

Notes sur un article de Vaughan de 1974

Bruno Martin

18 mai 2011

Résumé

Soit A_n le plus grand coefficient en valeur absolue du polynôme cyclotomique d'ordre n . Vaughan [10] montre qu'il existe une infinité d'entiers n tels que

$$A_n > \exp\left(n^{\frac{\log 2}{\log_2 n}}\right).$$

Dans cette note, nous détaillons les calculs de [10].

1 Introduction

Pour $n \in \mathbb{N}^*$, on note Φ_n le n -ième polynôme cyclotomique soit

$$\Phi_n(X) = \prod_{\substack{1 \leq k \leq n \\ (k,n)=1}} (X - e(k/n))$$

Le polynôme Φ_n est unitaire de degré $\varphi(n)$ et l'on pose

$$\Phi_n(X) = \sum_{m=0}^{\varphi(n)} a(m, n) X^m.$$

Rappelons que Φ_n est à coefficients entiers et que l'on dispose de la formule

$$\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(n/d)},$$

qui se déduit *via* la formule d'inversion de Möbius de l'identité

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

On peut constater numériquement que pour $n < 105$, les coefficients de Φ_n ne prennent que les valeurs 0, 1 ou -1 . On note dans la suite

$$A_n = \max_{1 \leq m \leq \varphi(m)} |a(m, n)|.$$

Lehmer [6] fournit en 1937 une démonstration due à Schur du fait que A_n peut prendre des valeurs arbitrairement grandes. La démonstration étant élémentaire et courte, nous la reproduisons en annexe.

Erdős établit dans [3] qu'il existe $c_1 > 0$ et une infinité d'entiers n pour lesquels

$$A_n > \exp \left(c_1 (\log n)^{4/3} \right).$$

Il conjecture qu'il existe $c_2 > 0$ tel que pour une infinité d'entiers n

$$A_n > \exp \left(n^{\frac{c_2}{\log_2 n}} \right). \quad (1)$$

Il prouve lui-même cette conjecture de deux manières différentes ([4], [5]). Par ailleurs Erdős conjecture dans [3] que (1) est essentiellement optimale, autrement dit qu'il existe $c_3 > 0$ telle que pour tout entier n ,

$$A_n < \exp \left(n^{\frac{c_3}{\log_2 n}} \right).$$

Cette dernière estimation est obtenue très simplement par Bateman [1]. Il obtient

$$A_n < \exp \left(n^{(1+o(1)) \frac{\log 2}{\log_2 n}} \right) \quad (n \rightarrow \infty). \quad (2)$$

Là encore nous restituons la preuve de ce résultat en annexe. La constante $\log 2$ figurant dans (2) est en fait optimale, c'est ce qu'établit Vaughan en 1975 dans [10].

Théorème 1 (Vaughan) *Il existe une infinité d'entiers n tels que*

$$A_n > \exp \left(n^{\frac{\log 2}{\log_2 n}} \right). \quad (3)$$

En particulier un ordre maximal* pour $\log_2 A_n$ est $\frac{\log 2 \log n}{\log_2 n}$.

Remarque 1 *En fait, Vaughan établit (à peu de prix) un résultat plus fort, à savoir qu'il existe une infinité d'entiers n tels que*

$$\max_m a(m, n) > \exp \left(n^{\frac{\log 2}{\log_2 n}} \right).$$

L'objectif de cette note est de fournir les détails de la preuve du théorème 1. Cette preuve utilise des outils de nature analytique (transformées de Mellin, fonction L de Dirichlet). Nous verrons qu'il existe en fait une preuve plus élémentaire.

*. cf chapitre L5 de [9] par exemple pour la définition d'un ordre maximal.

2 Première démonstration du théorème 1

Dans tout ce qui suit, on désigne par $\tau(k)$ le nombre diviseurs de l'entier k .

La famille d'entiers n satisfaisant à (3) est construite de la manière suivante. On note χ le symbole de Legendre modulo 5. Pour y assez grand, on pose

$$n = n(y) = \prod_{\substack{p \leq y \\ \chi(p) = -1}}^* p \quad (4)$$

où l'étoile $*$ signifie que l'on rajoute ou non le facteur 2, de manière à ce que le nombre de facteurs premiers de n soit toujours impair, et donc $\mu(n) = -1$.

Il sera utile de disposer d'une estimation relativement précise du nombre de facteurs premiers de tels entiers n .

