ACTA ARITHMETICA
169.3 (2015)

Plus grand facteur premier de valeurs de polynômes aux entiers

par

R. de la Bretèche (Paris)

(avec un appendice par R. de la Bretèche et J.-F. Mestre)

1. Introduction. Le but de cet article est de généraliser le récent article de Dartyge [3] qui étudie la taille du plus grand facteur premier de valeurs aux entiers du douzième polynôme cyclotomique $\Phi_{12}(X) := X^4 - X^2 + 1$. Nous notons $P^+(n)$ le plus grand facteur premier d'un entier n avec la convention $P^+(1) = 1$. Son résultat est le suivant.

Théorème 1.1 ([3]). *Lorsque X tend vers l'infini, on a*

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

Dartyge utilise la méthode développée par Heath-Brown [5] pour le polynôme X^3+2. Pour l'historique de ce problème, nous renvoyons à l'introduction de [3]. Par la même méthode, nous nous proposons d'établir le résultat suivant.

Théorème 1.2. *Soit Φ un polynôme à coefficients entiers, irréductible sur $\mathbb{Q}$, pair, unitaire de degré 4, dont le groupe de Galois associé est isomorphe à $V_4 := \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Il existe une constante $c_\Phi > 0$ telle que, lorsque X tend vers l'infini, l'ensemble des entiers $n \le X$ tels que*

$$P^+(\Phi(n)) \ge X^{1+c_\Phi}$$

est de densité strictement positive.

Remarques. 1. Nous nous restreignons donc au cas où $\Phi(X) = X^4 + \mu_2 X^2 + \mu_0$ et nous notons ζ une racine du polynôme irréductible. Nous savons (cf. par exemple [9, Corollary 2.2.4]) que $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = V_4$ si et seulement s'il existe $u \in \mathbb{Z}^*$ tel que $\mu_0 = u^2$. Le polynôme Φ_{12} satisfait donc

2010 *Mathematics Subject Classification*: Primary 11N32.
Key words and phrases: Chebyshev's problem, largest prime factors in polynomial sequences, sieves problem, equidistribution results.

ces hypothèses. Cette restriction peut paraître décevante mais elle permet d'obtenir toutes les extensions K de degré 4 avec ce groupe de Galois. En effet, il existe D_1 et D_2 tels que $K = \mathbb{Q}[\sqrt{D_1}, \sqrt{D_2}]$. Le polynôme $\zeta = \sqrt{D_1} + \sqrt{D_2}$ engendre ce corps et annule le polynôme $X^4 - 2(D_1 + D_2)X^2 + (D_1 - D_2)^2$. La nullité des coefficients de Φ de degré 1 et 3 permet de rendre les calculs moins asphyxiants.

2. Un des points clés de la démonstration est le théorème 3.11 (théorème 8.1 de [3]) qui est un résultat d'équirépartition issu de la géométrie des nombres. Une extension de celui-ci permettrait d'étendre notre résultat à d'autres polynômes (voir la remarque suivant le théorème 3.11). Comme il est montré dans l'appendice en collaboration avec Mestre, pour être étendue à tous les polynômes de degré 4, la méthode développée ici nécessiterait des résultats d'équirépartition efficace pour des formes de degré 4. Il faudrait par exemple pouvoir prendre $Q_1 \geq M^{2+\varepsilon}$ et $Q_2 \geq M^{1+\varepsilon}$ dans le théorème 3.11, alors que nous énonçons un résultat non trivial que lorsque $Q_1 Q_2 \leq M^{3-\varepsilon}$ et $Q_1 + Q_2 \leq M^{2-\varepsilon}$.

3. Ainsi, le théorème 1.2 s'applique par exemple pour $\Phi(X) = X^4 + 1$, $\Phi(X) = X^4 - 10X^2 + 1$, mais pas pour $\Phi(X) = X^4 + 2$.

Plan de l'article. Dans la deuxième section, nous développons des calculs de résultants et de polynômes. Dans la troisième, nous développons les résultats techniques dont nous aurons besoin. Finalement la démonstration de notre théorème ne commence qu'à la section 4. Est mis en place la méthode initié par Erdős qui permet de se ramener à la majoration d'une somme S_1 (cf. section 5) et la minoration d'une somme S_0 (cf. section 6). Un appendice rédigé en collaboration avec Jean-François Mestre permet de généraliser les calculs de la section 2 à tout polynôme de degré n. Cela permet notamment d'expliquer pourquoi la méthode mise en œuvre ne peut être appliquée dans le cas où le groupe de Galois associé n'est pas V_4.

2. Quelques calculs de résultants.

La méthode de [3] repose sur certains calculs polynomiaux. Dans cette section, nous montrons que ces calculs se généralisent et mettons en évidence les raisons pour lesquelles ce travail ne s'applique pas aux polynômes dont le groupe de Galois associé diffère de V_4. Cette section peut être omise en première lecture. Elle permet d'introduire un certain nombre de notations utiles pour la suite.

Soit ζ une racine de Φ. Nous posons

$$\alpha = a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3 \tag{2.1}$$

avec les $a_i \in \mathbb{Z}$ et nous introduisons la norme de cet élément,

$$N(\alpha) := \prod_{\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})} \big(a_0 + a_1\tau(\zeta) + a_2\tau(\zeta)^2 + a_3\tau(\zeta)^3\big). \tag{2.2}$$

Afin que N soit vu comme un polynôme des variables $\mathbf{a} = (a_0, a_1, a_2, a_3)$, nous définissons N le polynôme de $\mathbb{Z}[a_0, a_1, a_2, a_3]$ par

$$N(a_0, a_1, a_2, a_3) := \prod_{\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})} \big(a_0 + a_1\tau(\zeta) + a_2\tau(\zeta)^2 + a_3\tau(\zeta)^3\big). \tag{2.3}$$

La matrice M_α de la multiplication par α dans la base $\{1, \zeta, \zeta^2, \zeta^3\}$ est

$$M_\alpha := \begin{pmatrix} a_0 & -\mu_0 a_3 & -\mu_0 a_2 & -\mu_0 a_1 + \mu_0\mu_2 a_3 \\ a_1 & a_0 & -\mu_0 a_3 & -\mu_0 a_2 \\ a_2 & a_1 - \mu_2 a_3 & a_0 - \mu_2 a_2 & -\mu_2 a_1 + (-\mu_0 + \mu_2^2) a_3 \\ a_3 & a_2 & a_1 - \mu_2 a_3 & a_0 - \mu_2 a_2 \end{pmatrix}.$$

Soient $\{B_{ij}\}_{1 \le i,j \le 4}$ la famille des cofacteurs de M_α, de sorte que

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

Les formules de Cramer permettent d'écrire

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

et donc, comme $M_\alpha^{-1} = M_{\alpha^{-1}}$, nous avons

$$M_\alpha^{-1} = \frac{1}{N(\alpha)} \begin{pmatrix} B_{11} & -\mu_0 B_{14} & -\mu_0 B_{13} & -\mu_0 B_{12} + \mu_0\mu_2 B_{14} \\ B_{12} & B_{11} & -\mu_0 B_{14} & -\mu_0 B_{13} \\ B_{13} & B_{12} - \mu_2 B_{14} & B_{11} - \mu_2 B_{13} & -\mu_2 B_{12} + (\mu_2^2 - \mu_0) B_{14} \\ B_{14} & B_{13} & B_{12} - \mu_2 B_{14} & B_{11} - \mu_2 B_{13} \end{pmatrix}.$$

De simples calculs fournissent

$$\begin{aligned} B_{14} &= -a_3 a_0^2 + 2a_1 a_2 a_0 + \mu_0\mu_2 a_3^3 - (\mu_2^2 + \mu_0) a_1 a_3^2 \\ &\quad + \mu_0 a_1^2 a_3 + 2\mu_2 a_1^2 a_3 - a_1^3 - \mu_2 a_1 a_2^2, \\ B_{13} &= -a_2 a_0^2 + (-2\mu_2 a_1 a_3 + (-\mu_0 + \mu_2^2) a_3^2 + \mu_2 a_2^2 + a_1^2) a_0 \\ &\quad + \mu_0 a_2 (2a_1 a_3 - \mu_2 a_3^2 - a_2^2). \end{aligned}$$

De même, B_{12} est un polynôme quadratique en a_0 de coefficient dominant $-a_1$.

Avec les manipulations (4.4) de [3], nous obtenons l'analogue de (4.5) de [3],

$$B_{14}\zeta \equiv B_{24} \equiv B_{13} \pmod{\alpha}, \tag{2.4}$$

puis l'analogue de (5.2) de [3],

$$B_{13}\zeta \equiv B_{23} \equiv B_{12} - \mu_2 B_{14} \pmod{\alpha}. \tag{2.5}$$

Les relations (2.4) et (2.5) fournissent alors

$$B_{12}B_{14} - \mu_2 B_{14}^2 - B_{13}^2 \equiv 0 \pmod{N(\alpha)}.$$

En identifiant le coefficient de degré 4 en a_0, nous obtenons

$$B_{12}B_{14} - \mu_2 B_{14}^2 - B_{13}^2 = N(\alpha) q_4(a_1, a_2, a_3), \tag{2.6}$$

où

$$q_4(a_1, a_2, a_3) = a_1 a_3 - \mu_2 a_3^2 - a_2^2. \tag{2.7}$$

La forme quadratique q_4 est de rang 3 ; elle est donc irréductible sur $\mathbb{Q}$.

Notant $\mathrm{Rés}(P_1, P_2; x)$ le résultant des polynômes P_1 et P_2 suivant la variable x, nous introduisons les résultants suivants :

$$\begin{aligned} R &:= R(a_1, a_2, a_3) = \mathrm{Rés}(B_{14}, N; a_0), \\ R_0 &:= R_0(a_1, a_2, a_3) = \mathrm{Rés}(B_{13}, B_{14}; a_0). \end{aligned} \tag{2.8}$$

Lemme 2.1. *Nous avons*

$$q_4^2 R = R_0^2.$$

Démonstration. La forme quadratique q_4 ne dépend pas de a_0 et $\deg_{a_0}(B_{14}) = 2$, donc

$$\begin{aligned} q_4^2 R &= \mathrm{Rés}(B_{14}, -q_4 N; a_0) = \mathrm{Rés}(B_{14}, B_{13}^2 - B_{12}B_{14} + \mu_2 B_{14}^2; a_0) \\ &= \mathrm{Rés}(B_{14}, B_{13}^2; a_0) = R_0^2. \ \blacksquare \end{aligned}$$

Nous avons

$$\mathrm{Disc}(\Phi) = 16\mu_0(4\mu_0 - \mu_2^2)^2.$$

Un calcul grâce à Maple fournit

$$R_0 = q_1 q_2 q_3 q_4$$

avec

$$\begin{aligned} q_1(a_1, a_2, a_3) &:= a_1^2 + (\mu_2 + 2u)a_2^2 - 2(u + \mu_2)a_1 a_3 + (\mu_2 + u)^2 a_3^2 \\ &= (a_1 - (\mu_2 + u)a_3)^2 + (\mu_2 + 2u)a_2^2, \\ q_2(a_1, a_2, a_3) &:= q_2(a_1, a_3) = a_1^2 - \mu_2 a_1 a_3 + \mu_0 a_3^2, \\ q_3(a_1, a_2, a_3) &:= a_1^2 + (\mu_2 - 2u)a_2^2 + 2(u - \mu_2)a_1 a_3 + (\mu_2 - u)^2 a_3^2 \\ &= (a_1 - (\mu_2 - u)a_3)^2 + (\mu_2 - 2u)a_2^2. \end{aligned} \tag{2.9}$$

Nous détaillerons ces calculs dans un cadre général dans la section suivante pour expliquer pourquoi notre méthode ne s'applique qu'au cas $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = V_4$.

Notons que

$$(\mu_2 - 2u)q_1 + 4uq_2 = (\mu_2 + 2u)q_3. \tag{2.10}$$

Il existe deux polynômes $U, V \in \mathbb{Z}[\mathbf{a}]$ de degré total ≤ 5 tels que

$$UB_{13} + VB_{14} = -R_0 = -qq_4 \tag{2.11}$$

avec $q = q_1q_2q_3$.

