Séminaire Delange-Pisot-Poitou. Théorie des nombres

Philippe Barkan

Partitions quadratiques et cyclotomie

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 16, n° 2 (1974-1975), exp. n° G13, p. G1-G12

<http://www.numdam.org/item?id=SDPP_1974-1975__16_2_A12_0>

Séminaire DELANGE-PISOT-POITOU
(Groupe d'étude de théorie des nombres)
16e année, 1974/75, n° G13, 12 p.

17 mars 1975

PARTITIONS QUADRATIQUES ET CYCLOTOMIE

par Philippe BARKAN

Cet exposé donne un aperçu sur quelques relations entre la représentation explicite des nombres premiers par diverses formes quadratiques à l'aide de différents types de sommes de racines de l'unité, et quelques problèmes de cyclotomie qui y sont liés.

1. Sommes de Gauss et sommes de Jacobi.

Soient $p = mn + 1$ un nombre premier, et g une racine primitive fixée de p. Le nombre cyclotomique d'ordre m, noté (i , j), est le nombre de solutions (s , t) de la congruence

$$(1) \qquad g^{ms+i} + 1 \equiv g^{mt+j} \pmod p \qquad \begin{cases} 0 \leqslant i , j \leqslant m - 1 , \\ 0 \leqslant s , t \leqslant n - 1 . \end{cases}$$

L. E. DICKSON [8] s'est posé le problème d'obtenir des formules explicites pour les nombres cyclotomiques, problème déjà résolu par GAUSS pour $m = 3$ et $m = 4$ ([12], [13]) en fonction des coordonnées des partitions quadratiques de $4p=x^2+27y^2$ et de $p = u^2 + v^2$ respectivement.

Ces nombres cyclotomiques apparaissent comme coefficients des sommes de Jacobi d'ordre m

$$(2) \qquad J(a , b) = \sum_{x=2}^{x=p-1} \theta^{a \operatorname{Ind}_g x + b \operatorname{Ind}_g (1-x)} \quad , \text{ où } \theta = \exp(2\pi i/m)$$

liées à la somme de Gauss

$$(3) \qquad G(a) = \sum_{x=1}^{x=p-1} \theta^{a \operatorname{Ind}_g x} \zeta^x \quad \text{où} \quad \zeta = \exp(2\pi i/p)$$

par la relation

$$(4) \qquad J(a , b) = \frac{G(a)\, G(b)}{G(a + b)}$$

si m ne divise ni a, ni b, ni $a + b$. Il en résulte

$$(5) \qquad G(a)\, G(- a) = (- 1)^{an} p \quad \text{si } m \text{ ne divise pas } a .$$

Avec les mêmes conditions que dans (4), on a

$$(6) \qquad J(a , b) = J(b , a) = (- 1)^{na} J(m - a - b , b) .$$

Par (5) et (4), si m ne divise ni a, ni b, ni $a + b$:

$$(7) \qquad J(a , b)\, J(m - a , m - b) = p .$$

La somme $J(a , b)$ étant périodique (mod m) en a et en b, on peut la développer en série de Fourier finie double [32] sous la forme

$$(8) \qquad J(a , b) = (- 1)^{na} \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} (i , j)\, \theta^{ai+bj} .$$

La formule d'inversion de Fourier finie donne (i , j) par

$$(9) \qquad m^2(i , j) = \sum_{a=0}^{m-1} \sum_{b=0}^{m-1} (-1)^{na} J(a , b) \theta^{-(ai+bj)} .$$

En groupant les exposants de (2) modulo m ,

$$J(a , b) = \sum_{i=0}^{m-1} c_i \theta^i ,$$

et les coefficients c_i s'expriment à l'aide des nombres cyclotomiques d'après (8). Leur expression se simplifie lorsque m a au plus deux facteurs premiers distincts. Dans ce cas, par (6), chaque somme admet une représentation du type $J(a , va)$, où v est entier. En transformant (2), on trouve

$$(10) \qquad J(a , va) = (-1)^{vna} \sum_{i=0}^{m-1} B_m(i , v) \theta^{ai}$$

avec la "somme de Dickson-Hurwitz"

$$(11) \qquad B_m(i , v) = \sum_{h=0}^{m-1} (h , i - vh) .$$

DICKSON cherchait une formule explicite fonction de p , et de coordonnées de partitions quadratiques de p . Pour obtenir une telle solution, on doit résoudre les problèmes suivants :

1° Déterminer les relations entre couples de sommes de Jacobi d'ordre m et d'ordre un diviseur de m .

2° En déduire des relations entre coefficients des sommes de Jacobi.

