SUR LE PROBLÈME DE KUMMER

Autor(en): **Moreno, Carlos Julio**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **20 (1974)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **25.05.2024**

Persistenter Link: https://doi.org/10.5169/seals-46894

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

SUR LE PROBLÈME DE KUMMER

par Carlos Julio MORENO

§ 1. INTRODUCTION

Soit p un nombre premier de la forme $p = 1 + 3t$ et g un générateur du groupe multiplicatif $(Z/pZ)^*$. Soit encore χ le caractère cubique non principal défini par le symbole

$$\chi(k) = \rho^{Indg(k)},$$

où $\rho = e^{\frac{2\pi i}{3}}$ et $k = g^{Indg}$ dans $(Z/pZ)^*$. La somme de Gauss pour le caractère χ est donnée par la formule

$$\tau_p = \sum_{k=1}^{p-1} \chi(k) e^{\frac{2\pi ik}{p}}. \tag{1}$$

On connaît deux résultats classiques sur la valeur du module de la somme de Gauss ([7] § 20)

A) $$|\tau_p| = p^{\frac{1}{2}}$$

B) $$\tau_p = p^{\frac{1}{2}} e^{i\theta_p},$$

où les angles θ_p sont bien définis à conjugaison près.

Kummer ([12], [13]) a calculé la valeur numérique de τ_p pour tous les nombres premiers $p \leq 499$ et a fait l'observation suivante (en utilisant une notation moderne):

Conjecture de Kummer

$$\sum_{\substack{p \leq x \\ p \equiv 1 \ (mod\ 3)}} \chi_h(\theta_p) = \frac{W_h x}{2\log x} + o\left(\frac{x}{\log x}\right), \quad h = 1, 2, 3,$$

où χ_1 (resp. χ_2, χ_3) est la fonction caractéristique de l'intervalle $(0, \frac{\pi}{3}]$ (resp. $(\frac{\pi}{3}, \frac{2\pi}{3}]$, $(\frac{2\pi}{3}, \pi]$), et

$$W_h = \begin{cases} \frac{1}{2}, & h = 1 \\ \frac{1}{3}, & h = 2 \\ \frac{1}{6}, & h = 3. \end{cases}$$

Un grand nombre des nouveaux calculs par Goldstine et von Neumann [6], Lehmer [15], et Cassels [1] nous ont conduits à douter de la véracité de la conjecture de Kummer; les mêmes calculs semblent aussi indiquer que les angles θ_p sont équirépartis dans l'intervalle $(0, \pi)$ pour la mesure de Lebesgue. Le but de cette note est de donner une démonstration du résultat suivant.

Théorème. Soit χ_I la fonction caractérisitique d'un sous-intervalle I de $(0, \pi]$, alors

$$\sum_{\substack{p \leq x \\ p \equiv 1 \, (mod\, 3)}} \chi_I(3\theta_p) = \frac{|I|\, x}{2 \log x} + o\left(\frac{x}{\log x}\right),$$

où $|I|$ est la mesure de Lebesgue de I.

Remarque. Le Théorème a été énoncé comme une loi de distribution des nombres premiers mais on peut dire simplement que les angles de la troisième puissance de τ_p sont équirépartis dans l'intervalle $(0, \pi]$ pour la mesure de Lebesgue.

§ 2. Démonstration du théorème

L'idée de la démonstration a été déjà considérée par Davenport-Hasse [4] et aussi par Weil [21]. Elle consiste à interpréter les sommes de Gauss comme des traces d'opérateurs de Frobenius.

Soit $E = Q(\rho)$ le corps quadratique imaginaire obtenu en adjoignant $\rho = e^{\frac{2\pi i}{3}}$ à Q et J_E son anneau d'entiers. L'arithmétique de J_E est bien connue et on sait que les nombres premiers dans J_E appartiennent a deux classes selon que la norme est un nombre premier rationnel ou le carré d'un nombre premier rationnel. Dans ce paragraphe, nous décrirons une construction locale des sommes de Gauss. Soit $\mathfrak{q}$ un nombre premier de J_E, $F\mathfrak{q}$ son corps résiduel et $N_{E/Q}(\mathfrak{q}) = q$ l'ordre de $F\mathfrak{q}$. Il est très facile de voir que $q \equiv 1 \pmod 3$, ce qui permet de construire un caractère cubique multipli-

