L'Enseignement Mathématique, t. 45 (1999), p. 301–309

UNE MAJORATION DE LA LONGUEUR DES POLYNÔMES CYCLOTOMIQUES

par Jean-Louis NICOLAS et Guy TERJANIAN[1])

ABSTRACT. Let us denote by $\beta(m)$ the length of Φ_m, the m-th cyclotomic nomial, i.e. the sum of the absolute values of its coefficients. We shall prove that $m \geq 7$ and $m \neq 10$ the following inequality holds: $\beta(m) \leq (\sqrt{2})^{\varphi(m)}$, where φ e Euler function.
Further, define $P_m(X) = \Phi_m(X) - (X-1)^{\varphi(m)}$ for $m \geq 2$. We shall deduce from above inequality that if this polynomial vanishes at some root of unity, then this of unity is of order 6.

1. INTRODUCTION

Nous noterons φ la fonction d'Euler, μ la fonction de Möbius et Φ_m le ème polynôme cyclotomique. On sait que ce polynôme vérifie

$$\Phi_m(X) = \prod_{d|m} (1 - X^{m/d})^{\mu(d)} .$$

s définissons les coefficients de Φ_m par

$$\Phi_m(X) = a_{m,0} + a_{m,1}X + \cdots + a_{m,\varphi(m)}X^{\varphi(m)} ,$$

ous posons

$$\beta(m) = |a_{m,0}| + |a_{m,1}| + \cdots + |a_{m,\varphi(m)}| .$$

man a donné dans [1] une démonstration très élégante de la majoration

$$\beta(m) \leq m^{\frac{1}{2}d(m)}$$

Recherche partiellement financée par le CNRS, Institut Girard Desargues, UPRES-A 5028 boratoire Émile Picard, UMR 5580.

où $d(m)$ désigne le nombre de diviseurs de m. Il a été démontré par différents auteurs (cf. [2] qui contient un bon historique du sujet) que $\beta(m)$ peut être très grand pour certaines valeurs de m. Cependant, pour les petites valeurs de m, ce phénomène n'apparaît pas. Par exemple, le plus petit m pour lequel

$$\beta(m) > 1 + \varphi(m)$$

est, d'après les calculs d'ordinateurs $m = 1365 = 3 \cdot 5 \cdot 7 \cdot 13$.

Nous nous proposons de démontrer le résultat suivant:

THÉORÈME 1. *Pour $m \geq 7$ et $m \neq 10$, on a*

$$\beta(m) < (\sqrt{2})^{\varphi(m)}. \tag{4}$$

A partir de la majoration de Wigert (cf. [4], chap. 18)

$$\log d(m) \leq (1 + o(1)) \frac{\log 2 \log m}{\log \log m}, \qquad m \to \infty \tag{5}$$

et de la minoration de $\varphi(m)$ (cf. [4], chap. 18)

$$\varphi(m) \geq (1 + o(1)) e^{-\gamma} \frac{m}{\log \log m}, \qquad m \to \infty \tag{6}$$

où γ désigne la constante d'Euler, il est facile de déduire de (3) que la relation (4) est vérifiée pour $m \geq m_0$. Le calcul de m_0 peut se faire en remplaçant (5) et (6) par les inégalités (cf. [8] et [10])

$$\log d(m) \leq 1{,}538 \frac{\log 2 \log m}{\log \log m}, \qquad m \geq 3 \tag{7}$$

$$\varphi(m) \geq \frac{m}{e^{\gamma} \log \log m + 2{,}51 / \log \log m}, \qquad m \geq 3. \tag{8}$$

L'étude (un peu technique) de la fonction de t

$$\frac{t(\log 2)/2}{e^{\gamma} \log \log t + 2{,}51/\log \log t} - \frac{\log t}{2} \exp\left(1{,}538 \frac{\log 2 \log t}{\log \log t}\right)$$

montre qu'elle est positive pour $t \geq 3786$, ce qui prouve le théorème 1 pour $m \geq m_0 = 3786$; il reste à vérifier (4) avec un ordinateur pour $m < m_0$. La démonstration du théorème 1 que nous donnerons est un peu plus longue, mais elle évite au maximum de faire des calculs sur ordinateur.

