Sur la représentation des entiers par les formes cyclotomiques de grand degré

Étienne Fouvry & Michel Waldschmidt

Pour chaque entier $d \geq 4$, nous étudions la suite des entiers positifs représentés par une des formes binaires cyclotomiques $\Phi_n(X, Y)$ pour les n positifs tels que $\varphi(n) \geq d$. Le cas $d = 2$ a été étudié dans notre précédent texte [**FLW**]. Notre démonstration repose sur une variante d'un énoncé de [**SX**] concernant les valeurs communes prises par deux formes binaires de même degré et de discriminants non nuls.

Toutes les constantes sont effectivement calculables.

1. Introduction

Rappelons ([**FLW**]) que la suite $(\Phi_n(X, Y))_{n\geq1}$ des *formes cyclotomiques* est définie par la formule de récurrence

$$X^n - Y^n = \prod_{k|n} \Phi_k(X, Y).$$

Le polynôme $\Phi_n(X, Y)$ est homogène de degré $\varphi(n)$ (φ fonction indicatrice d'Euler) et il est relié au polynôme cyclotomique $\phi_n(t) \in \mathbb{Z}[t]$ par la formule

$$\Phi_n(X, Y) = Y^{\varphi(n)}\phi_n(X/Y).$$

Puisque, pour $n \geq 3$, le polynôme $\phi_n(t)$ n'a aucun zéro réel, on a donc l'inégalité

$$\Phi_n(x, y) \gg \max(|x|^{\varphi(n)}, |y|^{\varphi(n)}),$$

uniformément sur x et y réels.

Pour $N \geq 2$ et d entier pair, on désigne par $\mathcal{A}_d(N)$ le cardinal de l'ensemble des entiers $1 \leq m \leq N$ tels qu'il existe un entier n et des entiers (x, y) vérifiant les trois conditions

$$\begin{cases} \varphi(n) \geq d, \\ \Phi_n(x, y) = m, \\ \max(|x|, |y|) \geq 2. \end{cases} \tag{1.1}$$

On s'intéresse au comportement asymptotique de $\mathcal{A}_d(N)$ pour d fixé et N tendant vers l'infini. Il est alors sage d'introduire la dernière condition de (1.1) puisque pour tout p premier on a $\Phi_p(1, 1) = p$ et le cardinal des $p \leq N$ masquerait le terme principal de l'estimation qui sera donnée en (1.6). Par convention, nous réservons la lettre p aux nombres premiers. Enfin, si n est un entier impair, on a l'égalité

$$\Phi_{2n}(X, Y) = \Phi_n(X, -Y).$$

On peut ainsi ajouter, aux conditions de (1.1), la condition de congruence

$$n \not\equiv 2 \bmod 4, \tag{1.2}$$

sans modifier l'étude de $\mathcal{A}_d(N)$.

Appelons *totient* toute valeur prise par la fonction φ. La suite croissante des totients est ainsi

$$\mathfrak{T} := \{1, 2, 4, 6, 8, 10, 12, 16, 18, 20, 22, 24, 28, 30, \ldots\}.$$

Cette suite contient la suite des $p-1$ mais reste mystérieuse à de nombreux points de vue (on se reportera avec profit aux articles de Ford [**Fo1**] et [**Fo2**] traitant, entre autres choses, de la fonction de comptage de la suite $\mathfrak{T}$ et du nombre de solutions à l'équation $\varphi(n) = d$). Il est naturel de restreindre l'étude de $\mathcal{A}_d(N)$ au cas où d est un totient pair. L'étude de $\mathcal{A}_2(N)$ a été traitée dans [**FLW**, Théorème 1.3] où il est prouvé qu'il existe deux constantes $C_2 = 1,403132\dots$ et $C_2' = 0,302316\dots$ telles que, uniformément pour $N \geq 2$, on a l'égalité

$$\mathcal{A}_2(N) = C_2 \frac{N}{(\log N)^{\frac{1}{2}}} - C_2' \frac{N}{(\log N)^{\frac{3}{4}}} + O\left(\frac{N}{(\log N)^{\frac{3}{2}}}\right). \tag{1.3}$$

Les constantes C_2 et C_2' se définissent au moyen des valeurs, au point $s = 1$, de certaines fonctions de Dirichlet $L(s,\chi)$ où χ est le caractère de Kronecker attaché aux corps quadratiques de discriminants -4, -3 et 12.

Pour d totient ≥ 4, les outils de [**FLW**] conduisent à la majoration

$$\mathcal{A}_d(N) = O\big(N^{\frac{2}{d}}(\log N)^{1,161}\big), \tag{1.4}$$

(voir corollaire 4.11 et sa preuve ci–dessous).

Par rapport à [**FLW**], le présent travail innove en injectant résultats et méthodes de [**SX**] que nous décrirons au §2. Contentons–nous pour l'instant de donner notre résultat principal qui améliore notablement (1.4). Pour son énoncé, nous introduisons les notations suivantes :

• si d est un totient, on note $d^\dagger$ le successeur immédiat de d dans la suite $\mathfrak{T}$.

• pour d entier ≥ 3, on pose

$$\eta_d = \begin{cases} 2/9 + 73/(108\sqrt{3}) \text{ si } d = 3, \\ (1/2 + 9/(4\sqrt{d}))/d \text{ si } 4 \leq d \leq 20, \\ 1/d \text{ pour } d \geq 21. \end{cases} \tag{1.5}$$

On prouvera donc le

Théorème 1.1. — *Soit $d \geq 4$ un totient. Alors, il existe une constante $C_d > 0$, telle que, pour tout $\varepsilon > 0$ et uniformément pour $N \geq 2$, on a l'égalité*

$$\mathcal{A}_d(N) = C_d N^{\frac{2}{d}} + O(N^{\frac{2}{d^\dagger}}) + O_\varepsilon(N^{\eta_d + \varepsilon}). \tag{1.6}$$

Remarque 1.2. — La formule (1.6) est d'autant plus précise que $d^\dagger - d$ est grand. Ainsi, dans le cas particulier où $d \geq 6$, la minoration triviale

$$d^\dagger \geq d + 2,$$

réduit la formule (1.6) en sa forme plus grossière

$$\mathcal{A}_d(N) = C_d N^{\frac{2}{d}} + O(N^{\frac{2}{d+2}}).$$

Remarque 1.3. — Le théorème 1.1 suppose $d \geq 4$. La formule (1.3) correspond donc au cas $d = 2$. Mais, par la présence au dénominateur du facteur $(\log N)^{\frac{1}{2}}$, elle diffère notablement de (1.6). Cette différence s'explique comme suit. Il y a trois formes cyclotomiques de degré 2. Ce sont les trois formes quadratiques binaires

$$\Phi_3(X,Y) = X^2 + XY + Y^2,\ \Phi_4(X,Y) = X^2 + Y^2,\ \text{et } \Phi_6(X,Y) = X^2 - XY + Y^2. \tag{1.7}$$

Puisque $\Phi_6(X,-Y)=\Phi_3(X,Y)$ les formes Φ_6 et Φ_3 représentent les mêmes entiers. Mais les formes Φ_3 et Φ_4 à la différence des formes cyclotomiques de degré au moins 4, ont un nombre infini d'automorphismes comme définis au §4.4. Par exemple on a $\mathrm{Aut}\Phi_4 = \mathrm{O}(2,\mathbb{Q})$ (le groupe des matrices orthogonales 2×2 à coefficients dans $\mathbb{Q}$).

L'objet des théorèmes 1.4 et 1.6 est de compléter la formule (1.6). Nous précisons d'abord la constante C_d.

Théorème 1.4. — *Soit $d \geq 4$ un totient. La constante C_d de la formule* (1.6) *vérifie l'égalité*

(1.8)
$$C_d = \sum_{\substack{n\not\equiv 2 \bmod 4\\ \varphi(n)=d}} w_n\, A_{\Phi_n}$$

où

(1.9)
$$w_n := \begin{cases} \frac14 & si\ 4 \nmid n,\\ \frac18 & si\ 4 \mid n,\end{cases}$$

et

$$A_{\Phi_n} = \iint_{\Phi_n(x,y)\leq 1} \mathrm{d}x\mathrm{d}y.$$

Voici deux exemples dans lesquels la formule (1.8) donnant la valeur de la constante C_d se simplifie.

1. Soit $p \geq 5$ un nombre premier de Sophie Germain, c'est-à-dire tel que le nombre $\ell = 2p+1$ soit premier. Alors ℓ est l'unique entier $\not\equiv 2 \bmod 4$ tel que $\varphi(\ell) = 2p$ et on a l'égalité
$$C_{2p} = \frac14 A_{\Phi_\ell}.$$
On conjecture qu'il y a une infinité de nombres premiers de Sophie Germain.
2. Supposons que $d \geq 4$ est une puissance de 2, disons $d = 2^k$.

   On désigne par $\mathcal{M}$ l'ensemble des nombres entiers $m \geq 1$ dont le développement binaire $m = 2^{a_1} + 2^{a_2} + \cdots + 2^{a_r}$ est tel que chacun des nombres $F_{a_i} = 2^{2^{a_i}} + 1$ est premier (nombre premier de Fermat). L'ensemble $\mathcal{M}$ contient les entiers $1,2,3,\ldots,31$; on ne connaît pas d'autre élément de $\mathcal{M}$. Pour chaque $m\in\mathcal{M}$ vérifiant $m \leq k$, on définit
$$\ell_k(m) = 2^{k-m+1} F_{a_1}F_{a_2}\cdots F_{a_r},$$
de sorte que $\varphi(\ell_k(m)) = 2^k$. Les entiers $n \not\equiv 2 \bmod 4$ tels que $\varphi(n) = d$ sont d'une part $n = 2d$, qui est multiple de 4, d'autre part les $\ell_k(m)$ avec $m < k$, qui sont aussi multiples de 4, et enfin, si $k \in \mathcal{M}$, $\ell_k(k)/2$ qui est impair, avec $A_{\Phi_{\ell_k(k)}} = A_{\Phi_{\ell_k(k)/2}}$. Alors
$$C_d = \begin{cases} \dfrac18 A_{\Phi_{2d}} + \dfrac18 \displaystyle\sum_{\substack{m\in\mathcal{M}\\ m<k}} A_{\Phi_{\ell_k(m)}} & \text{si } k \notin \mathcal{M},\\ \dfrac18 A_{\Phi_{2d}} + \dfrac18 \displaystyle\sum_{\substack{m\in\mathcal{M}\\ m<k}} A_{\Phi_{\ell_k(m)}} + \dfrac14 A_{\Phi_{\ell_k(k)}} & \text{si } k \in \mathcal{M},\end{cases}$$
avec
$$A_{\Phi_{2d}} = \int_{-\infty}^{\infty} \frac{\mathrm{d}t}{(1+t^d)^{2/d}} = \frac{2}{d}\frac{\Gamma(1/d)^2}{\Gamma(2/d)}$$

(cf. §6.1 et [**SX**, Corollaire 1.3 et § 5]).