LEMME 2.2. *Lorsque* $\alpha = a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3 \in \mathbb{Z}[\zeta]$, *nous avons*

$$UN(\alpha) - B_{13}q \equiv 0 \pmod{B_{14}}.$$

Démonstration. En rassemblant (2.6) et (2.11), nous obtenons

$$q_4(UN - B_{13}q) = B_{14}(-\mu_2 B_{14}U + B_{12}U + B_{13}V).$$

Le résultat découle de la factorialité de $\mathbb{Z}[a_0, a_1, a_2, a_3]$ et de la coprimalité de q_4 et B_{14} vus comme éléments de $\mathbb{Z}[a_0, a_1, a_2, a_3]$. ∎

Des calculs réalisés par Maple fournissent

$$U = U_1a_0 + U_0 \tag{2.12}$$

avec

$$\begin{aligned} U_1 &:= (\mu_0 - \mu_2^2)a_3^4 - a_1^2a_3^2 + 2a_1a_2^2a_3 - \mu_2a_2^2a_3^2 + 2\mu_2a_1a_3^3, \\ U_0 &:= -4a_1^2a_2^3 + (\mu_0 + 3\mu_2^2)a_1a_2a_3^3 - 2\mu_0\mu_2a_2a_3^4 \\ &\quad - 6\mu_2a_1^2a_2a_3^2 + 3\mu_2a_1a_2^3a_3 + 3a_1^3a_2a_3 - 2\mu_0a_2^3a_3^2. \end{aligned}$$

Nous utiliserons plus tard la relation

$$(\mu_2 + 2u)U_1 = a_3\{(2a_1 - \mu_2a_3)q_1 + 2(-a_1 + (\mu_2 + u)a_3)q_2\}. \tag{2.13}$$

De plus

$$\begin{aligned} V := {} & -a_1^3a_2^2 + a_1^4a_3 + 4\mu_0\mu_2a_1a_3^4 + 2\mu_2a_0a_1a_2a_3^2 - \mu_2a_0a_2^3a_3 - a_0a_1^2a_2a_3 \\ & + \mu_0a_0a_2a_3^3 - \mu_2^2a_0a_2a_3^3 + 5\mu_0a_1a_2^2a_3^2 - 5\mu_2^2a_1a_2^2a_3^2 - 4\mu_0\mu_2a_2^2a_3^3 \\ & + 4\mu_2a_1^2a_2^2a_3 - \mu_2a_1a_2^4 - 2\mu_0a_2^4a_3 + 6\mu_2^2a_1^2a_3^3 - 4\mu_2^3a_1a_3^4 - 4\mu_2a_1^3a_3^2 \\ & + \mu_2^2a_2^4a_3 + 2\mu_2^3a_2^2a_3^3 - 2\mu_0a_1^2a_3^3 - 2\mu_0\mu_2^2a_3^5 + \mu_0^2a_3^5 + \mu_2^4a_3^5 + 2a_0a_1a_2^3. \end{aligned}$$

3. Résultats préliminaires

3.1. Résultats intermédiaires faisant intervenir certaines congruences. Nous énonçons certains résultats de [3] généralisables à notre situation. Lorsque I est un idéal de $\mathbb{Z}[\alpha]$, nous introduisons

$$\rho(I) := \operatorname{card}\{0 \leq n < N(I) : n \equiv \zeta \pmod{I}\}. \tag{3.1}$$

Lorsque I est principal et engendré par α, nous noterons $\rho(\alpha) := \rho((\alpha))$. Le lemme suivant est l'analogue du lemme 3.1 de [3].

LEMME 3.1. *Soit I un idéal de $\mathbb{Z}[\zeta]$ tel que $(N(I), \operatorname{Disc}(\Phi)) = 1$. Si l'équation $n \equiv \zeta \pmod{I}$ admet une solution avec n entier, alors I est un produit d'idéaux premiers $\mathfrak{p}$ tels que $N(\mathfrak{p}) = p$. De plus, I ne peut être divisible par deux idéaux premiers différents de même norme. Réciproquement,*

si $N(I)$ est premier avec le discriminant de Φ, si I n'est pas divisible par deux idéaux premiers différents de même norme, et enfin si I est un produit d'idéaux premiers dont la norme est un nombre premier, alors cette congruence admet des solutions et $\rho(I) = 1$.

De plus, si I est un idéal tel que $(N(I), \mathrm{Disc}(\Phi)) = 1$ satisfaisant les conditions ci-dessus, alors $\rho(I) = 1$. Pour de tels I, pour tout $m \in \mathbb{Z}$, $I \mid m$ équivaut à $N(I) \mid m$.

Nous ne précisons pas la démonstration qui est identique à celle du lemme 3.1 de [3].

Le lemme suivant généralise le lemme 4.1 de [3].

LEMME 3.2. *Soit α défini par (2.1) satisfaisant $(B_{14}, N(\alpha)) = 1$ et $n \in \mathbb{Z}$. Il existe $k_\alpha \in \mathbb{Z}$ tel que $0 \le k_\alpha < N(\alpha)$ et que l'on ait l'équivalence*

$$n - \zeta \in (\alpha) \ \Leftrightarrow \ n \equiv k_\alpha \pmod{N(\alpha)}.$$

De plus, on a

$$k_\alpha \equiv B_{13}\overline{B_{14}} \pmod{N(\alpha)}.$$

De même, lorsque J est un idéal tel qu'il existe $\alpha \in \mathbb{Z}[\zeta]$ satisfaisant les hypothèses précédentes et $J \mid (\alpha)$, alors il existe un unique k_J ne dépendant que de J tel que $0 \le k_J < N(J)$ et

$$n - \zeta \in (J) \ \Leftrightarrow \ n \equiv k_J \pmod{N(J)}.$$

REMARQUE. Le dernier point quoiqu'élémentaire est un moyen de dépasser les obstacles liés au fait que $\mathbb{Z}[\zeta]$ peut ne pas être principal. L'idée de ce lemme remonte au moins à Hooley [6] et a été utilisée dans [5] et [3].

Démonstration du lemme 3.2. Le premier point découle de (2.4) et du lemme 3.1. Pour le dernier point, nous observons que $k_J = k_\alpha$ convient puisque $N(J) \mid N(\alpha)$, et qu'il est forcément unique. ∎

Nous généralisons le lemme 6.2 de [3], qui est un point clé de la méthode de Dartyge.

LEMME 3.3. *Soit $\alpha = a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3 \in \mathbb{Z}[\zeta]$ tel que $(q, B_{14}) = 1$. Alors $(N(\alpha), B_{14}) = 1$ et*

$$\frac{B_{13}\overline{B_{14}}}{N(\alpha)} - \frac{U\overline{B_{14}}}{q} \equiv \frac{B_{13}}{B_{14}N(\alpha)} - \frac{U}{qB_{14}} \pmod 1.$$

Démonstration. La relation $(N(\alpha), B_{14}) = 1$ découle du fait que q^2 est le résultant de $N(\alpha)$ et de B_{14}. Le point clé du lemme 6.2 de [3] est la relation

$$\frac{\overline{u}}{v} + \frac{\overline{v}}{u} \equiv \frac{1}{uv} \pmod 1. \tag{3.2}$$

Le lemme 2.2 fournit

$$\frac{B_{13}\overline{B_{14}}}{N(\alpha)} \equiv -\frac{B_{13}\overline{N(\alpha)}}{B_{14}} + \frac{B_{13}}{B_{14}N(\alpha)} \equiv -\frac{U\overline{q}}{B_{14}} + \frac{B_{13}}{B_{14}N(\alpha)} \pmod 1.$$

En réappliquant (3.2) au premier terme du membre de droite, nous obtenons le résultat. ∎

Le lemme suivant généralise le lemme 7.5 de [3].

LEMME 3.4. *Soit $\Phi \in \mathbb{Z}[X]$ satisfaisant les hypothèses du théorème* 1.2 *et $a_2, a_3 \in \mathbb{Z}$ et p un nombre premier tels que $(p, a_2a_3\operatorname{Disc}(\Phi)) = 1$. Lorsque $1 \le i < j \le 3$, le système de congruences*

$$\begin{cases} q_i(a_1, a_2, a_3) \equiv 0 \pmod p, \\ q_j(a_1, a_2, a_3) \equiv 0 \pmod p \end{cases}$$

admet une solution en a_1 si, et seulement si, $\Phi(a_2\overline{a}_3) \equiv 0 \pmod p$. Dans ce cas, la solution a_1 est déterminée de manière unique modulo p.

REMARQUE. Ce lemme nécessite l'hypothèse $\operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = V_4$.

Démonstration du lemme 3.4. Soient a_2 et a_3 des entiers tels que l'on a $\Phi(a_2\overline{a}_3) \equiv 0 \pmod p$. Grâce à (2.10) et à la condition $p \nmid \operatorname{Disc}(\Phi) = 14u^2(2u-\mu_2)^2(2u+\mu_2)^2$, nous pouvons nous contenter de traiter le cas $(i,j) = (1,3)$. Nous renvoyons à (2.9) pour l'expression des q_i. Posant $y = a_2\overline{a}_3$, on a $(y+u\overline{y})^2 \equiv -\mu_2 + 2u$ et ainsi les solutions de $q_3(a_1, a_2, a_3) \equiv 0 \pmod p$ s'écrivent $a_1^{(\varepsilon)} \equiv (\mu_2 - u)a_3 + \varepsilon(y + u\overline{y})a_2$ avec $\varepsilon = \pm 1$. On a

$$\begin{aligned} q_1(a_1^{(\varepsilon)}, a_2, a_3) &\equiv (-2ua_3 + \varepsilon(y+u\overline{y})a_2)^2 + (\mu_2 + 2u)a_2^2 \\ &\equiv 4a_3^2(u^2 + uy^2 - \varepsilon uy(y + u\overline{y})) \pmod p. \end{aligned}$$

Cette quantité est nulle si, et seulement si, $\varepsilon = 1$.

Réciproquement, prenons une solution a_1 du système. Nous avons

$$a_1 - \mu_2 a_3 = -\overline{(4ua_3)}(q_1 - q_3 - 4ua_2^2) \equiv a_3(a_2\overline{a}_3)^2 \pmod p,$$

puis

$$\begin{aligned} q_3(a_1, a_2, a_3) &\equiv a_3^2\big(((a_2\overline{a}_3)^2 + u)^2 + (\mu_2 - 2u)(a_2\overline{a}_3)^2\big) \\ &\equiv a_3^2\big((a_2\overline{a}_3)^4 + \mu_2(a_2\overline{a}_3)^2 + \mu_0\big) \pmod p, \end{aligned}$$

ce qui fournit le résultat recherché. ∎

En effet, nous pouvons faire un changement de variable $a_1' = a_1 - (\mu_2 + u)a_3$ pour que q_1 ne dépende que de (a_1', a_2) et que q_2 ne dépende que de (a_1', a_3). Ainsi

$$\begin{aligned} q_1(a_1, a_2, a_3) &= a_1'^2 + (\mu_2 + 2u)a_2^2, \\ q_2(a_1, a_2, a_3) &= a_1'^2 + (\mu_2 + 2u)a_1'a_3 + (u\mu_2 + 2\mu_0)a_3^2, \\ q_3(a_1, a_2, a_3) &= (a_1' + 2ua_3)^2 + (\mu_2 - 2u)a_2^2. \end{aligned} \tag{3.3}$$

Reprenant les notations de [3], lorsque $f \in \mathbb{Z}[X_1, X_2, X_3]$, posons

$$\sigma_f(m) := |\{0 < a_1, a_2, a_3 \le m : m \mid f(a_1, a_2, a_3)\}|,$$
$$\sigma_f^*(m) := |\{0 < a_1, a_2, a_3 \le m : m \mid f(a_1, a_2, a_3),\ (m, a_1a_2a_3) = 1\}|.$$

Nous notons

$$d_1 := -\mu_2 - 2u, \qquad d_2 := 4\mu_0 - \mu_2^2, \qquad d_3 := -\mu_2 + 2u.$$

Le lemme suivant est l'analogue du lemme 7.6 de [3]; la démonstration est évidente.

LEMME 3.5. *Soit $i \in \{1, 2, 3\}$. Lorsque $p \nmid 2d_i$ et $\nu \ge 1$, nous avons*

$$\sigma_{q_i}^*(p^\nu) = \phi(p^\nu)^2\left\{1 + \left(\frac{d_i}{p}\right)\right\}, \qquad \sigma_{q_i}(p) = p\left(1 + (p-1)\left\{1 + \left(\frac{d_i}{p}\right)\right\}\right). \ \blacksquare$$

3.2. Domaine fondamental pour l'action du groupe des unités de $\mathbb{Q}(\zeta)$. Comme dans [3], nous devons considérer l'action du groupe E des unités de $\mathbb{Q}(\zeta)$ sur les éléments de $\mathbb{Z}[\zeta]$. Nous avons deux cas possibles ([1]) :

(i) $\mathbb{Q}(\zeta) \not\subset \mathbb{R}$: il existe w une unité de module > 1 telle que $E = E_0 \times \langle w \rangle$ où E_0 est un groupe fini cyclique engendré par w_0 inclu dans le groupe des racines de l'unité appartenant à $\mathbb{Q}(\zeta)$.