3° Dériver de (7) des formes quadratiques diagonales représentant p ou un multiple de p .

4° Exprimer les nombres cyclotomiques par des formules du type

$$c(i , j) = \sum_k c(i , j , k) c'_k$$

les c'_k étant p , des constantes, ou des combinaisons linéaires de coefficients de sommes de Jacobi, si possible les coordonnées des formes quadratiques de 3°, et les $c(i , j , k)$ étant entiers rationnels, et c un entier dépendant de m .

En ce qui concerne le 1°, si σ_j change θ en θ^j , avec j et m premiers entre eux, on a

$$(12) \qquad \sigma_j G(a) = G(ja) .$$

Si d'autre part $m = cd$, et si $J_c(a , b)$ désigne une somme de Jacobi d'ordre c , DICKSON montra

$$J_c(a , b) = J(da , db) .$$

On connait deux types de relation multiplicative entre sommes de Gauss

(I) La relation de norme $G(a) G(-a) = (-1)^{na} p$.

(II) La relation due à DAVENPORT et HASSE [6]. Pour $m = cd$ et tout j ,

$$\prod_{i=0}^{d-1} G(ci + j) = \theta^{-jd \operatorname{Ind}_g(d)} G(dj) \prod_{i=1}^{d-1} G(ci)$$

déjà énoncée par JACOBI [16].

HASSE avait conjecturé que (I) et (II) sont les seules relations multiplicatives entre sommes de Gauss d'ordre donné, mais YAMAMOTO [37] prouva que ce n'est vrai que lorsqu'on considère les sommes de Gauss comme idéaux et que les relations (I) et (II) ne conduisent dans certains cas qu'à des identités entre carrés de sommes de Gauss, ou de Jacobi. Pour $m = 21$, on trouve

$$J(1 , 4)^2 = [\theta^{7 \text{ Ind } 7} J(3 , 6)]^2 ,$$

d'où une ambiguïté de signe qu'on rencontre aussi pour $m = 12$, $m = 15$, 20 , 21 , 24 , 28 , 39 , 55 , 56 , ... ([27], [28]), et qu'on peut associer

- soit à des conditions de congruence sur les coordonnées de certaines partitions quadratiques binaires. Pour $m = 21$,

$$J(1 , 4) = \varepsilon\theta^{7 \text{ Ind } 7} J(3 , 6)$$

et avec $p = A^2 + 7B^2$, "$\varepsilon = + 1$" équivaut à "3 divise B" et "$\varepsilon = - 1$" équivaut à "3 divise A" .

- soit à la division du genre principal de formes quadratiques de discriminant $- m$, pour $m = 39$, 55 , 56 , ... en deux classes. Pour $m = 39$, si

$$J = \theta^{13 \text{ Ind } 13} J(1 , 16) ,$$

alors $\sigma_2 J = \varepsilon J$, et ici "$\varepsilon = + 1$" équivaut à "$p = x^2 + 39y^2$" et "$\varepsilon = - 1$" équivaut à "$p = 3z^2 + 13t^2$" .

Pour connaître les relations entre sommes de Jacobi d'ordre m , on doit savoir quand une somme de Jacobi est égale à une racine $2m$-ième de l'unité fois une image automorphe d'une autre, et quelle est la racine de l'unité. La recherche systématique pour m donné peut se faire en utilisant un théorème de KUMMER sur la décomposition des sommes de Jacobi en idéaux premiers, en vérifiant que ces deux sommes ont la même décomposition (voir [9]). La racine de l'unité restante se détermine à l'aide de l'identité (II), et il reste une éventuelle ambiguïté de signe à mettre en évidence. Ces relations ont été déterminées par YAMAMOTO pour $m = 2r$, où r est premier, en liaison avec le problème des ensembles de différences [38].

En ce qui concerne le 2°, beaucoup de relations entre coefficients des sommes de Jacobi résultent de la définition des nombres cyclotomiques. En particulier,

(13) $$(i , j) = (m - i , j - i) .$$

(14) $$(i , j) = \begin{cases} (j , i) & \text{si } n \text{ pair,} \\ (j + \frac{m}{2} , i + \frac{m}{2}) & \text{si } n \text{ impair.} \end{cases}$$

(15) $$B(i , 0) = \begin{cases} n - 1 & \text{si } m \text{ divise } i , \\ n & \text{sinon.} \end{cases}$$

(16) $$B(i , a) = B(i , b) \quad \text{si} \quad a + b \equiv - 1 \pmod m .$$

DICKSON prouva, avec $m = cd$, dans [10],

$$B_c(i , v) = \sum_{k=0}^{d-1} B_m(i + ck , v) .$$

La relation importante suivante est due à WHITEMAN [33]

