). \tag{13·8}$$

On intervertit les sommes puis on évalue celles sur les idéaux A et K de la même façon que dans l'article de Heath-Brown ([24] pp. 574-576) :

$$\sum_{K\in\mathcal{K}}\frac{\varrho(K)}{N(K)} = \log(5/4)+o(1), \tag{13·9}$$

la condition $(K,q)=1$ pouvant être retirée au prix d'un terme d'erreur assez petit. La somme $\sum_{(A,q)=1}\frac{\lambda^-_{N(A)}}{N(A)}$ est analogue à la quantité $\sigma_2(q)$ définie dans les pages 574 et 560 de [24] vu que les idéaux A sont tels que $\varrho(A)=1$. Les poids λ_d^- du crible de Rosser-Iwaniec sont les mêmes que ceux choisis par Heath-Brown avec ϑ_0 à la place du δ de [24]. On obtient alors

$$\sum_{(A,q)=1}\frac{\lambda^-_{N(A)}}{N(A)}\geqslant (C_0+o(1))\prod_{p|q}\Big(1-\frac{g(p)}{p}\Big)^{-1}\prod_{p<X^{\vartheta_0}}\Big(1-\frac{g(p)}{p}\Big), \tag{13·10}$$

avec les notations du Lemme 13.1. Il ne reste plus qu'à reporter (13·9) et (13·10) dans (13·8) pour terminer la preuve du Lemme 13.1.

14. Le terme S_0, suite : découpage de $\mathcal{R}$ en pavés

D'après le Lemme 13.1 on a sous certaines conditions sur α_0,ϑ_0

$$S_0\geqslant (C_0+o(1))\log(5/4)\prod_{p<X^{\vartheta_0}}\Big(1-\frac{g(p)}{p}\Big)T_0,$$

où maintenant,

$$T_0=\sum_{(b,c,d)\in\mathcal{C}}I(b,c,d)h(q).$$

Dans ce paragraphe on découpe $\mathcal{R}$ en pavés disjoints sur lesquels la valeur de l'intégrale $I(b,c,d)$ varie peu. Cette partie reprend les idées de Heath-Brown [24] pp. 582-583.

On divise $\mathcal{R}$ en pavés disjoints de la forme

$$\mathcal{B}=]A,A+M]\times]B,B+M]\times]C,C+M]\times]D,D+M]\subset\mathbb{R}^4. \tag{14·1}$$

Soit $\eta>0$ un paramètre arbitrairement petit. Suivant la terminologie adoptée par Heath-Brown ([24] p. 583), on dira que $\mathcal{B}$ est un "bon pavé" si $\mathcal{B}\subset\mathcal{R}_0$ avec

$$\mathcal{R}_0=\mathcal{R}\cap\{(a,b,c,d)\in\mathcal{R}:M^4X^\eta\leqslant N(\alpha)<N^4\},$$

avec $\alpha=a+b\zeta_{12}+c\zeta_{12}^2+d\zeta_{12}^3$. Notons $\mathcal{B}_{\mathcal{R}}$ l'ensemble des bons pavés.

On a alors

$$\sum_{(b,c,d)\in\mathcal{C}}I(b,c,d)h(q)\geqslant\sum_{\mathcal{B}\in\mathcal{B}_{\mathcal{R}}}\sum_{(b,c,d)\in\mathcal{C}}\int_{\mathcal{B}}\frac{\mathrm{d}t}{N(t,b,c,d)}h(q).$$

En profitant du Lemme 10.1 et des formules (10·11) et (10·12), on vérifie facilement que

$$\|\nabla_{(a,b,c,d)}N^{-1}\|\ll N(\alpha)^{-5/4}. \tag{14·2}$$

En reprenant les arguments de Heath-Brown [24] p. 583, on vérifie que pour $\mathcal{B}$ un bon pavé défini par (14·1), on a :

$$\int_{(t,b,c,d)\in\mathcal{B}}\frac{\mathrm{d}t}{N(t,b,c,d)}=\frac{M(1+o(1))}{N(A,B,C,D)}. \tag{14·3}$$

Pour $\mathcal{B}\in\mathcal{B}_{\mathcal{R}}$ un pavé défini par (14·1), on note

$$\mathcal{V}_{\mathcal{B}}=]B,B+M]\times]C,C+M]\times]D,D+M].$$

Pour b, c, d donnés, $b^2 + c^2 \ll N^2 = X^{(1+\alpha_0)/2}$, il existe au plus $\frac{1+\alpha_0}{2\vartheta_{11}}$ nombres premiers q_{11} divisant $b^2 + c^2$. De même pour $(i, j) \in \{(1, 2), (2, 1), (2, 2), (3, 1)\}$, il existe au plus $\frac{1+\alpha_0}{2\vartheta_{ij}}$ nombres premiers q_{ij} divisant $q_i(b, c, d)$.

On en déduit que

$$T_0 \geqslant (1 + o(1))\frac{2^5\vartheta_{31}\prod_{(i,j)\in\{1,2\}^2}\vartheta_{ij}}{(1+\alpha_0)^5}U_0,$$

avec

$$U_0 = \sum_{\mathcal{B}\in\mathcal{B}_{\mathcal{R}}}\frac{M}{N(A,B,C,D)}\sum_{X^{\vartheta_{ij}}<q_{ij}<X^{\vartheta'_{ij}}}\sum_{\substack{(b,c,d)\in\mathcal{V}_{\mathcal{B}}\\(cd,q)=1=(c,d)}}^{*} h(q),$$

où l'étoile indique maintenant que la somme porte sur les (b, c, d) tels que $q_i(b, c, d) \equiv 0 \pmod{q_{i1}q_{i2}}$ pour $i = 1, 2$ et $q_3(b, c, d) \equiv 0 \pmod{q_{31}}$.

On a alors

$$U_0 \geqslant \sum_{\mathcal{B}\in\mathcal{B}_R}\frac{M}{N(A,B,C,D)}U(\mathcal{B}),$$

avec

$$U(\mathcal{B}) = \sum_{\substack{X^{\vartheta_{ij}}<q_{ij}<X^{\vartheta'_{ij}}\\(i,j)\in\{1,2\}^2\cup\{(3,1)\}}}\sum_{\substack{(b,c,d)\in\mathcal{V}_{\mathcal{B}}\\(c,d)=1=(q,cd)}}^{*} h(q). \tag{14·4}$$

Inversement d'après (14·3), pour toute fonction $\psi : \mathbb{R}^3 \to \mathbb{R}$, on a :

(14·5)

$$\begin{aligned}\sum_{\mathcal{B}\in\mathcal{B}_{\mathcal{R}}}\frac{M}{N(A,B,C,D)}\sum_{(b,c,d)\in\mathcal{V}_{\mathcal{B}}}|\psi(b,c,d)| &\ll \sum_{\mathcal{B}\in\mathcal{B}_{\mathcal{R}}}\sum_{(b,c,d)\in\mathcal{V}_{\mathcal{B}}}|\psi(b,c,d)|\int_{(t,b,c,d)\in\mathcal{B}}\frac{dt}{N(t,b,c,d)}\\ &\ll \sum_{(b,c,d)\in\mathcal{C}}|\psi(b,c,d)|I(b,c,d)\\ &\ll NM^{-4}\sum_{(b,c,d)\in\mathcal{C}}|\psi(b,c,d)|.\end{aligned}$$

Cette remarque nous servira dans les paragraphes suivants.

15. Le terme S_0, suite : une série de convolutions

Dans cette partie, on montre que les différentes conditions sur b, c, d peuvent se ramener à étudier la répartition des valeurs des formes $q_i(b, c, d)$ dans certaines progressions arithmétiques. Nous serons alors en mesure d'appliquer le Théorème 8.1.