Lemme 1 *On a pour $n \geq 10$, de la forme (4),*

$$\omega(n) = \sum_{\substack{p \leq y \\ \chi(p) = -1}} 1 + O(1) = \frac{\log n}{\log_2 n} \left(1 + \frac{1 - \log 2}{\log_2 n} + O\left(\frac{1}{(\log_2 n)^2}\right) \right).$$

Démonstration On a

$$\begin{aligned} \log n &= \sum_{\substack{p \leq y \\ \chi(p) = -1}} \log p + O(1) \\ &= \sum_{\substack{p \leq y \\ p \equiv 1 \text{ ou } 4 \pmod{5}}} \log p + O(1) \end{aligned}$$

D'après le théorème des nombres premiers en progressions arithmétiques, on a pour $(a, 5) = 1$,

$$\pi(t, a; 5) = \frac{\text{li}(t)}{\pi(5)} + R(t),$$

avec

$$\text{li}(t) = \int_2^t \frac{du}{\log u},$$

et

$$R(t) = O\left(\frac{t}{(\log t)^3}\right) \quad (t \geq 2).$$

Par conséquent,

$$\begin{aligned}\log n &= \frac{1}{2} \int_2^y \log t \, d\text{li}(t) + O\left(\int_2^y \log t \, dR(t)\right) \\ &= \frac{1}{2} y \left(1 + O\left(\frac{1}{(\log y)^2}\right)\right),\end{aligned}$$

d'où

$$\log_2 n = \log y - \log 2 + O\left(\frac{1}{(\log y)^2}\right)$$

À présent, on a, toujours d'après le théorème des nombres premiers en progressions arithmétiques,

$$\begin{aligned}\sum_{\substack{p \leq y \\ \chi(p) = -1}} 1 &= \sum_{\substack{p \leq y \\ p \equiv 1 \text{ ou } 4 \pmod{5}}} 1 \\ &= \frac{1}{2} \frac{y}{\log y} + O\left(\frac{y}{(\log y)^3}\right).\end{aligned}$$

D'après ce qui précède (sans oublier $y \sim \log n$ quand $n, y \rightarrow \infty$),

$$\begin{aligned}\frac{y}{\log y} &= \frac{2 \log n \left(1 + O(1/(\log_2 n)^2)\right)}{\log_2 n \left(1 + \log 2 / \log_2 n + O(1/(\log_2 n)^3)\right)} \\ &= \frac{2 \log n}{\log_2 n} \left(1 - \frac{\log 2}{\log n} + O\left(\frac{1}{(\log_2 n)^2}\right)\right),\end{aligned}$$

de sorte que l'on obtient bien la conclusion souhaitée. \square

En quelques mots, la preuve du théorème 1 consiste à fournir une minoration de $\sup_{|z| \leq 1} |\Phi_n(z)|$, puis à appliquer la majoration triviale

$$\sup_{|z| \leq 1} |\Phi_n(z)| \leq (\varphi(n) + 1) A_n.$$

Il est donc utile de disposer d'une représentation de $|\Phi_n(z)|$. Dans la suite, on pose

$$c_m = c_m(n) = \frac{1}{m} \sum_{r|(m,n)} r \mu(r),$$

où n est un entier de la forme (4). Nous donnons dans le lemme suivant les principales propriétés de c_m dont nous aurons l'usage.

Lemme 2 *On suppose que n est entier de la forme (4).*

i) *La fonction $m \mapsto c_m$ est multiplicative.*

ii) *Lorsque p est premier, $\nu \in \mathbb{N}^*$,*

$$c_{p^\nu} = \begin{cases} \frac{1-p}{p^\nu} & \text{si } p \mid n \\ \frac{1}{p^\nu} & \text{sinon.} \end{cases}$$

iii) *On a pour tout $m \geq 1$,*

$$|c_m| < 1.$$

iv) *On a pour $m \in \mathbb{N}^*$,*

$$c_{5m} = \frac{1}{5}c_m.$$

v) *Pour tout $0 < \varepsilon < 1$, il existe $C(\varepsilon) > 0$ tel que*

$$|c_m| \leq \frac{C(\varepsilon)}{m^\varepsilon}.$$

Démonstration

i) C'est facile : écrire que tout diviseur de (mm', n) avec $(m, m') = 1$ est de la forme uv avec $(u, u') = 1$, $u \mid (m, n)$, $u' \mid (m', n)$.

ii) C'est un calcul élémentaire.

iii) Cela résulte directement de i) et ii).

iv) Remarquons que 5 ne divise pas n . Par conséquent,

$$c_{5m} = \frac{1}{5m} \sum_{d \mid (5m, n)} d\mu(d) = \frac{1}{5m} \sum_{d \mid (m, n)} d\mu(d) = \frac{1}{5}c_m.$$

v) D'après ii) on a $|c_{p^\nu}| \leq 1/p^{\nu-1}$ et donc

$$\lim_{p^\nu} c_{p^\nu} p^{\varepsilon\nu} = 0.$$

Comme $m \mapsto c_m$ est multiplicative, on obtient la conclusion en employant par exemple le théorème 5.2 de [9].