(18) $$B(i\ ,\ v) = B(v'\ i\ ,\ v') \quad \text{si} \quad vv' \equiv 1 \pmod m .$$

La relation suivante résultant de (15) et (17) par la périodicité (mod d) de B_d ne semble pas bien connue

(19) $$\sum_{k=0}^{c-1} B_m(i + kd\ ,\ \ell d) = B_d(i\ ,\ 0) = \begin{cases} cn - 1 & \text{si d divise i ,} \\ cn & \text{sinon.} \end{cases}$$

Ces relations simplifient les calculs explicites des partitions de l'étape 3°.

Exemple. - Soit $p = 7n + 1$. Partons du produit

$$T(\theta) = G(1)\ G(2)\ G(4) = J(1\ ,\ 2)p$$

par (4) et (5) et qui, d'après (12), est invariant par σ_1 , σ_2 , σ_4 laissant $\sqrt{-7} = \theta + \theta^2 + \theta^4 - (\theta^3 + \theta^5 + \theta^7)$ invariant. Le développement en série de Fourier finie

$$J(1\ ,\ 2) = \sum_{i=0}^{6} B(i\ ,\ 2)\theta^i = \sum_{i=0}^{6} a_i\ \theta^i$$

s'écrit, puisque $B(i\ ,\ 2) = B(4i\ ,\ 4)$ par (18), donc $a_i = a_{2i} = a_{4i}$,

$$J(1\ ,\ 2) = a_0 + a_1(\theta + \theta^2 + \theta^4) + a_3(\theta^3 + \theta^5 + \theta^6) ,$$

d'où

$$2J(1\ ,\ 2) = 2a_0 - a_1 - a_3 + (a_1 - a_3)\sqrt{-7}$$

et

$$4p = (2a_0 - a_1 - a_3)^2 + 7(a_1 - a_3)^2 .$$

Pour obtenir la représentation d'une puissance de p par la forme $x^2 + my^2$, on considère un produit de sommes de Gauss indépendant de ζ , ou un produit de sommes de Jacobi, invariant par les $\frac{1}{2}\varphi(m)$ automorphismes de $\mathbb{Q}(\theta)$ laissant $\sqrt{-m}$ invariant où $-m$ est un discriminant de corps quadratique complexe. Un tel produit a été construit par CAUCHY [5] et par JACOBI [16] pour $p \equiv 1 \pmod m$ et généralisé par STICKELBERGER [30] au cas d'un nombre premier quelconque. En généralisant les sommes de Gauss au corps fini $\mathbb{F}_q$, $q = p^f$, f étant l'ordre de p (mod m) et p tel que $(\frac{-m}{p}) = 1$, il considère le produit

$$T(\theta) = \prod_k G(k)$$

étendu aux $\frac{1}{2}\varphi(m)$ entiers naturels $k < m$ tels que $(\frac{-m}{k}) = +1$, donc invariant par les σ_k , car ces k forment un sous-groupe du groupe multiplicatif des entiers (mod m) premiers à m . A l'aide de la décomposition en idéaux premiers de ces sommes de Gauss généralisées, il détermine la plus grande puissance de p divisant T .

L'exposant K est tel que $\Sigma k = mK$. Par les relations $k' = m - k$ et $(\frac{-m}{k'}) = -1$ et $\Sigma k' = mK'$, et en remarquant $K' - K = h(-m)$ nombre de classes de formes quadratiques binaires primitives de discriminant $-m$, il prouve que $4p^r$ et $4p^h$ sont représentables par la forme $x^2 + my^2$ $(r = \frac{1}{2}\varphi(m))$ et donne la congruence

(20) $$x \equiv \prod_{k'} \left[\frac{pk'}{m}\right]! \pmod{p} ,$$

où le crochet désigne la partie entière. Si $h(-m) > 1$, on n'obtient pas p lui-même. Si h et m sont petits, la relation (II) permet de se ramener à une seule somme de Jacobi. On connaît quelques résultats explicites si $h = 2$ et $h = 4$ ([25], [26], [28]). Pour $m = 55$ ou 56, il est impossible d'obtenir la partition à l'aide d'une seule somme, et on doit considérer un produit de trois sommes divisé par p. Pour $m = 11$, on ne peut obtenir p à l'aide d'une somme, mais cela devient possible en se plaçant dans le corps des racines 22e de l'unité, et ZEE [40] obtient ainsi $p = 22n + 1 = x^2 + xy + 3y^2$ explicitement.