Nous montrerons que l'on a

$$\lim_{n\to\infty} A_{\Phi_n} = 4.$$

C'est une conséquence de l'énoncé plus précis suivant, concernant le *domaine fondamental cyclotomique* $\mathcal{O}_n$ défini par

$$\mathcal{O}_n = \{(x,y) \in \mathbb{R}^2 \mid \Phi_n(x,y) \le 1\}.$$

Théorème 1.5. — *Soit $\varepsilon > 0$. Il existe $n_0 = n_0(\varepsilon)$ tel que, pour $n \ge n_0$, le domaine fondamental cyclotomique $\mathcal{O}_n$ d'indice n contient le carré centré en O de côté $2 - n^{-1+\varepsilon}$ et est contenu dans le carré centré en O de côté $2 + n^{-1+\varepsilon}$.*

Enfin nous discutons de l'optimalité de la formule (1.6)

Théorème 1.6. — *On adopte les notations du théorème 1.1. Soit $d \ge 4$ un entier tel que d et $d+2$ soient des totients. Il existe une constante positive $v_d > 0$ telle que pour N suffisamment grand, on ait l'inégalité*

$$\mathcal{A}_d(N) \ge C_d N^{\frac{2}{d}} + v_d N^{\frac{2}{d+2}}.$$

Remarque 1.7. — Il est naturel de conjecturer qu'il y a une infinité de d tels que $d+2$ soit aussi un totient : c'est une conséquence de la conjecture des nombres premiers jumeaux. Enfin, on peut tout à fait envisager des énoncés analogues sous l'hypothèse $d^\dagger = d + \nu$ où ν est un entier pair fixé. Cette extension nécessiterait une adaptation des propriétés de confinement décrites aux §4.1, §4.2 et §4.3.

2. Valeurs prises par une forme binaire

L'objet de cette section est de décrire précisément le résultat de Stewart et Xiao [**SX**]. Ce résultat déja mentionné plus haut est à la base de notre travail. Dans toute cette section $F = F(X,Y)$ est un polynôme homogène de $\mathbb{Z}[X,Y]$ de degré $d \ge 3$. On dit alors que F est une *forme binaire de degré d*. Un entier m est dit *représenté* par une forme binaire F s'il existe $(x,y) \in \mathbb{Z}^2$ tel que $F(x,y) = m$. On désigne par $R_F(N)$ le cardinal de l'ensemble des entiers m représentés par F et vérifiant $0 \le |m| \le N$. On appelle *automorphisme* de F toute matrice U de $\mathrm{Gl}(2,\mathbb{Q})$

$$U = \begin{pmatrix} u_1 & u_2 \\ u_3 & u_4 \end{pmatrix},$$

telle que

$$F(X,Y) = F(u_1X + u_2Y, u_3X + u_4Y). \tag{2.1}$$

Muni de la multiplication des matrices, l'ensemble des automorphismes de F forme un sous–groupe fini de $\mathrm{Gl}(2,\mathbb{Q})$, noté $\mathrm{Aut}F$. Il existe alors une ensemble $\mathcal{G}$ de dix sous–groupes finis de $\mathrm{Gl}(2,\mathbb{Z})$ tel que que pour toute forme binaire F de degré $d \ge 3$, il existe $T \in \mathrm{Gl}(2,\mathbb{Q})$ et un unique $G \in \mathcal{G}$ vérifiant

$$\mathrm{Aut}F = TGT^{-1}.$$

L'ensemble $\mathcal{G}$ contient en particulier les deux groupes suivants

1. $\mathbb{D}_2$, groupe diédral à quatre éléments, engendré par
$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ et } \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},$$
2. $\mathbb{D}_4$, groupe diédral à huit éléments, engendré par
$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ et } \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

À partir de la décomposition précédente, Stewart et Xiao construisent un nombre rationnel W_F (voir [**SX**, Theorem 1.2]) dont la définition, de nature algébrique, est longue puisqu'elle envisage les dix possibilités pour G. Disons, pour mémoire, que W_F tient compte des déterminants des réseaux de $\mathbb{Z}^2$ dont l'image, par certains sous–groupes de Aut$F$, est incluse dans $\mathbb{Z}^2$. En vue des applications, nous nous restreignons à deux cas particuliers

1. Cas où $G = \mathbb{D}_2$. Soit Λ le sous–réseau des éléments $(v, w) \in \mathbb{Z}^2$ tels que, pour tout $A \in \mathrm{Aut}F$ on ait $A \begin{pmatrix} v \\ w \end{pmatrix} \in \mathbb{Z}^2$. On pose alors

$$W_F = \frac{1}{2}\Big(1 - \frac{1}{2|\det(\Lambda)|}\Big). \tag{2.2}$$

2. Cas où $G = \mathbb{D}_4$. D'abord Λ est défini comme précédemment. Le groupe Aut$F$ possède exactement trois sous–groupes de cardinal 4, notés G_1, G_2 et G_3. On désigne par Λ_i $(1 \leq i \leq 3)$ le sous–réseau des éléments $(v, w) \in \mathbb{Z}^2$ tels que, pour tout $A \in G_i$ on ait $A \begin{pmatrix} v \\ w \end{pmatrix} \in \mathbb{Z}^2$. On pose alors

$$W_F = \frac{1}{2}\Big(1 - \frac{1}{2|\det(\Lambda_1)|} - \frac{1}{2|\det(\Lambda_2)|} - \frac{1}{2|\det(\Lambda_3)|} + \frac{3}{4|\det(\Lambda)|}\Big). \tag{2.3}$$

Notons
$$A_F := \iint_{|F(x,y)| \leq 1} \mathrm{d}x\mathrm{d}y,$$
l'aire de la région fondamentale associée à F. Enfin, pour $d \geq 4$ entier pair, nous introduisons la constante β_d^* définie par

$$\beta_d^* = \begin{cases} 3/(d\sqrt{d}) \text{ pour } d = 4,\, 6,\, 8 \\ 1/d \text{ pour } d \geq 10. \end{cases} \tag{2.4}$$

Nous pouvons maintenant énoncer le résultat fondamental de [**SX**, Theorem 1.1].

Théorème 2.1. — *Pour tout $d \geq 3$ il existe une constante $\beta_d < 2/d$ ayant la propriété suivante : Pour toute forme binaire F de degré d, de discriminant non nul, pour tout $\varepsilon > 0$, on a, uniformément pour $N \geq 2$ l'égalité*

$$R_F(N) = A_F\, W_F N^{\frac{2}{d}} + O_{F,\varepsilon}(N^{\beta_d + \varepsilon}). \tag{2.5}$$

Si, dans la formule (2.5), on se restreint aux formes binaires F de degré pair $d \geq 4$, de discriminant non nul, sans facteur linéaire réel, on peut donner à β_d la valeur β_d^*, définie en (2.4).

3. Valeurs communes à deux formes binaires

Aux formes binaires $F_1 = F_1(X_1, X_2)$ et $F_2 = F_2(X_3, X_4)$ on associe les deux fonctions de comptage suivantes :

1. Pour $B \geq 2$, $\mathcal{N}_{F_1,F_2}(B)$ est le cardinal de l'ensemble

$$\Big\{(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4 \mid \max_{i=1,2,3,4} |x_i| \leq B,\ F_1(x_1, x_2) = F_2(x_3, x_4)\Big\}.$$

2. Pour $N \geq 2$, $R_{F_1,F_2}(N)$ est le cardinal de l'ensemble

$$\Big\{n \mid |n| \leq N,\, n = F_1(x_1, x_2) = F_2(x_3, x_4),\ \text{pour certains } (x_1, x_2, x_3, x_4) \in \mathbb{Z}^4\Big\}.$$

Généralisant la définition (2.1), on dit que F_1 et F_2 sont *isomorphes* s'il existe $U \in \mathrm{Gl}(2, \mathbb{Q})$ tel que

$$F_1(X_1, X_2) = F_2(u_1X_1 + u_2X_2, u_3X_1 + u_4X_2). \tag{3.1}$$

En particulier deux formes isomorphes ont même degré. Nous prouverons au §3.1 le

Théorème 3.1. — *Soient F_1 et F_2 deux formes non isomorphes de même degré $d \geq 3$. On suppose de plus que les discriminants de F_1 et de F_2 sont non nuls et qu'au moins une des formes F_i n'est pas divisible par une forme linéaire non nulle à coefficients rationnels. Alors, pour tout $\varepsilon > 0$ on a la majoration*

$$\mathcal{N}_{F_1,F_2}(B) = O(B^{d\eta_d+\varepsilon}), \tag{3.2}$$

où η_d est défini en (1.5).

Remarque 3.2. — La condition que l'une des formes F_1 et F_2 ne contient pas de facteur linéaire sur $\mathbb{Q}$ est importante. Considérons les deux formes

$$F_1(X_1, X_2) = X_1(X_1^2 + X_2^2)$$

et

$$F_2(X_3, X_4) = X_3(X_3^2 + 2X_4^2).$$

Elles ne sont pas isomorphes. L'égalité $F_1(0, x_2) = F_2(0, x_4) = 0$ implique l'inégalité $\mathcal{N}_{F_1,F_2}(B) \gg B^2$, ce qui est supérieur à la partie droite de (3.2).

Du théorème 3.1 nous déduirons le

Corollaire 3.3. — *Soient F_1 et F_2 deux formes vérifiant les hypothèses du théorème 3.1. On suppose de plus que les deux formes F_1 et F_2 sont définies positives. Alors pour tout $\varepsilon > 0$ on a l'inégalité*

$$R_{F_1,F_2}(N) \ll N^{\eta_d+\varepsilon}.$$

Démonstration du corollaire 3.3. — Les hypothèses impliquent les inégalités

$$|\, F_1(x_1, x_2)\,| \gg \max(|x_1^d|, |x_2^d|) \text{ et } |\, F_2(x_3, x_4)\,| \gg \max(|x_3^d|, |x_4^d|),$$

uniformément pour $x_i \in \mathbb{R}$. Par conséquent, si on a

$$-N \leq F_1(x_1, x_2) = F_2(x_3, x_4) \leq N,$$

on a alors

$$\max_{i=1,2,3,4} |x_i| \ll N^{\frac{1}{d}}.$$

Il suffit alors de remplacer B par $O(N^{\frac{1}{d}})$ dans la majoration (3.2). $\square$

3.1. Preuve du théorème 3.1. — Puisque les formes F_1 et F_2 sont de discriminants non nuls, l'hypersurface $\mathbb{X}$ de $\mathbb{P}^3(\mathbb{C})$ définie par l'équation

$$\mathbb{X} : F_1(X_1, X_2) - F_2(X_3, X_4) = 0 \tag{3.3}$$

est lisse. Nous inspirant de [**SX**], nous décomposons $\mathcal{N}_{F_1,F_2}(B)$ en

$$\mathcal{N}_{F_1,F_2}(B) = \mathcal{N}^{(1)}_{F_1,F_2}(B) + \mathcal{N}^{(2)}_{F_1,F_2}(B) + 1, \tag{3.4}$$

où

• $\mathcal{N}^{(1)}_{F_1,F_2}(B)$ est le nombre de quadruplets non nuls (x_1, x_2, x_3, x_4) de $\mathbb{Z}^4$, vérifiant $\max |x_i| \leq B$, et tels que le point projectif associé $(x_1 : x_2 : x_3 : x_4)$ appartienne à $\mathbb{X}$, mais ne se situe pas sur une droite (complexe) contenue dans $\mathbb{X}$,

• $\mathcal{N}^{(2)}_{F_1,F_2}(B)$ est le nombre de quadruplets non nuls (x_1, x_2, x_3, x_4) de $\mathbb{Z}^4$, vérifiant $\max |x_i| \leq B$, et tels que le point projectif associé $(x_1 : x_2 : x_3 : x_4)$ appartienne à une droite (complexe) contenue dans $\mathbb{X}$.