□

Lemme 3 Pour $|z| < 1$, $n \in \mathbb{N}^*$ de la forme (4), on a

$$|\Phi_n(z)| = \exp \left(\Re \sum_{m=1}^{\infty} c_m z^m \right),$$

Démonstration Maintenant et dans la suite, \log désigne la détermination principale du logarithme. On a pour $|z| < 1$,

$$\begin{aligned} |\Phi_n(z)| &= \left| \prod_{d|n} (z^d - 1)^{\mu(n/d)} \right| \\ &= \left| \prod_{d|n} (1 - z^d)^{\mu(n/d)} \right| \quad (\text{car } \sum_{d|n} \mu(n/d) = 0) \\ &= \prod_{d|n} \left| (1 - z^d)^{\mu(n/d)} \right| \\ &= \exp \left(\sum_{d|n} \mu\left(\frac{n}{d}\right) \log |1 - z^d| \right) \\ &= \exp \left(\Re \sum_{d|n} \mu\left(\frac{n}{d}\right) \log(1 - z^d) \right) \quad (\text{car pour } z \in \mathbb{C} \setminus \mathbb{R}_-, \log |z| = \Re \log z) \\ &= \exp \left(- \Re \sum_{d|n} \mu\left(\frac{n}{d}\right) \sum_{k \geq 1} \frac{z^{kd}}{k} \right) \quad (\text{car } |z| < 1). \end{aligned}$$

On peut réarranger les termes de la double somme (c'est aisé à justifier) :

$$\begin{aligned} \sum_{d|n} \mu\left(\frac{n}{d}\right) \sum_{k \geq 1} \frac{z^{kd}}{k} &= \sum_{m=1}^{\infty} \sum_{d|n} \sum_{kd=m} \mu(n/d) \frac{z^{kd}}{k} \\ &= \sum_{m=1}^{\infty} z^m \sum_{d|n, d|m} \mu(n/d) \sum_{k=m/d} \frac{d}{m} \\ &= \mu(n) \sum_{m=1}^{\infty} z^m \sum_{d|n, d|m} \mu(d) \sum_{k=m/d} \frac{d}{m} \quad (\text{car pour } n \text{ de la forme (4), } \mu(n/d) = \mu(d)\mu(n)) \\ &= - \sum_{m=1}^{\infty} c_m z^m \quad (\text{car } \mu(n) = -1). \end{aligned} \quad \square$$

En posant $z = e(a)e^{-1/x}$ avec $a \in \mathbb{R}$, $x > 0$ nous avons

$$|\Phi_n(z)| = \exp \left(\Re \sum_{m=1}^{\infty} c_m e(am) e^{-m/x} \right). \quad (5)$$

Dans la suite, on choisit $a = 1/5$, et nous minorons

$$\sup_{x \geq 1} F(x)$$

avec

$$F(x) = F(x, n) = \Re \sum_{m=1}^{\infty} c_m e\left(\frac{m}{5}\right) e^{-m/x} \quad (x > 0).$$

Lemme 4 *On a pour $n \in \mathbb{N}^*$ de la forme (4),*

$$|F(x)| \leq x \quad (x > 0),$$

et pour $0 < \varepsilon < 1$,

$$|F(x)| \ll_{\varepsilon} x^{2(1-\varepsilon)} \quad (x \geq 1),$$

Démonstration D'après le lemme 2, on a

$$|F(x)| \leq \left| \sum_{m=1}^{\infty} c_m e\left(\frac{m}{5}\right) e^{-m/x} \right| \leq \sum_{m=1}^{\infty} e^{-m/x} = \frac{1}{e^{1/x} - 1} \leq x,$$

où la dernière majoration résulte de l'inégalité de convexité $e^u - 1 \geq u$ ($u \in \mathbb{R}$). Par ailleurs, d'après le point v) de 2,

$$\begin{aligned} |F(x)| &\leq \sum_{m=1}^{\infty} |c_m| e^{-m/x} \\ &\ll_{\varepsilon} \sum_{m < x^2} \frac{1}{m^{\varepsilon}} + \sum_{m \geq x^2} e^{-m/x} \\ &\ll_{\varepsilon} x^{2(1-\varepsilon)} + \frac{e^{-x}}{e^{1/x} - 1} \\ &\ll_{\varepsilon} x^{2(1-\varepsilon)} + x e^{-x} \\ &\ll_{\varepsilon} x^{2(1-\varepsilon)}. \end{aligned}$$

□

La stratégie de Vaughan consiste alors à considérer

$$M_F(\sigma) := \int_0^{\infty} F(x) \frac{dx}{x^{\sigma+1}} \quad (0 < \sigma < 1).$$

Notons que le lemme 4 garantit la convergence absolue de $M_F(\sigma)$.