On ne connaît pas de solution générale explicite, même lorsque h est une puissance de 2.

Exemple 2. - Si $m = 15$, $h(-15) = 2$, on peut obtenir $p = 15n + 1$ sous la forme $x^2 + 15y^2$. On part du produit

$$T = G(1)\ G(2)\ G(4)\ G(8) ,$$

qui s'écrit

$$T = J(1 , 4)\ \sigma_2\ J(1 , 4)p .$$

De la relation (II) résulte

$$\sigma_2\ J(1 , 4) = \theta^5\ \mathrm{Ind}\ 5\ J(1 , 4) .$$

En posant $B(i , 4) = a_i$, il vient $a_i = a_{4i}$ par (18) et, avec $\theta^5 = \zeta$ et $\theta^3 = \eta$, on trouve $\theta^i = \zeta^{2u}\ \eta^{2v}$ si $i \equiv u \pmod 3$ et $i \equiv v \pmod 5$, d'où

$$J(1 , 4) = a_0 + a_5\ \zeta + a_{10}\ \zeta^2 + (a_3 + a_2\ \zeta + a_7\ \zeta^2)(\eta + \eta^4) + (a_6 + a_{11}\ \zeta + a_1\ \zeta^2)(\eta^2 + \eta^3) .$$

En utilisant deux fois de suite l'identité

$$2(a + b\zeta + c\zeta^2) = 2a - (b + c) + (b - c)(\zeta - \zeta^2)$$

et remarquant

$$\zeta - \zeta^2 = \sqrt{-3} , \quad \eta + \eta^4 - (\eta^2 + \eta^3) = \sqrt{5} ,$$

on trouve

$$4J(1 , 4) = a + b\sqrt{-3} + c\sqrt{5} + d\sqrt{-15}$$

avec des expressions pour a, b, c, d, qui se simplifient par (16) et (19) car $a_i = B(i , 4) = B(i , 10)$, d'où

$$a_i + a_{i+5} + a_{i+10} = \begin{cases} 3n - 1 & \text{si } 5 \text{ divise } i , \\ 3n & \text{sinon.} \end{cases}$$

Tous calculs faits, il vient

$$\begin{cases} a = 6a_0 - 3(a_3 + a_6) + 2 \\ b = 2(a_5 - a_{10}) - (a_2 - a_7) - (a_{11} - a_1) \\ c = 3(a_3 - a_6) \\ d = a_2 - a_7 + a_1 - a_{11} \end{cases}$$

De $\sigma_2(\sqrt{-3}) = -\sqrt{-3}$ et $\sigma_2(\sqrt{5}) = -\sqrt{5}$, on déduit

$$\zeta^{\mathrm{Ind}\ 5}(a + b\sqrt{-3} + c\sqrt{5} + d\sqrt{-15}) = a - b\sqrt{-3} - c\sqrt{5} + d\sqrt{-15}\ .$$

En utilisant le fait que $(1\ ,\ \sqrt{-3}\ ,\ \sqrt{5}\ ,\ \sqrt{-15})$ est une base de $\mathbb{Q}(\sqrt{-3}\ ,\ \sqrt{5})$, on trouve que

- si $\mathrm{Ind}\ 5 \equiv 0 \pmod 3$, alors $b = c = 0$, d'où $a_3 = a_6$, $d = 2(a_2 - a_{11})$ et $p = x^2 + 15y^2$ avec $2x = 3(a_0 - a_3) + 1$, $2y = a_2 - a_{11}$.

- si $\mathrm{Ind}\ 5 \equiv \varepsilon \pmod 3$, alors $a = -\varepsilon b$, $c = 3\varepsilon d$, d'où ici $2y = a_1 - a_7$, resp. $a_2 - a_{11}$, suivant que $\varepsilon = +1$, resp. -1. On peut aussi prouver la congruence

$$2x \equiv \binom{5n}{n}^2 / \binom{7n}{n} \pmod p\ .$$

En suivant une marche analogue, on trouve quelques exemples avec $m = 3d$ et $m = 4d$, où d est premier.

