3. DÉMONSTRATION DU THÉORÈME 2

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **45 (1999)**

Heft 3-4: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **01.05.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

et comme $k \geq 3$, 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 $m \geq 75$ et comme le plus petit nombre m avec $k = \omega'(m) \geq 3$ est $105 = 3 \cdot 5 \cdot 7$, (4) est démontrée pour tous les m avec $k = \omega'(m) \geq 3$, 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 $m \geq 2$. 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 $m \geq 3$. Les formules (18), (20) et (14) montrent que pour $m \geq 3$, $\Phi_m(-1)$ 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 $r \neq 6$ 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

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

D'où en prenant les modules,

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

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

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

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.)