Nous commençons par traiter la condition $(q, cd) = 1$ avec la formule d'inversion de Möbius :

$$U(\mathcal{B}) = \sum_s \mu(s)\sum_{X^{\vartheta_{ij}}<q_{ij}<X^{\vartheta'_{ij}}}\sum_{\substack{(b,c,d)\in\mathcal{V}_{\mathcal{B}}\\(c,d)=1\\s|cd,\ s|q}}^{*} h(q).$$

Notons $T_1(\mathcal{B})$ la contribution à $U(\mathcal{B})$ des $s > Z$ pour un $Z > 0$ que nous préciserons bientôt. On écrit ensuite $s = s_1s_2$ avec $c = s_1c'$, $d = s_2d'$:

$$T_1(\mathcal{B}) \ll \sum_{Z<s\ll N^2}\mu^2(s)\sum_{\substack{s_1s_2=s\\\max(s_1,s_2)\ll N}}\sum_{\substack{(b,s_1c,s_2d)\in\mathcal{V}_{\mathcal{B}}\\s|q(b,s_1c,s_2d)}}\tau(q(b,cs_1,ds_2)).$$

Le terme avec la fonction τ est majoré par une puissance de X arbitrairement petite. Pour c, d, s_1, s_2 donnés, le nombre de b vérifiant les conditions ci-dessus est un $O(X^{\varepsilon_1}(1+Ns^{-1}))$ avec $\varepsilon_1 > 0$ arbitrairement petit. Ensuite le nombre de c et d est un $O(N^2 s^{-1})$. En appliquant (14·5) on trouve :

$$\begin{aligned}\sum_{\mathcal{B}\in\mathcal{B}_{\mathcal{R}}} \frac{MT_1(\mathcal{B})}{N(A,B,C,D)} &\ll NM^{-4} \sum_{(b,c,d)\in\mathcal{C}} \sum_{Z<s\ll N^2} \mu^2(s) \sum_{\substack{s_1s_2=s\\ s_1|c\\ s_2|d}} \sum_{s|q(b,c,d)} X^{\varepsilon_1}\\ &\ll X^{\varepsilon} NM^{-4} \sum_{Z<s\ll N^2} \mu^2(s)\frac{N^2}{s}\Big(1+\frac{N}{s}\Big)\\ &\ll N^3M^{-4}X^{\varepsilon_1} + N^4M^{-4}X^{\varepsilon_1}Z^{-1} = O(X^{-\varepsilon'}),\end{aligned}$$

pour

$$Z = X^{\alpha_0+\varepsilon}, \tag{15·1}$$

$\varepsilon > \varepsilon_1$ arbitrairement petits et $\varepsilon' > 0$ assez petit ($\varepsilon' < \varepsilon - \varepsilon_1$).

Nous nous occupons maintenant de la condition $(c,d) = 1$ *via* de nouveau la formule de Möbius :

$$\begin{aligned}U_0 \geqslant \sum_{\mathcal{B}\in\mathcal{B}_{\mathcal{R}}} \frac{M}{N(A,B,C,D)} &\sum_{\substack{X^{\vartheta_{ij}}<q_{ij}<X^{\vartheta'_{ij}}\\ (i,j)\in\{1,2\}^2\cup\{(3,1)\}}} \sum_{s<Z}\mu(s)\sum_{s_1s_2=s}\sum_{t}\mu(t)\\ &\times \sum^{*}_{\substack{b,c,d\in\mathcal{V}_{\mathcal{B}}\\ s_1|c,\ s_2|d \text{ et } t|(c,d)\\ s|q}} h(q) + O(X^{-\varepsilon'}).\end{aligned} \tag{15·2}$$

Notons $\tilde{U}_0$ le membre de droite de (15·2). De nouveau nous pouvons restreindre la somme sur t à $t < Z$ au prix d'une erreur en $O(X^{-\varepsilon'})$ pour un $\varepsilon' > 0$ assez petit.

Le terme $h(q)$, est également traité avec de la convolution. On écrit $h(n) = \sum_{u|n}\ell(u)$, avec $\ell = \mu * h$. Ainsi ℓ est la fonction multiplicative caractérisée par

$$\ell(p) = h(p) - 1 = \begin{cases} \frac{g(p)-2}{p-g(p)} & \text{si } p > 256\\ -1 & \text{sinon,}\end{cases}$$

puis si $k \geqslant 2$, $\ell(p^k) = h(p^k) - h(p^{k-1})$. On en déduit que

$$\ell(p^2) = -h(p) = \begin{cases} -\frac{p-2}{p-g(p)} & \text{si } p > 256\\ 0 & \text{sinon,}\end{cases}$$

et $\ell(p^k) = 0$ pour $k \geqslant 3$.

Nous reprenons les idées des pages 580-581 de l'article de Heath-Brown [24]. Toutefois on a vu que si q est sans facteur carré alors $(b, q_{11}q_{12}) = 1 = (b, q_{21}q_{22})$. Dans la suite nous conservons cette condition de coprimalité. Ainsi en notant $q_1^* = q_{11}q_{12}$, $q_2^* = q_{21}q_{22}$ on a :

$$\begin{aligned}\tilde{U}_0 = \sum_{\mathcal{B}\in\mathcal{B}_{\mathcal{R}}} \frac{M}{N(A,B,C,D)} &\sum_{X^{\vartheta_{ij}}<q_{ij}<x^{\vartheta'_{ij}}} \sum_{s,t<Z}\mu(s)\mu(t)\\ &\times \sum_{s_1s_2=s} \sum^{*}_{\substack{b,c,d,\ (b,q_1^*q_2^*)=1\\ [t,s_1]|c,\ [t,s_2]|d\\ s|q}} \sum_{u|q}\ell(u) + O(X^{-\varepsilon'}).\end{aligned}$$

Or $\ell(u)=0$ si u est divisible par le cube d'un nombre premier. Si $\ell(u)\neq 0$, on peut écrire u sous la forme $u=v^2w$ avec $\mu^2(vw)=1$. Dans ce cas, $\ell(u)\ll x^\varepsilon/w$. On vérifie alors que la contribution des $w>Z$ est assez petite. Il reste à majorer la contribution des $v>V$ avec V à choisir plus tard. Soit U_2 cette contribution. Pour v donné sans facteur carré tel que $v^2|q$, on écrit $v=v_1v_2v_3v_4$, avec

$$v_1=\prod_{\substack{p|v\\ p^2|q_1(b,c)}} p,\ v_2=\prod_{\substack{p|(v/v_1)\\ p^2|q_2(b,d)}} p,\ v_3=\prod_{\substack{p|(v/(v_1v_2))\\ p^2|q_3(b,c,d)}} p,\ v_4=\frac{v}{v_1v_2v_3}.$$

Pour $i=1,2,3,4$ on note V_i la contribution des $v_i>V^{1/4}$. Ainsi, $U_2\ll V_1+V_2+V_3+V_4$.

On commence par majorer V_1. Pour cela on s'inspire des pages 580-581 de [24]. Rappelons que $\ell(v^2)\ll X^\varepsilon$.

On écrit $V_1=V_1'+V_1''$ où dans V_1' le diviseur v_1 est un multiple de q_{11} tandis que dans V_1'', $q_{11}\nmid v_1$ (rappelons que q_{11} est un nombre premier). Pour V_1' on a * :

$$V_1'\ll X^\varepsilon NM^{-4}\sum_{X^{\vartheta_1}<q_{11}<X^{\vartheta_1'}}\sum_{t,s<Z}\mu^2(s)\sum_{\substack{v_1>V^{1/4}\\ q_{11}|v_1}}\sum_{\substack{b,c,d\\ [t,s_1]|c,\ [t,s_2]|d\\ [s,v_1]|q}}\mu^2(v_1).$$

On intervertit certaines sommes :

$$V_1'\ll X^\varepsilon NM^{-4}\sum_{X^{\vartheta_{11}}<q_{11}<X^{\vartheta_{11}'}}\sum_{\substack{b,c,d\\ q_{11}^2|q_1(b,c)}}\tau((c,d))\tau(c)\tau(d)\tau(q)^2.$$

Le produit des fonctions τ est un $O(X^\varepsilon)$ tandis que le nombre d'entiers b,c tels que $q_{11}^2|q_1(b,c)$ est inférieur à $O(N^2/q_{11}^2+N)$. On a donc

$$V_1'\ll X^\varepsilon N^2M^{-4}\sum_{X^{\vartheta_{11}}<q_{11}<X^{\vartheta_{11}'}}\Big(\frac{N^2}{q_{11}^2}+N\Big)\ll X^\varepsilon N^4M^{-4}X^{-\vartheta_{11}}+X^\varepsilon N^3M^{-4}X^{\vartheta_{11}'}.$$

Pour V_1'', q_{11} ne divise pas v_1. On en déduit que $v_1\ll Nq_{11}^{-1/2}\ll NX^{-\vartheta_{11}/2}$:

$$V_1''\ll X^\varepsilon NM^{-4}\sum_{V^{1/4}<v_1\ll NX^{-\vartheta_{11}/2}}\mu^2(v_1)\sum_{\substack{b,c,d\\ v_1^2|q_1(b,c)}}\tau(c)^2\tau(d)^2\tau(q).$$