En 1935, DICKSON [9] montra comment les nombres cyclotomiques d'ordre m (m premier impair) pour $p = mn + 1$ dépendaient des solutions d'un système de $\frac{1}{2}(m-1)$ équations diophantiennes quadratiques, donnant aussi la représentation d'un multiple de p par une forme quadratique diagonale en $m - 1$ lettres. Pour $m = 5$, il étudie complètement le système

$$\begin{cases} 16p = x^2 + 50(u^2 + v^2) + 125w^2 \\ xw = (v - 2u)^2 - 5u^2 \quad \text{et} \quad x \equiv 1 \pmod 5 \end{cases}$$

qui admet exactement quatre solutions entières : $(x\ ,\ u\ ,\ v\ ,\ w)$, $(x, \pm v, \pm u, -w)$ et $(x\ ,\ -u\ ,\ -v\ ,\ w)$. P. A. LEONARD et K. S. WILLIAMS [22] viennent de traiter complètement le cas $m = 7$, donnant les nombres cyclotomiques d'ordre 7 en fonction des coordonnées d'un système analogue. Le cas $m = 11$ devrait paraître aux "Acta Arithmetica".

Ces résultats permettent également d'obtenir des critères de résiduation de petits nombres premiers, donnant une condition nécessaire et suffisante pour qu'une congruence $x^m \equiv q \pmod p$ ait lieu [21].

Ces critères s'expriment généralement en termes de condition de congruence sur les coefficients des sommes de Jacobi ([15], [24]).

On peut aussi les déduire de

$$\prod_{i=1,(i,m)=1}^{m-1}(1 - \theta^i) = \begin{cases} q & \text{si } m = q^k\ , \quad q \text{ premier,} \\ 1 & \text{sinon.} \end{cases}$$

et du lemme de KUMMER [18]

$$\mathrm{Ind}(1-\theta^j) \equiv \frac{p-1}{2} + \sum_{i=1}^{m-1} i(i\ ,\ j) \pmod m\ ,$$

permettant d'exprimer dans des cas simples le caractère de reste de puissance m-ième d'un nombre algébrique décomposable en un produit de $1-\theta^j$ par des conditions de congruence sur les coordonnées d'une ou plusieurs partitions quadratiques convenables de p, en particulier si ce nombre est entier rationnel, ou l'unité fondamentale d'un corps quadratique réel ([19], [20], [21], [23], [24]).

Soit par exemple $\varepsilon_5 = \frac{1}{2}(1+\sqrt{5}) = -\theta^6(1+\theta^3)$. Avec $m = 3d$, et $a_i = B(i,2d)$, on trouve, pour $i \neq 0$, les congruences

$$\mathrm{Ind}(1-\theta^{3i}) \equiv -(a_i - a_{i+d}) \equiv a_i - a_{i+2d} \pmod 3\ ,$$

d'où avec $d = 5$ et faisant $i = 1$ et $i = 2$, et utilisant l'expression explicite de y,

"Ind $\varepsilon_5 \equiv 0 \pmod 3$" équivaut à "$p = x^2 + 15y^2$ et $y \equiv 0 \pmod 3$"

soit, en introduisant la suite de Fibonacci

(21) $u_{(p-1)/3} \equiv 0 \pmod p$ équivaut à $p = x^2+15y^2$ et $y \equiv 0 \pmod 3$.

En généralisant ce qui précède aux corps finis $\underset{\sim}{F}_{p^2}$, on montre que (21) est vrai pour $p = 15n + 4$.

La généralisation de ces critères s'effectue plus simplement par d'autres méthodes (Voir [20] et [23]).

Ce qui précède permet de déterminer les nombres cyclotomiques d'ordre 3, avec $p = 3n + 1$. Les formules (13) et (14) réduisent les neuf nombres $(i\ ,\ j)$ aux quatre suivants $(0\ ,\ 0)$, $(0\ ,\ 1)$, $(0\ ,\ 2)$, $(1\ ,\ 2)$. Par (15), on a

(a) $(0\ ,\ 0) + (0\ ,\ 1) + (0\ ,\ 2) = n - 1$.

(b) $(0\ ,\ 1) + (0\ ,\ 2) + (1\ ,\ 2) = n$.

Avec $B(i\ ,\ 1) = (0\ ,\ i) + (1\ ,\ i-1) + (2\ ,\ i-2) = b_i$, il vient

$$J(1\ ,\ 1) = b_0 + b_1\,\theta + b_2\,\theta^2$$

soit

$$4p = (2b_0 - b_1 - b_2)^2 + 3(b_1 - b_2)^2 = L^2 + 27M^2$$

avec

$$L = 2(0\ ,\ 0) + 4(1\ ,\ 2) - 3(0\ ,\ 1) - 3(0\ ,\ 2)\ , \quad M = (0\ ,\ 1) - (0\ ,\ 2)\ .$$