(ii) $\mathbb{Q}(\zeta) \subset \mathbb{R}$: il existe trois unités $w_3 > w_2 > w_1 > 1$ telles que $E = E_0 \times \langle w_1, w_2, w_3 \rangle$ où $E_0 = \{\pm 1\}$. Dans ce groupe, les unités totalement positives ([2]) forment un sous-groupe E_+ d'indice au plus 16. Nous notons w_1^+, w_2^+, w_3^+ trois de ces générateurs.

Pour compter α dans $\mathbb{Z}[\zeta]/E$, nous comptons dans un domaine fondamental pour l'action de E ou plus précisément dans un domaine $\mathcal{D}$ qui est au plus la copie d'un nombre fini de domaines fondamentaux.

Nous pouvons adapter le lemme 9.1 de [3] à cette situation plus générale. Dans le cas (i), nous nous restreignons au domaine $\mathcal{D}$ défini par

$$1 \le \frac{|u|^2}{|N(u)|^{1/2}} < |w|^2. \tag{3.4}$$

Celui-ci correspond à $|E_0|$ copies d'un domaine fondamental. Dans le cas (ii), nous nous inspirons des travaux de [2] et [11] et les appliquons à notre cas particulier. Nous nous restreignons au domaine $\mathcal{D}$ défini par

$$\mathcal{D} = \bigcup_{\sigma \in S_3} \mathcal{D}_\sigma$$

([1]) Voir par exemple [10, Theorem 3.13].

([2]) Ce sont les unités satisfaisant $\tau(w) > 0$ pour tout $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$.

où S_3 est le groupe des permutations à trois éléments et les $\mathcal{D}_\sigma$ sont les cônes engendrés par les $\{f_{\sigma,j}\}_{j=1,2,3,4}$ avec

$$f_{\sigma,1}=1, \quad f_{\sigma,2}=w^+_{\sigma(1)}, \quad f_{\sigma,3}=w^+_{\sigma(1)}w^+_{\sigma(2)}, \quad f_{\sigma,4}=w^+_{\sigma(1)}w^+_{\sigma(2)}w^+_{\sigma(3)}.$$

Nous avons ici plongé les $f_{\sigma,j}$ dans $\mathbb{R}^4$ par l'application qui à $a_0+a_1\zeta+a_2\zeta^2+a_3\zeta^3$ associe (a_0,a_1,a_2,a_3). Nous choisissons d'inclure ou d'exclure les faces des $\mathcal{D}_\sigma$ afin que les $\mathcal{D}_\sigma$ soient disjoints. Contrairement aux applications envisagées dans [2], ce choix n'est pas crucial pour nous car les faces sont de mesure nulle. Grâce à [2], on sait que $\mathcal{D}$ est au plus la copie d'un nombre fini d de domaines fondamentaux ([3]). Notons d_0 le maximum de ce nombre d et du cardinal $|E_0|$ intervenant dans le cas (i).

LEMME 3.6. *Soit $\alpha\in\mathbb{Z}[\zeta]$. Il y a au plus d_0 éléments $\alpha'\in\mathcal{D}$ tels que $(\alpha)=(\alpha')$.*

Démonstration. Le cas (ii) découlant de [2], seul le cas (i) nécessite une démonstration. On a $|N(\alpha)|=|N(\alpha')|$. Il existe une unité θ de $Q(\zeta)$ telle que $\alpha'=\theta\alpha$ avec $\theta\in\langle w\rangle$. L'encadrement (3.4) valable pour α et α' implique que θ satisfait $1/w<|\theta|<w$ et donc $N(\theta)=1$. Il vient $|\theta|=1$ et ainsi $\theta\in E_0$. ∎

3.3. Majoration des $|a_i|$. Nous nous plaçons dans le cas où $\rho(\alpha)=1$, $(N(\alpha),\mathrm{Disc}(\Phi))=1$, $\alpha\in\mathcal{D}\cap\mathbb{Z}[\zeta]$. La relation $\alpha\in\mathcal{D}$ fournit $N(\alpha)>0$. Le lemme 10.1 de [3] se généralise :

LEMME 3.7. *Lorsque $\alpha=a_0+a_1\zeta+a_2\zeta^2+a_3\zeta^3\in\mathcal{D}\cap\mathbb{Z}[\zeta]$, nous avons $N(\alpha)>0$ et*

$$\max\{|a_0|,|a_1|,|a_2|,|a_3|\}\ll N(\alpha)^{1/4}.$$

Démonstration. Dans le cas (i), il existe $\tau\in\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ tel que $N(\alpha)=|\alpha\tau(\alpha)|^2$. La condition (3.4) fournit

$$\max\{|\alpha|,|\tau(\alpha)|\}\le|w|N(\alpha)^{1/4}$$

et le membre de gauche peut être vu comme une norme de $\mathbf{a}$. L'équivalence des normes de $\mathbb{R}^4$ nous donne alors le résultat.

Traitons maintenant le cas (ii). Pour tout

$$\alpha=x_1f_{\sigma,1}+x_2f_{\sigma,2}+x_3f_{\sigma,3}+x_4f_{\sigma,4}\in\mathcal{D}_\sigma,$$

nous avons $x_j\ge0$ et

$$N(\alpha)=\prod_{\tau\in\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})}(x_1\tau(f_{\sigma,1})+x_2\tau(f_{\sigma,2})+x_3\tau(f_{\sigma,3})+x_4\tau(f_{\sigma,4}))\ge\sum_{j=1}^4x_j^4,$$

([3]) Citons [4] qui permet d'avoir une expression d'un domaine fondamental pour l'action de E_+ à partir des $\mathcal{D}_\sigma$ par inclusion-exclusion de ces cônes.

puisque $\tau(f_{\sigma,j}) > 0$ pour tout (τ, j) et $N(f_{\sigma,j}) = 1$. Nous avons donc

$$\max_i x_i \le N(\alpha)^{1/4}.$$

Les normes $\max_i |x_i|$ et $\max\{|a_0|, |a_1|, |a_2|, |a_3|\}$ sont des normes de α dans $\mathbb{R}^4$, et leur équivalence fournit le résultat. ∎

3.4. Le théorème de Heath-Brown sur les sommes courtes à dénominateur friable. Afin d'appliquer ce théorème de Heath-Brown, nous avons besoin d'un analogue du lemme 12.2 de [3].

LEMME 3.8. *Soit α défini par* (2.1) *tel que q est sans facteur carré, $P^-(q) > 256$, et $(a_2a_3, q) = 1$, et soit $p \,|\, q = q_1q_2q_3$ avec $p \nmid \mathrm{Disc}(\Phi)$. Alors il n'existe pas de polynôme ℓ de degré ≤ 8 vérifiant*

$$U \equiv B_{14}\ell \pmod p.$$

Démonstration. Rappelons la relation $U = U_1a_0 + U_0$ introduite en (2.12) et l'identité (2.13). Montrons tout d'abord que $(U_1, p) = 1$ lorsque $p \,|\, q$.

Supposons que $p \,|\, (q_1, U_1)$. La relation (2.13) implique alors $p \,|\, (-a_1 + (\mu_2 + u)a_3)q_2$. Si $p \,|\, (-a_1 + (\mu_2 + u)a_3)$, on a

$$p \,|\, q_1 - (-a_1 + (\mu_2 + u)a_3)^2 = (\mu_2 + 2u)a_2^2,$$

ce qui n'est pas possible. Donc $p \,|\, q_2$, ce qui est en contradiction avec la condition q sans facteur carré.

Supposons que $p \,|\, (q_2, U_1)$. La relation (2.13) implique $p \,|\, (2a_1 - \mu_2a_3)q_1$. Si $p \,|\, 2a_1 - \mu_2a_3$, alors $p \,|\, 4q_2(\overline{2}\mu_2a_3, a_3) = (4\mu_0 - \mu_2^2)a_3^2$, ce qui n'est pas possible. Donc $p \,|\, q_1$, ce qui est en contradiction avec la condition q sans facteur carré.

Supposons que $p \,|\, (q_3, U_1)$. De (2.10) et (2.13), il vient

$$(\mu_2 - 2u)U_1 = a_3\{(2a_1 - \mu_2a_3)q_3 + 2(-a_1 + (\mu_2 - u)a_3)q_2\}.$$

Nous avons donc $p \,|\, (-a_1 + (\mu_2 - u)a_3)q_2$. Si $p \,|\, (-a_1 + (\mu_2 - u)a_3)$, alors la relation

$$p \,|\, q_3 - (-a_1 + (\mu_2 - u)a_3)^2 = (\mu_2 - 2u)a_2^2$$

aboutit à une impossibilité. Donc $p \,|\, q_2$, ce qui est en contradiction avec la condition q sans facteur carré. Nous avons donc bien $(U_1, p) = 1$ lorsque $p \,|\, q = q_1q_2q_3$.

Ainsi $U = U_1a_0 + U_0$ est un polynôme en a_0 de degré exactement 1. Comme $p \nmid a_3$, B_{14} est un polynôme en a_0 de degré exactement 2, ce qui permet de conclure que la congruence du lemme ne peut être une identité en a_0. ∎

Le lemme suivant rassemble les résultats contenus dans les lemmes 13.2 et 13.3 de [3] sous une forme légèrement différente.

LEMME 3.9. *Pour tout $p \mid q$ avec $\mu^2(q) = 1$,*

$$|\{0 \le a_0 < p : B_{14} \equiv 0 \pmod p\}| = 2 \quad (p \mid q_1 q_3),$$
$$|\{0 \le a_0 < p : B_{14} \equiv 0 \pmod p\}| = 1 \quad (p \mid q_2),$$
$$|\{0 \le a_0 < p : B_{13} \equiv 0 \pmod p,\ B_{14} \equiv 0 \bmod p\}| = 1.$$

Démonstration. Soient Δ_{13} le discriminant de B_{13} et Δ'_{14} le discriminant réduit de B_{14}. Nous vérifions les relations

$$\Delta_{13} = q_1 q_3, \quad \Delta'_{14} = -q_2 q_4.$$

Lorsque $p \mid q_1$, le polynôme B_{13} a une racine double

$$a_0 = \overline{a}_2(-2\mu_2 a_1 a_3 + (-\mu_0 + \mu_2^2)a_3^2 + \mu_2 a_2^2 + a_1^2),$$

qui est une racine simple de B_{14} puisque $R_0 \equiv 0 \pmod p$ et que $\Delta_{14} \not\equiv 0 \pmod p$. En effet, $p \nmid q_2$ car q est sans facteur carré et $p \nmid (\mu_2 + 2u)q_4 = q_2 - q_1$ pour la même raison ; dans le premier cas, il faut compter aussi l'autre racine de B_{13}, ce qui fait un total de 2. Nous ne détaillons pas les autres cas qui peuvent être traités de la même manière. ∎

Nous énonçons le théorème de Heath-Brown [5, Theorem 2] légèrement modifié obtenu grâce au q-analogue de la méthode de van der Corput.

LEMME 3.10 ([5]). *Soient $k \ge 1$, $D \ge 1$ et $\varepsilon > 0$. Soient $f, g, v \in \mathbb{Z}[X]$ trois polynômes de degré $\le D$ et $q = q_0 \cdots q_k$ un entier sans facteur carré n'ayant que des facteurs premiers $> 2^k D$. Nous supposons de plus que pour tout $p \mid q$, il n'existe pas de polynôme $w \in \mathbb{Z}[X]$ de degré inférieur ou égal à $k+1$ tel que $f(X) \equiv w(X)g(X) \pmod p$ ou $v(X) \equiv 0 \pmod p$ soient vérifiés. Alors, lorsque $A, B, h \ge 1$, nous avons*

$$\sum_{\substack{A < n \le A+B \\ (v(n)g(n), q) = 1}} \mathrm{e}\left(\frac{h f(n)\overline{g}(n)}{q}\right)$$
$$\ll_{k,D,\varepsilon} q^{\varepsilon} B\left(\left(\frac{\Delta}{q_0}\right)^{1/2^{k+1}} + \left(\frac{q_0}{\Delta B^2}\right)^{1/2^{k+1}} + \sum_{j=1}^{k}\left(\frac{q_{k+1-j}}{B}\right)^{1/2^j}\right)$$

avec $\Delta = (q_0, h)$ et $\mathrm{e}(t) := \exp\{2\pi i t\}$ pour $t \in \mathbb{R}$.