Soit $\omega(m)$ le nombre de facteurs premiers distincts de m et $\omega'(m)$ le nombre de facteurs premiers impairs distincts de m. Naturellement, on a

$$\omega'(m) \leq \omega(m) \leq \omega'(m) + 1. \tag{9}$$

D'abord, nous utiliserons au lieu de (3) l'amélioration donnée dans [2]

$$\beta(m) \leq m^{2^{k-1}/k}, \qquad k = \omega'(m) \geq 1. \tag{10}$$

Ensuite, pour minorer $\varphi(m)$, nous remplaçons (8) par la minoration très simple

$$\varphi(m) \geq \frac{m}{\omega(m) + 1} \geq \frac{m}{\omega'(m) + 2}, \qquad m \geq 1. \tag{11}$$

Pour démontrer (11), on écrit $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, $2 \leq p_1 < p_2 < \dots < p_r$, $r = \omega(m)$. On a $p_i \geq i + 1$, $i = 1, 2, \dots, r$ et il s'ensuit que

$$\frac{\varphi(m)}{m} = \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) \geq \prod_{i=1}^{r} \left(1 - \frac{1}{i+1}\right) = \frac{1}{r+1}$$

qui, avec (9), prouve (11). Enfin, nous remplacerons (7) par la majoration de $\omega'(m)$ donnée par le lemme 1 ci-dessous. La démonstration du théorème 1 fera l'objet du paragraphe 2.

Considérons maintenant le polynôme

$$P_m(X) = \Phi_m(X) - (X - 1)^{\varphi(m)}. \tag{12}$$

Dans [11], G. Terjanian a étudié la factorisation du polynôme P_m sur le corps des rationnels. De façon plus précise, il a montré que l'on pouvait écrire

$$P_m(X) = \Phi_m(1) X (X^2 - X + 1)^{e(m)} E_m(X), \qquad m \geq 3 \tag{13}$$

où $E_m(X)$ est un polynôme qui est premier avec $X(X^2 - X + 1)$. La fonction $e(m)$ est assez compliquée:

- $e(m) = 0$ si $m = 3$ ou si $m = 2p^n$ pour p premier, $p \equiv 2 \bmod 3$ et $n \geq 0$ ou si $m = 6q^n$ pour q premier et $n \geq 0$.
- $e(m) = 2$ si $m = A$ ou $m = 2^k A$ où k est un entier impair, $k \geq 3$ et où A est un entier distinct de 1 dont tous les facteurs premiers sont congrus à 1 modulo 6.
- $e(m) = 1$ dans tous les autres cas.

Il est facile de voir que

$$\Phi_m(1) = 1 \quad \text{ou} \quad \Phi_m(1) = p \tag{14}$$

suivant que m a deux diviseurs premiers distincts ou qu'il est une puissance du nombre premier p.

Dans [5] (cf. aussi [3]), les polynômes

$$M_n(X) = (X+1)^n - X^n - 1 \tag{15}$$

sont appelés *polynômes de Cauchy-Mirimanoff*. Lorsque $n \geq 3$ est premier, on a $M_n(X) = -(X+1)P_n(-X)$. Cauchy a montré que

$$M_n(X) = X(X+1)^{a_n}(X^2+X+1)^{b_n}H_n(X) \tag{16}$$

avec $a_n = b_n = 0$ si n est pair, et, si n est impair, $a_n = 1$ et $b_n = 0, 2, 1$ suivant que $n \equiv 0, 1, 2 \bmod 3$. Il est conjecturé que $H_n(X)$ est irréductible pour tout $n \geq 2$. On sait que (cf. [5]), lorsque n est premier, $n \geq 9$, $H_n(X) = E_n(-X)$ est réductible modulo p pour tout p premier.

G. Terjanian conjecture que le polynôme E_m défini par (13) est irréductible sur les rationnels pour tout m. Cette conjecture a été vérifiée jusqu'à $m = 264$ (cf. [11], p. 93) et à l'aide du système de calcul formel *Maple*®, nous avons pu étendre les calculs jusqu'à $m = 1000$ par une méthode que nous expliquerons au paragraphe 3. En direction de cette conjecture, nous démontrerons comme conséquence du théorème 1

THÉORÈME 2. *Soit z une racine de l'unité telle que $P_m(z) = 0$, où le polynôme P_m est défini par (12) et $m \geq 2$. Alors, z est d'ordre 6, autrement dit, $z^2 - z + 1 = 0$.*

La démonstration du théorème 2 fera l'objet du paragraphe 3.