Soit $v_1'=(c,v_1)$. Alors $v_1'=(v_1,b)$ et

$$\sum_{q_1(b,c)\equiv 0\,(\mathrm{mod}\,v_1^2)}1\ll\sum_{v_1'|v_1}\sum_{\substack{b,c\ll(v_1')^{-1}N\\ q_1(b,c)\equiv 0\,(\mathrm{mod}\,(v_1/v_1')^2)}}1\ll X^\varepsilon\frac{N}{v_1'}\Big(1+\frac{Nv_1'}{v_1^2}\Big).$$

On obtient alors

$$V_1''\ll X^\varepsilon N^4M^{-4}X^{-\vartheta_{11}/2}+X^\varepsilon N^4M^{-4}V^{-1/4}.$$

On obtient quasiment de la même façon les majorations pour $i=2,3$:

$$V_i\ll X^\varepsilon N^4M^{-4}X^{-\vartheta_{i1}/2}+X^\varepsilon N^3M^{-4}X^{\vartheta_{i1}'}+X^\varepsilon N^4M^{-4}V^{-1/4}.$$

---

* certaines sommes comme par exemple celles sur les nombres premiers q_{ij} sont majorées par une puissance de $\tau(q)$ et *a fortiori* par un $O(X^\varepsilon)$.

Pour $i=3$, il y a une légère différence due au fait que le polynôme q_3 est en 3 variables.

On s'intéresse maintenant à V_4. Soit p un facteur premier de v_4. Par construction de v_4, il existe i,j, $1 \leqslant i < j \leqslant 3$ tel que $p|(q_i(b,c,d), q_j(b,c,d))$. Or $q_3(b,c,d) = 4q_2(b,c,d) - 3q_1(b,c,d)$ (avec les notations $q_1(b,c,d) = q_1(b,c)$ et $q_2(b,c,d) = q_2(b,d)$).

Donc si $p > 3$ alors p divise $(q_1(b,c,d), q_2(b,c,d), q_3(b,c,d))$. Comme v_4 est sans facteur carré, on en déduit que $v_4/(v_4,6)$ divise également ce p.g.c.d. Ainsi

$$V_4 \ll X^{\varepsilon} NM^{-4} \sum_{v_4 > V^{1/4}} \mu^2(v_4) \sum_{\substack{b,c,d \\ v_4 | 6(q_1(b,c), q_2(b,d))}} 1.$$

Pour $i=1,2$, on note V_{4i} la contribution des v_4 divisibles par q_{2i}, puis V_4' celle des v_4 qui sont premiers avec $q_{21}q_{22}$. (On profite également ici du fait que les entiers q_{21} et q_{22} soient des nombres premiers).

$$V_{4i} \ll X^{\varepsilon} NM^{-4} \sum_{X^{\vartheta_{2i}} < q_{2i} < X^{\vartheta'_{2i}}} \sum_{\substack{b,c,d \\ q_{2i} | (q_1(b,c,d), q_2(b,c,d))}} 1.$$

Pour $i=1,2$ et b donnés, il existe $O(N/q_{2i})$ entiers c tels que $q_1(b,c) \equiv 0 \,(\mathrm{mod}\, q_{2i})$ et un $O(N/q_{2i})$ nombre d'entiers d tels que $q_2(b,d) \equiv 0 \,(\mathrm{mod}\, q_{2i})$. On en déduit que

$$V_{4i} \ll X^{\varepsilon} N^4 M^{-4} X^{-\vartheta_{2i}}. \tag{15·3}$$

Il reste à majorer V_4'. Si v_4 est compté dans V_4' alors $(v_4, q_{21}q_{22}) = 1$. On en déduit que $v_4 \ll N^2 X^{-\vartheta_{21}-\vartheta_{22}}$ (avec $\vartheta_{21}+\vartheta_{22} > (1+\alpha_0)/4$ d'après les majorations de R_3 et R_4 obtenues dans (12·16)). Ainsi pour $\alpha_0 < 1/3$ on a :

$$V_4' \ll X^{\varepsilon} NM^{-4} \sum_{V^{1/4} \leqslant v_4 \ll N^2 X^{-(\vartheta_{21}+\vartheta_{22})}} \sum_{\substack{b,c,d \\ \frac{v_4}{(v_4,6)} | (q_1(b,c), q_2(b,d))}} 1 \ll X^{\varepsilon} N^4 M^{-4} V^{-1/4}.$$

On choisit alors

$$V = Z^4 = X^{4\alpha_0 + 4\varepsilon}. \tag{15·4}$$

Finalement, on obtient moyennant diverses conditions sur nos paramètres et pour $\varepsilon' > 0$ assez petit

$$\tilde{U}_0 = \sum_{\mathcal{B} \in \mathcal{B}_R} \frac{MU_0(\mathcal{B})}{N(A,B,C,D)} + O(x^{-\varepsilon'}),$$

avec

$$U_0(\mathcal{B}) = \sum_{X^{\vartheta_{ij}} < q_{ij} < X^{\vartheta'_{ij}}} \sum_{\substack{s,t<Z \\ u<Z^9}} \mu(s)\mu(t)\ell(u) \sum_{s_1 s_2 = s} \sideset{}{^*}\sum_{\substack{(b,c,d) \in \mathcal{V}_{\mathcal{B}}, \ (b, q_{11}q_{12}q_{21}q_{22}) = 1 \\ [t,s_1] | c, \ [t,s_2] | d \\ s | q, \ u | q}} 1. \tag{15·5}$$

Plus précisément $\vartheta_{ij}, \vartheta'_{ij}$ devront alors vérifier les conditions supplémentaires suivantes :

$$2\alpha_0 < \vartheta_{1i} < \vartheta'_{1i} < 1/4 - 3\alpha_0/4 - \varepsilon \text{ pour } i = 1,2,3 \tag{15·6}$$

et

$$\vartheta_{21} + \vartheta_{22} > \frac{1+\alpha_0}{4}. \tag{15·7}$$

16. Application du Théorème 8.1

Dans (15·5), les triplets (b,c,d) appartiennent à des ensembles du type les ensembles $\mathcal{A}(m_1,m_2,m_3,\mathbf{u})$ étudiés dans le paragraphe 8. Nous pouvons appliquer maintenant le Théorème 8.1 pour estimer les quantités $U_0(\mathcal{B})$ définies par (15·5). L'entier m_3 de ce théorème correspond à $\delta=[s,t,u,q_{31}]$ et les congruences associées sont $b\equiv z_1\,(\mathrm{mod}\,\delta)$, $c\equiv z_2\,(\mathrm{mod}\,\delta)$, $d\equiv z_3\,(\mathrm{mod}\,\delta)$, où les triplets (z_1,z_2,z_3), $0\leqslant z_1,z_2,z_3<\delta$ parcourent les solutions du système $\mathcal{S}$ défini par :

$$t|(z_2,z_3),\ s|z_2z_3,\ [s,u]|q(z_1,z_2,z_3),\ q_{31}|q_3(z_1,z_2,z_3).$$

On a donc $m_3<Z^{11}X^{\vartheta'_{31}}$. On observe également que le nombre de solutions de $\mathcal{S}$ est un $O(\delta^{2+\varepsilon})$. D'autre part les entiers m_1 et m_2 du Théorème 8.1 sont de la forme $m_1=q_{11}q_{12}$, $m_2=q_{21}q_{22}$; on prend alors $Q_1=X^{\vartheta'_{11}+\vartheta'_{12}}$, $Q_2=X^{\vartheta'_{21}+\vartheta'_{22}}$. Les polynômes f_1 et f_2 du Théorème 8.1 sont les formes q_1 et q_2. On a alors :

$$U_0(\mathcal{B})=T_0(\mathcal{B})+E(\mathcal{B}),$$

avec

$$T_0(\mathcal{B})=\sum_{\substack{s,t<Z\\u<Z^9}}\mu(s)\mu(t)\ell(u)\times\sum_{X^{\vartheta_{31}}<q_{31}<X^{\vartheta'_{31}}}\ \sum_{(z_1,z_2,z_3)\in\mathcal{S}}\ \sum_{\substack{X^{\vartheta_{ij}}<q_{ij}<X^{\vartheta'_{ij}}\\(i,j)\in\{1,2\}^2}}M^3\frac{\varrho^*_{q_1}(q_{11}q_{12})\varrho^*_{q_2}(q_{21}q_{22})}{q_{11}^2q_{12}^2q_{21}^2q_{22}^2\delta^3}$$

et $E(\mathcal{B})$ est la contribution des termes d'erreurs issus du Théorème 8.1.