Nous prouverons d'abord la

Proposition 3.4. — *Pour tout $\varepsilon > 0$ et uniformément pour $B \geq 1$, on a l'inégalité*

$$\mathcal{N}^{(1)}_{F_1,F_2}(B) \ll B^{d\eta_d+\varepsilon}.$$

Puis la

Proposition 3.5. — *Uniformément pour $B \geq 1$, on a l'inégalité*

$$\mathcal{N}^{(2)}_{F_1,F_2}(B) \ll B.$$

En combinant ces deux propositions et la formule (3.4) on complète la preuve du théorème 3.1.

3.1.1. *Preuve de la Proposition 3.4.* — Si $\boldsymbol{x} = (x_1 : x_2 : x_3, : x_4)$ est un point de $\mathbb{P}^3(\mathbb{Q})$, on désigne par $h(\boldsymbol{x})$ la hauteur de $\boldsymbol{x}$, c'est–à–dire le maximum des $|x_i|$, si (x_1, x_2, x_3, x_4) est un quadruplet d'entiers premiers entre eux dans leur ensemble, représentant $\boldsymbol{x}$. Notons aussi $N^{(1)}(\mathbb{X}, B)$ le cardinal de l'ensemble des $\boldsymbol{x}$ de $\mathbb{P}^3(\mathbb{Q})$ appartenant à $\mathbb{X}$ mais non situés sur une droite contenue dans $\mathbb{X}$ et de hauteur $h(\boldsymbol{x}) \leq B$. En décomposant suivant la valeur δ du pgcd de (x_1, x_2, x_3, x_4) on déduit l'inégalité

$$\mathcal{N}^{(1)}_{F_1,F_2}(B) \leq \sum_{1 \leq \delta \leq B} N^{(1)}(\mathbb{X}, B/\delta). \tag{3.5}$$

Un résultat de Salberger [**Sa**, Theorem 0.1], donne l'inégalité

$$N^{(1)}(\mathbb{Y}, B) \ll B^{d\eta_d+\varepsilon}$$

valable pour toute surface projective $\mathbb{Y} \subset \mathbb{P}^n(\mathbb{Q})$, géométriquement intègre de degré $d > 2$. La surface $\mathbb{X}$ vérifie cette propriété. En effet supposons qu'il existe des polynômes A et B de degré ≥ 1 tels que

$$F_1(X_1, X_2) - F_2(X_3, X_4) = A(X_1, X_2, X_3, X_4)B(X_1, X_2, X_3, X_4).$$

Calculant les dérivées partielles par rapport à chacun des X_i, on voit que tout point $(x_1 : x_2 : x_3 : x_4)$ de $\mathbb{P}^3(\mathbb{C})$ tel que

$$A(x_1, x_2, x_3, x_4) = B(x_1, x_2, x_3, x_4) = 0,$$

est un point singulier de $\mathbb{X}$. Puisqu'on est dans $\mathbb{P}^3(\mathbb{C})$, les deux surfaces d'équation $A = 0$ et $B = 0$ ont une intersection non vide. Ainsi $\mathbb{X}$ serait singulière, ce qui contredit la propriété de lissité énoncée au §3.1.

Il suffit de sommer sur $\delta < B$ l'inégalité (3.5) pour compléter la preuve de la Proposition 3.4.

3.1.2. *Droites contenues dans* $\mathbb{X}$. — Afin de démontrer la Proposition 3.5, nous donnons des conditions nécessaires pour qu'une droite projective de $\mathbb{P}^3(\mathbb{C})$ appartienne à $\mathbb{X}$ en exploitant le fait que dans l'équation (3.3) définissant $\mathbb{X}$, les paires de variables (X_1, X_2) et (X_3, X_4) sont séparées.

Lemme 3.6. — *Sous les hypothèses du théorème 3.1, si une droite projective de* $\mathbb{P}^3(\mathbb{C})$ *appartient à l'hypersurface* $\mathbb{X}$ *définie par* (3.3) *et contient un point rationnel, elle est définie par des équations*

$$\begin{cases} X_1 &= u_1X_3 + u_2X_4 \\ X_2 &= u_3X_3 + u_4X_4, \end{cases} \tag{3.6}$$

où l'un au moins des u_i *est irrationnel.*

Démonstration. — Pour $\mathbf{a} = (a_1, a_2, a_3, a_4)$ et $\mathbf{b} = (b_1, b_2, b_3, b_4)$ deux quadruplets non nuls et non proportionnels de nombres complexes, on suppose que la droite projective $\mathbb{D}_{\mathbf{a},\mathbf{b}}$ de $\mathbb{P}^3(\mathbb{C})$ définie par les équations

$$\mathbb{D}_{\mathbf{a},\mathbf{b}} \;:\; \begin{cases} a_1X_1 + a_2X_2 + a_3X_3 + a_4X_4 &= 0 \\ b_1X_1 + b_2X_2 + b_3X_3 + b_4X_4 &= 0 \end{cases} \tag{3.7}$$

est contenue dans $\mathbb{X}$ et contient un point rationnel.

• Si $a_1 = a_2 = 0$ et $a_3 \neq 0$, on substitue $X_3 = -(a_4/a_3)X_4$ dans la deuxième équation de (3.7) qui devient ainsi

$$b_1X_1 + b_2X_2 = \frac{a_4b_3 - a_3b_4}{a_3}X_4. \tag{3.8}$$

⋄ Si $a_4b_3 - a_3b_4 = 0$, cela signifie que $\mathbb{X}$ contient une droite de la forme

$$\begin{cases} a_3X_3 + a_4X_4 = 0 \\ b_1X_1 + b_2X_2 = 0. \end{cases} \tag{3.9}$$

Exploitant la forme particulière de l'équation (3.3) définissant $\mathbb{X}$, on déduit

$$b_1X_1 + b_2X_2 \text{ divise } F_1(X_1, X_2) \text{ et } a_3X_3 + a_4X_4 \text{ divise } F_2(X_3, X_4).$$

Compte tenu de l'hypothèse sur les F_i, ces conditions de divisibilité contredisent l'hypothèse qu'il y a un point rationnel sur la droite définie par (3.9).

⋄ Si $a_4b_3 - a_3b_4 \neq 0$, on remplace X_3 par la valeur donnée par la première équation de (3.7) et X_4 par la valeur donnée en (3.8) conduisant à

$$F_1(X_1, X_2) = F_2(X_3, X_4) = (a_4b_3 - a_3b_4)^{-d}F_2(-a_4, a_3)(b_1X_1 + b_2X_2)^d,$$

ce qui contredit l'hypothèse que le discriminant de F_1 est non nul.

• Si $a_1 = a_2 = 0$ et $a_4 \neq 0$, par le même type de raisonnement suivi précédemment, on est ramené au cas où $(a_1, a_2) \neq (0, 0)$.

• Par symétrie, on suit le même raisonnement dans les trois cas suivants : si $a_3 = a_4 = 0$, si $b_1 = b_2 = 0$ ou si $b_3 = b_4 = 0$.

• En conclusion de la discussion précédente, nous avons prouvé que si $\mathbb{D}_{\mathbf{a},\mathbf{b}}$, contenue dans $\mathbb{X}$, possède un point rationnel, on a nécessairement

$$(a_1, a_2),\ (a_3, a_4),\ (b_1, b_2),\ \text{et } (b_3,\ b_4) \text{ sont } \neq (0,0). \tag{3.10}$$

• Supposons maintenant $a_1b_2 = a_2b_1$ et $a_1 \neq 0$. Multipliant la première équation de (3.7) par $-b_1$ et la seconde par a_1, on obtient que dans ce cas le système d'équations définissant $\mathbb{D}_{\mathbf{a},\mathbf{b}}$ est équivalent à

$$\begin{cases} a_1X_1 + a_2X_2 + a_3X_3 + a_4X_4 & = 0 \\ (a_1b_3 - a_3b_1)X_3 + (a_1b_4 - a_4b_1)X_4 & = 0. \end{cases}$$

Or (3.10) a éliminé le cas $(b_1, b_2) = (0, 0)$. On en déduit que l'hypothèse $a_1b_2 = a_2b_1$ et $a_1 \neq 0$ est impossible.

• Supposons maintenant $a_1b_2 = a_2b_1$ et $a_2 \neq 0$. Mais ce cas est impossible par un raisonnement identique. Puisque par (3.10) le cas $(a_1, a_2) = (0, 0)$ est interdit, on est ramené à supposer que $a_1b_2 \neq a_2b_1$.

• Pour finir on suppose donc que $a_1b_2 \neq a_2b_1$. Par résolution d'un système (2,2) en les inconnues X_1 et X_2 et de déterminant non nul, on voit que le système (3.7) est équivalent à

$$\begin{cases} X_1 & = u_1X_3 + u_2X_4 \\ X_2 & = u_3X_3 + u_4X_4, \end{cases}$$

où les u_i sont des nombres complexes. On a donc l'égalité

$$F_2(X_3, X_4) = F_1(u_1X_3 + u_2X_4, u_3X_3 + u_4X_4). \tag{3.11}$$

$\diamond$ Si $\det \begin{pmatrix} u_1 & u_2 \\ u_3 & u_4 \end{pmatrix} = 0$, cela signifie que par exemple, on a, pour un certain λ complexe, l'égalité $u_1X_3 + u_2X_4 = \lambda(u_3X_3 + u_4X_4)$ donc en reportant, on déduit l'égalité

$$F_2(X_3, X_4) = (u_3X_3 + u_4X_4)^d F_1(\lambda, 1),$$

ce qui contredit l'hypothèse de non nullité du discriminant de F_2.

$\diamond$ Si $\det \begin{pmatrix} u_1 & u_2 \\ u_3 & u_4 \end{pmatrix} \neq 0$, par (3.11) on voit que les formes F_1 et F_2 sont isomorphes par un changement de variables linéaires à coefficients complexes. L'hypothèse de non isomorphisme, sur $\mathrm{Gl}(2, \mathbb{Q})$, de F_1 et F_2 implique que parmi les u_i l'un au moins est irrationnel.

Ceci termine la démonstration du lemme 3.6. $\square$

3.1.3. *Preuve de la proposition 3.5.* — On sait que pour tout $d \geq 3$, il existe un entier $\ell(d)$, tel que, toute surface lisse de $\mathbb{P}^3(\mathbb{C})$ de degré d contient au plus $\ell(d)$ droites. Pour des études fines concernant cette constante $\ell(d)$ on se reportera à [**Se**] et à [**BS**] par exemple.

Grâce au lemme 3.6, on est ramené à dénombrer l'ensemble des quadruplets d'entiers $(x_1, \ldots, x_4)$ avec $\max |x_i| \leq B$, vérifiant

$$\begin{cases} x_1 & = u_1x_3 + u_2x_4 \\ x_2 & = u_3x_3 + u_4x_4, \end{cases}$$

sachant que l'un au moins des u_i est irrationnel. Disons que c'est u_1.