Proposition 1 *On a pour $n \in \mathbb{N}^*$ de la forme (4),*

$$\sup_{x \geq 1} F(x) \geq \limsup_{\sigma \rightarrow 0} \sigma M_F(\sigma).$$

Démonstration Notant $K = \sup_{x \geq 1} F(x)$, on obtient

$$\begin{aligned} M_F(\sigma) &\leq \int_0^1 \frac{dx}{x^\sigma} + K \int_0^1 \frac{dx}{x^{\sigma+1}} \quad (\text{d'après le lemme 4}) \\ &= \frac{1}{1-\sigma} + \frac{K}{\sigma}, \end{aligned}$$

d'où l'on déduit

$$K \geq \sigma M_F(\sigma) - \frac{\sigma}{1-\sigma},$$

ce qui fournit le résultat espéré. □

On pourra alors compléter la preuve après avoir démontré la proposition suivante.

Proposition 2 *Pour $n \in \mathbb{N}^*$ de la forme (4), on a*

$$\lim_{\sigma \rightarrow 0} \sigma M_F(\sigma) = \frac{\sqrt{5}}{4} L(1, \chi) \tau(n),$$

où $s \mapsto L(s, \chi)$ désigne la série de Dirichlet associée à χ .

Preuve du théorème 1

D'après les propositions 1 et 2, on a pour n de la forme (4)

$$\sup_{x \geq 1} F(x) \geq \frac{\sqrt{5}}{4} L(1, \chi) \tau(n),$$

et donc, comme

$$A_n(\varphi(n) + 1) \geq \sup_{|z| \leq 1} |\Phi_n(z)| \geq \sup_{x \geq 1} \left| \Phi_n(e(1/5)e^{-1/x}) \right|$$

on obtient

$$A_n \geq \frac{1}{\varphi(n) + 1} \sup_{x \geq 1} \exp(F(x)) \geq \exp\left(\frac{\sqrt{5}}{4} L(1, \chi) \tau(n) - \log(\varphi(n) + 1)\right).$$

Or, comme n est sans facteur carré, $\tau(n) = 2^{\omega(n)}$, et d'après le lemme 1, on obtient en posant $B = \frac{\sqrt{5}}{4}L(1, \chi)$,

$$\begin{aligned} A_n &\geq \exp \left(B \exp \left(\log 2 \frac{\log n}{\log_2 n} \left(1 + \frac{1 - \log 2}{\log_2 n} + O\left(\frac{1}{(\log_2 n)^2} \right) \right) - \log(\varphi(n) + 1) \right) \right) \\ &= \exp \left(\exp \left(\log 2 \frac{\log n}{\log_2 n} + \frac{1 - \log 2}{(\log_2 n)^2} + O\left(\frac{1}{(\log_2 n)^3} \right) \right) \right), \end{aligned}$$

l'égalité résultant du fait que $\varphi(n) \leq n$. Comme $1 - \log 2 > 0$, on obtient pour n assez grand,

$$A_n > \exp \left(\exp \left(\log 2 \frac{\log n}{\log_2 n} \right) \right),$$

ce qui est exactement le résultat souhaité.

La suite de cette section est dévolue à la preuve de la proposition 2.

Lemme 5 *Pour $m \in \mathbb{N}^*$, on a*

$$\Re\left(\frac{m}{5}\right) = \frac{1}{4} \left(4[m \mid 5] - [m \nmid 5] + \sqrt{5}\chi(m) \right),$$

où l'on a utilisé la notation d'Iverson : $[P]$ vaut 1 ou 0 suivant que la propriété P est satisfaite ou non.

Démonstration On a

$$\begin{aligned} \Re\left(\frac{m}{5}\right) &= \frac{1}{2} \left(e\left(\frac{m}{5}\right) + e\left(-\frac{m}{5}\right) \right) \\ &= \frac{1}{4} \left(\sum_{k=1}^4 e\left(\frac{km}{5}\right) + \sum_{k=1}^4 \chi(k) e\left(\frac{km}{5}\right) \right) \quad (\text{car les carrés inversibles modulo 5 sont 1 et 4.}) \end{aligned}$$

Or d'une part, d'après la classique relation d'orthogonalité, on a

$$\sum_{k=0}^4 e\left(\frac{km}{5}\right) = \begin{cases} 5 & \text{si } m \mid 5 \\ 0 & \text{sinon,} \end{cases}$$

et par conséquent

$$\sum_{k=1}^4 e\left(\frac{km}{5}\right) = \begin{cases} 4 & \text{si } m \mid 5 \\ -1 & \text{sinon.} \end{cases}$$