En formant $2(a) - 5(b)$, on trouve $-p-1$, d'où

$$L = 9(1\ ,\ 2) - p - 1$$

et finalement

$$9(0\ ,\ 0) = p - 8 + L \quad , \quad 9(1\ ,\ 2) = p + 1 + L \ ,$$

$$18(0\ ,\ 1) = 2p - 4 - L + 9M \ , \quad 18(0\ ,\ 2) = 2p - 4 - L - 9M \ .$$

En général, l'ordre des $[1/6(m^2 + 3m + 6)]$ nombres cyclotomiques d'ordre m distincts dépend du choix de la racine primitive g choisie, et les nombres premiers $p \equiv 1 \pmod m$ se groupent en classes d'équivalence, dépendant des $\mathrm{Ind}_g(d) \bmod m/d$ pour les diviseurs premiers d de m, avec des formules différentes pour les nombres premiers de chaque classe, dépendant aussi d'une éventuelle ambiguïté de signe. Une solution complète du type de celle cherchée par DICKSON a été trouvée pour $m \leqslant 12$ et $m = 16$, 20 ainsi que des solutions partielles d'autres valeurs de m.

(Pour les méthodes utilisées, voir [26], [27], [33], [22]).

D'autres exemples de système d'équations diophantiennes quadratiques sont donnés par ZEE [39].

En liaison avec la représentation explicite d'un nombre premier par une forme quadratique à l'aide de la cyclotomie, une importante équivalence entre condition de congruence sur les nombres de classes de corps quadratiques, condition de congruence sur les coordonnées de partitions quadratiques binaires, et critères de résiduation a été découverte par P. BARRUCAND ([2], [19], [20]).

2. Les sommes d'Eisenstein.

En 1848, EISENSTEIN représenta les nombres premiers de la forme $8n + 3$ par la forme $x^2 + 2y^2$, et ceux des formes $7n + 2$ et $7n + 4$ par la forme $x^2 + 7y^2$, à l'aide d'un nouveau type de sommes de racines de l'unité [11].

Soient, par exemple, $p = 8n + 3$, et s un non-reste quadratique de p. Alors $p(x) = x^2 - s$ est irréductible sur $\mathbb{F}_p$, et les restes $a + bx \bmod p(x)$, a et b parcourant $\mathbb{F}_p$, donnent une représentation du corps fini $\mathbb{F}_{p^2}$. Soit g un générateur du groupe cyclique $\mathbb{F}_{p^2}^{x}$.

La somme d'Eisenstein

$$E(a) = \sum_{b=0}^{p-1} \theta^{a\, \mathrm{Ind}_g(1+bt)} = \sum_{i=0}^{7} a_i\, \theta^{ai} \quad \text{avec} \quad \theta = \exp\left(\frac{2\pi i}{8}\right) \ ,$$

où $t^2 = s$ et où a_i est le nombre de valeurs de b dans $\mathbb{F}_p$, telles que $\mathrm{Ind}_g(1 + bt) \equiv i \pmod 8$, vérifie la relation

$$E(a)\ E(-a) = p \quad \text{si} \quad a \quad \text{impair.}$$

De $(1 + bt)^p = 1 - bt$, on déduit $\theta^{\mathrm{Ind}(1-bt)} = \theta^{pi} = \theta^{3i}$, d'où une bijection entre les nombres de la forme $1 + bt$ d'indice $\equiv i \pmod 8$ et ceux d'indice $\equiv pi \pmod 8$. De là

$$a_i = a_{3i} \quad \text{et} \quad E(1) = E(3)$$

et, avec

$$E(1) = a_0 - a_4 + (a_1 - a_5)\theta + (a_2 - a_6)\theta^2 + (a_3 - a_7)\theta^3$$

et $a_2 = a_6$, $a_1 = a_3$, $a_5 = a_7$, on trouve

$$E(1) = a_0 - a_4 + (a_1 - a_5)(\theta + \theta^3) = d_0 + d_1\sqrt{-2} ,$$

soit

$$p = d_0^2 + 2d_1^2 .$$

Les sommes d'Eisenstein étendues au corps fini $\underset{\sim}{F}_{p^f}$ ont été reliées par STICKELBERGER aux sommes de Gauss généralisées [30] . Pour $f = 2$, les analogues des nombres cyclotomiques d'ordre m s'expriment en fonction des coefficients de ces sommes. Ces coefficients ont des propriétés analogues aux coefficients des sommes de Jacobi, en particulier du type (19). On parvient à des partitions explicites de puissances de nombres premiers et à des congruences du type (20), mais les exposants sont en général supérieurs à $h(-m)$. Leur étude a été reprise récemment, en liaison avec le calcul des sommes de Brewer ([14], [27], [35]).