– si $\dim_{\mathbb{Q}}(1, u_1, u_2) = 3$, la seule solution en $(x_1, x_3, x_4) \in \mathbb{Z}^3$ de l'équation $x_1 = u_1x_3 + u_2x_4$ est $(0, 0, 0)$,

– si $\dim_{\mathbb{Q}}(1, u_1, u_2) = 2$, on exprime $u_2 = a + bu_1$, avec a et b rationnels et on est ramené à l'équation

$$x_1 - ax_4 = (x_3 + bx_4)u_1,$$

qui implique $x_1 - ax_4 = x_3 + bx_4 = 0$. Donc le système (3.6) admet $O(B)$ quadruplets $(x_1, \dots, x_4)$ solutions de hauteur inférieure à B.

Ceci termine la preuve de la proposition 3.5.

4. Quelques propriétés des formes cyclotomiques

Dans ce paragraphe nous prouvons quelques résultats généraux concernant les formes cyclotomiques $\Phi_n(X,Y)$ dont le degré est $d = \varphi(n)$. Ces divers résultats seront nécessaires lors de la preuve des théorèmes 1.1, 1.4, 1.5 et 1.6. En particulier les résultats des sections §4.1, §4.2 et §4.3. ne seront utilisés que pour la preuve du Théorème 1.6. Nous rappelons d'abord plusieurs formules classiques sur les $\Phi_n(X,Y)$. Ces formules ne sont que la version homogène des formules correspondantes sur les $\phi_n(x)$.

Nous rappelons certaines notations et conventions : si $n \geq 1$ est un entier, on désigne par $\mu(n)$ la valeur de la fonction de Möbius, $\omega(n)$ est le nombre de facteurs premiers distincts de n, $\kappa(n)$ est le *radical* de n, c'est–à–dire le produit de tous les premiers divisant n, $d(n)$ le nombre de diviseurs. On dit que deux nombres rationnels u et v sont congrus modulo le nombre premier p si on a $u - v \in p\mathbb{Z}_p$, où $\mathbb{Z}_p$ est l'anneau des entiers p–adiques.

Si $n \geq 2$ est factorisé en $n := p^r m$, avec $p \nmid m$ et $r \geq 1$, la forme Φ_n vérifie les identités suivantes

$$\Phi_n(X,Y) = \prod_{d|n} (X^d - Y^d)^{\mu(n/d)},$$

$$\Phi_n(X,Y) = \frac{\Phi_m(X^{p^r}, Y^{p^r})}{\Phi_m(X^{p^{r-1}}, Y^{p^{r-1}})}, \tag{4.1}$$

et

$$\Phi_n(X,Y) = \Phi_{pm}(X^{p^{r-1}}, Y^{p^{r-1}}).$$

Par itération de cette dernière formule, on parvient à

$$\Phi_n(X,Y) = \Phi_{\kappa(n)}(X^{n/\kappa(n)}, Y^{n/\kappa(n)}). \tag{4.2}$$

Nous rappelons quelques valeurs de ϕ_n en certains points :

$$\phi_n(1) = \begin{cases} 0 & \text{si } n = 1, \\ p & \text{si } n = p^k \ (k \geq 1), \\ 1 & \text{si } \omega(n) \geq 2, \end{cases} \tag{4.3}$$

et

$$\phi_n(-1) = \begin{cases} -2 & \text{si } n = 1, \\ \phi_{n/2}(1) & \text{si } n \geq 2,\ 2\|n, \\ 1 & \text{si } n \geq 3,\ 2 \nmid n, \\ 1 & \text{si } n \geq 4,\ 4|n,\ n \neq 2^\ell, \\ 2 & \text{si } n \geq 4,\ n = 2^\ell. \end{cases} \tag{4.4}$$

Pour majorer les coefficients de Φ_n nous utiliserons le résultat suivant, dû à P. Bateman [**Ba**, p.1181]. Quand P est un polynôme, nous désignons par $\mathrm{L}(P)$ (*longueur de* P) la somme des valeurs absolues des coefficients de P.

Lemme 4.1. — *Pour tout* $n \geq 1$, *on a*

$$\mathrm{L}(\phi_n) \leq n^{d(n)/2}.$$

Les majorations classiques des fonctions arithmétiques $d(n)$ et $\varphi(n)$ impliquent alors que pour tout $\varepsilon > 0$ et pour n suffisamment grand, on a

$$\varphi(n)\mathrm{L}(\phi_n) \leq e^{n^\varepsilon}. \tag{4.5}$$

4.1. Propriétés de confinement modulo p. — Nous prouvons que pour tout a et b entiers $\Phi_n(a,b)$ est, pour tout m divisant n, restreint à quelques classes de congruence modulo m.

Proposition 4.2. — *Soient* $n \geq 2$ *et* p *un premier divisant* n. *Alors pour tout* a *et* b *de* $\mathbb{Z}$ *on a*

$$\Phi_n(a,b) \equiv 0,\ 1 \bmod p. \tag{4.6}$$

Démonstration. — Remarquons d'abord que lorsque $p = 2$ ou lorsque $b \equiv 0 \bmod p$, l'énoncé précédent est trivial. Enfin on peut se restreindre au cas

$$n \text{ sans facteur carré.}$$

C'est une conséquence de l'inclusion des images $\Phi_n(\mathbb{Z},\mathbb{Z}) \subset \Phi_{\kappa(n)}(\mathbb{Z},\mathbb{Z})$, qui se déduit directement de (4.2). Commençons par le cas où n est un nombre premier. On a

Lemme 4.3. — *Soient* $p \geq 3$ *un nombre premier,* a *et* b *deux entiers. Alors on a les congruences*

1. *Si* $a \not\equiv b \bmod p$, *on a*
$$\Phi_p(a,b) \equiv 1 \bmod p,$$
2. *Si* $a \equiv b \bmod p$, *on a*
$$\Phi_p(a,b) \equiv pa^{p-1} \bmod p^2.$$

Démonstration du lemme 4.3. — C'est une conséquence de la formule $a^p \equiv a \bmod p$. Dans le premier cas, on écrit

$$\Phi_p(a,b) = (a^p - b^p)/(a-b) \equiv (a-b)/(a-b) \equiv 1 \bmod p.$$

Dans le second cas, on écrit

$$\Phi_p(a,b) = a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1},$$

on pose $b = a + pt$ avec t entier et on développe suivant la formule du binôme pour obtenir le résultat. □

Poursuivons la démonstration de la proposition 4.2. On suppose donc que n est sans facteur carré et on pose

$$n = pm = pp_2 \cdots p_t.$$

Par itération de (4.1), on a l'égalité

$$\Phi_n(a,b) = \prod_{m_1 \mid m} \Phi_p(a^{m_1}, b^{m_1})^{\mu(m/m_1)}. \tag{4.7}$$

Ceci nous amène à décomposer le produit à droite de l'égalité (4.7) en

$$\Phi_n(a,b) = \Phi_n^{\dagger}(a,b)\tilde{\Phi}_n(a,b),$$

où $\Phi_n^{\dagger}$ correspond à la condition $a^{m_1} \not\equiv b^{m_1} \bmod p$ et $\tilde{\Phi}$ le produit complémentaire. Par le lemme 4.3, on a $\Phi_p(a^{m_1}, b^{m_1}) \equiv 1 \bmod p$ si et seulement si $a^{m_1} \not\equiv b^{m_1} \bmod p$. Ceci implique que $\Phi_n^{\dagger}(a,b)$ est un nombre rationnel qui est produit et quotient d'entiers congrus à $1 \bmod p$. C'est donc un nombre rationnel congru à $1 \bmod p$.

Par définition, on a l'égalité

$$\tilde{\Phi}_n(a,b) := \prod_{\substack{m_1 \mid m \\ (a/b)^{m_1} \equiv 1 \bmod p}} \Phi_p(a^{m_1}, b^{m_1})^{\mu(m/m_1)}. \tag{4.8}$$

D'après ce qui précède, pour compléter la preuve de la congruence (4.6), il reste à prouver que $\tilde{\Phi}_n(a,b)$ est un rationnel congru à 0 ou $1 \bmod p$.

Soit ℓ l'ordre de (a/b) modulo p. Ainsi ℓ divise $p-1$ et le produit apparaissant dans (4.8) est sur les m_1 tels que

$$\ell \text{ divise } m_1 \text{ et } m_1 \text{ divise } m.$$

Ce produit est vide lorsque $\ell \nmid m$; c'est par exemple le cas si $a \not\equiv b \bmod p$ et si $(p-1, m) = 1$. On suppose donc que $\ell \mid m$. Quitte à réindicer les p_j, on peut supposer que ℓ est de la forme

$$\ell = p_2 \cdots p_r,$$

avec $1 \leq r \leq t$, avec la convention que $\ell = 1$ si $r = 1$. Posant alors $h = p_{r+1} \cdots p_t = m/\ell$ et $m_1 = \ell m_2$, on récrit la définition (4.8) comme

$$\tilde{\Phi}_n(a,b) := \prod_{m_2 \mid h} \Phi_p(a^{\ell m_2}, b^{\ell m_2})^{\mu(h/m_2)}. \tag{4.9}$$

On articule la discussion suivant plusieurs cas.

- si $h = 1$, le produit apparaissant dans (4.9) ne contient qu'un seul terme à savoir $\Phi_p(a^{\ell}, b^{\ell})$. Il est congru à $0 \bmod p$, d'après le lemme 4.3.2.

- si $h \neq 1$, en utilisant la formule de Möbius, on écrit (4.9) sous la forme

$$\tilde{\Phi}_n(a,b) = \prod_{m_2 \mid h} \Big(\frac{\Phi_p(a^{\ell m_2}, b^{\ell m_2})}{p} \Big)^{\mu(h/m_2)},$$

où maintenant chaque fraction du produit est congrue à $a^{\ell m_2 (p-1)}$ modulo p (lemme 4.3.2). Ainsi chacune de ces fractions est un entier premier à p. Le nombre rationnel $\tilde{\Phi}_n(a,b)$ vérifie donc

$$\tilde{\Phi}_n(a,b) \equiv a^{\ell m_2 (p-1) \sum_{m_2 \mid h} \mu(h/m_2)} \equiv 1 \bmod p,$$

en utilisant de nouveau la formule de Möbius. Ceci termine la preuve de la proposition 4.2. $\square$

4.2. Propriétés de confinement modulo 9. — Par la proposition 4.2, on sait que si $3 \mid n$, on a $\Phi_n(a,b) \equiv 0,\ 1 \bmod 3$. Ce n'est pas assez satisfaisant pour la future application. Nous utiliserons une version plus précise avec la

Proposition 4.4. — *Soit $k \geq 2$. Alors pour tout a et tout b entiers, on a la congruence*

$$\Phi_{3^k}(a,b) \equiv 0,\ 1,\ 3 \bmod 9.$$

Démonstration. — Les cubes modulo 9 forment l'ensemble

$$\mathfrak{Q}(9) := \{0,\ 1,\ -1\}.$$

Or

$$\Phi_3(u,v) = u^2 + uv + v^2.$$

Si u et v parcourent l'ensemble $\mathfrak{Q}(9)$ on voit que $\Phi_3(u,v)$ parcourt l'ensemble

$$\mathcal{E} = \{0, 1, 3 \bmod 9\}.$$

Pour terminer la preuve de la proposition, il suffit d'utiliser le fait que

$$\Phi_{3^k}(a,b) = \Phi_3(a^{3^{k-1}}, b^{3^{k-1}}),$$

conséquence de (4.2). □

4.3. Propriétés de confinement modulo 4. — Nous envisageons maintenant le cas où n est pair. Par la remarque (1.2), on peut même supposer que $4 \mid n$ et on écrit que $2^k \| n$ avec $k \geq 2$.