En sommant sur les triplets (z_1,z_2,z_3) appartenant à $\mathcal{S}$ puis sur $m_3<Z^{11}X^{\vartheta'_{31}}$ les majorations des quantités $E(m_3)$ données par le Théorème 8.1, on constate qu'il suffit de choisir nos paramètres de sorte qu'il existe $\varepsilon>0$ tel que (rappelons que $\min(Q_1,Q_2)\geqslant M$)

$$\max(Q_1Q_2Z^{33}X^{3\vartheta'_{31}},(Q_1Q_2)^{1/2}M^{3/2}Z^{99/4}X^{9\vartheta'_{31}/4})\ll M^3X^{-\varepsilon}$$
$$\max((Q_1Q_2)^{1/3}M^2Z^{11}X^{\vartheta'_{31}},Z^{11}X^{\vartheta'_{31}}M^2(\sqrt{Q_1}+\sqrt{Q_2}))\ll M^3X^{-\varepsilon},$$

pour que la contribution de tous les termes d'erreur $E(\mathcal{B})$ soit assez petite.

Ces conditions sont remplies si on impose

$$(16\cdot1)\quad 11\alpha_0+\vartheta'_{31}<\frac{1}{18},\ \max(\vartheta'_{11}+\vartheta'_{12},\vartheta'_{21}+\vartheta'_{22})<\frac{1}{3},\ \vartheta'_{11}+\vartheta'_{12}+\vartheta'_{21}+\vartheta'_{22}<\frac{5}{9},$$

On se consacre maintenant au terme principal. Nous avons choisi les exposants ϑ_{ij}, ϑ'_{ij} de sorte que $(q_{ij},q_{k\ell})=1$ si $(i,j)\neq(k,\ell)$. Ainsi $\varrho^*_{q_1}(q_{11}q_{12})=\varrho^*_{q_1}(q_{11})\varrho^*_{q_1}(q_{12})$. Pour $(i,j)\in\{1,2\}^2$, on peut appliquer le Théorème de Nagell [44] vu que $\varrho^*_{q_i}(q_{ij})=\varphi(q_{ij})\tilde{\varrho}_{q_i}(q_{ij})$:

$$\sum_{X^{\vartheta_{ij}}<q_{ij}<X^{\vartheta'_{ij}}}\frac{\varrho^*_{q_i}(q_{ij})}{q_{ij}^2}=\log\log X^{\vartheta'_{ij}}-\log\log X^{\vartheta_{ij}}+O((\log X)^{-1})=\log(\vartheta'_{ij}/\vartheta_{ij})+o(1).$$

Nous imposerons encore que $X^{\vartheta_{31}}>Z^{11}$ et ainsi $(q_{31},stu)=1$. On en déduit

$$|\mathcal{S}|=\sigma_{q_3}(q_{31})|\mathcal{S}'|$$

où $\mathcal{S}'$ est l'ensemble des triplets (z_1, z_2, z_3), $0 \leqslant z_1, z_2, z_3 < [s,t,u]$ vérifiant :

$$s|z_2z_3,\ t|(z_2,z_3),\ [s,u]|q(z_1,z_2,z_3).$$

Notons $S(s,t,u)$ le cardinal de $\mathcal{S}'$.

La somme sur q_{31} est indépendante des autres sommes.

On a vu que $\left(\frac{3}{p}\right) = 1$ pour $p \equiv \pm 1 \pmod{12}$. On a donc

$$\sigma_{q_3}(p) = \begin{cases} 2p^2 - p & \text{si } p \equiv \pm 1 \pmod{12} \\ p & \text{si } p \not\equiv \pm 1 \pmod{12} \end{cases}$$

et ainsi

$$\sum_{X^{\vartheta_{31}} < q_{31} < X^{\vartheta'_{31}}} \frac{\sigma_{q_3}(q_{31})}{q_{31}^3} = (1+o(1)) \log(\vartheta'_{31}/\vartheta_{31}).$$

On arrive à

$$T_0(\mathcal{B}) = M^3(1+o(1)) \prod_{\substack{i=1,2,3 \\ j=1,2 \\ (i,j)\neq(3,2)}} \log(\vartheta'_{ij}/\vartheta_{ij}) \sum_{\substack{s,t<Z \\ u<Z^9}} \frac{\mu(s)\mu(t)\ell(u)}{[s,t,u]^3} S(s,t,u).$$

Lemme 16.1. *On a l'estimation :*

$$\sum_{\substack{s,t<Z \\ u<Z^9}} \frac{\mu(s)\mu(t)\ell(u)}{[s,t,u]^3} S(s,t,u) = (1+o(1)) \sum_{m\geqslant 1} \frac{F(k)}{k^3} \qquad (Z \to +\infty), \tag{16·2}$$

avec

$$F(k) = \sum_{[s,t,u]=k} \mu(s)\mu(t)\ell(u) S(s,t,u).$$

Avant de vérifier ce lemme nous montrons que la somme dans le membre de droite est convergente.

En faisant beaucoup de calculs on obtient :

Lemme 16.2. *On a la formule :*

$$\sum_{k\geqslant 1} \frac{F(k)}{k^3} = \frac{7}{54} C_1C_2C_3C_4 > \frac{7}{1800},$$

avec

$$C_1 = \prod_{\substack{p<256 \\ p\equiv 1 \pmod{12}}} \Big(1 + \frac{-6p^2+10p-5}{p^3}\Big) = \prod_{\substack{p<256 \\ p\equiv 1 \pmod{12}}} \Big(1-\frac{1}{p}\Big)\Big(1-\frac{5}{p}+\frac{5}{p^2}\Big)$$

$$C_2 = \prod_{\substack{3<p<256 \\ p\not\equiv 1 \pmod{12}}} \Big(1 + \frac{-2p^2-2p+3}{p^3}\Big) = \prod_{\substack{3<p<256 \\ p\not\equiv 1 \pmod{12}}} \Big(1-\frac{1}{p}\Big)\Big(1-\frac{1}{p}-\frac{3}{p^2}\Big),$$

$$C_3 = \prod_{\substack{p>256 \\ p\equiv 1 \pmod{12}}} \Big(1 + \frac{2p^2+9p-8}{p^3(p-4)} + \frac{-(p-2)(10p^2-28p+18)}{p^4(p-4)}\Big),$$

$$C_4 = \prod_{\substack{p>256\\ p\not\equiv 1 \,(\mathrm{mod}\, 12)}} \Big(1 - \frac{(2p-1)(5p-4)}{p^4} + \frac{-2(p-2)(p-1)^2}{p^5}\Big).$$

Remarque. On vérifie avec des calculs standard que $0 < C_i < +\infty$, pour $i = 1, 2, 3, 4$.

Preuve. On commence par observer que cette fonction F est multiplicative. Soient k_1 et k_2 tels que $(k_1, k_2) = 1$. Pour tous s, t, u tels que $[s, t, u] = k_1 k_2$ on peut décomposer de manière unique chaque terme $s = s_1 s_2$, $t = t_1 t_2$, $u = u_1 u_2$, , où les termes d'indices 1 divisent k_1 et ceux d'indice 2 divisent k_2 :

$$F(k_1 k_2) = \sum_{\substack{[s_1,t_1,u_1]=k_1\\ [s_2,t_2,u_2]=k_2}} \prod_{i=1}^{2} \mu(s_i)\mu(t_i)\ell(u_i) S(s_1 s_2, t_1 t_2, u_1 u_2).$$

Puis on termine en remarquant que

$$S(s,t,u) = \prod_{p | k_1 k_2} S(p^{v_p(s)}, p^{v_p(t)}, p^{v_p(u)}) = S(s_1, t_1, u_1) S(s_2, t_2, u_2),$$

où v_p est la valuation p-adique. On en déduit que $\sum_{k\geqslant 1} \frac{F(k)}{k^3}$ peut s'écrire sous la forme d'un produit eulérien :

$$\sum_{k\geqslant 1} \frac{F(k)}{k^3} = \prod_{p} \Big(1 + \frac{F(p)}{p^3} + \frac{F(p^2)}{p^6}\Big). \tag{16·3}$$

Il s'agit maintenant d'évaluer ce produit.

