Bulletin
de la SOCIÉTÉ MATHÉMATIQUE DE FRANCE

# SUR LA REPRÉSENTATION DES ENTIERS PAR LES FORMES CYCLOTOMIQUES DE GRAND DEGRÉ

Étienne Fouvry & Michel Waldschmidt

Tome 148
Fascicule 2

2020

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

pages 253-282

Le *Bulletin de la Société Mathématique de France* est un périodique trimestriel de la Société Mathématique de France.

Fascicule 2, tome 148, juin 2020



***Diffusion***

Maison de la SMF
Case 916 - Luminy
13288 Marseille Cedex 9
France
commandes@smf.emath.fr

AMS
P.O. Box 6248
Providence RI 02940
USA
www.ams.org

***Tarifs***

*Vente au numéro :* 43 € ($ 64)
*Abonnement électronique* : 135 € ($ 202),
*avec supplément papier* : Europe 179 €, hors Europe 197 € ($ 296)
Des conditions spéciales sont accordées aux membres de la SMF.

***Secrétariat : Bulletin de la SMF***

*Bulletin de la Société Mathématique de France*
Société Mathématique de France
Institut Henri Poincaré, 11, rue Pierre et Marie Curie
75231 Paris Cedex 05, France
Tél : (33) 1 44 27 67 99 • Fax : (33) 1 40 46 90 96
bulletin@smf.emath.fr • smf.emath.fr



ISSN 0037-9484 (print) 2102-622X (electronic)

Directeur de la publication : Stéphane SEURET

*Bull. Soc. Math. France*
**148** (2), 2020, p. 253-282

# SUR LA REPRÉSENTATION DES ENTIERS PAR LES FORMES CYCLOTOMIQUES DE GRAND DEGRÉ

par Étienne Fouvry & Michel Waldschmidt

Résumé. — 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 avec C. Levesque (« Representation of integers by cyclotomic binary forms », *Acta Arith.* **184** (2018), no. 1, p. 67–86, `http://arxiv.org/abs/1701.01230`). Notre démonstration repose sur une variante d'un énoncé de C.L. Stewart and S.Y. Xiao (« On the representation of integers by binary forms », *Math. Ann.* **375** (2019), p. 133–163, `http://arxiv.org/abs/1605.03427`) concernant les valeurs communes prises par deux formes binaires de même degré et de discriminants non nuls. Toutes les constantes sont effectivement calculables.

Abstract (*On the representation of integers by cyclotomic forms with large degree*). — For each integer $d \geq 4$, we study the sequence of positive integers which are represented by one at least of the cyclotomic binary forms $\Phi_n(X, Y)$, with $n$ a positive integer satisfying $\varphi(n) \geq d$. The case $d = 2$ was studied in our previous work with C. Levesque ("Representation of integers by cyclotomic binary forms", *Acta Arith.* **184** (2018), no. 1, p. 67–86, `http://arxiv.org/abs/1701.01230`). Our proof is based on a variant of a statement of C.L. Stewart and S.Y. Xiao ("On the representation of integers by binary forms", *Math. Ann.* **375** (2019), p. 133–163, `http://arxiv.org/abs/1605.03427`) concerning the common values taken by two binary forms of the same degree and non-zero discriminants. All constants are effectively computable.

*Texte reçu le 8 mai 2019, modifié le 4 septembre 2019, accepté le 9 septembre 2019.*

Étienne Fouvry, Université Paris–Saclay, CNRS, Laboratoire de Mathématiques d'Orsay, F–91405 Orsay, France • *E-mail :* `etienne.fouvry@universite-paris-saclay.fr`
Michel Waldschmidt, Sorbonne Université, Institut Mathématique de Jussieu IMJ-PRG, F-75005 Paris, France • *E-mail :* `michel.waldschmidt@imj-prg.fr`

Classification mathématique par sujets (2020). — 11E76.

Mots clefs. — Formes cyclotomiques.