1. Soit a pair et b impair. Par application itérée de (4.1), on voit $\Phi_n(X,Y)$ est produit et quotient de polynômes de la forme $\Phi_{2^k}(X^\alpha, Y^\alpha)$ où α et β sont des nombres impairs. Puisque $\Phi_{2^k}(X,Y) = X^{2^{k-1}} + Y^{2^{k-1}}$ et $k \geq 2$, on déduit que $\Phi_{2^k}(a^\alpha, b^\beta) \equiv 0 + 1 \equiv 1 \bmod 4$ et, par conséquent, que
$$\Phi_n(a,b) \equiv 1 \bmod 4.$$
2. Soit a et b pairs. Puisque $\Phi_n(X,Y)$ est somme de monômes de la forme $c_{\mu,\nu}X^\mu Y^\nu$ avec $\mu + \nu = \varphi(n)$ et $c_{\mu,\nu}$ entier, on voit que $4 \mid c_{\mu,\nu}a^\mu b^\nu$, d'où
$$\Phi_n(a,b) \equiv 0 \bmod 4.$$
3. Supposons $a \equiv b \equiv 1 \bmod 4$. On écrit $\Phi_n(a,b) = b^{\varphi(n)}\phi_n(a/b) \equiv \phi_n(1) \bmod 4$. Et, d'après (4.3), ceci vaut $2 \bmod 4$ si $n = 2^k$ avec $k \geq 2$ ou $1 \bmod 4$ si $n \neq 2^k$. D'où
$$\Phi_n(a,b) \equiv 1,\ 2 \bmod 4.$$
4. Supposons $a \equiv -b \equiv 1 \bmod 4$. On écrit $\Phi_n(a,b) = b^{\varphi(n)}\phi_n(a/b) \equiv \phi_n(-1) \bmod 4$. Il suffit d'appliquer les deux dernières lignes de (4.4) pour conclure que l'on a, dans ce cas
$$\Phi_n(a,b) \equiv 1,\ 2 \bmod 4.$$
5. Supposons $a \equiv -1 \bmod 4$. On utilise la relation $\Phi_n(a,b) = \Phi_n(-a,-b)$ valable pour $n \geq 3$.

Nous rassemblons ces divers résultats sous la forme de la

Proposition 4.5. — *Soit n un entier divisible par* 4. *Alors pour tout a et tout b entiers, on a la congruence*

$$\Phi_n(a,b) \equiv 0,\ 1,\ 2 \bmod 4.$$

4.4. Automorphismes des formes cyclotomiques. — Soit $\Phi_n(X,Y)$ une forme cyclotomique de degré $d = \varphi(n)$. Par la définition (2.1), rechercher les automorphismes de Φ_n consiste à rechercher les matrices U de $\mathrm{Gl}(2,\mathbb{Q})$

$$U = \begin{pmatrix} u_1 & u_2 \\ u_3 & u_4 \end{pmatrix},$$

telles que

$$\Phi_n(X,Y) = \Phi_n(u_1X + u_2Y, u_3X + u_4Y). \tag{4.10}$$

Cette égalité formelle entraîne que l'ensemble $\mathbb{U}_n$ des racines primitives n–ièmes de l'unité est stable par l'application $\mathcal{H}$ de $\widehat{\mathbb{C}}$ dans $\widehat{\mathbb{C}}$ définie par

$$z \mapsto \mathcal{H}(z) := \frac{u_1z + u_2}{u_3z + u_4}. \tag{4.11}$$

Si $\mathbb{U}_n$ a au moins trois éléments (c'est–à–dire $n \geq 5$ et $n \neq 6$), il y a un cercle et un seul contenant $\mathbb{U}_n$. Il s'agit du cercle $\mathbb{S}^1$ et celui–ci est stable par $\mathcal{H}$. Les transformations de $\widehat{\mathbb{C}}$ de la forme $(az+b)/(cz+d)$ (avec $(a,b,c,d) \in \mathbb{C}^4$ et $ad-bc \neq 0$) laissant $\mathbb{S}^1$ globalement invariant sont connues : il s'agit des transformations $z \mapsto \rho z$ et $z \mapsto \rho/z$ avec ρ nombre complexe de module 1. Ainsi la fonction $\mathcal{H}$ définie en (4.11) a nécessairement une des quatre formes

$$\mathcal{H}(z) = z,\ -z,\ 1/z,\ -1/z,$$

puisque les u_i sont des rationnels. Enfin pour tout $n \geq 1$, on a l'équivalence

$$\xi \in \mathbb{U}_n \iff 1/\xi \in \mathbb{U}_n$$

et seulement pour $n \equiv 0 \bmod 4$, l'équivalence

$$\xi \in \mathbb{U}_n \iff -\xi \in \mathbb{U}_n.$$

Nous voyons donc que si

1. si $n \equiv 0 \bmod 4$, et $n \geq 8$, on a $\frac{u_1z+u_2}{u_3z+u_4} = z,\ -z,\ \frac{1}{z},\ -\frac{1}{z}$,
2. si $n \not\equiv 0 \bmod 4$, $n \geq 5$ et $n \neq 6$, on a $\frac{u_1z+u_2}{u_3z+u_4} = z,\ -z$.

Revenant à la définition (4.10) et rappelant que Φ_n est une forme homogène de degré $\varphi(n)$ on obtient les matrices U:

1. Pour $n \equiv 0 \bmod 4$, et $n \geq 8$, on a
$$U = \begin{pmatrix} \pm1 & 0 \\ 0 & \pm1 \end{pmatrix}, \begin{pmatrix} \pm1 & 0 \\ 0 & \mp1 \end{pmatrix}, \begin{pmatrix} 0 & \pm1 \\ \pm1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \pm1 \\ \mp1 & 0 \end{pmatrix}$$
2. Pour $n \not\equiv 0 \bmod 4$, $n \geq 5$ et $n \neq 6$, on a
$$U = \begin{pmatrix} \pm1 & 0 \\ 0 & \pm1 \end{pmatrix}, \begin{pmatrix} 0 & \pm1 \\ \pm1 & 0 \end{pmatrix}.$$

Les petites valeurs de n (celles vérifiant $\varphi(n) = 2$) se font directement grâce aux formes explicites données en (1.7). En notant $\mathbb{D}_k$ le groupe diédral à $2k$ éléments, on obtient la

Proposition 4.6. — *Soit $n \geq 3$ un entier. Alors le groupe des automorphismes* $\mathrm{Aut}\Phi_n$ *de* $\Phi_n(X,Y)$ *est*

$$\mathrm{Aut}\,\Phi_n = \begin{cases} \mathbb{D}_4 & \textit{si 4 divise } n, \\ \mathbb{D}_2 & \textit{dans le cas contraire.} \end{cases}$$

Nous en déduisons:

Corollaire 4.7. — *Pour $n \geq 3$, on a $W_{\Phi_n} = w_n$ où w_n est défini par* (1.9).

Démonstration. — Les groupes d'automorphismes des formes cyclotomiques sont constitués de matrices à coefficients entiers. Ainsi, dans les définitions (2.2) et (2.3), quand F est une forme cyclotomique, les réseaux Λ et Λ_i sont égaux à $\mathbb{Z}^2$, leur déterminant vaut 1. □

4.5. Isomorphismes entre formes cyclotomiques. — Rappelons que la définition d'isomorphisme entre deux formes binaires a été donnée en (3.1). La proposition suivante caractérise les formes binaires cyclotomiques isomorphes.

Proposition 4.8. — *Soient n_1 et n_2 deux entiers positifs avec $n_1 < n_2$. Les conditions suivantes sont équivalentes.*
(1) *On a $\varphi(n_1) = \varphi(n_2)$ et les deux formes binaires cyclotomiques Φ_{n_1} et Φ_{n_2} sont isomorphes.*
(2) *Les deux formes binaires cyclotomiques Φ_{n_1} et Φ_{n_2} représentent les mêmes entiers.*
(3) *n_1 est impair et $n_2 = 2n_1$.*

Les formes binaires cyclotomiques $\Phi_n(X, Y)$ avec $\varphi(n) = d$ et n non congru à 2 modulo 4 forment donc un système complet de représentants des classes d'isomorphisme des formes binaires cyclotomiques de degré d.

La démonstration de la proposition 4.8 utilisera le lemme suivant:

Lemme 4.9. — *Soit n un entier positif. Le groupe de torsion du corps cyclotomique $\mathbb{Q}(\zeta_n)$ est cyclique, d'ordre n si n est pair, d'ordre $2n$ si n est impair.*

Démonstration du lemme 4.9. — Le groupe de torsion du corps cyclotomique $\mathbb{Q}(\zeta_n)$ est cyclique, d'ordre multiple de n. S'il est d'ordre supérieur à n, alors il contient une racine primitive de l'unité d'ordre pn, avec p premier, dont le degré est $\varphi(pn)$. On en déduit $\varphi(pn) = \varphi(n)$, d'où il résulte que $p = 2$ et que n est impair. □

Démonstration de la proposition 4.8. —
(1) $\Longrightarrow$ (3) Supposons Φ_{n_1} et Φ_{n_2} isomorphes avec $n_1 < n_2$. Il existe une matrice

$$\begin{pmatrix} u_1 & u_2 \\ u_3 & u_4 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q})$$

telle que

$$\zeta_{n_1} = \frac{u_1\zeta_{n_2} + u_2}{u_3\zeta_{n_2} + u_4}\cdot$$

On en déduit que les corps cyclotomiques $\mathbb{Q}(\zeta_{n_1})$ et $\mathbb{Q}(\zeta_{n_2})$ coïncident, et le lemme 4.9 donne le résultat.
(3) $\Longrightarrow$ (2). Si n_1 est impair et $n_2 = 2n_1$, alors $\phi_{n_2}(t) = \phi_{n_1}(-t)$, donc les deux formes binaires cyclotomiques Φ_{n_1} et Φ_{n_2} représentent les mêmes entiers.
(2) $\Longrightarrow$ (1). En utilisant les notations du théorème 2.1 et du corollaire 3.3, nous avons, par hypothèse les égalités

$$R_{\Phi_1}(N) = R_{\Phi_2}(N) = R_{\Phi_1,\Phi_2}(N), \tag{4.12}$$

pour tout $N \geq 1$. Par le théorème 2.1 la première égalité de (4.12) implique $\varphi(n_1) = \varphi(n_2)$. Enfin si Φ_{n_1} et Φ_{n_2} n'étaient pas isomorphes, le corollaire 3.3 entraînerait que la deuxième égalité de (4.12) serait impossible pour N suffisamment grand. □

4.6. Résultats auxiliaires de comptage. — Notre démonstration du théorème 1.1 au §5 utilisera l'énoncé suivant [**FLW**, Theorem 1.1].