On commence par évaluer $F(p)$. On vérifie facilement que $S(1, p, 1) = p$, $S(p, p, 1) = S(p, p, p) = S(1, p, p) = 1$ et $S(p, 1, p) = S(p, 1, 1)$. On obtient :

$$F(p) = -p + 1 - (1 + \ell(p)) S(p, 1, 1) + \ell(p) S(1, 1, p).$$

Les valeurs de $S(1, 1, p) = \sigma_q(p)$ sont données par le Lemme 7.8 et celles de $S(p, 1, 1)$ se calculent à l'aide du premier tableau donné dans la preuve de ce lemme :

$$S(p, 1, 1) = \begin{cases} 9p - 8 & \text{si } p \equiv 1 \,(\mathrm{mod}\, 12) \\ 5p - 4 & \text{sinon} \end{cases} \qquad (p \geqslant 5).$$

Pour calculer $F(p^2)$, il suffit d'évaluer les quantités $S(p^{v_s}, p^{v_t}, p^2)$ avec $(v_s, v_t) \in \{0, 1\}^2$. En fait grâce à certaines compensations on a :

$$\begin{aligned} F(p^2) &= \ell(p^2)(S(1, 1, p^2) - S(p, 1, p^2)) \\ &= \ell(p^2) |\{0 \leqslant b, c, d < p^2 : p^2 | q(b, c, d) \text{ et } p \nmid cd\}|. \end{aligned}$$

Ainsi $F(p^2) = 0$ si $p < 256$ tandis que pour $p > 256$, on détermine le cardinal ci-dessus à l'aide du deuxième tableau de la preuve du Lemme 7.8. Après quelques calculs, on obtient pour $p > 256$:

$$F(p^2) = \begin{cases} -\frac{(p-2)(10p^2-28p+18)p^2}{p-4} & \text{si } p \equiv 1 \,(\mathrm{mod}\, 12) \\ -2p(p-2)(p-1)^2 & \text{si } p \not\equiv 1 \,(\mathrm{mod}\, 12). \end{cases}$$

La constante $7/54$ dans le Lemme 16.2 est la contribution des nombres premiers 2 et 3 : $F(2) = -6$, $F(3) = -13$.

Preuve du Lemme 16.1. On a :

$$\sum_{\substack{s,t<Z\\ u<Z^5}} \frac{\mu(s)\mu(t)\ell(u)}{[s,t,u]^3} S(s,t,u) = \sum_{m\geqslant 1} \frac{F(k)}{k^3} + O\Big(\sum_{m>Z} \frac{G(m)}{m^3}\Big), \tag{16·4}$$

où maintenant,

$$G(m) = \sum_{[s,t,u]=m} \mu^2(s)\mu^2(t)\ell^2(u)S(s,t,u).$$

En adaptant les calculs de la preuve du Lemme 16.2, on vérifie que la série de Dirichlet $\sum_{m\geqslant 1} \frac{G(m)}{m^z}$ est absolument convergente sur $\mathcal{R}e\ z > 2$, si bien que le terme d'erreur de (16·4) est un $O(Z^{-1+\varepsilon})$ avec $\varepsilon > 0$.

Remarque. En utilisant SAGE par exemple et des approximations standard, on vérifie que le produit $C_1C_2C_3C_4 > 0.03$ et ainsi

$$\sum_{k\geqslant 1} \frac{F(k)}{k^3} \geqslant \frac{7}{1800}. \tag{16·5}$$

17. Avant dernière étape : recollement des pavés

On rappelle les notations pour $\alpha = a + b\zeta_{12} + c\zeta_{12}^2 + d\zeta_{12}^3$:

$$N(\alpha) = N(a,b,c,d) = |\alpha|^2|\alpha_3|^2,$$

α_3 étant donné par (10·12). On cherche maintenant à évaluer

$$W := \sum_{\mathcal{B}\in\mathcal{B}_{\mathcal{R}}} \frac{M^4}{N(A,B,C,D)}.$$

Les arguments de Heath-Brown [24] p. 584 permettent de montrer

$$\frac{M^4}{N(A,B,C,D)} = (1+o(1)) \iiiint_{\mathcal{B}} \frac{\mathrm{d}a\,\mathrm{d}b\,\mathrm{d}c\,\mathrm{d}d}{N(a,b,c,d)},$$

et ainsi,

$$W = (1+o(1) \iiiint_{\mathcal{R}_1} \frac{\mathrm{d}a\,\mathrm{d}b\,\mathrm{d}c\,\mathrm{d}d}{N(a,b,c,d)},$$

où $\mathcal{R}_1 = \cup_{\mathcal{B}\in\mathcal{B}_{\mathcal{R}}}\mathcal{B}$ est la région formée par tous les bons pavés.

On commence par vérifier que la condition (10·5) sur les tailles de B_{14} et q peut être retirée moyennant un terme d'erreur négligeable.

Lemme 17.1. *Pour $\beta_0 > 9\alpha_0/2$, on a l'égalité : $W = W_1(1+o(1))$, avec*

$$W_1 := \iiiint_{\mathcal{R}_2} \frac{\mathrm{d}a\,\mathrm{d}b\,\mathrm{d}c\,\mathrm{d}d}{N(a+b\zeta_{12}+c\zeta_{12}^2+d\zeta_{12}^3)},$$

où $\mathcal{R}_2$ est la réunion des pavés $\mathcal{B}$ qui sont contenus dans

$$\mathcal{R}_3 := \Big\{(a,b,c,d)\in\mathbb{R}^4 : M^4X^\eta \leqslant N(\alpha) < N^4 \text{ et } 1 \leqslant \frac{|\alpha|^2}{N(\alpha)^{1/2}} < 2+\sqrt{3}\Big\}.$$

Preuve. On verra dans le Lemme 17.2 *infra* que $W_1 \asymp \log X$. Pour montrer le Lemme 17.1, il suffit de vérifier que les deux intégrales :

$$I_1 := \iiiint_{\substack{(a,b,c,d)\in\mathcal{R}_3\\ q\leqslant M^6X^{-\beta_0}}} \frac{\mathrm{d}a\,\mathrm{d}b\,\mathrm{d}c\,\mathrm{d}d}{N(a+b\zeta_{12}+c\zeta_{12}^2+d\zeta_{12}^3)},$$

$$I_2 := \iiiint_{\substack{(a,b,c,d)\in\mathcal{R}_3\\ B_{14}\leqslant M^3X^{-2\beta_0}}} \frac{\mathrm{d}a\,\mathrm{d}b\,\mathrm{d}c\,\mathrm{d}d}{N(a+b\zeta_{12}+c\zeta_{12}^2+d\zeta_{12}^3)}$$

sont des $o(1)$.

Si $q \leqslant M^6X^{-\beta_0}$, il existe $i \in \{1,2,3\}$ tel que $q_i(b,c,d) \leqslant M^2X^{-\beta_0/3}$. Pour $i = \{1,2\}$ il est clair que cela implique que $\min(|b|,|c|,|d|) \leqslant MX^{-\beta_0/6}$. Si $i = 3$ alors

$$|(c\sqrt{3}-(b+2d))(c\sqrt{3}+(b+2d))| \leqslant M^2X^{-\beta_0/3}.$$

On en déduit que si a, c, d sont donnés, b appartient à au plus deux intervalles de longueur $MX^{-\beta_0/6}$. En minorant $N(\alpha)$ par M^4, on obtient :

$$I_1 \ll \frac{MX^{-\beta_0/6}N^3}{M^4} \leqslant X^{3\alpha_0/4-\beta_0/6}. \tag{17·1}$$

Pour I_2 on procède de la même façon. On reprend la notation Δ'_{14} pour le discriminant réduit de B_{14} par rapport à a. La valeur de ce discriminant a été calculée dans (13·5). Si $|B_{14}| \leqslant M^3X^{-2\beta_0}$ alors

$$d\Big|a-\frac{bc+\sqrt{\Delta'_{14}}}{d}\Big|\Big|a+\frac{bc+\sqrt{\Delta'_{14}}}{d}\Big| \leqslant M^3X^{-2\beta_0}. \tag{17·2}$$

Cette inégalité entraîne que l'un des deux facteurs ci-dessus est de module inférieur à $d^{-1/2}M^{3/2}X^{-\beta_0}$. On a vu précédemment que la contribution des $|d| \leqslant MX^{-\beta_0}$ est négligeable. Pour $|d| > MX^{-\beta_0}$, (17·2) implique que a appartient à une union finie d'intervalles de taille inférieure à $MX^{-\beta_0/2}$ et ainsi $I_2 \ll N^3MX^{-\beta_0/2}M^{-4} \ll X^{3\alpha_0/4-\beta_0/2}$.