D'autre part, comme χ est primitif, on a

$$\sum_{k=1}^4 \chi(k) e\left(\frac{km}{5}\right) = \tau(\chi) \chi(m),$$

où $\tau(\chi) = \sum_{k=1}^4 \chi(r) e\left(\frac{k}{5}\right)$. On a $\tau(\chi) = \sqrt{5}$ (calcul élémentaire ou bien theorem 9.17 de [7]). On obtient bien le résultat souhaité. \square

Lemme 6 *Pour $x > 0$, $n \in \mathbb{N}^*$ de la forme (4), on a*

$$F(x) = \frac{1}{4} \left(\sum_{m=1}^{\infty} c_m \left(e^{-5m/x} - e^{-m/x} \right) + \sqrt{5} \sum_{m=1}^{\infty} c_m \chi(m) e^{-m/x} \right).$$

Démonstration On a

$$\begin{aligned} F(x) &= \Re \sum_{m=1}^{\infty} c_m e\left(\frac{m}{5}\right) e^{-m/x} \\ &= \sum_{m=1}^{\infty} c_m \Re e\left(\frac{m}{5}\right) e^{-m/x} \quad (\text{par convergence absolue et continuité de } \Re) \\ &= \frac{1}{4} \left(4 \sum_{5 \mid m} c_m e^{-m/x} - \sum_{5 \nmid m} c_m e^{-m/x} + \sqrt{5} \sum_{m=1}^{\infty} c_m \chi(m) e^{-m/x} \right) \quad (\text{d'après le lemme 5}). \end{aligned}$$

Or

$$\begin{aligned} 4 \sum_{5 \mid m} c_m e^{-m/x} - \sum_{5 \nmid m} c_m e^{-m/x} &= 5 \sum_{m=1}^{\infty} c_{5m} e^{-5m/x} - \sum_{m=1}^{\infty} c_m e^{-m/x} \\ &= \sum_{m=1}^{\infty} c_m e^{-5m/x} - \sum_{m=1}^{\infty} c_m e^{-m/x}, \quad (\text{d'après le lemme 2}) \end{aligned}$$

ce qui achève le calcul. \square

Lemme 7 Pour $\sigma > 0$, $n \in \mathbb{N}^*$ de la forme (4), on a

$$\sum_{m=1}^{\infty} \frac{\chi(m)c_m}{m^\sigma} = L(1 + \sigma, \chi) \prod_{p|n} (1 + p^{-\sigma}), \quad (6)$$

et

$$\sum_{m=1}^{\infty} \frac{c_m}{m^\sigma} = \zeta(1 + \sigma) \prod_{p|n} (1 - p^{-\sigma}).$$

Démonstration Démontrons la première de ces égalités, la deuxième pouvant s'obtenir par des calculs similaires. Rappelons que d'après le lemme 2, la fonction $m \mapsto c_m$ est multiplicative et par conséquent la fonction $m \mapsto \chi(m)c_m m^{-\sigma}$ l'est aussi. De plus, on a

$$\begin{aligned} \sum_p \sum_{\nu \geq 1} \left| \frac{\chi(p^\nu)c_{p^\nu}}{p^{\sigma\nu}} \right| &= \sum_{p|n} \sum_{\nu \geq 1} \frac{1-p}{p^{\nu(\sigma+1)}} + \sum_{p \nmid n} \sum_{\nu \geq 1} \frac{1}{p^{\nu(\sigma+1)}} \\ &\leq C(n) + \sum_p \sum_{\nu \geq 1} \frac{1}{p^{\nu(\sigma+1)}} < \infty. \end{aligned}$$

Par conséquent la série de Dirichlet figurant en (6) est absolument convergente pour $\sigma > 0$ et

$$\begin{aligned} \sum_{m=1}^{\infty} \frac{\chi(m)c_m}{m^\sigma} &= \prod_p \sum_{\nu \geq 0} \frac{c_{p^\nu} \chi(p^\nu)}{p^{\nu\sigma}} \\ &= \prod_{p|n} \left(1 + \sum_{\nu \geq 1} \frac{(1-p)\chi(p^\nu)}{p^{\nu(\sigma+1)}} \right) \prod_{p \nmid n} \sum_{\nu \geq 0} \frac{\chi(p^\nu)}{p^{\nu(\sigma+1)}} \\ &= \prod_{p|n} \left(1 + \frac{1-p}{p^{\sigma+1}} \left(1 - \frac{\chi(p)}{p^{\sigma+1}} \right)^{-1} \right) \prod_{p \nmid n} \left(1 - \frac{\chi(p)}{p^{\sigma+1}} \right)^{-1} \\ &= L(1 + \sigma, \chi) \prod_{p|n} \left(1 - \frac{\chi(p)}{p^{\sigma+1}} + \frac{\chi(p)}{p^{\sigma+1}} (1-p) \right). \end{aligned}$$

