1. Introduction

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 polynomial, i.e. the sum of the absolute values of its coefficients. We shall prove that for $m \geq 7$ and $m \neq 10$ the following inequality holds: $\beta(m) \leq (\sqrt{2})^{\varphi(m)}$, where φ is the Euler function.

Further, define $P_m(X) = \Phi_m(X) - (X-1)^{\varphi(m)}$ for $m \geq 2$. We shall deduce from the above inequality that if this polynomial vanishes at some root of unity, then this root of unity is of order 6.

1. INTRODUCTION

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

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

Nous définissons les coefficients de Φ_m par

$$\Phi_m(X) = a_{m,0} + a_{m,1}X + \cdots + a_{m,\varphi(m)}X^{\varphi(m)} , \tag{2}$$

et nous posons

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

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

$$\beta(m) \leq m^{\frac{1}{2}d(m)} \tag{3}$$

[1]) Recherche partiellement financée par le CNRS, Institut Girard Desargues, UPRES-A 5028 et Laboratoire 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 $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, $2 \leq p_1 < p_2 < \cdots < p_r$, $r = \omega(m)$. 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

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

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

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