On considère maintenant l'intégrale

$$I := \iiiint_{\mathcal{R}_3} \frac{\mathrm{d}a\,\mathrm{d}b\,\mathrm{d}c\,\mathrm{d}d}{N(a+b\zeta_{12}+c\zeta_{12}^2+d\zeta_{12}^3)}.$$

Avant de vérifier que $W_1 = (1+o(1))I$, nous déterminons la valeur de I.

Lemme 17.2. *On a la formule*

$$I = \frac{4\pi^2}{3}\log(2+\sqrt{3})\log(N/(MX^{\eta/4})).$$

L'idée consiste à écrire $\alpha = \alpha_1 = re^{it}$ et $\alpha_3 = se^{iu}$. En exprimant les différents α_i en fonction de a, b, c, d et de r, t, s, u, on a :

$$\begin{pmatrix} r\cos t\\ r\sin t\\ s\cos u\\ s\sin u\end{pmatrix} = \begin{pmatrix} 1 & \frac{\sqrt{3}}{2} & \frac{1}{2} & 0\\ 0 & \frac{1}{2} & \frac{\sqrt{3}}{2} & 1\\ 1 & -\frac{\sqrt{3}}{2} & \frac{1}{2} & 0\\ 0 & \frac{1}{2} & -\frac{\sqrt{3}}{2} & 1\end{pmatrix}\begin{pmatrix} a\\ b\\ c\\ d\end{pmatrix}.$$

En inversant la matrice ci-dessus on obtient

$$\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{6} & \frac{1}{2} & \frac{1}{2} \\ \frac{\sqrt{3}}{3} & 0 & -\frac{\sqrt{3}}{3} & 0 \\ 0 & \frac{\sqrt{3}}{3} & 0 & -\frac{\sqrt{3}}{3} \\ -\frac{\sqrt{3}}{6} & \frac{1}{2} & \frac{\sqrt{3}}{6} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} r\cos t \\ r\sin t \\ s\cos u \\ s\sin u \end{pmatrix}.$$

Le jacobien lié à ce changement de variables vaut $rs/3$, ainsi

$$I = \iiiint_{\substack{M^4X^\eta \leqslant r^2s^2 < N^4 \\ 1 \leqslant \frac{r}{s} \leqslant 2+\sqrt{3} \\ 0 \leqslant t,u < 2\pi}} \frac{\mathrm{d}r\,\mathrm{d}t\,\mathrm{d}s\,\mathrm{d}u}{3rs}.$$

Nous effectuons ensuite le changement de variables $v = rs$, $w = r/s$:

$$I = \frac{4\pi^2}{3} \iint_{\substack{M^4X^\eta \leqslant v^2 < N^4 \\ 1 \leqslant w \leqslant 2+\sqrt{3}}} \frac{\mathrm{d}v\,\mathrm{d}w}{2vw} = \frac{4\pi^2}{3} \log(2+\sqrt{3}) \log(N/(MX^{\eta/4})).$$

On établit ensuite le lemme suivant :

Lemme 17.3. *On a $W_1 = (1+o(1))I$.*

Preuve. Il s'agit de vérifier que la contribution des $(a,b,c,d) \in \mathcal{R}_3 \smallsetminus \mathcal{R}_2$ est négligeable. Nous adaptons maintenant les idées de [24] p. 586. Soit $x \in \mathcal{R}_3 \smallsetminus \mathcal{R}_2$. Il existe alors x' au bord de $\mathcal{R}_3$ tel que $\|x - x'\| \ll M$.

• On commence par étudier le cas où $|x'|^2 N(x')^{-1/2} \in \{1, 2+\sqrt{3}\}$.

On observe à partir des formules (10·11), (10·12) et (10·13) :

$$\begin{aligned} \frac{|x|^2}{\sqrt{N(x)}} &= \frac{|x'|^2}{\sqrt{N(x')}} + O(MN(x')^{-1/4} + M^2N(x')^{-1/2}) \\ &= \begin{cases} 1 + O(X^{-\eta/4}) & \text{si } |x'|^2N(x')^{-1/2} = 1 \\ 2+\sqrt{3} + O(X^{-\eta/4}) & |x'|^2N(x')^{-1/2} = 2+\sqrt{3}. \end{cases} \end{aligned}$$

En reprenant les changements de variables du Lemme 17.2, on vérifie que la contribution des x proches d'un x' tels que $|x'|^2 = \sqrt{N(x')}$ est inférieure à

$$\iint_{\substack{M^4X^\eta \leqslant v^2 < N^4X \\ |w-1| \ll X^{-\eta/4}}} \frac{\mathrm{d}v\,\mathrm{d}w}{2vw} \ll X^{-\eta/4} \log X.$$

Le cas où $|x'|^2 = (2+\sqrt{3})\sqrt{N(x')}$ se majore de la même façon.

• Il reste à traiter le cas où $N(x') \in \{M^4X^\eta, N^4\}$. On a alors

$$N(x) = N(x') + O(MN(x)^{3/4}) = \begin{cases} X^{1+\alpha_0} + O(X^{1+3\alpha_0/4}) & \text{si } N(x') = X^{1+\alpha_0} \\ X^{1+\eta} + O(X^{1+3\eta/4}) & \text{si } N(x') = X^{1+\eta}. \end{cases}$$

En reprenant à nouveau les changements de variables du Lemme 17.2, on vérifie que la contribution des $x \in \mathcal{R}_3 \smallsetminus \mathcal{R}_2$ proches d'un x' de norme $X^{1+\alpha_0}$ est inférieure à

$$\iint_{\substack{N^4 \leqslant v^2 < N^4 + O(X^{1+3\alpha_0/4}) \\ 1 \leqslant w \leqslant 2+\sqrt{3}}} \frac{\mathrm{d}v\,\mathrm{d}w}{2vw} \ll |\log((N^4 + O(X^{1+3\alpha_0/4}))/N^4)| = O(X^{-\alpha_0/4}).$$

On vérifie de la même façon que celle des x proche d'un x' de norme M^4X^η est un $O(X^{-\eta/4})$.

18. Fin de la preuve du Théorème 1.1

On rassemble les différentes conditions sur nos paramètres imposées lors des paragraphes précédents. D'après (10·10), (11·3), (11·4), (12·3), (12·9), (12·11), (12·14), (12·15), (12·16), (13·7), (15·6), (15·7), (16·1) et (17·1), les paramètres $\alpha_0, \beta_0, \eta_0, \vartheta_0$, et pour $(i,j) \in \{1,2\}^2 \cup \{(3,1)\}$, $\vartheta_{ij}, \vartheta'_{ij} = \vartheta_{ij} + \tau_{ij}$ doivent satisfaire le système de contraintes :

$$\alpha_0 > 3\vartheta_0/4,\ \eta_0 > \alpha_0 + 3\vartheta_0, \quad \frac{3\alpha_0}{4} + 3\vartheta_0 < 1/4, \quad \frac{9\alpha_0}{4} + 3\beta_0 + \eta_0 + 3\vartheta_0 < 1,$$

$$7\alpha_0 + \beta_0 + 3\vartheta_0 < 1/2, \quad \frac{3}{4} + 6\alpha_0 + \frac{\vartheta'_{31}}{256} + 3\vartheta_0 + \eta_0 < 1,$$

$$\frac{511}{512} + \frac{5\alpha_0}{4} + \frac{\vartheta'_{31} + 6\alpha_0 + \beta_0 + 3\vartheta_0}{256} + \eta_0 < 1,\ 1 + \frac{165\alpha_0}{128} + \frac{3\vartheta_0}{128} - \frac{\vartheta_{31}}{256} + \eta_0 < 1,$$

$$\vartheta_{21} + \vartheta_{22} > \frac{1}{4} + \frac{31\alpha_0}{4} + 3\vartheta_0 + 2\eta_0, \quad \vartheta_{11} + \vartheta_{12} > \frac{1}{4} + \frac{41\alpha_0}{4} + 3\vartheta_0 + 4\eta_0$$