Démonstration. La seule différence par rapport à [5, Theorem 2] est la condition supplémentaire $(v(n), q) = 1$. Le lecteur consciencieux vérifiera qu'elle est compatible avec la démonstration par récurrence sur k développée dans [5]. ∎

3.5. Un résultat d'équirépartition. Lorsque $f \in \mathbb{Z}[X_1, X_2]$ est une forme binaire, nous notons

$$\rho_f(m) := |\{0 \le x_1, x_2 < m : f(x_1, x_2) \equiv 0 \pmod m\}|,$$
$$\rho_f^*(m) := |\{0 \le x_1, x_2 < m : f(x_1, x_2) \equiv 0 \pmod m,\ (x_1, x_2, m) = 1\}|,$$
$$\tilde\rho_f(m) := |\{0 \le x < m : f(1, x) \equiv 0 \pmod m,\ (x, m) = 1\}|.$$

Soient $f_1, f_2 \in \mathbb{Z}[x, y]$ deux formes irréductibles sur $\mathbb{Q}$ de degré $\nu_1, \nu_2 \ge 2$. Dans notre application, $\nu_1 = \nu_2 = 2$. Soit

$$P =]A_1, A_1 + M] \times]A_2, A_2 + M] \times]A_3, A_3 + M]$$

satisfaisant

$$M \ge \max\{|A_1|, |A_2|, |A_3|\}^\theta, \tag{3.5}$$

où θ est une constante absolue.

Lorsque $\mathbf{u}, \mathbf{v} \in \mathbb{Z}^3$ et $m \in \mathbb{Z}$, nous noterons $\mathbf{u} \equiv \mathbf{v} \pmod m$ lorsque $u_i \equiv v_i \pmod m$ pour tout $1 \le i \le 3$. Comme dans [3], nous considérons l'ensemble

$$\mathcal{A}(\mathbf{m}, \mathbf{u}) := \left\{ (a_1, a_2, a_3) \in P : \begin{array}{c} m_1 \mid f_1(a_1, a_2),\ m_2 \mid f_2(a_1, a_3) \\ (a_1, a_2, m_1) = 1,\ (a_1, a_3, m_2) = 1 \\ (a_1, a_2, a_3) \equiv \mathbf{u} \pmod{m_3} \end{array} \right\}.$$

Nous cherchons à estimer en moyenne le cardinal de $\mathcal{A}(\mathbf{m}, \mathbf{u})$, c'est-à-dire à majorer

$$E(m_3, M, Q_1, Q_2) := \sum_{\substack{(m_1, m_2) \\ (m_1, m_2) = (m_1 m_2, m_3) = 1 \\ m_i \le Q_i}}{}^{\!*} \left| |\mathcal{A}(\mathbf{m}, \mathbf{u})| - \frac{M^3 \rho_{f_1}^*(m_1) \rho_{f_2}^*(m_2)}{m_1^2 m_2^2 m_3^3} \right|,$$

où l'étoile signifie que de plus nous imposons $(m_i, f_i(1,0) f_i(0,1)) = 1$ pour $i = 1, 2$.

Le théorème 8.1 de [3] nous suffit :

Théorème 3.11 ([3]). *Soient $\varepsilon, \theta > 0$ et $f_1, f_2 \in \mathbb{Z}[x, y]$ deux formes irréductibles sur $\mathbb{Q}$ de degré $\nu_1, \nu_2 \ge 2$. Dans notre application, $\nu_1 = 4$. Soit*

$$P =]A_1, A_1 + M] \times]A_2, A_2 + M] \times]A_3, A_3 + M]$$

satisfaisant la relation (3.5). *Pour tout $\mathbf{u} \in \mathbb{Z}^3$, $m_3 \ge 1$, nous avons*

$$E(m_3, M, Q_1, Q_2) \ll (\log M)^7 \left(Q_1 Q_2 + \frac{(Q_1 Q_2)^{1/2} M^{3/2}}{m_3^{3/4}} + \frac{(Q_1 Q_2)^{1/3} M^2}{m_3^2} \right)$$
$$+ M^{1+\varepsilon}(Q_1 + Q_2) + M^{2+\varepsilon} + \frac{M^{2+\varepsilon}}{m_3^2}(Q_1^{1/2} + Q_2^{1/2}).$$

Remarque. La quantité $M^{3+\varepsilon}$ correspond à une borne triviale pour E, de sorte que ce résultat est non trivial lorsque $Q_1 Q_2 \le M^{3-\delta}$ et $Q_1 + Q_2 \le M^{2-\delta}$. Un tel résultat valable pour un polynôme quadratique f_1 et un polynôme quartique f_2 avec un majorant non trivial pour des bornes Q_i

satisfaisant $Q_1 = M^{1+\delta}$ et $Q_2 = M^{2+\delta}$ avec $\delta > 0$ permettrait d'établir le résultat du théorème 1.2 pour des polynômes dont le groupe de Galois associé n'est pas isomorphe à $V_4 := \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

4. Préliminaires de la démonstration du théorème 1.2. Nous reprenons la démarche initiée par Erdős qui a été utilisée dans [5]. Nous introduisons les fonctions $\log^{(1)}$ et $\log^{(2)}$ définies par

$$\log^{(1)}(m) := \sum_{\substack{p^\nu | m \\ p \le DX}} \log p, \qquad \log^{(2)}(m) := \sum_{\substack{p^\nu | m \\ p > DX}} \log p,$$

où D satisfait $D^3 > 16(1 + |\mu_2| + \mu_0)$, ainsi que l'ensemble

$$\mathcal{A} := \{X < n \le 2X : \log^{(1)}(\Phi(n)) \ge (1 + \delta_0) \log X\}. \tag{4.1}$$

LEMME 4.1. *Soit Φ un polynôme irréductible de degré 4. Soit $\delta_0, \delta_1 > 0$ pour lesquels l'ensemble $\mathcal{A}$ défini en* (4.1) *est tel qu'il existe X_0 satisfaisont $|\mathcal{A}| \ge \delta_1 X$ pour tout $X \ge X_0$. Alors l'ensemble des entiers n tels que $X < n \le 2X$ et $P^+(\Phi(n)) \gg X^{1+\delta_0\delta_1/3}$ est de cardinal $\ge (\delta_1\delta_0^2 + o(1))X$ lorsque X tend vers l'infini.*

REMARQUE. La démonstration est la même que celle de [5, lemme 2] par exemple. Cela permet d'avoir une densité positive d'entiers tels que $\Phi(n)$ a un grand facteur premier, alors que, dans [3], est uniquement énoncée une minoration du plus grand facteur premier du produit des $\Phi(n)$ lorsque n varie entre X et $2X$.

Il s'agit donc de minorer le cardinal de $\mathcal{A}$.

Nous considérons $\mathcal{J}$ un sous-ensemble d'éléments $\alpha = a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3$ de $\mathbb{Z}[\zeta] \cap \mathcal{D}$ dont nous préciserons ultérieurement la définition exacte, et l'ensemble $\mathcal{A}'$ défini ([4]) par

$$\mathcal{A}' := \{X < n \le 2X : \exists \alpha \in \mathcal{J} \;\; n - \zeta \in (\alpha)\}.$$

Pour tout n, on note $r_{\mathcal{J}}(n)$ le nombre d'éléments $\alpha \in \mathcal{J}$ satisfaisant la relation $n - \zeta \in (\alpha)$. Il vient la relation

$$|\mathcal{A}'| \ge \frac{1}{M_{\mathcal{J}}} \sum_{\alpha \in \mathcal{J}} |\mathcal{A}_\alpha| \tag{4.2}$$

avec

$$M_{\mathcal{J}} := \max_{X < n \le 2X} r_{\mathcal{J}}(n), \qquad \mathcal{A}_\alpha := \{X < n \le 2X : n - \zeta \in (\alpha)\}.$$

Nous définissons alors le terme résiduel $R(X, \alpha)$ par

$$|\mathcal{A}_\alpha| = X\frac{\rho(\alpha)}{N(\alpha)} + R(X, \alpha), \tag{4.3}$$

([4]) $\mathcal{A}'$ est noté $\mathcal{A}_1$ dans [3].

où ρ a été défini en (3.1) et N a été défini en (2.2). Nous imposons la condition

$$(N(\alpha), \mathrm{Disc}(\Phi)B_{14}) = 1 \quad (\forall \alpha \in \mathcal{J}), \tag{4.4}$$

de sorte que nous puissions appliquer les lemmes 3.1 et 3.2. Ainsi, lorsque $\alpha \in \mathcal{J}$, la relation $n - \zeta \in (\alpha)$ équivaut à

$$n \equiv B_{13}\overline{B_{14}} \pmod{N(\alpha)}.$$

Lorsque $(N(\alpha), \mathrm{Disc}(\Phi)B_{14}) = 1$, on a

$$R(X,\alpha) = \psi\Big(\frac{X - B_{13}\overline{B_{14}}}{N(\alpha)}\Big) - \psi\Big(\frac{2X - B_{13}\overline{B_{14}}}{N(\alpha)}\Big) \tag{4.5}$$

où $\psi(t) = \{t\} - 1/2$ et $\{t\}$ désigne la partie fractionnaire de t.

Pour choisir l'ensemble $\mathcal{J}$, il convient de s'assurer que $M_{\mathcal{J}}$ est fini et d'autre part que nous pouvons estimer la somme des $\mathcal{A}_\alpha$. Afin d'exprimer la définition de $\mathcal{J}$, nous considérons les paramètres θ_{ij}, τ_{ij} lorsque $i \geq 1$ et $0 \leq j \leq 2$ sont tels que les intervalles $[\theta_{ij}, \theta_{ij} + \tau_{ij}] \subset]0,1[$ soient disjoints. Nous spécifierons leurs valeurs à la fin de la démonstration ainsi que des paramètres α_0 et θ_0 introduits *infra* tels que $3\theta_0 < 4\alpha_0$. Nous notons aussi

$$M = X^{1/4}, \quad N = X^{(1+\alpha_0)/4}.$$

Tout d'abord nous notons $\mathcal{C}$ l'ensemble des (a_1, a_2, a_3) tels que :

(i) $q = q_1q_2q_3$ est sans facteur carré et satisfait $P^-(q) > 256$ et $q \gg M^6$, $(a_2, a_3) = (a_2a_3, q) = 1$.

(ii) Il existe des nombres premiers q_{11}, q_{12}, q_{21}, q_{22}, q_{31} satisfaisant

$$q_{ij} \in]X^{\theta_{ij}}, X^{\theta_{ij}+\tau_{ij}}] \tag{4.6}$$

tels que

$$q_1 = q_{10}q_{11}q_{12}, \quad q_2 = q_{20}q_{21}q_{22}, \quad q_3 = q_{30}q_{31}.$$

Nous choisissons $\mathcal{J}$ l'ensemble des $\alpha = a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3$ de $\mathbb{Z}[\zeta]$ satisfaisant $(a_1, a_2, a_3) \in \mathcal{C}$ ainsi que :

(iii) $\rho(\alpha) = 1$ et $\alpha \in \mathcal{D}$.

(iv) $|B_{14}| \gg M^3$ et $(q, B_{14}) = 1$.

(v) Il existe des idéaux K, L tels que $(\alpha) = KL$ avec

$$X^{1+\alpha_0/2} < N(\alpha) \leq X^{1+\alpha_0}$$

où K est un idéal premier satisfaisant

$$X^{4\alpha_0} < N(K) \leq X^{5\alpha_0} \tag{4.7}$$

et L satisfait

$$P^-(N(L)) > X^{\theta_0}. \tag{4.8}$$

Reste à observer que ces choix permettent bien d'avoir $\mathcal{A}' \subset \mathcal{A}$. En effet, nous avons $N(\alpha) \,|\, \Phi(n)$, et $P^+(N(\alpha)) \le \max\{X^{5\alpha_0}, X^{1-3\alpha_0}\} \le X$ pourvu que $\alpha_0 \le 1/5$, ce qui fournit

$$\log^{(1)} \Phi(n) \ge \big(1 + \tfrac{1}{2}\alpha_0\big) \log X.$$

Nous avons l'inclusion recherchée avec $\delta_0 = \frac{1}{2}\alpha_0$.

Le choix des paramètres θ_{ij}, τ_{ij}, α_0, η_0 et θ_0 (voir *infra* pour ces deux derniers) peut être optimisé pour obtenir une meilleure valeur de δ_0 et de δ_1 et donc de c_Φ. Ici, nous ne cherchons pas à donner une valeur explicite de c_Φ. Nous constaterons que les choix faits dans [3] permettent de vérifier toutes conditions de taille dont nous aurons besoin ici en observant que l'indice $(i, 3)$ a été remplacé ici par $(i, 0)$ pour $i = 1, 2$ et $(3, 2)$ par $(3, 0)$. Ces vérifications ne seront pas explicitées, mais le lecteur incrédule pourra les faire en se reportant aux valeurs choisies dans [3].

Les conditions (4.7) et (4.8) nous assurent que $(N(\alpha), \mathrm{Disc}(\Phi)) = 1$ dès que X est pris suffisamment grand. Nous nous sommes restreints ici aux idéaux principaux engendrés par α qui s'écrivent sous la forme KL, mais il n'est pas nécessaire que K ou L soit principal. L'anneau $\mathbb{Z}[\zeta]$ n'a pas besoin d'être principal.