Une conjecture sans doute plus facile que celle de l'irréductibilité du polynôme E_m est la suivante: Est-ce-que toute racine multiple de P_m est une racine 6-ième de l'unité? Nous avons vu que $\exp(-\frac{2i\pi}{3})$ est racine double de P_m pour une infinité de valeurs de m, par exemple les nombres premiers m qui vérifient $m \equiv 1 \bmod 6$.

2. DÉMONSTRATION DU THÉORÈME 1

LEMME 1. *Soit $\omega'(n)$ le nombre de facteurs premiers impairs distincts de n, et ε un nombre réel positif. On pose*

$$n_0 = n_0(\varepsilon) = \prod_{3 \leq p \leq \exp(1/\varepsilon)} p .$$

Alors, pour tout $n \geq 1$, on a

$$\omega'(n) \leq \varepsilon \log(n) + (\omega'(n_0) - \varepsilon \log(n_0)) .$$

Cas particulier: $\varepsilon = 0,32/\log 2$. On a pour tout $n \geq 1$

$$\omega'(n) \leq \frac{0,32}{\log 2} \log n + 0,852 .$$

ou encore

$$2^{\omega'(n)} \leq 1,81 n^{0,32} .$$

Démonstration. Nous utiliserons implicitement la méthode des "nombres hautement composés supérieurs" introduite par Ramanujan (cf. [9], paragraphe 32).

Pour $\alpha \in \mathbf{N}$, on définit $f(\alpha) = 1$ si $\alpha \geq 1$ et $f(\alpha) = 0$ si $\alpha = 0$. La fonction ω' est additive; on a $\omega'(2^\alpha) = 0$ et $\omega'(p^\alpha) = f(\alpha) \leq \alpha$ pour tout $\alpha \in \mathbf{N}$, et p premier impair. Soit $\mathcal{P}$ l'ensemble des nombres premiers. On écrit

$$n = \prod_{p \in \mathcal{P}} p^{\alpha_p} , \quad \alpha_p \geq 0$$

et il s'ensuit que

$$\begin{aligned}
&\omega'(n) - \varepsilon \log(n) - (\omega'(n_0) - \varepsilon \log(n_0)) \\
&\quad = -\varepsilon \alpha_2 \log 2 + \sum_{3 \leq p \leq \exp(1/\varepsilon)} \big(f(\alpha_p) - \varepsilon \alpha_p \log p - (1 - \varepsilon \log p)\big) \\
&\qquad + \sum_{p > \exp(1/\varepsilon)} \big(f(\alpha_p) - \varepsilon \alpha_p \log p\big) \\
&\quad \leq \sum_{3 \leq p \leq \exp(1/\varepsilon)} (f(\alpha_p) - 1)(1 - \varepsilon \log p) + \sum_{p > \exp(1/\varepsilon)} f(\alpha_p)(1 - \varepsilon \log p) \leq 0 .
\end{aligned}$$

Pour $\varepsilon = 0,32/\log 2$, on a $\exp(1/\varepsilon) = 8,724\ldots$, $n_0 = 3 \cdot 5 \cdot 7 = 105$ et $\omega'(n_0) - \varepsilon \log(n_0) \leq 0,852$.

Rappelons d'abord les formules de calcul de Φ_m (cf. [6], 4.6.2, exercice 32):

(17) pour p premier, $\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1}$

(18) si p premier divise n, $\Phi_{pn}(X) = \Phi_n(X^p)$

(19) si p premier ne divise pas n, $\Phi_{pn}(X) = \dfrac{\Phi_n(X^p)}{\Phi_n(X)}$

(20) si n est impair, $\Phi_{2n}(X) = \dfrac{\Phi_n(X^2)}{\Phi_n(X)} = \Phi_n(-X)$.

Soit $n = \ker m$ le noyau impair de m : si $m = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, $3 \le p_1 < p_2 < \dots < p_k$, on a $n = p_1 p_2 \dots p_k$. Les formules (18) et (20) montrent que

$$\beta(m) = \beta(n). \tag{21}$$

Démontrons d'abord que le théorème 1 est vrai lorsque $k = \omega'(m) \le 2$.

- Si $k = 0$, $m = 2^\alpha$ et par (21), $\beta(m) = \beta(1) = 2$, tandis que $\varphi(m) = 2^{\alpha-1}$ et (4) est vérifié pour $\alpha \ge 3$. Les exceptions sont donc $m = 1, 2, 4$.