Théorème 4.10. — *Soit m un entier positif et soient n, x, y des entiers rationnels vérifiant $n \geq 3$, $\max\{|x|, |y|\} \geq 2$ et $\Phi_n(x, y) = m$. Alors*

$$\max\{|x|, |y|\} \leq \frac{2}{\sqrt{3}}\, m^{\frac{1}{\varphi(n)}} \quad \textit{et par conséquent,} \quad \varphi(n) \leq \frac{2}{\log 3} \log m.$$

Nous en déduisons le

Corollaire 4.11. — *Pour $d \geq 2$ et $N \geq 1$, on a la majoration*

$$\mathcal{A}_d(N) \leq 29 N^{\frac{2}{d}} (\log N)^{1.161}.$$

Démonstration du corollaire 4.11. — D'après le théorème 4.10, les conditions $\varphi(n) \geq d$ et $\Phi_n(x, y) \leq N$ impliquent $\max\{|x|, |y|\} \leq \frac{2}{\sqrt{3}} N^{\frac{1}{d}}$. Notons que $\mathcal{A}_d(N) = 0$ pour $N = 1$ et $N = 2$. La condition $\max\{|x|, |y|\} \geq 2$ permet d'obtenir $\varphi(n) \leq \frac{2}{\log 3} \log N$, donc $n \leq 5.383 (\log N)^{1.161}$ (formule (1.1) de [**FLW**]). Il en résulte que le nombre de triplets (n, x, y) tels que $\varphi(n) \geq d$ et $\Phi_n(x, y) \leq N$ est majoré par

$$\frac{16}{3} 5.383 N^{\frac{2}{d}} (\log N)^{1.161}.$$

□

5. Démonstration des théorèmes 1.1 et 1.4

Pour n entier avec $\varphi(n) \geq 4$ et $N \geq 1$, on désigne par $\mathcal{B}_n(N)$ l'ensemble

$$\mathcal{B}_n(N) := \big\{ m \leq N \mid m = \Phi_n(a, b) \text{ avec } \max(|a|, |b|) \geq 2 \big\}. \tag{5.1}$$

Par le théorème 4.10, on a l'implication

$$\mathcal{B}_n(N) \neq \emptyset \Rightarrow \varphi(n) \ll \log N,$$

soit encore

$$\mathcal{B}_n(N) \neq \emptyset \Rightarrow n \ll \log N \log\log\log N,$$

uniformément pour $N > 10$. Ainsi, par la définition de $\mathcal{A}_d(N)$ et par la restriction (1.2), nous avons l'égalité

$$\mathcal{A}_d(N) = \Big| \bigcup_{\substack{n \not\equiv 2 \bmod 4 \\ \varphi(n) \geq d}} \mathcal{B}_n(N) \Big|, \tag{5.2}$$

où cette réunion porte sur un nombre fini de n.

Le terme principal dans l'estimation du cardinal de $\mathcal{A}_d(N)$ sera

$$\sum_{\substack{n \not\equiv 2 \bmod 4 \\ \varphi(n) = d}} \big| \mathcal{B}_n(N) \big|.$$

L'égalité $\left|\mathcal{B}_n(N)\right| = R_{\Phi_n}(N)$ permet d'appliquer le théorème 2.1 à chacun des termes de cette somme:

$$\left|\mathcal{B}_n(N)\right| = A_{\Phi_n}\, W_{\Phi_n} N^{\frac{2}{d}} + O_{\Phi_n,\varepsilon}(N^{\beta_d^*+\varepsilon}).$$

Grâce au corollaire 4.7, on a $W_{\Phi_n} = w_n$. On obtient

$$\sum_{\substack{n\not\equiv 2 \bmod 4\\ \varphi(n)=d}} \left|\mathcal{B}_n(N)\right| = C_d N^{\frac{2}{d}} + O(N^{\beta_d^*+\varepsilon}) \tag{5.3}$$

avec la valeur de C_d annoncée dans la formule (1.8).

5.1. Minoration de $\mathcal{A}_d(N)$. — En restreignant le nombre de termes dans l'égalité (5.2), on a la minoration

$$\begin{aligned}\mathcal{A}_d(N) &\geq \Big|\bigcup_{\substack{n\not\equiv 2 \bmod 4\\ \varphi(n)=d}} \mathcal{B}_n(N)\Big|\\ &\geq \sum_{\substack{n\not\equiv 2 \bmod 4\\ \varphi(n)=d}} \left|\mathcal{B}_n(N)\right| - \sum\sum_{\substack{n_1<n_2\\ \varphi(n_1)=\varphi(n_2)=d\\ n_1,\ n_2\not\equiv 2 \bmod 4}} \Big|\mathcal{B}_{n_1}(N)\cap\mathcal{B}_{n_2}(N)\Big|.\end{aligned} \tag{5.4}$$

La première partie du membre de droite de (5.4) est traitée dans (5.3).

Pour la seconde partie, on écrit l'égalité $\left|\mathcal{B}_{n_1}(N)\cap\mathcal{B}_{n_2}(N)\right| = R_{\Phi_{n_1},\Phi_{n_2}}(N)$. Par la proposition 4.8 les formes Φ_{n_1} et Φ_{n_2} ne sont pas isomorphes. Le corollaire 3.3 donne ainsi la majoration

$$\left|\mathcal{B}_{n_1}(N)\cap\mathcal{B}_{n_2}(N)\right| = O(N^{\eta_d+\varepsilon}).$$

En conclusion, nous avons prouvé la minoration suivante de $\mathcal{A}_d(N)$:

$$\mathcal{A}_d(N) \geq C_d N^{\frac{2}{d}} - O(N^{\beta_d^*+\varepsilon}) - O(N^{\eta_d+\varepsilon}),$$

qui se simplifie en

$$\mathcal{A}_d(N) \geq C_d N^{\frac{2}{d}} - O(N^{\eta_d+\varepsilon}), \tag{5.5}$$

puisque, d'après (1.5) et (2.4), on a pour tout $d\geq 4$ pair, l'inégalité

$$\eta_d \geq \beta_d^*. \tag{5.6}$$

5.2. Majoration de $\mathcal{A}_d(N)$. — On écrit maintenant

$$\mathcal{A}_d(N) \leq \Big|\bigcup_{\substack{n\not\equiv 2 \bmod 4\\ \varphi(n)=d}} \mathcal{B}_n(N)\Big| + \mathcal{A}_{d^\dagger}(N),$$

dont on déduit la majoration

$$\mathcal{A}_d(N) \leq \sum_{\substack{n\not\equiv 2 \bmod 4\\ \varphi(n)=d}} \left|\mathcal{B}_n(N)\right| + \mathcal{A}_{d^\dagger}(N). \tag{5.7}$$

Le premier terme de cette majoration a déja été traité en (5.3). Pour majorer $\mathcal{A}_{d^\dagger}(N)$ on utilise le corollaire 4.11 avec d remplacé par $d^\dagger$. Revenant en (5.7), on a donc prouvé la majoration

$$\mathcal{A}_d(N) \leq C_d N^{\frac{2}{d}} + O(N^{\beta_d^*+\varepsilon}) + O\big(N^{\frac{2}{d^\dagger}}(\log N)^{1.161}\big). \tag{5.8}$$

Cette formule appliquée en remplaçant d par $d^\dagger$ donne la majoration

$$\mathcal{A}_{d^\dagger}(N) \ll N^{\frac{2}{d^\dagger}},$$

où il n'y a plus de puissance de $\log N$ parasite. Reportant cette dernière majoration dans (5.7), l'inégalité (5.8) est améliorée en

$$\mathcal{A}_d(N) \le C_d N^{\frac{2}{d}} + O(N^{\beta_d^* + \varepsilon}) + O(N^{\frac{2}{d^\dagger}}). \tag{5.9}$$

En combinant (5.5), (5.9) et l'inégalité (5.6), on termine la preuve de (1.6). Les preuves des théorèmes 1.1 et 1.4 sont complètes.

6. Preuve du théorème 1.5

6.1. Région fondamentale d'une forme binaire définie positive. — Quand F est une forme binaire définie positive de degré d, on désigne par $\mathcal{O}(F)$ l'ensemble des $(x, y) \in \mathbb{R}^2$ tels que $F(x, y) \le 1$. C'est un compact du plan euclidien rapporté au repère orthonormé $(O, \vec{i}, \vec{j})$. Il est délimité par une courbe algébrique de degré d et de classe C^∞, d'équation $F(x, y) = 1$. Rappelons (§ 1) que A_F désigne l'aire de $\mathcal{O}(F)$. Le changement de variable $(x, y) \to (t, y)$ avec $x = ty$ donne

$$A_F = \iint_{F(x,y)\le 1} \mathrm{d}x\mathrm{d}y = \int_{-\infty}^{+\infty} \frac{\mathrm{d}t}{F(t,1)^{2/d}}.$$

Quand F a ses coefficients algébriques, ce nombre est une période au sens de Kontsevich – Zagier. L'article [**Be**] est consacré au calcul de A_F.

On désigne par $\mathrm{L}(F)$ la longueur du polynôme $F(X, 1)$ et par $\mathrm{m}(F)$ le minimum de la fonction $F(t, 1)$ sur $\mathbb{R}$. Comme F est homogène de degré d, on a, pour tout $(x, y) \in \mathbb{R}^2$,

$$\mathrm{m}(F) \max\{|x|, |y|\}^d \le F(x, y) \le \mathrm{L}(F) \max\{|x|, |y|\}^d.$$

Il en résulte que $\mathcal{O}(F)$ contient le carré centré en O de côté $\mathrm{L}(F)^{-1/d}$, à savoir

$$\{(x, y) \in \mathbb{R}^2 \mid \max\{|x|, |y|\} \le \mathrm{L}(F)^{-1/d}\},$$

et qu'il est contenu dans le carré centré en O de côté $\mathrm{m}(F)^{-1/d}$:

$$\{(x, y) \in \mathbb{R}^2 \mid \max\{|x|, |y|\} \le \mathrm{m}(F)^{-1/d}\}.$$

Par conséquent,

$$4\mathrm{L}(F)^{-2/d} \le A_F \le 4\mathrm{m}(F)^{-2/d}.$$

6.2. Le domaine fondamental cyclotomique $\mathcal{O}_n$ pour $n \ge 3$. — Pour $n \ge 3$, $\mathcal{O}_n = \mathcal{O}(\Phi_n)$ est la région fondamentale de la forme cyclotomique Φ_n et son aire est A_{Φ_n}.

Pour $n \ge 3$, $\mathcal{O}_n$ est symétrique par rapport à la première bissectrice et symétrique par rapport au point O. De plus, si n est divisible par 4, $\mathcal{O}_n$ est symétrique par rapport aux axes de coordonnées. Si n est impair, $\mathcal{O}_{2n}$ s'obtient à partir de $\mathcal{O}_n$ par symétrie par rapport à un des axes de coordonnées.