À la suite, nous introduisons les notations suivantes : $\mathcal{K}$ désignera l'ensemble des idéaux premiers satisfaisant (4.7) et $(N(K), \mathrm{Disc}(\Phi)) = 1$, et $\mathcal{L}(K)$ l'ensemble des L tels que $KL = (\alpha)$ avec α satisfaisant les conditions précédentes. La famille peut contenir des répétitions lorsqu'il existe α et α' distincts satisfaisant $(\alpha) = (\alpha')$.

Le domaine $\mathcal{R}$ sera l'ensemble des $\mathbf{a} = (a_0, a_1, a_2, a_3) \in \mathbb{R}^4$ tels que l'on ait α qui s'écrit comme dans (2.1), appartient à $\mathcal{D}$ et ([5])

$$X^{1+\alpha_0/2} < N(\alpha) \le X^{1+\alpha_0}, \quad |B_{14}| \ge M^3, \quad |q| \ge M^6. \tag{4.9}$$

Lemme 4.2. *Pour ce choix de $\mathcal{J}$, nous avons*

$$M_{\mathcal{J}} \le d_0 \frac{2^{[4/\theta_0]}}{\alpha_0},$$

où d_0 apparaît au lemme 3.6.

Démonstration. En effet, comme $N(KL) \,|\, \Phi(n)$ pour $n \le X$ fixé et que

$$\Phi(n) \le (2X)^4 + O(X^2) < X^{(1+[4/\theta_0])\theta_0},$$

il y a au plus $2^{[4/\theta_0]}$ idéaux L. De même il y a au plus $1/\alpha_0$ choix pour K. Le résultat s'en déduit grâce au lemme 3.6. ∎

Comme dans [5] et [3], nous utilisons les poids $\{\lambda_d^-\}$ du crible de Rosser–Iwaniec [7], [8] pour traiter la condition $P^-(N(L)) > X^{\theta_0}$. Posant $P(z) :=$

([5]) Par rapport à [3], nous avons choisi $\beta_0 = 0$.

$\prod_{p\le z} p$, on voit que $\lambda_d^- \neq 0$ implique $d \le X^{3\theta_0}$ et $d \,|\, P(X^{\theta_0})$. La condition $3\theta_0 < 4\alpha_0$ assure qu'alors $(d, N(K)) = 1$.

De (4.2) et (4.3), nous obtenons

$$|\mathcal{A}'| \ge \frac{1}{M_{\mathcal{J}}}(XS_0 + S_1) \tag{4.10}$$

avec

$$\begin{aligned} S_0 &:= \sum_{K\in\mathcal{K}} \sum_{L\in\mathcal{L}(K)} \Big(\sum_{\substack{d\mid N(L)\\ d\mid P(X^{\theta_0})}} \lambda_d^- \Big) \frac{\rho(KL)}{N(KL)}, \\ S_1 &:= \sum_{K\in\mathcal{K}} \sum_{L\in\mathcal{L}(K)} \Big(\sum_{\substack{d\mid N(L)\\ d\mid P(X^{\theta_0})}} \lambda_d^- \Big) R(X, KL). \end{aligned} \tag{4.11}$$

L'enjeu est donc maintenant d'estimer S_0 et de majorer S_1.

5. Majoration de S_1. Soit $\mathrm{e}(t) := \exp\{2\pi i t\}$ pour $t \in \mathbb{R}$. Comme dans [3], nous pouvons montrer la majoration suivante concernant S_1.

Lemme 5.1. *Nous supposons*

$$\alpha_0 < \eta_0 < 1 - \tfrac{9}{4}\alpha_0, \qquad 12\theta_0 + 19\alpha_0 \le 1. \tag{5.1}$$

Lorsque $X \ge 2$ et $H = X^{\eta_0}$, on a la majoration

$$S_1 \ll (\log H) \sum_{K\in\mathcal{K}} \sum_{\substack{A\\ N(A)\mid P(X^{\theta_0})\\ N(A)\le X^{3\theta_0}}} \sum_{h\le H^2} \frac{|E_1(X,h;KA)| + |E_2(X,h;KA)|}{h + h^2/H} + o(X)$$

avec

$$E_k(X,h;KA) := \sum_{\substack{\alpha\in\mathcal{J}\\ KA\mid(\alpha)}} \mathrm{e}\Big(\frac{hkX}{N(\alpha)} - \frac{hU\overline{B_{14}}}{q}\Big).$$

Remarque. 1. Un point clé de la méthode de [3] est que dorénavant nous avons à majorer des sommes d'exponentielles E_k dont le dénominateur q ne dépend pas de a_0. La condition $KA \,|\, (\alpha)$ équivaut à une congruence sur a_0 modulo $N(KA)$. L'idéal KA satisfait les hypothèses du dernier point du lemme 3.2 et donc il existe $k_{KA} \in \mathbb{Z}$ tel que $\zeta \equiv k_{KA} \pmod{KA}$. La relation $a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3 \equiv 0 \pmod{KA}$ fournit alors à l'aide du lemme 3.1 la condition

$$a_0 \equiv -k_{KA}(a_1 + a_2 k_{KA} + a_3 k_{KA}^2) \pmod{N(KA)}.$$

2. Ce lemme reprend la démarche de [3] en améliorant les contraintes sur η_0.

Démonstration du lemme 5.1. En intervertissant les sommations, S_1 devient

$$S_1 = \sum_{K\in\mathcal{K}} \sum_{\substack{A\\ N(A)|P(X^{\theta_0}),\, N(A)\le X^{3\theta_0}\\ (N(A),\mathrm{Disc}(\Phi))=1}} \lambda^-_{N(A)} \sum_{\substack{\alpha\in\mathcal{J}\\ AK|(\alpha)}} R(X,\alpha),$$

où A décrit un ensemble d'idéaux tel que $(N(A),\mathrm{Disc}(\Phi))=1$ et $N(A)$ soit sans facteur carré. En effet, comme il est très clairement expliqué dans [5, début de la section 4], les idéaux $A=\langle L,d\rangle$ où $d=N(A)$ décrivent cet ensemble.

La relation (4.5) et des méthodes de comparaison de la fonction ψ et de séries trigonométriques (voir [5] et [3]) fournissent

$$S_1 \ll \sum_{K\in\mathcal{K}} \sum_{\substack{A\\ N(A)|P(X^{\theta_0}),\, N(A)\le X^{3\theta_0}\\ (N(A),\mathrm{Disc}(\Phi))=1}} |\lambda^-_{N(A)}| \Bigg(\frac{\log H}{H} \sum_{\substack{\alpha\in\mathcal{J}\\ KA|(\alpha)}} 1 + (\log H) \sum_{h\le H^2} \frac{|\tilde{E}_1(X,h;KA)| + |\tilde{E}_2(X,h;KA)|}{h+h^2/H} \Bigg) \tag{5.2}$$

avec

$$\tilde{E}_k(X,h;KA) := \sum_{\substack{\alpha\in\mathcal{J}\\ KA|(\alpha)}} \mathrm{e}\Big(\frac{h(kX-B_{13}\overline{B_{14}})}{N(\alpha)}\Big).$$

La première remarque suivant le lemme 5.1 fournit

$$\sum_{\substack{\alpha\in\mathcal{J}\\ KA|(\alpha)}} 1 \ll N^3\Big(\frac{N}{N(KA)}+1\Big).$$

La contribution du premier terme du majorant de (5.2) est

$$\ll \frac{\log H}{H} N^3 \sum_{K\in\mathcal{K}} \sum_{\substack{A\\ N(A)|P(X^{\theta_0})\\ N(A)\le X^{3\theta_0}}} \Big(\frac{N}{N(KA)}+1\Big)$$

$$\ll \frac{\log H}{H} N^3 (N(\log N) + X^{3\theta_0+5\alpha_0}) \ll \frac{\log H}{H} N^4 (\log N),$$

pourvu que $3\theta_0+5\alpha_0 \le \frac{1}{4}(1+\alpha_0)$ ([6]).

([6]) Cette inégalité est largement vérifiée par les valeurs des paramètres choisies dans [3]. On peut aussi procéder comme dans [3]. La contribution du premier terme est

$$\frac{\log H}{H} X^{3\theta_0} \sum_{K\in\mathcal{K}} \sum_{\substack{\alpha\in\mathcal{J}\\ K|(\alpha)}} 1 \ll \frac{\log H}{H} X^{1+\alpha_0+3\theta_0} = o(X)$$

pourvu que $\eta_0 > \alpha_0 + 3\theta_0$.

Pour approcher les sommes d'exponentielles, nous appliquons le lemme 3.3 en constatant que le membre de droite de la congruence est $O(N^5/M^9)$ puisque $B_{13} \ll N^3$, $B_{14} \gg M^3$, $q \gg M^6$, $N(\alpha) \geq M^2N^2$ et $U \ll N^5$. Nous en déduisons la majoration

$$\tilde{E}_k(X,h;KA) - E_k(X,h;KA) \ll \frac{hN^5}{M^9} \sum_{\substack{\alpha\in\mathcal{J}\\ AK|(\alpha)}} 1,$$

ce qui fournit une contribution $O(H(\log H)^2(\log N)N^9/M^9)$ d'après les calculs ci-dessus. Le choix du paramètre η_0 tel que $\eta_0 < 1 - \frac{9}{4}\alpha_0$ permet de montrer que la contribution du premier terme de (5.2) est $o(X)$. ∎

Nous sommes maintenant en mesure d'appliquer le lemme 3.10 pour montrer avec un choix adéquat de paramètres que $S_1 = o(X)$. Pour $(a_1,a_2,a_3) \in \mathcal{C}$, nous notons

$$\mathcal{R}(a_1,a_2,a_3) := \{a_0 \in \mathbb{R} : (a_0,a_1,a_2,a_3) \in \mathcal{R}\}. \tag{5.3}$$

Ces ensembles sont des réunions finies d'intervalles de longueur $O(N)$. Nous écrivons

$$E_k(X,h;KA) = \sum_{(a_1,a_2,a_3)\in\mathcal{C}} \sum_{\substack{a_0\in\mathcal{R}(a_1,a_2,a_3)\\ a_0\equiv\tilde{a}_0 \,(\mathrm{mod}\, N(KA))\\ (B_{14},q)=1}} \mathrm{e}\Big(\frac{hkX}{N(\alpha)} - \frac{hU\overline{B_{14}}}{q}\Big),$$

avec

$$\tilde{a}_0 = \tilde{a}_0(a_1,a_2,a_3;KA) \equiv -k_{KA}(a_1 + a_2k_{KA} + a_3k_{KA}^2) \ (\mathrm{mod}\ N(KA)).$$

Nous pouvons faire le changement de variable $a_0 = \tilde{a}_0 + mN(KA)$. Nous considérons

$$t = (N(KA),q), \quad t' = q/t. \tag{5.4}$$

La somme en a_0 est nulle si $(B_{14}(\mathbf{a}),t) > 1$. Nous nous plaçons donc dans le cas où $(B_{14}(\mathbf{a}),t) = 1$. La relation (3.2) pour $(u,v) = (t,t')$ fournit

$$\mathrm{e}\Big(-\frac{hU\overline{B_{14}}}{q}\Big) = \mathrm{e}\Big(-\frac{hU\overline{t'B_{14}}}{t} - \frac{h\bar{t}U\overline{B_{14}}}{t'}\Big).$$

Nous avons la relation

$$U(\tilde{a}_0 + mN(KA),a_1,a_2,a_3)\overline{B_{14}(a_0+mN(KA),a_1,a_2,a_3)} \equiv U(\tilde{\mathbf{a}})\overline{B_{14}(\tilde{\mathbf{a}})} \ (\mathrm{mod}\ t)$$

avec $\tilde{\mathbf{a}} := (\tilde{a}_0,a_1,a_2,a_3)$, de sorte que, posant

$$f(m) = U(\tilde{a}_0 + mN(KA)), \quad g(m) = B_{14}(\tilde{a}_0 + mN(KA)),$$

il vient

$$E_k(X,h;KA)$$
$$= \sum_{(a_1,a_2,a_3)\in\mathcal{C}} \mathrm{e}\left(-\frac{hU(\tilde{\mathbf{a}})\overline{t'B_{14}(\tilde{\mathbf{a}})}}{t}\right) \sum_{\substack{m\in\mathcal{R}'(a_1,a_2,a_3)\\(v(m),t')=1}} \mathrm{e}\left(\frac{hkX}{N(\alpha)} - \frac{h\bar{t}f(m)\overline{g(m)}}{t'}\right)$$

avec $\mathcal{R}'(a_1,a_2,a_3) := \{m : \tilde{a}_0 + mN(KA) \in \mathcal{R}(a_1,a_2,a_3)\}$ et $v(m) = B_{14}(\tilde{a}_0 + mN(KA), a_1, a_2, a_3)$.