$$\vartheta'_{12} < \frac{1}{4} - \frac{59\alpha_0}{4} - 3\vartheta_0 - 8\eta_0, \quad \vartheta'_{22} < \frac{1}{4} - \frac{99\alpha_0}{4} - 3\vartheta_0 - 16\eta_0$$

$$\vartheta'_{21} < \frac{1}{4} - \frac{179\alpha_0}{4} - 3\vartheta_0 - 32\eta_0, \quad \vartheta'_{11} < \frac{1}{4} - \frac{339\alpha_0}{4} - 3\vartheta_0 - 64\eta_0$$

$$\vartheta'_{31} < \frac{1}{4} - \frac{659\alpha_0}{4} - 3\vartheta_0 - 128\eta_0, \quad 6\alpha_0 + 5\vartheta_0 < 1/4, \quad 9\alpha_0 < 2\beta_0, 11\alpha_0 < \vartheta_{31},$$

$$11\alpha_0 + \vartheta'_{31} < \frac{1}{18},\ \max(\vartheta'_{11} + \vartheta'_{12}, \vartheta'_{21} + \vartheta'_{22}) < \frac{1}{3},\ \vartheta'_{11} + \vartheta'_{12} + \vartheta'_{21} + \vartheta'_{22} < \frac{5}{9},$$

$$2\alpha_0 < \vartheta_{i1} < \vartheta'_{i1} < \frac{1}{4} - \frac{3\alpha_0}{4} \quad (i = 1,2,3).$$

Pour de tels paramètres strictement positifs tels que les intervalles $[\vartheta_{ij}, \vartheta'_{ij}]$ soient deux à deux disjoints, on obtient $|\mathcal{A}_1| \geqslant \alpha_1 X$ où α_1 vérifie la minoration :

(18·1)

$$\alpha_1 \geqslant \frac{\alpha_0 2^{-[4/\vartheta_0]}}{12} \frac{2\log 2}{3} \log\Big(\frac{5}{4}\Big) \frac{1}{\vartheta_0} C_{-1} \frac{2^5 \vartheta_{31} \prod_{1 \leqslant i,j \leqslant 2} \vartheta_{ij}}{(1+\alpha_0)^5} \prod_{(i,j) \in \{1,2\}^2 \cup \{(3,1)\}} \log\Big(\frac{\vartheta'_{ij}}{\vartheta_{ij}}\Big)$$
$$\times \Big(\sum_{k \geqslant 1} \frac{F(k)}{k^3}\Big) \frac{4\pi^2}{3} \log(2+\sqrt{3}) \log(1 + \alpha_0 - \varepsilon).$$

avec

$$C_{-1} = \prod_{p < X^{\vartheta_0}} \Big(1 - \frac{g(p)}{p}\Big)\Big(1 - \frac{1}{p}\Big)^{-1}.$$

Les arguments de Heath-Brown [24] pp. 587-588 s'adaptent sans peine pour évaluer C_{-1} :

$$C_{-1} = \frac{\Big(1 + O(\log X)^{-1}\Big)}{\mathrm{Res}(\zeta_{\mathbb{Q}(\zeta_{12})}(s) : s = 1)} \prod_{p \equiv 1 \pmod{12}} \Big(1 - \frac{4}{p}\Big)\Big(1 - \frac{1}{p}\Big)^{-4}. \tag{18·2}$$

En appliquant divers résultats classiques sur les corps de nombres ([37] par exemple), on obtient

$$\mathrm{Res}(\zeta_{\mathbb{Q}(\zeta_{12})}(s) : s = 1) = \frac{\pi \log(2+\sqrt{3})}{18}.$$

Notons C_{-2} le produit eulérien du membre de droite de (18·2) :

$$C_{-2} = \prod_{p\equiv 1 \,(\mathrm{mod}\, 12)} \Big(1-\frac{4}{p}\Big)\Big(1-\frac{1}{p}\Big)^{-4} > 0,94.$$

Notons $\Theta = (\vartheta_{11}, \vartheta'_{11}, \vartheta_{12}, \vartheta'_{12}, \vartheta_{21}, \vartheta'_{21}, \vartheta_{22}, \vartheta'_{22}, \vartheta_{31}, \vartheta'_{31})$. On a alors

$$\alpha_1 > 0.07 \times A(\alpha_0, \vartheta_0, \Theta),$$

avec

$$A(\alpha_0,\vartheta_0,\Theta) = \frac{\alpha_0 2^{-[4/\vartheta_0]}\vartheta_{31}\vartheta_{11}\vartheta_{12}\vartheta_{21}\vartheta_{22}}{\vartheta_0(1+\alpha_0)^5} \times \log\Big(\frac{\vartheta'_{11}}{\vartheta_{11}}\Big)\log\Big(\frac{\vartheta'_{12}}{\vartheta_{12}}\Big)\log\Big(\frac{\vartheta'_{21}}{\vartheta_{21}}\Big)\log\Big(\frac{\vartheta'_{22}}{\vartheta_{22}}\Big)\log\Big(\frac{\vartheta'_{31}}{\vartheta_{31}}\Big)\log(1+\alpha_0).$$

Dans la formule ci-dessus le terme en $2^{-[4/\vartheta_0]}$ est le terme le plus déterminant. On choisit donc nos différents paramètres de sorte que ϑ_0 soit le plus grand possible. Cela revient à maximiser ϑ_0, les paramètres $\alpha_0, \beta_0, \eta_0, \vartheta_0, \Theta$ devant vérifier un système linéaire avec une trentaine d'inéquations. Si on écrit

$$y = (\alpha_0, \beta_0, \eta_0, \vartheta_0, \vartheta_{11}, \vartheta'_{11}, \vartheta_{12}, \vartheta'_{12}, \vartheta_{21}, \vartheta'_{21}, \vartheta_{22}, \vartheta'_{22}, \vartheta_{31}, \vartheta'_{31}),$$

cela correspond à résoudre le programme linéaire

$$\max_{\substack{Ay\leqslant B-\varepsilon \\ y\in[0,+\infty[^{14}}} \vartheta_0, \tag{18·3}$$

pour une matrice A et un vecteur B adéquats et un paramètre $\varepsilon > 0$. Le symbole "$\leqslant$" de (18·3) signifie que pour tout k, la k ème coordonnée de Ay est inférieure ou égale à la kème coordonnée de $B-\varepsilon$.

Ce programme linéaire est résolu par la méthode du simplexe programmée dans le langage pari-gp par Bruno Pinçon. L'ensemble des calculs s'effectue dans $\mathbb{Q}$ si bien que les valeurs rationnelles données dans les tableaux ci-dessous sont exactes. En procédant par dichotomie pour le choix de ε, nous avons pris $\varepsilon = 4.5472\ 10^{-9}$ dans (18·3). Les valeurs obtenues sont données dans les trois tableaux suivants.

α_0	β_0	η_0	ϑ_0
$\frac{78128312351}{2290781250000000}$	$\frac{156258939511}{1018125000000000}$	$\frac{781220623667}{4581562500000000}$	$\frac{156235791421}{3436171875000000}$
$3,41\ 10^{-5}$	$1,15\ 10^{-4}$	$1,71\ 10^{-4}$	$4,546\ 10^{-5}$

Dans ce premier tableau, les valeurs données dans la 3 ème lignes sont arrondies pour des raisons de place. Dans les trois tableaux suivants les approximations sont plus précises car les exposants ϑ_{ij} et ϑ'_{ij} sont très proches, en fait, $\vartheta'_{ij} - \vartheta_{ij} \simeq 10^{-9}$.

ϑ_{11}	ϑ_{12}	ϑ_{21}	ϑ_{22}
$\frac{968734128851}{305437500000000}$	$\frac{2272422179928127}{9163125000000000}$	$\frac{70799515139}{15908203125000}$	$\frac{150453167830361}{610875000000000}$
0.00317162800524166	0.247996418244663	0.00445050359130362	0.246291250796580

ϑ'_{11}	ϑ'_{12}	ϑ'_{21}	ϑ'_{22}
$\frac{2421838794341}{763593750000000}$	$\frac{2272422221594689}{9163125000000000}$	$\frac{2265586799257}{509062500000000}$	$\frac{752265853040659}{3054375000000000}$
0.00317163255244166	0.247996422791863	0.00445050813850362	0.246291255343780

ϑ_{31}	ϑ'_{31}
$\frac{63203096365429}{1145390625000000}$	$\frac{252812406294997}{4581562500000000}$
0.0551803856133614	0.0551803901605614

Si on résout (18·3) avec $\varepsilon = 0$ le meilleur exposant ϑ_0 possible semble être $\vartheta_0 = 2/43983 \simeq 4,547211\ 10^{-5}$. L'exposant que nous obtenons dans le 1er tableau est ainsi quasiment optimal. On en déduit que

$$A(\alpha_0, \vartheta_0, \Theta) > 1.53029\ 10^{-26529},$$

puis $\alpha_1 > 1,07\ 10^{-26530}$ et

$$P_X > X^{1+10^{-26531}}.$$

Bibliographie

[1] A. Balog, V. Blomer, C. Dartyge and G. Tenenbaum, Friable values of binary forms, *Commentarii Math. Helv.* 87 (2012), 639-667.