3. Les sommes de Jacobsthal et les sommes de Brewer.

Ce sont des sommes rationnelles de symboles de Legendre, à la différence des sommes de Gauss, de Jacobi, ou d'Eisenstein, qui sont en général irrationnelles. En 1906, JACOBSTHAL [17] obtint la représentation d'un nombre premier $p = 4n + 1$ sous la forme $u^2 + v^2$ à l'aide de la somme

$$\varphi_m(a) = \sum_{x=1}^{p-1} \left(\frac{x}{p}\right)\left(\frac{x^m + a}{p}\right) , \quad 1 \leqslant a \leqslant p - 1 ,$$

sous la forme

$$2u = \varphi_2(r) , \quad 2v = \varphi_2(n) ,$$

où r est un reste quadratique mod p , et n un non-reste. En posant $x = ay$, on a

$$\varphi_2(a^2 b) = \left(\frac{a}{p}\right) \varphi_2(b)$$

donc quand a parcourt $(1 , p - 1)$, $\varphi_2(a)$ ne prend que deux valeurs et

$$\sum_{a=1}^{p-1} \varphi_2(a)^2 = \frac{p - 1}{2} (\varphi_2(1)^2 + \varphi_2(g)^2) ,$$

où g est un non-reste quadratique. Par un calcul direct, on montre

$$\sum_{a=1}^{p-1} \varphi_2(a)^2 = 2p(p - 1) ,$$

d'où la partition cherchée. En appliquant le crotère d'Euler, on en tire la congruence

$$2u \equiv -\binom{2n}{n} \pmod{p}$$

déjà démontrée par GAUSS [13] par une autre méthode.

Les relations entre cyclotomie et sommes de Jacobsthal ont été étudiées par WHITEMAN ([31], [34], [35]). Ces sommes et des sommes analogues sont liées aux

coefficients des sommes de Jacobi. En particulier [31],

$$mB(i\ ,\ 1) = p - 1 + \varphi_m(4g^i) \quad \text{pour} \quad m \quad \text{impair},$$

où g est une racine primitive mod p. On obtient ainsi une solution du système diophantien de DICKSON pour m premier $m = 3$, 5 et le cas $m = 7$ vient d'être traité par P. A. LEONARD et K. S. WILLIAMS. Une solution élémentaire, pour $m = 7$, a été donnée par WILLIAMS [36].

Ces sommes permettent également l'étude de la répartition des restes quadratiques ([17], [29]).

Un autre type de somme rationnelle a été étudié par B. W. BREWER. Il utilise la suite de polynômes de permutation de DICKSON définie par

$$v_1(x\ ,\ Q) = x\ ,\quad v_2(x\ ,\ Q) = x^2 - 2Q$$
$$v_{n+2}(x\ ,\ Q) = xv_{n+1}(x) - Qv_n(x\ ,\ Q)$$

pour construire la somme de symboles de Legendre

$$\Lambda_n(Q) = \sum_{x=1}^{p-1} \left(\frac{v_n(x\ ,\ Q)}{p}\right).$$

Il calcule $\Lambda_n(1)$ pour $1 \leqslant n \leqslant 5$ dans [3] et $\Lambda_5(Q)$ dans [4] à l'aide de congruences entre coefficients du binôme liées à la formule (II), en fonction de coordonnées de partitions quadratiques. Ses résultats ont été obtenus par WHITEMAN à l'aide des sommes de Jacobi et d'Eisenstein [34], [35].

Ces sommes, quand elles sont non nulles, s'expriment comme combinaison linéaire de coordonnées de plusieurs partitions quadratiques simultanées de p. L'article [14] fait le point sur ces sommes et leurs relations avec les sommes de Jacobi et de Jacobsthal.

La bibliographie donne les articles importants ou récents sur la question.

BIBLIOGRAPHIE

[1] BACHMANN (P.). - Die Lehre von der Kreisteilung und ihre Beziehungen zur Zahlentheorie. 2te Auflage. - Leipzig, B. G. Teubner, 1921.

[2] BARRUCAND (P.) and COHN (H.). - Note on primes of type $x^2 + 32y^2$, class number, and residuacity, J. für reine und angew. Math., t. 238, 1969, p. 67-70.

[3] BREWER (B. W.). - On certain character sums, Trans. Amer. math. Soc., t. 99, 1961, p. 241-245.

[4] BREWER (B. W.). - On primes of the form $u^2 + 5v^2$, Proc. Amer. math. Soc., t. 17, 1966, p. 502-509.