Nous majorons la sommation sur m grâce au lemme 3.10. À cause du terme $hkX/N(\alpha)$ dans l'exponentielle, nous sommes obligés de faire une intégration par parties à partir de la majoration de la somme

$$\sum_{\substack{m\le B\\(v(m),t')=1}} \mathrm{e}\left(-\frac{h\bar{t}f(m)\overline{g(m)}}{t'}\right)$$

avec la contrainte $(B_{14},q)=1$ lorsque l'on choisit $a_0 = \tilde{a}_0 + mN(KA)$. Notons que le paramètre B du lemme 3.10 satisfait $B \ll N/N(KA)+1 \ll N/N(KA)$, où la dernière majoration découle de (5.1). Nous écrivons $\mathcal{R}'(a_1,a_2,a_3)$ comme une réunion finie d'intervalles $I'(a_1,a_2,a_3)$. Puisque $\partial N^{-1}/\partial a_0 \ll N(\mathbf{a})^{-5/4}$, il vient

$$\sum_{\substack{m\in I'(a_1,a_2,a_3)\\(v(m),t')=1}} \mathrm{e}\left(\frac{hkX}{N(\alpha)} - \frac{h\bar{t}f(m)\overline{g(m)}}{t'}\right)$$
$$\ll \left(1+\frac{H^2XN}{M^5}\right) \max_{B\ll N/N(KA)} \Bigg| \sum_{\substack{m\le B\\(v(m),t')=1}} \mathrm{e}\left(\frac{h\bar{t}f(m)\overline{g(m)}}{t'}\right)\Bigg|$$
$$\ll X^{2\eta_0+\alpha_0/4} \max_{B\ll N/N(KA)} \Bigg| \sum_{\substack{m\le B\\(v(m),t')=1}} \mathrm{e}\left(\frac{h\bar{t}f(m)\overline{g(m)}}{t'}\right)\Bigg|.$$

Nous prenons $k=7$, $D=2$. Nous choisissons pour cela $v=N(\alpha)$ vu comme un polynôme en m via le changement de variable $a_0 = \tilde{a}_0 + mN(KA)$. Le lemme 3.8 permet de s'assurer de la vérification de la relation entre les polynômes f et g.

Notons que $N/N(KA) \ge M^{1-12\theta_0-15\alpha_0}$. Nous factorisons q sous la forme $m_0m_1\cdots m_7$ avec $m_0 = q_{30}$ et $m_1 < \cdots < m_7$ choisis parmi q_{10}, q_{11}, q_{12}, q_{20}, q_{21}, q_{22} et q_{31} ([7]). Le résultat fourni est satisfaisant – autrement dit

([7]) Le choix des paramètres de [3] correspond à
$$(m_1,\dots,m_7) = (q_{11},q_{21},q_{31},q_{22},q_{12},q_{20},q_{10}).$$

$S_1 = o(X)$ – s'il existe $\varepsilon > 0$ tel que

$$\begin{aligned} X^{2\eta_0+\alpha_0/4} M^{4(\varepsilon+\alpha_0)} &\ll q_{30}^{1/2^8} \\ &\ll M^{-4(\varepsilon+\alpha_0)} M^{2^{-7}(1-12\theta_0-15\alpha_0)} X^{-(2\eta_0+\alpha_0/4)}, \\ m_k &\ll M^{-2^{10-k}(\varepsilon+\alpha_0)-2^{8-k}(8\eta_0+\alpha_0)} M^{1-12\theta_0-15\alpha_0} \quad (1 \le k \le 7). \end{aligned} \tag{5.5}$$

En effet, avec (5.5), nous obtenons

$$\begin{aligned} S_1 &\ll N^{\varepsilon} \sum_{K\in\mathcal{K}} \sum_{\substack{A \\ N(A)|P(X^{\theta_0}),\, N(A)\le X^{3\theta_0} \\ (N(A),\mathrm{Disc}(\Phi))=1}} \frac{N^4}{N(KA)} (\log H) M^{-4\varepsilon-4\alpha_0} \\ &\qquad \times \sum_{h\le H^2} \frac{(h, q_{30})}{h} + o(X) \\ &\ll N^{4+\varepsilon} M^{-3\varepsilon-4\alpha_0} + o(X). \end{aligned}$$

Grâce à (5.1), cela nous permet d'obtenir $S_1 = o(X)$.

6. Estimation de S_0

6.1. Sommation par rapport à la variable a_0. Pour sommer par rapport aux variables a_0, a_1, a_2, a_3, nous nous laissons guider par [3, §§14, 15]. Tout d'abord, nous recouvrons $\mathcal{R}$ par des pavés disjoints de la forme

$$\mathcal{B} =]A_0, A_0 + M] \times]A_1, A_1 + M] \times]A_2, A_2 + M] \times]A_3, A_3 + M]. \tag{6.1}$$

Nous conviendrons que $\mathcal{B}$ est un bon pavé si $\mathcal{B} \subset \mathcal{R}$ et nous noterons $\mathcal{B}_{\mathcal{R}}$ l'ensemble de ces bons pavés. Pour un tel pavé, nous noterons $\mathcal{B}'$ sa projection sur $\mathbb{R}^3$ définie par

$$\mathcal{B}' :=]A_1, A_1 + M] \times]A_2, A_2 + M] \times]A_3, A_3 + M].$$

En reprenant la définition (4.11) de S_0, en intervertissant les sommations comme pour la majoration de S_1, nous avons

$$S_0 \ge \sum_{\mathcal{B}\in\mathcal{B}_{\mathcal{R}}} \sum_{K\in\mathcal{K}} \sum_{A} \lambda^-_{N(A)} \sum_{(a_1,a_2,a_3)\in\mathcal{C}\cap\mathcal{B}'} \sum_{\substack{a_0\in]A_0,A_0+M] \\ a_0\equiv\tilde{a}_0 \,(\mathrm{mod}\, N(KA)) \\ (B_{14},q)=1}} \frac{\rho(\alpha)}{N(\alpha)}.$$

Nous appelons σ_0 la somme intérieure. Pour tenir compte de la condition $(B_{14}, q) = 1$, nous faisons une inversion de Möbius. Il vient

$$\sigma_0 = \sum_{r|q} \mu(r) \sum_{\substack{a_0\in]A_0,A_0+M] \\ a_0\equiv\tilde{a}_0 \,(\mathrm{mod}\, N(KA)) \\ r|B_{14}}} \frac{\rho(\alpha)}{N(\alpha)}.$$

Rappelant la notation (5.4), nous écrivons $N(KA) = nt$. Nous savons que $(n, tq) = 1$ puisque $N(KA)$ et q sont sans facteur carré. Nous écrivons $r = r_1 r_2$ avec $r_2 \mid t$ et $(r_1, t) = 1$. La condition $a_0 \equiv \tilde{a}_0 \pmod{N(KA)}$ est équivalente à $a_0 \equiv \tilde{a}_0 \pmod{nt/r_2}$, $r_2 \mid (N(\alpha), B_{14})$, $r_1 \mid B_{14}$. Or comme $(q, q_4) = 1$, la condition $r_2 \mid (N(\alpha), B_{14})$ revient d'après (2.6) à

$$r_2 \mid B_{12}B_{14} - \mu_2 B_{14}^2 - B_{13}^2, \quad r_2 \mid B_{14},$$

ce qui équivaut à $r_2 \mid (B_{13}, B_{14})$. D'après le lemme 3.9 et le lemme chinois, il existe un unique $\tilde{a}_{02} \pmod{r_2}$ tel que $\tilde{a}_0 \equiv \tilde{a}_{02} \pmod{r_2}$ satisfait cette condition. D'après le lemme 3.9, il existe exactement $2^{\omega((r_1, q_1q_3))}$ résidus $\tilde{a}_{01} \pmod{r_1}$ tels que $\tilde{a}_0 \equiv \tilde{a}_{01} \pmod{r_1}$ satisfait la condition $r_1 \mid B_{14}$. Donc $\tilde{a}_0$ appartient à exactement $2^{\omega((r_1, q_1q_3))}$ progressions arithmétiques de raison $N(KA)r_1$.

Ainsi, en reprenant la méthode développée dans [3], il vient

$$\sigma_0 = \sum_{r_1 \mid q/t} \sum_{r_2 \mid (q, N(KA))} \mu(r_1) 2^{\omega((r_1, q_1q_3))} \mu(r_2) \left\{ \frac{I(a_1, a_2, a_3)}{r_1 N(KA)} + O\left(\frac{1}{M^4}\right) \right\},$$

avec

$$I(a_1, a_2, a_3) := \int\limits_{a_0 \in]A_0, A_0 + M]} \frac{da_0}{N(a_0, a_1, a_2, a_3)}.$$

La contribution du terme d'erreur à S_0 est

$$\ll X^{3\theta_0 + 5\alpha_0 + o(1)} N^5 M^{-6} \ll X^{25\alpha_0/4 + 3\theta_0 - 1/4 + o(1)}$$

et donc $o(1)$ si

$$12\theta_0 + 25\alpha_0 < 1. \tag{6.2}$$

Cette condition identique à celle de [3, (13·7)] est bien vérifiée par les valeurs de [3]. En notant $\tilde{\sigma}_0$ la contribution du terme principal, cette contribution $\tilde{\sigma}_0$ est nulle lorsque $(q, N(KA)) > 1$. Lorsque $(q, N(KA)) = 1$, nous obtenons

$$\tilde{\sigma}_0 = \frac{I(a_1, a_2, a_3)}{N(KA)} \prod_{p \mid (q/t, q_1q_3)} \left(1 - \frac{2}{p}\right) \prod_{p \mid (q/t, q_2)} \left(1 - \frac{1}{p}\right).$$

Par souci de complétude, nous copions [3] et nous utilisons la minoration

$$\tilde{\sigma}_0 \geq \frac{I(a_1, a_2, a_3)}{N(KA)} \prod_{p \mid q/t} \left(1 - \frac{2}{p}\right).$$

Posant $g(p) := \#\{\mathfrak{p} : N(\mathfrak{p}) = p\}$, en suivant [5, pp. 574–575], nous avons

$$\sum_{K \in \mathcal{K}} \frac{\rho(K)}{N(K)} = \sum_{X^{4\alpha_0} < p \leq X^{5\alpha_0}} \frac{g(p)}{p} = \log(5/4) + o(1),$$

$$\sum_{A} \frac{\lambda^-_{N(A)}}{N(A)} \geq 2(C_0 + o(1)) \prod_{p \mid q} \left(1 - \frac{g(p)}{p}\right)^{-1} \prod_{p \leq X^{\theta_0}} \left(1 - \frac{g(p)}{p}\right)$$

avec d'après la théorie du crible $C_0 := \frac{2}{3}e^\gamma \log 2$. En rassemblant ces estimations, nous obtenons

$$S_0 \geq 2(C_0+o(1))\log(5/4)\prod_{p\leq X^{\theta_0}}\Big(1-\frac{g(p)}{p}\Big)T_0$$

avec

$$T_0 := \sum_{(a_1,a_2,a_3)\in\mathcal{C}} h(q(a_1,a_2,a_3))I(a_1,a_2,a_3),$$
$$h(q) := \mu(q)^2\prod_{p|q}\frac{1-2/p}{1-g(p)/p}\mathbf{1}_{P^-(q)>256}.$$

Ainsi se clôt la partie concernant la sommation par rapport à la variable a_0.

6.2. Sommation en a_1, a_2, a_3 : découpage en pavés et conclusion. Il nous suffit d'estimer

$$\sum_{(a_1,a_2,a_3)\in\mathcal{C}\cap\mathcal{B}'} h(q(a_1,a_2,a_3))I(a_1,a_2,a_3)$$

sachant que

$$T_0 \geq \sum_{\mathcal{B}\in\mathcal{B}_\mathcal{R}}\sum_{(a_1,a_2,a_3)\in\mathcal{C}\cap\mathcal{B}'} h(q(a_1,a_2,a_3))I(a_1,a_2,a_3).$$

Pour pallier le fait que plusieurs q_{ij} satisfaisant (4.6) peuvent diviser les formes quadratiques q_k (au plus $\leq (1+\alpha_0)/(2\theta_{ij})$ grâce à $q_k \ll X^{(1+\alpha_0)/2}$), nous minorons T_0 :

$$T_0 \geq \frac{2^5\prod_{(i,j),j\geq 1}\theta_{ij}}{(1+\alpha_0)^5} \times \sum_{\mathcal{B}\in\mathcal{B}_\mathcal{R}}\sum_{q_{ij}\in]X^{\theta_{ij}},X^{\theta_{ij}+\tau_{ij}}]}\sum_{\substack{(a_1,a_2,a_3)\in\mathcal{B}'\\ q_{i1}q_{i2}|q_i\\ (a_2,a_3)=(a_2a_3,q)=1}} h(q(a_1,a_2,a_3))I(a_1,a_2,a_3).$$

Pour chaque bon pavé $\mathcal{B}$, on a

$$\int_{a_0\in]A_0,A_0+M]}\frac{da_0}{N(a_0,a_1,a_2,a_3)} = \frac{M(1+o(1))}{N(A_0,A_1,A_2,A_3)}$$

de sorte que

$$T_0 \geq \frac{2^5\prod_{(i,j),j\geq 1}\theta_{ij}}{(1+\alpha_0)^5}U_0(1+o(1))$$

avec

$$U_0 := \frac{M}{N(A_0,A_1,A_2,A_3)}\sum_{\mathcal{B}\in\mathcal{B}_\mathcal{R}}U(\mathcal{B})$$

et

$$U(\mathcal{B}) = \sum_{q_{ij}\in]X^{\theta_{ij}},X^{\theta_{ij}+\tau_{ij}}]} \sum_{\substack{(a_1,a_2,a_3)\in\mathcal{B}'\\ q_{i1}q_{i2}|q_i\\ (a_2,a_3)=(a_2a_3,q)=1}} h(q(a_1,a_2,a_3)).$$

Ici, nous avons utilisé la convention $q_{32}=1$ afin d'alléger les notations.