Comme $\chi(p) = -1$ lorsque $p \mid n$, cela donne le résultat escompté. □

Lemme 8 On a pour tout $m \in \mathbb{N}$, $n \in \mathbb{N}^*$ de la forme (4), $\sigma > 0$,

$$\int_0^\infty e^{-m/x} \frac{dx}{x^{\sigma+1}} = \frac{\Gamma(\sigma)}{m^\sigma} \quad (\sigma > 0).$$

Démonstration Il suffit d'effectuer le changement de variables $u = m/x$ dans la formule classique

$$\Gamma(\sigma) = \int_0^\infty e^{-u} u^{\sigma-1} du \quad (\sigma > 0).$$

□

Lemme 9 Pour $\sigma > 0$, on a

$$M_F(\sigma) = \frac{\Gamma(\sigma)}{4} \left(\sqrt{5}L(1+\sigma, \chi) \prod_{p|n} (1+p^{-\sigma}) - (1-5^{-\sigma})\zeta(1+\sigma) \prod_{p|n} (1-p^{-\sigma}) \right).$$

Démonstration Pour $\sigma > 0$, on a (l'interversion est aisée à justifier, je ne donne pas les détails)

$$\begin{aligned} M_F(\sigma) &= \frac{1}{4} \int_0^\infty \left(\sum_{m=1}^\infty c_m (e^{-5m/x} - e^{-m/x}) + \sqrt{5} \sum_{m=1}^\infty c_m \chi(m) e^{-m/x} \right) \frac{dx}{x^{\sigma+1}} \quad (\text{d'après le lemme 6}) \\ &= \frac{1}{4} \sum_{m=1}^\infty c_m \int_0^\infty (e^{-5m/x} - e^{-m/x}) \frac{dx}{x^{\sigma+1}} + \sqrt{5} \sum_{m=1}^\infty c_m \chi(m) \int_0^\infty e^{-m/x} \frac{dx}{x^{\sigma+1}} \\ &= \frac{\Gamma(\sigma)}{4} \left((5^{-\sigma} - 1) \sum_{m=1}^\infty \frac{c_m}{m^\sigma} + \sqrt{5} \sum_{m=1}^\infty \frac{c_m \chi(m)}{m^\sigma} \right) \quad (\text{d'après le lemme 8}) \\ &= \frac{\Gamma(\sigma)}{4} \left(\sqrt{5}L(1+\sigma, \chi) \prod_{p|n} (1+p^{-\sigma}) - (1-5^{-\sigma})\zeta(1+\sigma) \prod_{p|n} (1-p^{-\sigma}) \right), \end{aligned}$$

la dernière égalité résultant du lemme 7.

□

Preuve de la proposition 2.

On emploie le lemme 9 : sachant que $\lim_{\sigma \rightarrow 0} \sigma \Gamma(\sigma) = 1$ (Γ a un pôle simple en 0 de résidu 1), que la fonction $\sigma \mapsto (1-5^{-\sigma})\zeta(1+\sigma)$ est bornée au voisinage de 0 (ζ a un pôle simple en 1), et que

$$\lim_{\sigma \rightarrow 0} \prod_{p|n} (1+p^{-\sigma}) = 2^{\omega(n)} = \tau(n), \quad \lim_{\sigma \rightarrow 0} \prod_{p|n} (1-p^{-\sigma}) = 0,$$

on obtient bien la limite souhaitée.

3 Une démonstration plus expéditive du théorème 1

Il est en fait possible d'obtenir de manière élémentaire le théorème 1. C'est l'objet de l'exercice 4.3.9 de [7]. Apparemment cette méthode est obtenue par Saffari, qui ne l'a pas publiée, mais est décrite dans [2].

Lemme 10 *Pour n de la forme (4), $d \mid q$, on a*

$$|e(d/5) - 1| = \begin{cases} |e(1/5) - 1| & \text{si } \omega(d) \text{ est pair;} \\ |e(2/5) - 1| & \text{si } \omega(d) \text{ est impair.} \end{cases}$$

Démonstration Supposons $\omega(d)$ pair. Dans ce cas, par multiplicativité de χ , on a $\chi(d) = 1$. Donc soit $d \equiv 1 \pmod{5}$ auquel cas on a bien $|e(d/5) - 1| = |e(1/5) - 1|$, soit $d \equiv -1 \pmod{5}$, et comme deux nombres complexes conjugués ont même module, on trouve $|e(d/5) - 1| = |e(-1/5) - 1| = |e(1/5) - 1|$. La démarche est identique pour le cas $\omega(d)$ impair. \square