Pour $n = 4$, $\mathcal{O}_4$ est le disque $x^2 + y^2 \le 1$ et

$$A_{\Phi_4} = \int_{-\infty}^{+\infty} \frac{\mathrm{d}t}{1+t^2} = \pi.$$

Quand p est un nombre premier impair on a

$$A_{\Phi_p} = \int_{-\infty}^{+\infty} \frac{\mathrm{d}t}{(1+t+t^2+\cdots+t^{p-1})^{(p-1)/2}}\cdot$$

Par exemple $\mathcal{O}_3$ est l'intérieur de l'ellipse $x^2+xy+y^2=1$ et

$$A_{\Phi_3} = \int_{-\infty}^{+\infty} \frac{\mathrm{d}t}{1+t+t^2} = \frac{2\pi}{\sqrt{3}}\cdot$$

6.3. Démontration du théorème 1.5. — La démonstration du théorème 1.5 repose sur des estimations de $\Phi_n(t)$: majorations et minorations. L'estimation de $\mathrm{m}(\phi_n)$ donnée dans [**FLW**] ne suffit pas pour démontrer le théorème 1.5.

Montrer que $\mathcal{O}_n$ contient le petit carré revient à démontrer, pour n suffisamment grand,

$$\Phi_n(x,y) < 1 \quad \text{quand} \quad \max\{|x|,|y|\} < 1 - n^{-1+\varepsilon}, \tag{6.1}$$

alors que montrer que $\mathcal{O}_n$ est contenu dans le grand carré revient à démontrer, pour n suffisamment grand,

$$\Phi_n(x,y) > 1 \quad \text{quand} \quad \max\{|x|,|y|\} > 1 + n^{-1+\varepsilon}. \tag{6.2}$$

Les relations $\Phi_n(x,y) = \Phi_n(y,x) = \Phi_n(-x,-y)$ (pour $n \geq 3$) permettent de se limiter au domaine $|y| \leq x$.

Si $P \in \mathbb{R}[X]$ est un polynôme de degré d, on a

$$|P(t)| \leq \mathrm{L}(P)\max\{1,|t|\}^d$$

pour tout $t \in \mathbb{R}$. En particulier

$$\phi_n(t) \leq \mathrm{L}(\phi_n)\max\{1,|t|\}^{\varphi(n)}$$

pour tout $t \in \mathbb{R}$.

De (4.5) on déduit, pour tout $\varepsilon > 0$, pour n suffisamment grand et pour tout $t \in \mathbb{R}$, l'inégalité

$$\phi_n(t) \leq e^{n^\varepsilon}\max\{1,|t|\}^{\varphi(n)}. \tag{6.3}$$

Montrons que cela implique (6.1). Soit n suffisamment grand et soit (x,y) satisfaisant

$$0 < |y| \leq x < 1 - n^{-1+\varepsilon}.$$

Posons $t = x/y$. On a $|t| \geq 1$ et, en utilisant (6.3) avec $\varepsilon/3$,

$$\Phi_n(x,y) = y^{\varphi(n)}\phi_n(t) \leq y^{\varphi(n)}e^{n^{\varepsilon/3}}t^{\varphi(n)} = x^{\varphi(n)}e^{n^{\varepsilon/3}} < \bigl(1-n^{-1+\varepsilon}\bigr)^{\varphi(n)}e^{n^{\varepsilon/3}}.$$

Pour n suffisamment grand on a

$$\varphi(n) > n^{1-\varepsilon/3}, \qquad \log x \leq \log\bigl(1-n^{-1+\varepsilon}\bigr) < -n^{-1+\varepsilon},$$

d'où

$$\varphi(n)\log x < -n^{2\varepsilon/3},$$

c'est-à-dire

$$x^{\varphi(n)} < e^{-n^{2\varepsilon/3}}.$$

Ceci complète la démonstration de (6.1).

Pour démontrer (6.2), on doit minorer $\phi_n(t)$. Nous utiliserons les estimations données par les deux lemmes suivants; la première nous sera utile quand $|t|-1$ n'est pas trop petit, la suivante quand $|t|-1$ est positif et petit.

Lemme 6.1. — *Pour tout $t \in \mathbb{R}$ et pour tout $n \geq 3$, on a*

$$\phi_n(t) \geq |t|^{\varphi(n)-1}(|t|-1) \prod_{\substack{d|n \\ d \neq n}} \mathrm{L}(\phi_d)^{-1}.$$

Démonstration. — Le résultat est trivial si $|t| \leq 1$. Pour commencer prenons $t > 1$. De

$$t^n - 1 = \phi_n(t) \prod_{\substack{d|n \\ d \neq n}} \phi_d(t) \tag{6.4}$$

on déduit

$$t^n - 1 \leq \phi_n(t) \prod_{\substack{d|n \\ d \neq n}} (\mathrm{L}(\phi_d) t^{\varphi(d)}) = \phi_n(t) t^{n-\varphi(n)} \prod_{\substack{d|n \\ d \neq n}} \mathrm{L}(\phi_d). \tag{6.5}$$

On minore $t^n - 1$ par $(t-1)t^{n-1}$. Par conséquent,

$$t^{\varphi(n)-1}(t-1) \leq \phi_n(t) \prod_{\substack{d|n \\ d \neq n}} \mathrm{L}(\phi_d),$$

ce qui est la conclusion du lemme 6.1 pour $t > 1$.

Supposons $t < -1$ et n pair. Dans ce cas, $t^n - 1 = |t|^n - 1$; dans le produit (6.4) il y a deux facteurs négatifs, à savoir $\phi_1(t) = t - 1$ et $\phi_2(t) = t + 1$, et on remplace (6.5) par

$$|t|^n - 1 \leq \phi_n(t) |t|^{n-\varphi(n)} \prod_{\substack{d|n \\ d \neq n}} \mathrm{L}(\phi_d).$$

On conclut avec

$$|t|^n - 1 \geq (|t|-1)|t|^{n-1}.$$

Enfin pour $t < -1$ et n impair, le membre de gauche de (6.4) est $-|t|^n - 1$, et dans le membre de droite le seul facteur négatif est celui correspondant à $d = 1$, à savoir $\phi_1(t) = -|t| - 1$. Ainsi

$$|t|^n + 1 = \phi_n(t) \prod_{\substack{d|n \\ d \neq n}} |\phi_d(t)| \leq \phi_n(t) |t|^{n-\varphi(n)} \prod_{\substack{d|n \\ d \neq n}} \mathrm{L}(\phi_d).$$

Comme $|t|^n + 1$ est minoré par $|t|^n$ on a une estimation plus précise que celle du lemme 6.1, à savoir

$$|t|^{\varphi(n)} \leq \phi_n(t) \prod_{\substack{d|n \\ d \neq n}} \mathrm{L}(\phi_d).$$

□

Lemme 6.2. — *Pour tout $t \in \mathbb{R}$ et pour tout $n \geq 1$, on a*

$$|\phi_n(t) - \phi_n(1)| \leq |t-1| \max\{1, |t|\}^{\varphi(n)-1} \varphi(n) \mathrm{L}(\phi_n)$$

et

$$|\phi_n(t) - \phi_n(-1)| \leq |t+1| \max\{1, |t|\}^{\varphi(n)-1} \varphi(n) \mathrm{L}(\phi_n).$$

Démonstration. — On pourrait faire intervenir la dérivée de ϕ_n dont la longueur est majorée par $\varphi(n)\mathrm{L}(\phi_n)$, mais on peut aussi faire un calcul direct comme ceci. Écrivons

$$\phi_n(t)=\sum_{j=0}^{\varphi(n)} a_j t^j.$$

Alors $a_0+a_1+\cdots+a_{\varphi(n)}=\phi_n(1)$, $|a_0|+|a_1|+\cdots+|a_{\varphi(n)}|=\mathrm{L}(\phi_n)$ et

$$\phi_n(t)-\phi_n(1)=\sum_{j=1}^{\varphi(n)} a_j(t^j-1).$$

On écrit

$$\frac{t^j-1}{t-1}=\sum_{i=0}^{j-1} t^i$$

et

$$\frac{|t^j-1|}{|t-1|}\le j\max\{1,|t|\}^{j-1}\le \varphi(n)\max\{1,|t|\}^{\varphi(n)-1},$$

ce qui donne

$$|\phi_n(t)-\phi_n(1)|\le |t-1|\max\{1,|t|\}^{\varphi(n)-1}\varphi(n)\sum_{j=1}^{\varphi(n)}|a_j|.$$

La même démonstration donne

$$|\phi_n(t)-\phi_n(-1)|\le |t+1|\max\{1,|t|\}^{\varphi(n)-1}\varphi(n)\sum_{j=1}^{\varphi(n)}|a_j|.$$

□

Démonstration de (6.2). — Soit n un entier suffisamment grand et soit $(x,y)\in\mathbb{R}^2$ vérifiant $0<|y|<x$ et

$$x>1+n^{-1+\varepsilon}.$$

On a

$$\log x>\frac{1}{2}n^{-1+\varepsilon}\qquad\text{et}\qquad \varphi(n)\log x>n^{2\varepsilon/3}.$$

On pose $t=x/y$, de sorte que $|t|>1$. On écrit

$$\Phi_n(x,y)=y^{\varphi(n)}\phi_n(t)$$

et on minore $\phi_n(t)$ en considérant deux cas.

• *Premier cas.* Supposons

$$|t|>1+e^{-n^{\varepsilon/2}}.$$

Cette minoration implique

$$\frac{|t|-1}{|t|}>\frac{1}{2}e^{-n^{\varepsilon/2}}.$$

On utilise les lemmes 6.1 et (4.5), où ε est remplacé par $\varepsilon/2$, pour obtenir

$$\phi_n(t)\ge |t|^{\varphi(n)-1}(|t|-1)e^{-n^{\varepsilon/2}}\ge\frac{1}{2}t^{\varphi(n)}e^{-2n^{\varepsilon/2}},$$

d'où

$$\Phi_n(x,y)\ge\frac{1}{2}x^{\varphi(n)}e^{-2n^{\varepsilon/2}}.$$

On a
$$\varphi(n)\log x > n^{2\varepsilon/3} > 2n^{\varepsilon/2} + \log 2,$$
ce qui donne $\Phi_n(x,y) > 1$ pour n suffisamment grand.

• *Deuxième cas.* Supposons maintenant
$$1 < |t| \leq 1 + e^{-n^{\varepsilon/2}}.$$
On a
$$\frac{|t|-1}{|t|} \leq |t| - 1 \leq e^{-n^{\varepsilon/2}} \text{ et } \log(|t|-1) - \log|t| \leq -n^{\varepsilon/2}.$$
On utilise les majorations
$$\varphi(n)\log|t| < n(|t|-1) \leq ne^{-n^{\varepsilon/2}}$$
et
$$\log(|t|-1) + (\varphi(n)-1)\log|t| + n^{\varepsilon/3} + \log 2 \leq -n^{\varepsilon/2} + ne^{-n^{\varepsilon/2}} + n^{\varepsilon/3} + \log 2 < 0$$
pour n suffisamment grand. Les lemmes 6.2 et (4.5), où ε est remplacé par $\varepsilon/3$, donnent
$$|\phi_n(t) - \phi_n(1)| < \frac{1}{2} \text{ si } \; t > 1, \quad |\phi_n(t) - \phi_n(-1)| < \frac{1}{2} \text{ si } \; t < -1,$$
ce qui implique $\phi_n(t) > 1/2$. Alors
$$\Phi_n(x,y) > \frac{1}{2}y^{\varphi(n)}$$
avec $|y| = x/|t|$. On a
$$\varphi(n)\log|y| = \varphi(n)\log x - \varphi(n)\log|t|,$$
$$\log|t| \leq e^{-n^{\varepsilon/2}}, \quad \varphi(n)\log|t| \leq ne^{-n^{\varepsilon/2}},$$
d'où
$$\varphi(n)\log x - \varphi(n)\log|t| \geq n^{2\varepsilon/3} - ne^{-n^{\varepsilon/2}} > \log 2$$
pour n suffisamment grand, ce qui implique $\Phi_n(x,y) > 1$. □

La preuve du théorème 1.5 est complète.