L'estimation du membre de gauche se fait comme dans [3, §15]. Nous n'indiquons que quelques étapes sans plus de détails. La méthode développée dans [5] et [3] consiste à écrire $h = 1 * \ell$ avec ℓ une fonction multiplicative définie par

$$\ell(p^\nu) = \begin{cases} \frac{g(p)-2}{p-g(p)} & \text{si } p > 256,\ \nu = 1,\\ -1 & \text{si } p \le 253,\ \nu = 1,\\ -h(p) & \text{si } \nu = 2,\\ 0 & \text{si } \nu \ge 3. \end{cases}$$

Suivant [3], nous posons $Z = X^{\alpha_0+\varepsilon}$ et nous approchons les sommes $U(\mathcal{B})$ par

$$U_0(\mathcal{B}) := \sum_{q_{ij}\in]X^{\theta_{ij}},X^{\theta_{ij}+\tau_{ij}}]} \sum_{\substack{s=s_1s_2,\,t<Z\\ u<Z^4}} \mu(s)\mu(t)\ell(u) \sum_{\substack{(a_1,a_2,a_3)\in\mathcal{B}'\\ q_{i1}q_{i2}|q_i\\ (b,q_{11}q_{12}q_{21}q_{22})=1\\ [t,s_1]|a_2,\,[t,s_2]|a_3,\,s|q,\,u|q}} 1.$$

Les exposants doivent pour cela vérifier les conditions (15·6) et (15·7) de [3],

$$2\alpha_0 < \theta_{1i} < \theta_{1i}+\tau_{1i} < \tfrac{1}{4} - \tfrac{3}{4}\alpha_0, \qquad \tfrac{1}{4}(1+\alpha_0) < \theta_{21}+\theta_{22}. \tag{6.3}$$

Pour estimer cette somme, nous appliquons le théorème 3.11 avec, d'après (3.3),

$$\begin{aligned} &f_1(a_1,a_2,a_3) = a_1^2 + (\mu_2+2u)a_2^2,\\ &f_2(a_1,a_2,a_3) = a_1^2 + (\mu_2+2u)a_1a_3 + (u\mu_2+2\mu_0)a_3^2,\\ &Q_1 = X^{\theta_{11}+\tau_{11}+\theta_{12}+\tau_{12}}, \quad Q_2 = X^{\theta_{21}+\tau_{21}+\theta_{22}+\tau_{22}},\\ &m_1 = q_{11}q_{12}, \quad m_2 = q_{21}q_{22}, \quad m_3 = [t,s,u,q_{31}],\\ &(a_1,a_2,a_3) \equiv (z_1,z_2,z_3) \pmod{m_3}, \end{aligned}$$

et (z_1,z_2,z_3) parcourant un ensemble $\mathcal{S}(s,t,u,q_{31}) \in (\mathbb{Z}/m_3\mathbb{Z})^3$ de résidus satisfaisant les conditions

$$t \,|\, (a_2,a_3), \qquad s \,|\, a_2a_3, \qquad s \,|\, q, \qquad u \,|\, q, \qquad q_{31} \,|\, q_3.$$

D'après [3, (16·1)], le théorème 3.11 fournit un terme d'erreur satisfaisant

lorsque

$$\begin{aligned} &11\alpha_0+\theta_{31}+\tau_{31}<\tfrac{1}{18},\\ &\max\{\theta_{11}+\tau_{11}+\theta_{12}+\tau_{12},\theta_{21}+\tau_{21}+\theta_{22}+\tau_{22}\}<\tfrac{2}{5},\\ &\theta_{11}+\tau_{11}+\theta_{12}+\tau_{12}+\theta_{21}+\tau_{21}+\theta_{22}+\tau_{22}<\tfrac{2}{3}. \end{aligned} \tag{6.4}$$

Nous approchons ainsi $U_0(\mathcal{B})$ par $T_0(\mathcal{B})$ avec

$$T_0(\mathcal{B}):=\sum_{\substack{s,t<Z\\ u<Z^4}}\mu(s)\mu(t)\ell(u)\\ \times\sum_{q_{ij}\in]X^{\theta_{ij}},X^{\theta_{ij}+\tau_{ij}}]}|\mathcal{S}(s,t,u,q_{31})|M^3\frac{\rho^*_{q_1}(q_{11})\rho^*_{q_1}(q_{12})\rho^*_{q_2}(q_{21})\rho^*_{q_2}(q_{22})}{(q_{11}q_{12}q_{21}q_{22})^2m_3^3},$$

où nous avons utilisé les relations $\rho^*_{q_i}=\rho^*_{f_i}$ pour $i=1,2$ et la multiplicativité de ces fonctions. D'après le lemme 3.5, lorsque $(i,j)\in\{1,2\}^2$, nous avons

$$\rho^*_{q_i}(q_{ij})=\sigma^*_{q_i}(q_{ij})/\phi(q_{ij})=\phi(q_{ij})\tilde{\rho}_{q_i}(q_{ij})$$

et

$$\sum_{q_{ij}\in]X^{\theta_{ij}},X^{\theta_{ij}+\tau_{ij}}]}\frac{\rho^*_{q_i}(q_{ij})}{q_{ij}^2}=\log(1+\tau_{ij}/\theta_{ij})+o(1).$$

Nous imposons $X^{\theta_{31}}>Z^{11}$, de sorte que $(q_{31},stu)=1$ et donc $m_3=q_{31}[s,t,u]$. Il vient

$$|\mathcal{S}(s,t,u,q_{31})|=|\mathcal{S}'(s,t,u)|\sigma_{q_3}(q_{31})$$

avec $f_3(a_1'',a_2)=a_1''^2+(\mu_2-2u)a_2^2$ et $\mathcal{S}'(s,t,u)$ l'ensemble des triplets de $(\mathbb{Z}/[s,t,u]\mathbb{Z})^3$ satisfaisant

$$t\,|\,(a_2,a_3),\qquad s\,|\,a_2a_3,\qquad s\,|\,q,\qquad u\,|\,q.$$

D'après le lemme 3.5, nous avons de même

$$\sum_{q_{31}\in]X^{\theta_{31}},X^{\theta_{31}+\tau_{31}}]}\frac{\sigma_{q_3}(q_{31})}{q_{31}^3}=\log(1+\tau_{31}/\theta_{31})+o(1).$$

Nous avons aussi

$$\frac{|\mathcal{S}'(s,t,u)|}{[s,t,u]^3}\ll\frac{\tau(s)^2\tau(u)(s,t)^2(u,t^2)}{t^3s^2}u.$$

Suivant [3], on remarque que si $\ell(u)\neq0$, alors il existe u_1 et u_2 sans facteur carré tels que $u=u_1u_2^2$ de sorte que $\ell(u)\le e^{O(\omega(u))}/u_1$. En rassemblant ces

résultats nous obtenons

$$T_0(\mathcal{B}) = (1+o(1))M^3 \prod_{\substack{i=1,2,3\\ j=1,2}} \log(1+\tau_{ij}/\theta_{ij}) \sum_{\substack{s,t<Z\\ u<Z^4}} \frac{\mu(s)\mu(t)\ell(u)}{[s,t,u]^3} |\mathcal{S}'(s,t,u)|$$
$$= (1+o(1))CM^3 \prod_{\substack{i=1,2,3\\ j=1,2}} \log(1+\tau_{ij}/\theta_{ij})$$

avec

$$C := \sum_{s,t,u\geq 1} \frac{\mu(s)\mu(t)\ell(u)}{[s,t,u]^3} |\mathcal{S}'(s,t,u)|.$$

Des manipulations faciles fournissent

$$C = \frac{6}{\pi^2} \sum_{s,u\geq 1} \frac{\mu(s)\ell(u)}{[s,u]^3} |\mathcal{S}''(s,[s,u])| \prod_{p\mid [s,u]} \frac{1}{1-1/p^2}$$

avec

$$\mathcal{S}''(s,v) := \operatorname{card}\{(a_1,a_2,a_3) \in (\mathbb{Z}/v\mathbb{Z})^3 : s \mid a_2a_3,\ v \mid q\}.$$

La somme intervenant dans l'expression de C a un terme général étant multiplicatif. Il vient

$$C = \frac{6}{\pi^2} \prod_p \left(1 + \frac{\ell(p)|\mathcal{S}''(1,p)| - h(p)|\mathcal{S}''(p,p)|}{p(p^2-1)} + \frac{\ell(p^2)(|\mathcal{S}''(1,p^2)| - |\mathcal{S}''(p,p^2)|)}{p^4(p^2-1)}\right)$$

Pour montrer la positivité de C, il suffit de reproduire les calculs de [3, lemme 16.2]. Nous n'avons pas besoin d'une valeur explicite. Nous ne donnons pas plus de détails.

Nous avons donc

$$T_0 \geq C(1+o(1)) \frac{2^5 \prod_{(i,j),j\geq 1} \theta_{ij}}{(1+\alpha_0)^5} \prod_{\substack{i=1,2,3\\ j=1,2}} \log(1+\tau_{ij}/\theta_{ij}) W,$$

avec

$$W := \sum_{\mathcal{B}\in\mathcal{B}_{\mathcal{R}}} \frac{M^4}{N(A_0,A_1,A_2,A_3)}.$$

Après avoir remarqué, comme dans [5, p. 584], que

$$\frac{M^4}{N(A_0,A_1,A_2,A_3)} = (1+o(1)) \int_{\mathcal{B}} \frac{da_0\, da_1\, da_2\, da_3}{N(a_0,a_1,a_2,a_3)},$$

on a donc

$$W = (1+o(1)) \iiiint\limits_{\mathcal{R}_1} \frac{da_0\, da_1\, da_2\, da_3}{N(a_0,a_1,a_2,a_3)} \quad \text{avec} \quad \mathcal{R}_1 := \bigcup_{\mathcal{B}\in\mathcal{B}_{\mathcal{R}}} \mathcal{B}.$$

Rappelant la définition (4.9), nous obtenons comme dans [3] l'estimation

$$W = (1+o(1)) \iiiint\limits_{\substack{\alpha\in\mathcal{D}\\ X^{1+\alpha_0/2}<N(\mathbf{a})\le X^{1+\alpha_0}}} \frac{da_0\, da_1\, da_2\, da_3}{N(a_0,a_1,a_2,a_3)}. \tag{6.5}$$

En effet, pour passer de $\mathcal{R}_1$ à $\mathcal{R}$, il suffit de remarquer que $\mathcal{R}\setminus\mathcal{R}_1$ est un domaine où une des variables, disons a_0, est dans une réunion finie $I_1(a_1,a_2,a_3)$ d'intervalles dépendant des autres variables de taille $\ll M$. En faisant un découpage dyadique et en utilisant le lemme 3.7, nous obtenons

$$\begin{aligned}\int\limits_{\mathcal{R}\setminus\mathcal{R}_1} \frac{da_0\, da_1\, da_2\, da_3}{N(a_0,a_1,a_2,a_3)} &\ll \sum_{\substack{k\\ 2^k\ge (MN)^{1/2}}} \frac{1}{2^{4k}} \iiint\limits_{\max\{a_1,a_2,a_3\}\ll 2^k} \int\limits_{I_1(a_1,a_2,a_3)} da_0\\ &\ll (M/N)^{1/2} \ll X^{-\alpha_0/8}.\end{aligned}$$

Il s'agit ensuite de minorer la contribution des (a_0,a_1,a_2,a_3) tels que l'on a $|q|\le M^6$ ou $|B_{14}|\le M^3$. Lorsque $q\le M^6$, il existe $i\in\{1,2,3\}$ tel que $q_i\le M^2$. Cela implique, lorsque a_0,a_2,a_3 sont fixés, que la variable est dans une réunion finie $I(a_0,a_2,a_3)$ d'intervalles de longueur $\ll M$. De la même manière que précédemment nous avons une contribution

$$\ll \sum_{\substack{k\\ 2^k\ge (MN)^{1/2}}} \frac{1}{2^{4k}} \iiint\limits_{\max\{a_0,a_2,a_3\}\ll 2^k} \int\limits_{I(a_0,a_2,a_3)} da_1 \ll (M/N)^{1/2} \ll X^{-\alpha_0/8}.$$

Le même type de manipulations permet d'exclure le cas $|B_{14}|\le M^3$. Cela clôt la preuve de (6.5).