Lemme 11 *our n de la forme (4), on a*

$$|\Phi_n(e(1/5))| = |e(1/5) + 1|^{\tau(n)/2}.$$

Démonstration D'après le lemme 10, on a

$$\begin{aligned} |\Phi_n(e(1/5))| &= \prod_{d \mid n} |e(d/5) - 1|^{\mu(n/d)} \\ &= \frac{|e(2/5) - 1|^{\#\{d \mid n : \omega(d) \text{ impair}\}}}{|e(1/5) - 1|^{\#\{d \mid n : \omega(d) \text{ pair}\}}} \end{aligned}$$

Or

$$\#\{d \mid n : \omega(d) \text{ impair}\} = \#\{d \mid n : \omega(d) \text{ pair}\}$$

En effet, posons $\omega(n) = 2k + 1$.

$$\begin{aligned} \#\{d \mid n : \omega(d) \text{ impair}\} &= \sum_{0 \leq j \leq k} \binom{2k+1}{2j+1} \\ &= \sum_{0 \leq j \leq k} \binom{2k+1}{2(n-j)} \\ &= \sum_{0 \leq j \leq k} \binom{2k+1}{2j} \\ &= \#\{d \mid n : \omega(d) \text{ pair}\}. \end{aligned}$$

Comme de plus,

$$\#\{d \mid n : \omega(d) \text{ impair} \} + \#\{d \mid n : \omega(d) \text{ pair} \} = 2^{\tau(n)} = \tau(n),$$

on obtient,

$$\#\{d \mid n : \omega(d) \text{ impair} \} = \#\{d \mid n : \omega(d) \text{ pair} \} = \frac{1}{2}\tau(n).$$

Ainsi,

$$|\Phi_n(e(1/5))| = \left| \frac{e(2/5) - 1}{e(1/5) - 1} \right|^{\tau(n)/2}.$$

La conclusion résulte alors de l'identité

$$\left| \frac{e(2/5) - 1}{e(1/5) - 1} \right| = |e(1/5) + 1|^{\tau(n)/2}. \quad \square$$

Il est maintenant aisé de conclure. On a

$$A_n(\varphi(n) + 1) \geq |\Phi_n(e(1/5))| = |e(1/5) + 1|^{\tau(n)/2},$$

et en employant le lemme 1, on obtient la minoration de Vaughan.

4 Annexe

4.1 Un résultat de Schur

Proposition 3 (Schur,1937) *On a*

$$\limsup_{n \rightarrow \infty} A_n = +\infty.$$

Démonstration Soit $t \in \mathbb{N}$, $t \geq 2$ et impair. Notons tout d'abord qu'il existe une suite de nombre premiers $p_1 < p_2 < \dots < p_t$ telle que $p_1 + p_2 > p_t$. En effet, supposons par l'absurde que ce ne soit pas le cas. Dans ce cas, pour tout entier naturel k , l'intervalle $[2^{k-1}, 2^k[$ contient au plus $t - 1$ nombres premiers (dans le cas contraire, on aurait $2^{k-1} \leq p_1 < p_2 < \dots < p_t < 2^k \leq 2p_1 < p_1 + p_2$). Par conséquent, on aurait $\pi(2^k) < kt$ pour tout k , ce qui irait à l'encontre de la minoration du nombre de nombres premiers de

Tchebycheff. À présent considérons $n = p_1 p_2 \dots p_t$ et la réduction de Φ_n modulo X^{p_t+1} de manière à pouvoir déterminer le coefficient d'ordre p_t :

$$\begin{aligned}
\Phi_n(X) &= \prod_{d|n} (X^d - 1)^{\mu(n/d)} \\
&\equiv \frac{\prod_{i=1}^t (X^{p_i} - 1)}{X - 1} \pmod{X^{p_t+1}} \quad (\text{car } t \text{ est impair et } p_1 p_2 > p_t) \\
&\equiv \frac{\prod_{i=1}^t (1 - X^{p_i})}{1 - X} \pmod{X^{p_t+1}} \quad (\text{car } t \text{ est impair}) \\
&\equiv (1 + X + X^2 + \dots + X^{p_t})(1 - X^{p_1} - X^{p_2} - \dots - X^{p_t}) \pmod{X^{p_t+1}} \quad (\text{car } p_1 + p_2 > p_t).
\end{aligned}$$

On constate que le coefficient d'ordre p_t de Φ_n vaut $1 - t$, ce qui achève la preuve. \square

Remarque 2 Cette preuve peut être adaptée pour montrer que tout entier relatif est coefficient d'au moins un polynôme cyclotomique (cf [8]). En revanche il ne semble pas connu que A_n puisse prendre toutes les valeurs entières positives.