0037-9484/2020/253/$ 5.00
doi:10.24033/bsmf.2805

## 1. Introduction

Rappelons ([6]) que la suite $(\Phi_n(X,Y))_{n\geq 1}$ 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 $\varphi(n)$ ($\varphi$ 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

$$\begin{cases} \varphi(n) \geq d, \\ \Phi_n(x,y) = m, \\ \max(|x|,|y|) \geq 2. \end{cases} \tag{1}$$

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) 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 (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), la condition de congruence

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

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

Appelons *totient* toute valeur prise par la fonction $\varphi$. 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 [4] et [5] 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 [6, Théorème 1.3] où il est prouvé qu'il existe deux constantes $C_2 = 1,403132\ldots$ et $C_2' = 0,302316\ldots$ telles que, uniformément pour $N \geq 2$, on a l'égalité

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

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 $\chi$ est le caractère de Kronecker attaché aux corps quadratiques de discriminants $-4$, $-3$ et $12$.

Pour un totient $d \geq 4$, les outils de [6] conduisent à la majoration

$$\mathcal{A}_d(N) = O\big(N^{\frac{2}{d}} (\log N)^{1,161}\big), \tag{4}$$

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

Par rapport à [6], le présent travail innove en injectant résultats et méthodes de [9] que nous décrirons au §2. Contentons–nous pour l'instant de donner notre résultat principal qui améliore notablement (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 $\geq 3$, on pose

$$\eta_d = \begin{cases} 2/9 + 73/(108\sqrt{3}) & \text{si } d = 3, \\ (1/2 + 9/(4\sqrt{d}))/d & \text{si } 4 \leq d \leq 20, \\ 1/d & \text{pour } d \geq 21. \end{cases} \tag{5}$$

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*

$$\mathcal{A}_d(N) = C_d N^{\frac{2}{d}} + O(N^{\frac{2}{d^\dagger}}) + O_\varepsilon(N^{\eta_d + \varepsilon}). \tag{6}$$

REMARQUE 1.2. — La formule (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 (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 (3) correspond donc au cas $d = 2$. Mais, par la présence au dénominateur du facteur $(\log N)^{\frac{1}{2}}$, elle diffère notablement de (6). Cette différence s'explique comme suit. Il y a

trois formes cyclotomiques de degré 2. Ce sont les trois formes quadratiques binaires

$$\Phi_3(X,Y)=X^2+XY+Y^2,\quad \Phi_4(X,Y)=X^2+Y^2,\quad \text{et} \tag{7}$$
$$\Phi_6(X,Y)=X^2-XY+Y^2.$$

Puisque $\Phi_6(X,-Y)=\Phi_3(X,Y)$ les formes $\Phi_6$ et $\Phi_3$ représentent les mêmes entiers. Mais les formes $\Phi_3$ et $\Phi_4$ 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 $2\times 2$ à coefficients dans $\mathbb{Q}$).

L'objet des théorèmes 1.4 et 1.6 est de compléter la formule (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* (6) *vérifie l'égalité*

$$C_d=\sum_{\substack{n\not\equiv 2 \bmod 4\\ \varphi(n)=d}} w_n\, A_{\Phi_n} \tag{8}$$

*où*

$$w_n:=\begin{cases}\frac{1}{4} & \text{si } 4\nmid n,\\ \frac{1}{8} & \text{si } 4\mid n,\end{cases} \tag{9}$$

*et*

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

Voici deux exemples dans lesquels la formule (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 $\ell$ est l'unique entier $\not\equiv 2 \bmod 4$ tel que $\varphi(\ell)=2p$ et on a l'égalité
$$C_{2p}=\frac{1}{4}A_{\Phi_\ell}.$$
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

$$C_d = \begin{cases} \dfrac{1}{8} A_{\Phi_{2d}} + \dfrac{1}{8} \displaystyle\sum_{\substack{m \in \mathcal{M} \\ m<k}} A_{\Phi_{\ell_k(m)}} & \text{si } k \notin \mathcal{M}, \\ \dfrac{1}{8} A_{\Phi_{2d}} + \dfrac{1}{8} \displaystyle\sum_{\substack{m \in \mathcal{M} \\ m<k}} A_{\Phi_{\ell_k(m)}} + \dfrac{1}{4} A_{\Phi_{\ell_k(k)}} & \text{si } k \in \mathcal{M}, \end{cases}$$

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 [9, 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

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

THÉORÈME 1.5. — *Soit $\varepsilon > 0$. Il existe $n_0 = n_0(\varepsilon)$ tel que, pour $n \geq n_0$, 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 (6)

THÉORÈME 1.6. — *On adopte les notations du théorème 1.1. Soit $d \geq 4$ 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*

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

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 $\nu$ est un entier pair fixé. Cette extension nécessiterait une adaptation des propriétés de confinement décrites aux §4.1, §4.2 et §4.3.