Puis, en faisant un changement de variables, il vient

$$W = \tfrac{1}{2}\alpha_0 C'\big(1+o(1)\big)\log X$$

avec

$$C' := \iiiint\limits_{\mathbf{a}\in\mathcal{D}_1} \frac{da_0\, da_1\, da_2\, da_3}{N(a_0,a_1,a_2,a_3)} > 0$$

où

$$\begin{aligned}\mathcal{D}_1 := \{(z_1,z_2,z_3,z_4)\in\mathbb{R}^4 : z_1+z_2\zeta+z_3\zeta^2+z_4\zeta^3\in\mathcal{D},\\ \exists i\le 4 \ \ |z_i|=1,\ |z_j|\le 1\ (\forall j)\}.\end{aligned}$$

Nous ne donnons pas plus de détails, la démarche étant identique à celle de [3]. Nous obtenons

$$T_0 \geq \frac{\alpha_0}{\theta_0} CC'C_0 \log(5/4)(1+o(1)) \frac{2^5 \prod_{(i,j),j\geq 1} \theta_{ij}}{(1+\alpha_0)^5} \times \prod_{\substack{i=1,2,3 \\ j=1,2}} \log(1+\tau_{ij}/\theta_{ij}) C''(X),$$

avec

$$C''(X) := \prod_{p \leq X^{\theta_0}} \left(1 - \frac{g(p)}{p}\right)\left(1 - \frac{1}{p}\right)^{-1}.$$

Lorsque X tend vers l'infini, la quantité $C''(X)$ tend vers une constante $C'' > 0$.

En utilisant le lemme 4.2, nous obtenons

$$\frac{|\mathcal{A}'|}{X} \geq \frac{\alpha_0^2(1+o(1))}{\theta_0 d_0 2^{[4/\theta_0]}} CC'C''C_0 \log(5/4) \frac{2^5 \prod_{(i,j),j\geq 1} \theta_{ij}}{(1+\alpha_0)^5} \prod_{\substack{i=1,2,3 \\ j=1,2}} \log(1+\tau_{ij}/\theta_{ij}),$$

ce qui permet de montrer le résultat pour tout c_Φ satisfaisant

$$0 < c_\Phi < \frac{\alpha_0^3}{6\theta_0 d_0 2^{[4/\theta_0]}} CC'C''C_0 \log(5/4) \frac{2^5 \prod_{(i,j),j\geq 1} \theta_{ij}}{(1+\alpha_0)^5} \times \prod_{\substack{i=1,2,3 \\ j=1,2}} \log(1+\tau_{ij}/\theta_{ij}). \blacksquare$$

Appendice : explications des calculs du résultant dans le cas général (par R. de la Bretèche et J.-F. Mestre). Soient k un corps de nombres et Φ un polynôme unitaire séparable de degré n de $k[X]$ dont la décomposition dans un corps de décomposition s'écrit

$$\Phi(X) = \prod_{j=1}^{n} (X - \zeta_j).$$

Nous notons $A = k[X]/\langle \Phi \rangle$.

L'application $f : A \to k[\zeta_1] \times \cdots \times k[\zeta_n]$ qui à $Q \pmod{\Phi}$ associe $(Q(\zeta_1), \ldots, Q(\zeta_n))$ est un isomorphisme de k-algèbres. Lorsque $a \in A$, nous considérons l'application $g_a : A \to A$ qui à x associe ax. Nous écrivons $a = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1}$ avec $a_j \in k$.

Nous déterminerons la forme du résultant $R \in k[a_1, \ldots, a_{n-1}]$ par rapport à la variable a_0 du déterminant $D \in k[a_1, \ldots, a_{n-1}][a_0]$ de g_a avec un des cofacteurs $M \in k[a_1, \ldots, a_{n-1}][a_0]$ de la matrice de l'application g_a choisi de manière quelconque. Comme dans le lemme 2.1, nous le comparons au résultant $R_0 \in k[a_1, \ldots, a_{n-1}]$ de deux cofacteurs M et N.

LEMME A.1. *Il existe $r_\Phi \in k$ tel que*

$$R = r_\Phi \prod_{1\le i<j\le n} (a(\zeta_i) - a(\zeta_j))^2. \tag{A.1}$$

Le résultant R_0 est divisible dans $k[a_1, \dots, a_{n-1}]$ par

$$\prod_{1\le i<j\le n} (a(\zeta_i) - a(\zeta_j)).$$

REMARQUE. Lorsque $n = 4$, nous numérotons les ζ_j de sorte que $\zeta_1 = -\zeta_3$, $\zeta_2 = -\zeta_4$ et nous posons

$$q_1(a_1,a_2,a_3) := \frac{(a(\zeta_1)-a(\zeta_2))(a(\zeta_3)-a(\zeta_4))}{(\zeta_1-\zeta_2)(\zeta_3-\zeta_4)},$$
$$q_2(a_1,a_2,a_3) := \frac{(a(\zeta_1)-a(\zeta_3))(a(\zeta_2)-a(\zeta_4))}{(\zeta_1-\zeta_3)(\zeta_2-\zeta_4)},$$
$$q_3(a_1,a_2,a_3) := \frac{(a(\zeta_1)-a(\zeta_4))(a(\zeta_2)-a(\zeta_3))}{(\zeta_1-\zeta_4)(\zeta_2-\zeta_3)}.$$

Nous avons $\zeta_1^2 + \zeta_2^2 = -\mu_2$, et $u = -\zeta_1\zeta_2$ vérifie $u^2 = \mu_0$. De simples calculs fournissent

$$q_1(a_1,a_2,a_3) = (a_1 - (\mu_2+u)a_3)^2 + (\mu_2+2u)a_2^2,$$
$$q_2(a_1,a_2,a_3) = a_1^2 - \mu_2 a_1 a_3 + \mu_0 a_3^2,$$
$$q_3(a_1,a_2,a_3) = (a_1 - (\mu_2-u)a_3)^2 + (\mu_2-2u)a_2^2.$$

Lorsque $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = V_4$, nous retrouvons les résultats de la partie précédente. Dans le cas contraire, nous constatons que le produit q_1q_3 est irréductible sur $\mathbb{Q}$.

Démonstration du lemme A.1. Soit $a \in A$. L'application $g_a : A \to A$ qui à x associe ax correspond à l'application $h_a = f \circ g_a \circ f^{-1}$ qui est la multiplication composante par composante définie par $h_a(y_1, \dots, y_n) = (b_1y_1, \dots, b_ny_n)$ avec $b_j = a(\zeta_j)$, et f est la matrice de changement de base de la base canonique à la base des polynômes de Lagrange qui valent 1 en ζ_j et 0 en les ζ_i pour tout $i \neq j$. La puissance extérieure $(n-1)$-ème $L_a = \Lambda^{(n-1)}(g_a)$ (qui donne la matrice des cofacteurs) correspond via f à l'application diagonale u_a :

$$(y_1, \dots, y_n) \mapsto ((b_2\cdots b_n)y_1, (b_1b_3\cdots b_n)y_2, \dots, (b_1b_2\cdots b_{n-1})y_n),$$

où $b_j = a(\zeta_j)$.

Montrons que le produit du membre de droite de (A.1) divise R, ce qui fournira le résultat en comparant les degrés. Le polynôme R vu comme un polynôme dépendant de $a_1, \dots, a_{n-1}$ est de degré $n(n-1)$ de même que le

membre de droite de (A.1). Nous avons

$$D = \prod_{j=1}^{n} a(\zeta_j).$$

Le résultant R, à constante (ne dépendant que de Φ) près, est le produit des $M(c)$, où c est une racine de D, vu comme polynôme en a_0, les coordonnées $a_1, \dots, a_{n-1}$ étant fixées. Ces racines sont les c_j définis par

$$c_j := a_0 - a(\zeta_j) = -a_1\zeta_j - a_2\zeta_j^2 - \cdots - a_{n-1}\zeta_j^{n-1} \quad (1 \le j \le n).$$

Le polynôme $P_j(X) = c_j + a_1X + \ + a_{n-1}X^{n-1}$ correspondant est tel que $P_j(\zeta_j) = 0$, donc u_{P_j} est de la forme $u_{P_j}(y_1, \dots, y_n) = (\prod_{i\neq j} b_i)(0, \dots, 0, y_j, 0, \dots, 0)$, donc un multiple (par $\prod_{i\neq j} b_i$) d'une application linéaire et indépendante de a_0. Il en est de même de L_{P_j}, et

$$b_i = c_j + a_1\zeta_i + a_i\zeta_i^2 + \cdots + a_{n-1}\zeta_i^{n-1} = a(\zeta_i) - a(\zeta_j)\,;$$

la première relation en découle.

Le deuxième point à montrer est équivalent à dire que si $a(\zeta_i) - a(\zeta_j) = 0$ (relation indépendante de a_0), alors il existe a_0 tel que M et N ont a_0 comme racine commune. Il suffit de prendre

$$a_0 = -\sum_{k=1}^{n-1} a_k\zeta_i^k = -\sum_{k=1}^{n-1} a_k\zeta_j^k.$$

Dans ce cas, l'application h_P avec $P = -\sum_{k=1}^{n-1} a_k\zeta_i^k + \sum_{k=1}^{n-1} a_kX^k$ est de rang $\le n-2$ (puisque $P(\zeta_i) = P(\zeta_j) = 0$), donc l'application u_P est nulle, de même que L_P : tous les cofacteurs sont nuls. Donc $M(a_0) = N(a_0) = 0$. ∎

Remerciements. L'auteur tient à remercier Cécile Dartyge pour la communication de [3] et les discussions éclairantes qu'ils ont eues sur le problème de Tchébychev. C'est avec l'aide de Jean-François Mestre que les calculs de résultants ont été effectués et expliqués. Qu'il soit ici remercié pour sa grande disponibilité. L'auteur tient aussi à remercier l'arbitre pour son travail minutieux de vérification. Une partie de ce travail a été réalisée à Bonn lors du trimestre thématique *Arithmetic & Geometry* au Hausdorff Research Institute for Mathematics. Que cette institution soit remerciée pour son invitation et les excellentes conditions de travail offertes. L'auteur est soutenu par une bourse IUF junior.

Bibliographie

[1] A. Balog, V. Blomer, C. Dartyge and G. Tenenbaum, *Friable values of binary forms*, Comment. Math. Helv. 87 (2012), 639–667.

[2] P. Colmez, *Résidu en $s = 1$ des fonctions zêta p-adiques*, Invent. Math. 91 (1988), 371–389.

[3] C. Dartyge, *Le problème de Tchébychev pour le douzième polynôme cyclotomique*, Proc. London Math. Soc., à paraître.
[4] F. Diaz y Diaz and E. Friedman, *Signed fundamental domains for totally real number fields*, Proc. London Math. Soc. (3) 108 (2014), 965–988.
[5] D. R. Heath-Brown, *The largest prime factor of* $X^3 + 2$, Proc. London Math. Soc. (3) 82 (2001), 554–596.
[6] C. Hooley, *On the greatest prime factor of a cubic polynomial*, J. Reine Angew. Math. 303/304 (1978), 21–50.
[7] H. Iwaniec, *Rosser's sieve*, Acta Arith. 36 (1980), 171–202.
[8] H. Iwaniec, *A new form of the error term in the linear sieve*, Acta Arith. 37 (1980), 307–320.
[9] C. U. Jensen, A. Ledet and N. Yui, *Generic Polynomials: Constructive Aspects of the Inverse Galois Problem*, Math. Sci. Res. Inst. Publ. 45, Cambridge Univ. Press, Cambridge, 2002.
[10] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 3rd ed., Springer Monogr. Math., Springer, Berlin, 2004.
[11] T. Shintani, *On evaluation of zeta functions of totally real algebraic number fields at non positive integers*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 23 (1976), 393–417.

R. de la Bretèche, J.-F. Mestre
Institut de Mathématiques de Jussieu
UMR 7586
Université Paris–Diderot
UFR de Mathématiques, case 7012
Bâtiment Sophie Germain
75205 Paris Cedex 13, France
E-mail: regis.de-la-breteche@imj-prg.fr
jean-francois.mestre@imj-prg.fr

Reçu le 2.9.2014
et révisé le 18.3.2015 (7913)