7. Preuve du théorème 1.6

On se place sous les hypothèses de ce théorème. Soit $d \geq 4$ un totient tel que $d+2$ soit aussi un totient. Soit $n_1 < n_2 < \cdots < n_t$ la liste des entiers tels que
$$n_i \not\equiv 2 \bmod 4 \text{ et } \varphi(n_i) = d,$$
et un entier m tel que $\varphi(m) = d+2$. On part de la minoration
$$\mathcal{A}_d(N) \geq \Big|\mathcal{B}_{n_1}(N) \cup \cdots \cup \mathcal{B}_{n_t}(N) \cup \mathcal{B}_m(N)\Big|$$
où on utilise la notation (5.1). Par le principe d'inclusion–exclusion on a la minoration

$$\mathcal{A}_d(N) \geq \Big|\mathcal{B}_{n_1}(N) \cup \cdots \cup \mathcal{B}_{n_t}(N)\Big| + \Big|\mathcal{C}_{\boldsymbol{n},m}(N)\Big|, \tag{7.1}$$

où $\mathcal{C}_{\boldsymbol{n},m}(N)$ est l'ensemble complémentaire
$$\mathcal{C}_{\boldsymbol{n},m}(N) := \big\{u \in \mathbb{Z} \;\mid\; u \in \mathcal{B}_m(N) \text{ et } u \notin B_{n_1}(N) \cup \cdots \cup \mathcal{B}_{n_t}(N)\big\}.$$

Le premier terme à droite de la minoration (7.1) est minoré en combinant (5.4) et (5.5):

$$\left|\mathcal{B}_{n_1}(N) \cup \cdots \cup \mathcal{B}_{n_t}(N)\right| \geq C_d N^{\frac{2}{d}} - O(N^{\eta_d+\varepsilon}).$$

Pour minorer le cardinal de $\mathcal{C}_{\boldsymbol{n},m}(N)$, nous commençons par exhiber un ensemble de couples d'entiers (a,b) de densité positive dont l'image par Φ_m appartient à $\mathcal{C}_{\boldsymbol{n},m}(\infty)$. On a

Lemme 7.1. — *Soit d, t, n_1, …, n_t et m des entiers comme ci–dessus. Il existe alors un entier D et des classes de congruence a_0 et b_0 mod D tels que*

$$a \equiv a_0 \text{ et } b \equiv b_0 \bmod D \Rightarrow \Phi_m(a,b) \notin \Big(\mathcal{B}_{n_1}(\infty) \cup \cdots \cup \mathcal{B}_{n_t}(\infty)\Big).$$

Démonstration du lemme 7.1. — À chaque entier n_i on associe l'entier $\varpi(n_i)$ défini comme suit:

- si n_i n'est pas de la forme 2^h3^k, alors $\varpi(n_i)$ est le plus petit diviseur premier ≥ 5 de n_i,
- si n_i est de la forme 2^h3^k avec $h \geq 2$, alors $\varpi(n_i) = 4$,
- si n_i est de la forme 3^k avec $k \geq 2$, alors $\varpi(n_i) = 9$.

On pose alors

$$D := \operatorname{ppcm}\{\varpi(n_i)\}.$$

Pour définir a_0 et b_0 mod D, nous allons fixer leurs classes de congruence modulo chacun des $\varpi(n_i)$, avant d'appliquer le théorème chinois pour remonter en des classes modulo D :

- Si $\varpi(n_i)$ est un nombre premier ≥ 5, alors $\varpi(n_i)$ divise n_i et $\varphi(\varpi(n_i)) = \varpi(n_i) - 1$ divise d. On a alors pour $a \equiv 0 \bmod \varpi(n_i)$ et $b \equiv 2 \bmod \varpi(n_i)$ les congruences

$$\Phi_m(a,b) \equiv b^{d+2} \equiv 4 \neq 0,\ 1 \bmod \varpi(n_i);$$

donc $\Phi_m(a,b)$ n'appartient pas à l'image de Φ_{n_i} d'après la proposition 4.2. On fixe $a_0 \equiv 0$ et $b_0 \equiv 2 \bmod \varpi(n_i)$.

- Si $\varpi(n_i) = 4$, c'est que n_i est de la forme 2^h3^k avec $h \geq 2$. On remarque que d est divisible par 4 (rappelons que $\varphi(n_i) = d \geq 4$). Dans ce cas $d+2$ est congru à 2 modulo 4. Les seuls m tels que $\varphi(m) = d+2$ et $m \not\equiv 2 \bmod 4$ sont de la forme $m = p^s$ avec $p \equiv 3 \bmod 4$ et $s \geq 1$. Par la formule (4.3), on a pour a et b congru à 1 modulo 4, $\Phi_m(a,b) \equiv \phi_m(1) \equiv p \equiv 3 \bmod 4$, et $\Phi_m(a,b)$ n'est pas dans l'image de Φ_{n_i}, d'après la proposition 4.5. On fixe donc $a_0 \equiv b_0 \equiv 1 \bmod 4$.

- Si $\varpi(n_i) = 9$, alors n_i est de la forme 3^k avec $k \geq 2$. Par conséquent, $6 \mid \varphi(n_i) = d$. Soit m tel que $\varphi(m) = d+2$. Alors $\Phi_m(0,b) = b^{d+2}$. Donc si $3 \nmid b$, on a $\Phi_m(0,b) \equiv b^2 \bmod 9$. Si on impose $a \equiv 0 \bmod 9$ et $b \equiv 2 \bmod 9$, on voit que $\Phi_m(a,b) \equiv 4 \bmod 9$. Ce n'est pas une valeur prise par Φ_{3^k}, par la proposition 4.4. On fixe donc $a_0 \equiv 0 \bmod 9$ et $b_0 \equiv 2 \bmod 9$.

Le lemme 7.1 en résulte. □

Soient $M \geq 2$ et $\mathcal{E}(M)$ l'ensemble des couples d'entiers (a,b) tels que $|a|$, $|b| \leq M$ et $a \equiv a_0$ et $b \equiv b_0 \bmod D$, avec les notations du lemme 7.1. Il existe $c_0 > 0$ tel que

$$\Phi_m(\mathcal{E}(c_0 N^{\frac{1}{d+2}})) \subset \mathcal{C}_{\boldsymbol{n},m}(N). \tag{7.2}$$

Notons $\tilde\rho(n)$ le nombre de solutions de l'équation $n = \Phi_m(a,b)$ avec $(a,b) \in \mathcal{E}(c_0 N^{\frac{1}{d+2}})$. On a donc l'égalité

$$\sum_n \tilde\rho(n) = |\mathcal{E}(c_0 N^{\frac{1}{d+2}})| \sim (4c_0^2/D^2) N^{\frac{2}{d+2}}. \tag{7.3}$$

Pour appliquer l'inégalité de Cauchy–Schwarz, on écrit la partie gauche de l'équation (7.3) comme

$$\sum_n \tilde\rho(n) = \sum_{\tilde\rho(n)\geq 1} 1\cdot\tilde\rho(n) \leq |\Phi_m(\mathcal{E}(c_0 N^{\frac{1}{d+2}}))|^{\frac12}\cdot\Big(\sum_n \rho^2(n)\Big)^{\frac12}, \tag{7.4}$$

où $\rho(n)$ est le nombre de solutions à l'équation $n = \Phi_m(a,b)$ avec $|a|$, $|b| \leq c_0 N^{\frac{1}{d+2}}$. Développant le carré, on voit que $\sum \rho^2(n)$ est le nombre de points entiers de hauteur $\ll N^{\frac{1}{d+2}}$ sur la surface de $\mathbb{P}^3(\mathbb{C})$ définie par

$$\Phi_m(X_1,X_2) - \Phi_m(X_3,X_4) = 0.$$

Cette surface est lisse de degré ≥ 3. Elle contient donc $O(1)$ droites. Sur chacune de ces droites il y a $O(N^{\frac{2}{d+2}})$ points de hauteur $\ll N^{\frac{1}{d+2}}$. Pour compter les points entiers non situés sur ces droites, on suit la même démonstration que pour la proposition 3.4 (voir aussi [**SX**, Lemma 2.4]). Le nombre de ces points entiers est en $O(N^\vartheta)$ pour un certain $\vartheta < 2/(d+2)$. Regroupant les deux contributions, on a donc la majoration

$$\sum_n \rho^2(n) \ll N^{\frac{2}{d+2}}.$$

Combinant (7.3) et (7.4) on obtient la minoration

$$|\Phi_m(\mathcal{E}(c_0 N^{\frac{1}{d+2}}))| \gg N^{\frac{2}{d+2}}.$$

Retournant à (7.2) puis à (7.1) on complète la preuve du théorème 1.6.

Références

[Ba] Bateman, P.T., *Note on the coefficients of the cyclotomic polynomials*, Bull. Amer. Math. Soc., (**55**) (1949), 1180–1181.

[Be] Bean, M. A., *The practical computation of areas associated with binary quartic forms*, Math. of Computation, (**66**) 219 (1997), 1269–1293.

[BS] Boissière, S. & Sarti, A., *Counting lines on surfaces,* Ann. Sc. Norm. Super. Pisa Cl. Sci. (5) (**6**) (2007), no. 1, 39–52.

[Fo1] Ford, K, *The distribution of totients. Paul Erdös (1913–1996),* Ramanujan J. (**2**) (1998), no. 1–2, 67–151.

[Fo2] Ford, K, *The number of solutions of $\phi(x) = m$,* Ann. of Math. (2) (**150**) (1999), no. 1, 283–311.

[FLW] Fouvry, É., Levesque, C. & Waldschmidt, M., *Representation of integers by cyclotomic binary forms*, Acta Arith., (**184**) (2018), no. 1, 67–86. `http://arxiv.org/abs/1701.01230`

[Sa] Salberger, P., *Rational points of bounded height on projective surfaces*, Math. Z. (**258**) (2008), no. 4, 805–826.

[Se] Segre, B., *The maximum number of lines lying on a quartic surface*, Quart. J. Math., Oxford Ser. (**14**) (1943), 86–96.

[SX] Stewart, C.L. & Xiao, S.Y., *On the representation of integers by binary forms*, Math. Annalen (to appear), `http://arxiv.org/abs/1605.03427`, v2 March 2018.

Étienne Fouvry, Institut de Mathématique d'Orsay, Université Paris–Sud, CNRS, Université Paris–Saclay, F–91405 ORSAY, France, E-mail: `etienne.fouvry@u-psud.fr`

Michel Waldschmidt, Sorbonne Université, Institut Mathématique de Jussieu IMJ-PRG, F–75005 Paris, France, E-mail: `michel.waldschmidt@imj-prg.fr`