catif pour le groupe cyclique $F^*\mathfrak{q} = F\mathfrak{q} - (0)$ en prenant la racine de l'unité $\chi\mathfrak{q}$ dans J_E qui satisfait à la congruence

$$\chi\mathfrak{q}(x) \equiv x^{\frac{q-1}{3}} \pmod{\mathfrak{q}}.$$

Pour $x \equiv 0 \pmod{\mathfrak{q}}$ nous posons $\chi\mathfrak{q}(x) = 0$. Soit $\psi(x)$ un caractère additif du groupe $F\mathfrak{q}$ distinct de l'unité. La somme de Gauss attachée au nombre premier $\mathfrak{q}$ est définie par

$$g(\chi\mathfrak{q}, \psi) = \sum_x \chi\mathfrak{q}(x)\psi(x),$$

où x décrit le corps résiduel $F\mathfrak{q}$. Le changement de x en $t\,x$, où $t \varepsilon F^*\mathfrak{q}$, donne

$$g(\chi\mathfrak{q}, \psi) = \chi\mathfrak{q}(t) \sum_x \chi\mathfrak{q}(x)\psi(xt),$$

ce qui prouve que le changement du caractère additif ψ en un autre dans la définition de la somme de Gauss ne fait que multiplier celle-ci par un facteur connu. Il en résulte que $g(\chi\mathfrak{q}, \psi)^3$ ne dépend que du nombre premier $\mathfrak{q}$.

Les propriétés suivantes des sommes de Gauss sont immédiates.

A') $|g(\chi\mathfrak{q}, \psi)|^2 = N_{E/Q}(\mathfrak{q})$.

C) Si $\mathfrak{g}$ est de degré 1 et $\psi(k) = e^{\frac{2\pi i k}{p}}$, où $p = N_{E/Q}(\mathfrak{g})$ il en résulte que la somme $g(\chi\mathfrak{q}, \psi)$ coincide avec la somme τ_p definie par (1) pour un choix du générateur g de $(Z/pZ)^*$ bien déterminé.

D) Le symbole local

$$\kappa\mathfrak{q} = g(\chi\mathfrak{q}, \psi)^3$$

ne dépend que de $\mathfrak{q}$.

Pour définir le symbole de Kummer global nous considérons l'ensemble des entiers $I_E(2(1-\rho)^2)$ qui sont premiers avec $2(1-\rho)^2$, et pour chaque $\mathfrak{a} \in I_E(2(1-\rho)^2)$ nous posons

$$\kappa(\mathfrak{a}) = \frac{\prod_{\mathfrak{q} \mid \mathfrak{a}} (-\kappa\mathfrak{q})^{ord\,\mathfrak{q}(\mathfrak{a})}}{N_{E/Q}(\mathfrak{a})^{\frac{3}{2}}}.$$

On a pour le symbole de Kummer $\kappa(\mathfrak{a})$ le résultat suivant.

Théorème (Deuring-Shimura-Weil). *Le symbole de Kummer* $\kappa(\mathfrak{a})$ *est un* « *Grössencharakter* ».

Pour la démonstration de ce résultat important nous renvoyons aux mémoires de Weil ([20] pp. 489-491), Shimura-Taniyama ([18] pp. 144-148: Main Theorem 4) et Deuring ([5]). Voir aussi notre mémoire ([16] § 3: Generalized Gauss sums as characters) où nous donnons une démonstration valable pour le cas d'une somme de Gauss générale.

Du fait que le symbole $\kappa(\mathfrak{a})$ est un Grössencharakter on peut construire les fonctions

$$L(s, \kappa^v) = \sum{}' \kappa^v(\mathfrak{a}) N(\mathfrak{a})^{-s} = \prod{}' (1 - \kappa^v(\mathfrak{q}) N(\mathfrak{q})^{-s})^{-1},$$

où $\mathfrak{a}$ (resp. $\mathfrak{q}$) sont des entiers (resp. nombres premiers) dans $I_E(2(1-\rho)^2)$ et v un entier rationnel $\geqq 1$. La théorie de Hecke [8] nous donne que

$$L(1 + \mathrm{i}t, \kappa^v) \neq 0$$

pout tous $-\infty \leqq t \leqq \infty$ et $v \in Z^+$. Alors un raisonnement du type Taubérien nous donne (voir Hecke [8], Serre [17] et Lang [14])

$$\sum_{N(\mathfrak{q}) \leqq x} \kappa_{\mathfrak{q}}^v = o\left(\frac{x}{\log x}\right).$$