4.2 La majoration de Bateman

Proposition 4 (Bateman, 1949) Pour tout $\varepsilon > 0$, $n \geq n_0(\varepsilon)$,

$$A_n < \exp \left(n^{(1+\varepsilon)\frac{\log 2}{\log 2 n}} \right). \quad (7)$$

Démonstration Dans cette démonstration, nous dirons qu'une série entière formelle $\sum_{n \geq 0} a_n x^n$ à coefficients réels majore $\sum_{n \geq 0} b_n x^n$ si $|a_n| \leq b_n \geq 0$ pour tout $n \geq 0$. Cet ordre est conservé par produit de séries entières (vérification facile) Considérons l'identité

$$\Phi_n(x) = \prod_{p|n} (1 - x^d)^{\mu(n/d)}.$$

Suivant que $\mu(n/d)$ vaut 0, 1 ou -1 , le facteur $(1 - x^d)^{\mu(n/d)}$ est toujours majoré par $1 + x^d + x^{2d} + \dots$. Par produit, et comme $\Phi_n(x)$ est un polynôme de degré $\varphi(n)$ et donc de degré strictement inférieur à n , on obtient que $\Phi_n(x)$ est majoré par

$$F_n(x) = \prod_{d|n} \left(1 + x^d + x^{2d} + \dots + x^{(n/d-1)d} \right).$$

Par conséquent, la quantité A_n n'excède pas la somme des coefficients de $F_n(x)$ c'est-à-dire $F_n(1)$. Ainsi,

$$A_n \leq F_n(1) = \prod_{d|n} \frac{d}{n} = \prod_{d|n} d = n^{\tau(n)/2}.$$

Or, on connaît l'ordre maximal de $\tau(n)$ [†](cf par exemple [7] theorem 2.11) : pour $n \geq 3$, on a

$$\tau(n) \leq \exp \left(\frac{\log n}{\log_2 n} \left(\log 2 + O\left(\frac{1}{\log_2 n}\right) \right) \right).$$

Donc pour $\varepsilon > 0$, $n \geq n_0(\varepsilon)$,

$$\tau(n) \leq \exp \left(\frac{\log n}{\log_2 n} (1 + \varepsilon/2) \log 2 \right),$$

et par suite,

$$\begin{aligned} A_n &\leq \exp \left(\frac{1}{2} \tau(n) \log n \right) \\ &\leq \exp \left(\exp \left(\frac{\log n}{\log_2 n} (1 + \varepsilon) \log 2 \right) \right) \quad (n \geq n_1(\varepsilon)). \end{aligned} \quad \square$$

5 Pourquoi choisir n de la forme (4) ?

À faire...

Références

- [1] P. T. BATEMAN – « Note on the coefficients of the cyclotomic polynomial », *Bull. Amer. Math. Soc.* **55** (1949), p. 1180–1181.
- [2] P. T. BATEMAN, C. POMERANCE & R. C. VAUGHAN – « On the size of the coefficients of the cyclotomic polynomial », in *Topics in classical number theory, Vol. I, II (Budapest, 1981)*, Colloq. Math. Soc. János Bolyai, vol. 34, North-Holland, Amsterdam, 1984, p. 171–202.
- [3] P. ERDÖS – « On the coefficients of the cyclotomic polynomial », *Bull. Amer. Math. Soc.* **52** (1946), p. 179–184.
- [4] — , « On the coefficients of the cyclotomic polynomial », *Portugaliae Math.* **8** (1949), p. 63–71.
- [5] — , « On the growth of the cyclotomic polynomial in the interval $(0, 1)$ », *Proc. Glasgow Math. Assoc.* **3** (1957), p. 102–104.

[†]. En réalité c'est l'ordre maximal de $\log \tau(n)$ qui est connu.

- [6] E. LEHMER – « On the order of magnitude of the coefficients of the cyclotomic polynomial », *Bull. Amer. Math. Soc.* **42** (1936), p. 389–392.
- [7] H. L. MONTGOMERY & R. C. VAUGHAN – *Multiplicative number theory. I. Classical theory*, Cambridge Studies in Advanced Mathematics, vol. 97, Cambridge University Press, Cambridge, 2007.
- [8] J. SUZUKI – « On coefficients of cyclotomic polynomials », *Proc. Japan Acad. Ser. A Math. Sci.* **63** (1987), no. 7, p. 279–280.
- [9] G. TENENBAUM – *Introduction à la théorie analytique et probabiliste des nombres*, second éd., Cours Spécialisés [Specialized Courses], vol. 1, Société Mathématique de France, Paris, 1995.
- [10] R. C. VAUGHAN – « Bounds for the coefficients of cyclotomic polynomials », *Michigan Math. J.* **21** (1974), p. 289–295 (1975).