- Si $k = 1$, on a $m = 2^\alpha p_1^{\alpha_1}$, et par (21), et (17), $\beta(m) = \beta(n) = \beta(p_1) = p_1$ et $\varphi(m) \ge (p_1 - 1)$. L'inégalité

$$p_1 < (\sqrt{2})^{p_1 - 1}$$

est vérifiée pour $p_1 \ge 7$. Pour $p_1 = 3$ ou 5, on a

$$p_1 < (\sqrt{2})^{2(p_1-1)}$$

et cela démontre (4) pour $m = 2^\alpha p_1$, avec $\alpha \ge 2$ ou pour $m = 2^\alpha p_1^{\alpha_1}$, avec $p_1 = 3$ ou 5, $\alpha = 0$ ou 1, et $\alpha_1 \ge 2$. Les exceptions sont donc $m = 3, 5, 6, 10$.

- Si $k = 2$, on sait depuis Migotti (cf. [7]) que dans (2) les coefficients $a_{m,i}$ valent -1, 0 ou 1 et cela entraîne

$$\beta(m) \le 1 + \varphi(m). \tag{22}$$

Pour $t \ge 6$, on a $1 + t \le (\sqrt{2})^t$, et donc (22) implique (4) dès que $\varphi(m) \ge 6$. Or, lorsque $k = 2$, on a $\varphi(m) \ge (p_1 - 1)(p_2 - 1) \ge 2 \cdot 4 = 8$.

On peut maintenant supposer $k \ge 3$. Par (10), on a

$$\log \beta(m) \le \frac{2^{k-1}}{k} \log m$$

et par (11), on a

$$\varphi(m) \log(\sqrt{2}) \ge \frac{1}{2} \frac{m}{k+2} \log 2.$$

Pour prouver (4), il suffit donc d'assurer

$$\frac{2^{k-1}}{k} \log m < \frac{1}{2} \frac{m}{k+2} \log 2$$

ou encore

$$2^k \left(1 + \frac{2}{k}\right) < \log 2 \frac{m}{\log m}$$

et comme $k \ge 3$, et en appliquant le lemme 1,

$$1,81 m^{0,32} < \frac{3 \log 2}{5} \frac{m}{\log m}.$$

Finalement, comme $\frac{5 \times 1,81}{3 \log 2} < 4,36$, il suffit de montrer

$$m^{0,68} - 4,36 \log m > 0.$$

L'inégalité ci-dessus est vérifiée pour tout $m \ge 75$ et comme le plus petit nombre m avec $k = \omega'(m) \ge 3$ est $105 = 3 \cdot 5 \cdot 7$, (4) est démontrée pour tous les m avec $k = \omega'(m) \ge 3$, et cela termine la preuve du théorème 1.

3. Démonstration du théorème 2

D'abord, on a $P_m(1) = \Phi_m(1)$ et par (14), 1 n'est pas racine de P_m pour $m \ge 2$. De même, -1 n'est pas racine de P_m : lorsque m est impair, (1) donne

$$\Phi_m(-1) = \prod_{d|m} 2^{\mu(d)} = 2^{\sum_{d|m} \mu(d)} = 1$$

dès que $m \ge 3$. Les formules (18), (20) et (14) montrent que pour $m \ge 3$, $\Phi_m(-1)$ est impair, sauf pour $m = 2^n$ où l'on a $\Phi_m(-1) = 2$. On ne peut donc avoir $P_m(-1) = 0$.

Soit maintenant z une racine de l'unité différente de 1 et -1 et d'ordre $r \ne 6$ telle que $P_m(z) = 0$. Par conjugaison, les autres racines d'ordre r sont aussi racines de P_m. Soit k l'ordre de $-z$. (Si $r \equiv 0 \bmod 4$, on a $k = r$; si $r \equiv 2 \bmod 4$, on a $k = r/2$; si r est impair, on a $k = 2r$.) On a $P_m(-\exp(\frac{2i\pi}{k})) = 0$, et comme $\varphi(m)$ est pair, il vient

$$\Phi_m\left(-\exp\left(\frac{2i\pi}{k}\right)\right) = \left(\exp\left(\frac{2i\pi}{k}\right) + 1\right)^{\varphi(m)}.$$

D'où en prenant les modules,

$$\beta(m) \ge \left|\Phi_m\left(-\exp\left(\frac{2i\pi}{k}\right)\right)\right| \ge \left(2 \cos \frac{\pi}{k}\right)^{\varphi(m)}.$$

Comme $z^2 \ne 1$, on a $k \ne 1, 2$. On a $k \ne 3$, sinon, z serait d'ordre $r = 6$. Donc $k \ge 4$ et

$$\beta(m) \ge (\sqrt{2})^{\varphi(m)}.$$

Par le théorème 1, m doit être égal à $2, 3, 4, 5, 6$ ou 10. Le calcul direct des polynômes P_m pour ces valeurs montre qu'ils vérifient aussi le théorème et cela achève la démonstration du théorème 2.