Mais nous savons que

$$\sum_{\substack{N\mathfrak{q} \leqq x \\ \deg \mathfrak{q} = 2}} \kappa_{\mathfrak{q}}^v = o\left(x^{\frac{1}{2}} (\log x)^2\right);$$

il en résulte, selon le critère de Weyl [22], que les angles $\theta\mathfrak{q}$ de $\kappa\mathfrak{q} = e^{i\theta\mathfrak{q}}$ pour les nombres premiers $\mathfrak{q}$ de degré 1 sont équirépartis dans le cercle $R/2\pi Z$ pour la mesure de Lebesgue. Pour vérifier notre Théorème il reste à observer que pour chaque nombre premier $\mathfrak{q}$ in $I_E(2(1-\rho)^2)$ de degré 1 on a par conjugaison un autre nombre premier $\overline{\mathfrak{q}}$ aussi de degré 1 avec la propriété

$$\overline{\kappa\mathfrak{q}} = \kappa\overline{\mathfrak{q}}.$$

Finalement nous faisons usage de l'égalité

$$\kappa\mathfrak{q} = p^{-\frac{3}{2}} \tau_p^{\,3},$$

où $p = N_{E/Q}(\mathfrak{q})$, ou ce qui est la même chose

$$N_{E|Q}(\mathfrak{q})^{\frac{3}{2}} e^{i\theta\mathfrak{q}} = p^{\frac{3}{2}} e^{i3\theta p}.$$

Cela démontre la proposition.

§ 3. Remarques

1. La fonction $L(s, \kappa)$ est essentiellement la fonction zêta globale de la courbe elliptique

$$y^2 = 4x^3 + 1$$

sur le corps $E = Q(\rho)$. On observe simplement que si N_p = nombre de points dans la courbe réduite

$$u^3 \equiv v(v+1) \pmod p,$$

on a

$$N_p = p + 1 + \frac{\tau_p^3}{p} + \frac{\bar{\tau}_p^3}{p} \quad \text{pour} \quad p \equiv 1 \pmod 3.$$

Pour plus de détails, voir Weil [19], [20] et aussi Moreno [16].

2. La méthode utilisée ici nous permet de donner une solution partielle au problème suivant de Hilbert [9] (§ 112 pp. 227) qui est une généralisation de celui de Kummer. Soient m un nombre premier et p un autre nombre premier de la forme $p = 1 + t\,m$. Soit χ un caractère mutliplicatif de $(Z/pZ)^*$ d'ordre m et définissons la somme de Gauss par

$$\tau_p = \sum_{k=1}^{p-1} \chi(k)\, e^{\frac{2\pi i k}{m}}.$$

Alors on a $\tau_p = p^{\frac{1}{2}} e^{i\theta_p}$. Dans notre mémoire [16] nous démontrerons que les angles à la $m-^{ie}$ puissance $\tau_p^m = p^{\frac{m}{2}} e^{im\theta_p}$ sont équirépartis dans l'intervalle $(0, \pi)$ pour la mesure de Lebesgue.

3. Notre théorème donne une solution du problème de Davenport [3] (§ 3 p. 27).

4. L'équirépartition des angles $3\,\theta_p$ donne des résultats partiels pour le problème de Chowla [2] (problème 48, p. 94) qui demande d'obtenir la meilleure constante pour laquelle l'inégalité

$$\left| \sum_{x=0}^{p-1} e^{\frac{2\pi i x^3}{p}} \right| \leq 2\,p^{\frac{1}{2}}, \quad p \equiv 1 \pmod 3$$

reste valable. Nos résultats prouvent que pour chaque $\varepsilon > 0$ il a y une infinité de nombres premiers tels que

$$\left| \sum_{x=0}^{p-1} e^{\frac{2\pi i x^3}{p}} \right| \geqq (1-\varepsilon)\, p^{\frac{1}{2}} .$$

On doit observer simplement que

$$\sum_{x=0}^{p-1} e^{\frac{2\pi i x^3}{p}} = \tau_p + \bar{\tau}_p = 2\, p^{\frac{1}{2}} \cos \theta_p .$$