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

[3] K. Belabas et E. Fouvry, Sur le 3-rang des corps quadratiques de discriminant premier ou pseudo-premier, *Duke Mathematical Journal*, Vol. 98 (1999), pp. 217-268.

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

[5] R. de la Bretèche and T. D. Browning, Sums of arithmetic functions over values of binary formes, *Acta Arith.*125 no. 3, (2006), 291-304.

[6] R. de la Bretèche & T.D. Browning, Binary linear forms as sums of two squares, *Compositio Mathematicae*, **144** (6), (2008), 1375-1402.

[7] R. de la Bretèche & T.D. Browning, Le problème des diviseurs pour des formes binaires de degré 4, *J. reine angew. Math.*, **646**, (2010), 1–44.

[8] R. de la Bretèche & T.D. Browning, Binary forms of two squares and Châtelet surfaces, *Israel Journal of Math.*, **191** (2012), 973-1012.

[9] R. de la Bretèche et G. Tenenbaum, Moyennes de fonctions arithmétiques de formes binaires, *Mathematika*, 58 (2012), 290-304.

[10] R. de la Bretèche et G. Tenenbaum, Sur la conjecture de Manin pour certaines surfaces de Châtelet, *J. Inst. Math. Jussieu*, à paraître.

[11] J. W. S. Cassels, *An introduction to the geometry of numbers*, Die Grundlehren der Mathematischen Wissenschaften, Band 99, Springer Verlag, Berlin Gottingen Heidelberg (1959).

[12] S. Daniel, On the divisor-sum problem for binary forms, *J. reine angew. Math.* **507** (1999), 107-129.

[13] C. Dartyge, Le plus grand facteur premier de $n^2 + 1$ où n est presque premier, *Acta Arith.* **76** (1996), 199-226.

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

[15] J.-M. Deshouillers and H. Iwaniec, Kloosterman sums and Fourier coefficients of cusp forms, *Invent. Math.* 70 (1982), no. 2, 219–288.

[16] J.-M. Deshouillers and H. Iwaniec, On the greatest prime factor of n^2+1, *Ann. Inst. Fourier (Grenoble)* 32 (1982/83) no 4, 1-11.

[17] P. Erdős, On the greatest prime factor of $\prod_{k=1}^{x} f(k)$, *J. London Math. Soc.*27, (1952), 379-384.
[18] P. Erdős and A. Schinzel, On the greatest prime factor of $\prod_{k=1}^{x} f(k)$ *Acta Arith.*, 55 (1990), 191-200.
[19] E. Fouvry, H. Iwaniec, Gaussian primes, *Acta Arith.* **79** (1997), 249-287.
[20] J. B. Friedlander and H. Iwaniec, The polynomial $X^2 + Y^4$ captures its primes, *Ann. of Math.* (2), 148(3), (1998), 945-1040.
[21] C. Gomez, B. Salvy et P. Zimmermann, *Calcul formel : mode d'emploi, exemples en Maple* Logique mathématiques informatique, ed. Masson (1995).
[22] G. Greaves, Large prime factors of binary forms, *J. Number Theory* **3** (1971), 35-59.
[23] H. Halberstam and H. Richert, *Sieve Methods* (2nd ed.). Dover. (2011)
[24] D. R. Heath-Brown, The largest prime factor of $X^3 + 2$, *Proc. London Math. Soc.* (3) 82 (2001), 554-596.
[25] D. R. Heath-Brown, Primes represented by $x^3 + 2y^3$, *Acta Math.*, 186 (1) :1-84, 2001.
[26] D.R. Heath-Brown, Linear relations amongst sums of two squares. *Number theory and algebraic geometry*, 133–176, Lond. Math. Soc. Lecture Note Ser. **303** CUP, 2003.
[27] D. R. Heath-Brown and B. Z. Moroz, Primes represented by binary cubic forms, *Proc. London Math. Soc.* 84, no. 2, (2002), 257-288.
[28] D. R. Heath-Brown and B. Z. Moroz, On the representation of primes by cubic polynomials in two variables, *Proc. London Math. Soc.* 88, no. 2, (2004), 289-312.
[29] K. Henriot, Nair-Tenenbaum bounds uniform with respect to the discriminant, *Math. Proc. Camb. Phil. Soc.* **152** (2012), 405-424
[30] C. Hooley, On the greatest prime factor of a quadratic polynomial, *Acta Math.* **117** (1967), 281-299.
[31] C. Hooley, *Application of sieve methods to the theory of numbers* Cambridge university press, (1976). - xiv, 122 p.
[32] C. Hooley, On the greatest prime factor of a cubic polynomial, *J. reine angew. Math.* 303/304 (1978) 21-50.
[33] H. Iwaniec, Primes represented by quadratic polynomials in two variables, *Acta Arith.*, 24 (1974), 435-459.
[34] H. Iwaniec, Almost-primes represented by quadratic polynomials, *Inven. Math.*, 47 (2), (1978), 171-188.
[35] H. Iwaniec, Rosser's sieve, *Acta Arith.*, 36 (1980), 171-202.
[36] H. Iwaniec, A new form of the error term in the linear sieve, *Acta Arith.*, 37 (1980), 307-320.
[37] S. Lang, *Algebraic Number Theory*, Second edition, GTM 110, Springer (1994).
[38] G. Lejeune Dirichlet, *Mathematische Werke. Bände I, II, Herausgegeben auf Veranlassung der Königlich Preussischen Akademie der Wissenschaften von L. Kronecker*, Chelsea Publ. Co., Bronx, NY, 1969.
[39] R. J. Lemke Oliver, Almost-primes represented by quadratic polynomials, *Acta Arithmetica*, 151 (2012), pp. 241-261
[40] G. Marasingha, On the representation of almost primes by pairs of quadratic forms, *Acta Arith.* 124. 4 (2006), 327-355.
[41] G. Marasingha, Almost primes represented by binary forms, *Journal of the London Mathematical Society* (2) 82 (2010), 295–316.
[42] A. A. Markov, Über die Primteiler des Zahlen von der Form $1 + 4x^2$, *Bull. Acad. Sci. St. Petersburg* 3 (1895) 55-59.
[43] J. Martinet, *Les réseaux parfaits des espaces euclidiens*, Ed. Masson (1996).
[44] T. Nagell Généralisation d'un théorème de Tchébychev, *J. de Mathématiques*, 4 (1921), 343-356.
[45] T. Nagell, *Introduction to number theory*, New York 1951.
[46] M. Nair and G. Tenenbaum, Short sums of certain arithmetic functions, *Acta Math.* 180 (1998), 119-144.
[47] G. Pólya, Généralisation d'un théorème de M. Störmer, Archiv for Mathematik og Naturvidenskab, t. XXXV, Kristiania, 1917
[48] A. Schinzel et W. Sierpiński, Sur certaines hypothèses concernant les nombres premiers, *Acta Arith.*, 4 (1958), 185-208.
[49] H. J. S. Smith, *Report on the theory of numbers*, Collected Mathematical Papers, vol. 1, reprinted, Chelsea, (1965).
[50] G. Tenenbaum, Sur une question d'Erdős et Schinzel, II, *Inv. Math.* 99 (1990), 215-224.
[51] G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres* 3ème édition, Collection Échelles, Édition Belin (2008).
[52] L. C. Washington, *Introduction to cyclotomic fields*, GTM 83, Springer, New York, Heidelberg, Berlin (1982).
[53] A. Weil, Sur les courbes algébriques et les variétés qui s'en déduisent, Publ. Inst. Math. Univ. Strasbourg 7 (1945), Hermann, Paris, (1948).