La vérification de l'irréductibilité sur $\mathbf{Z}[X]$ du polynôme E_m défini par (13) se fait sans problème en utilisant la procédure *irreduc* de *Maple*® jusqu'à $m = 290$. Ensuite pour les valeurs de m qui sont des nombres premiers, il y a un manque de mémoire. Nous avons donc séparé le travail en deux. Pour les nombres m composés, la procédure *irreduc* marche jusqu'à 1000. Pour les nombres m premiers, nous factorisons E_m (qui est unitaire) sur $\mathbf{F}_p[X]$ pour des petits nombres premiers p jusqu'à trouver une impossibilité à une factorisation dans $\mathbf{Z}[X]$. Par exemple, pour $m = 607$, E_m est de degré 600. Il se factorise modulo 2 en un produit de 6 facteurs irréductibles de degré 100, tandis que, modulo 5, il se factorise en un produit de 8 facteurs irréductibles: 3 de degré 4, 2 de degré 18 et 3 de degré 184. Cette méthode a permis de tester tous les nombres premiers m jusqu'à 1000.

Nous avons également utilisé la propriété démontrée dans [5]: lorsque m est premier, s'il existe un nombre premier p tel que E_m ait au plus 3 facteurs irréductibles modulo p, alors E_m est irréductible dans $\mathbf{Z}[X]$. Exemple: $m = 601$, $p = 23$, E_m a 2 facteurs irréductibles de degré 297; $m = 349$, $p = 3$, E_m a 3 facteurs irréductibles de degré 114.

RÉFÉRENCES

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

[2] BATEMAN, P.T., C. POMERANCE and R.C. VAUGHAN. On the size of the coefficients of the cyclotomic polynomials. In: *Colloquia Mathematica János Bolyai, vol. 34. Topics in Classical Number Theory.* Budapest (Hungary). North Holland, 1984, 171–202.

[3] DEBARRE, O. and M.J. KLASSEN. Points of low degree on smooth plane curves. *J. reine angew. Math. 446* (1994), 81–87.

[4] HARDY, G.H. and E.M. WRIGHT. *An Introduction to the Theory of Numbers.* 4th edition. Clarendon Press, Oxford, 1960.

[5] HÉLOU, C. Cauchy-Mirimanoff polynomials. *C. R. Math. Rep. Acad. Sci. Canada 19 (2)* (1997), 51–57.

[6] KNUTH, D.E. *The Art of Computer Programming, vol. 2 (Semi-numerical Algorithms).* 2nd edition. Addison Wesley, 1981.

[7] MIGOTTI, A. Zur Theorie des Kreistheilungsgleichung. *Sitz. Akad. Wiss. Wien (Math.) (2) 87* (1883), 7–14.

[8] NICOLAS, J.-L. et G. ROBIN. Majorations explicites pour le nombre de diviseurs de n. *Canad. Math. Bull. 26* (1983), 485–492.

[9] RAMANUJAN, S. Highly Composite Numbers. *Proc. London Math. Soc. (2) 14* (1915), 347–400. (*Collected Papers.* Cambridge University Press, 1927 and Chelsea, 1962, 78–128.)

[10] ROSSER, J.B. and L. SCHOENFELD. Approximate formulas for some functions of prime numbers. *Illinois J. Math. 6* (1962), 64–94.

[11] TERJANIAN, G. Sur la loi de réciprocité des puissances ℓ-ièmes. *Acta Arith. 54* (1989), 87–125.

(Reçu le 29 juin 1999)

Jean-Louis Nicolas

Institut Girard Desargues
Mathématiques, Bât. 101
Université Claude Bernard (Lyon 1)
43, bd du 11 novembre 1918
F-69622 Villeurbanne Cedex
France
e-mail: jlnicola@in2p3.fr

Guy Terjanian

Laboratoire de Mathématiques Emile Picard
Université Paul Sabatier (Toulouse 3)
118, route de Narbonne
F-31062 Toulouse Cedex
France