Cette idée remonte à Hasse [7] (§ 10.8, p. 171) qui l'avait déjà employée dans le cas de la somme de Gauss

$$\sum_{x=0}^{p-1} e^{\frac{2\pi i x^4}{p}}, \quad p \equiv 1 \pmod 4 .$$

5. La solution complète du problème de Kummer sera immédiate si on peut établir que les deux fonctions zêta définies par le produit d'Euler

$$L_v(s) = \prod_{\substack{p \\ p \equiv 1 \ (mod\ 3)}} (1 + \tau_p^v\, p^{-s})^{-1} (1 + \bar{\tau}_p^v\, p^{-s})^{-1}, \quad v = 1, 2$$

sont des fonctions holomorphes pour $Re(s) \geqq \frac{3}{2} - \varepsilon$ et $Re(s) \geqq 2 - \varepsilon$ resp. et ne s'annulent pas sur la droite de convergence absolue. Il serait aussi très intéressant de donner une interprétation de caractère 1-adique d'un élément de Frobenius d'expression $\tau_p + \bar{\tau}_p$.

Kubota [10], [11] a obtenu des résultats très profonds pour des fonctions analogues à $L_1(s)$ et $L_2(s)$ et nous espérons que sa méthode pourrait s'appliquer à notre problème.

BIBLIOGRAPHIE

[1] Cassels, J. N. S. On kummer sums. *Proc. London Math. Soc.* (3) *21* (1970), 19-27.

[2] Chowla, S. *The Riemann Hypothesis and Hilbert's Tenth Problem.* Gordon and Bleach, New York, 1965.

[3] Davenport, H. *Multiplicative number Theory.* Markham, Chicago, 1967.

[4] —— und H. Hasse. Die Nullstellen der Kongruenzzetafunktionen im gewissen zyklischen Fällen. *J. reine angew. Math, 172* (1935), 151-182.

[5] Deuring, M. Die Zetafunktion einer algebraischen Kurve von Geschlechte Eins. I, *Nachr. Akad. Wiss. Göttingen,* (1953),85-94.

[6] Goldstine, H. and J. von Neumann. A numerical study of a conjecture of Kummer. *Math. Tables Aids Comput. 7* (1953), 133-134.

[7] Hasse, H. *Vorlesungen über Zahlentheorie.* 1te Aufgabe, Springer, Berlin, 1964.

[8] Hecke, E. Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen. I, II, *Math. Zeitschr., 1* (1918), 357-376; *6* (1920), 11-51.

[9] Hilbert, D. Die Theorie der algebraischen Zalkörper. *Jahresbericht D. Math. Ver. Bd. 4* (1897), 175-546.

[10] KUBOTA, T. On a special kind of Dirichlet series. *Journ. Math. Soc. Japan, 20,* (1968), 193-207.

[11] —— Some results concerning reciprocity law and real automorphic functions. *Proceedings of Symposia in Pure Math. Vol. XX* (1971), 328-394.

[12] KUMMER, E. Eine Aufgabe betreffend die Theorie der kubischen Reste. *J. reine angew. Math. 23* (1842), 285-86.

[13] —— De residuis cubicis disquisitiones nonnulae analyticae, *J. reine angew. Math. 32* (1846), 341-59.

[14] LANG, S. *Algebraic Numbers.* Addison-Wesley, New York, 1964.

[15] LEHMER, E. On the location of Gauss sums. *Math. Tables Aids Comput. 10* (1956), 194-202.

[16] MORENO, C. Kummer sums and elliptic curves. *(à paraître).*

[17] SERRE, J.-P. *Abelian 1-adic representations and elliptic curves.* Benjamin, New York, 1968.

[18] SHIMURA, G. and Y. TANIYAMA. Complex multiplication of abelian varieties and its applications to number theory. *Publ. Math. Soc. Japan, n° 6,* 1971.

[19] WEIL, A. Number of solutions of equations in finite fields. *Bull. Amer. Math. Soc. 55* (1949), 497-508.

[20] —— Jacobi sums as "Grössencharactere". *Trans. Amer. Math. Soc. 73* (1952), 487-495.

[21] —— On some exponential sums. *Proc. Nat. Acad. Sc. USA, t. 34* (1948), 204-207.

[22] WEYL, H. Über die Gleichverteilung von Zahlen mod. Eins, *Math. Annalen 77* (1914), 313-352.

(Recu le 29 mai 1973)

Carlos Julio Moreno
The Center for Advanced Study
University of Illinois
912 West Illinois
Urbana, IL 61801
U.S.A.

vide-leer-empty