[5] CAUCHY (A. L.). - Mémoire sur la théorie des nombres, "Oeuvres complètes", 1re série, t. 3, p. 5-83. - Paris, Gauthier-Villars, 1911.

[6] DAVENPORT (H.) und HASSE (H.). - Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen, J. für reine und angew. Math., t. 172, 1934, p. 151-182.

[7] DICKSON (L. E.). - History of the theory of numbers, vol. 3 : Quadratic and higher forms. - Washington, Carnegie Institution, 1923 (réimp. Chelsea, 1971).

[8] DICKSON (L. E.). - Cyclotomy, higher congruences, and Waring's problem, Amer. J. of Math., t. 57, 1935, p. 391-424 et p. 463-474.

[9] DICKSON (L. E.). - Cyclotomy and trinomial congruences, Trans. Amer. math. Soc., t. 37, 1935, p. 363-380.

[10] DICKSON (L. E.). - Cyclotomy when e is composite, Trans. Amer. math. Soc., t. 38, 1935, p. 187-200.

[11] EISENSTEIN (G.). - Zur Theorie der quadratischen Zerfällung der Primzahlen $8n + 3$, $7n + 2$, und $7n + 4$, J. für reine und angew. Math., t. 37, 1848, p. 97-126.

[12] GAUSS (C. F.). - Recherches arithmétiques, Traduites par Poullet-Delisle. - Paris, Courcier, 1807 (Réimp. A. Blanchard, 1953).

[13] GAUSS (C. F.). - Werke, t. 2. - Göttingen, Königliche Gesellschaft der Wissenschaften, 1863.

[14] GIUDICI (R. E.), MUSKAT (J. B.) and ROBINSON (S. F.). - On the evaluation of Brewer's character sums, Trans. Amer. math. Soc., t. 171, 1972, p. 317-347.

[15] HAYASHI (H.). - On a criterion for power residuacity, Mem. Fac. Sc., Kyushu Univ., Ser. A, t. 27, 1973, p. 211-220.

[16] JACOBI (C. G. J.). - Über die Kreisteilung und ihre Anwendung auf die Zahlentheorie, J. für reine und angew. Math., t. 30, 1846, p. 166-182 ; et "Gesammelte Werke", t. 6, p. 254-274. - Berlin, G. Reimer, 1891.

[17] JACOBSTHAL (E.). - Über die Darstellung der Primzahlen der Form $4n + 1$ als Summe zweier Quadrate, J. für reine und angew. Math., t. 132, 1907, p. 238-245.

[18] KUMMER (E. E.). - Über die Ergänzzungssätze zu den allgemeinen Reziprozitätsgesetzen, J. für reine und angew. Math., t. 44, 1852, p. 93-146.

[19] LEHMER (E.). - On the quadratic character of some quadratic surds, J. für reine und angew. Math., t. 250, 1971, p. 42-48.

[20] LEHMER (E.). - On the cubic character of quadratic units, J. of number theory, t. 5, 1973, p. 385-389.

[21] LEONARD (P. A.) and WILLIAMS (K. S.). - The septic character of 2, 3, 5 and 7, Pacific J. of Math., t. 52, 1974, p. 143-147.

[22] LEONARD (P. A.) and WILLIAMS (K. S.). - A diophantine system of DICKSON, Atti Accad. naz. dei Lincei, Rendiconti, vol. 56, 1974, p. 145-150.

[23] LIENEN (H. von). - Primzahlen als achte Potenzreste, J. für reine und angew. Math., t. 266, 1974, p. 107-117.

[24] MUSKAT (J. B.). - Reciprocity and Jacobi sums, Pacific J. of Math., t. 20, 1967, p. 275-280.

[25] MUSKAT (J. B.). - On Jacobi sums of certain composite orders, Trans. Amer. math. Soc., t. 134, 1968, p. 483-502.

[26] MUSKAT (J. B.) and WHITEMAN (A. L.). - The cyclotomic numbers of order twenty, Acta Arithmetica, Warszawa, t. 17, 1970, p. 185-216.

[27] MUSKAT (J. B.). - Use of computers in number theory, "Computers in number theory", Edited by A. O. L. Atkin and B. J. Birch, p. 141-147. - New York and London, Academic Press, 1971.

[28] MUSKAT (J. B.) and ZEE (Y. C.). - Sign ambiguities of Jacobi sums, Duke Math. J., t. 40, 1973, p. 313-334.

[29] SCHRUTKA (L. von). - Eine Beweis für die Zerlegbarkeit der Primzahlen von der Form $6n + 1$ in ein einfaches und ein dreifaches Quadrat, J. für reine und angew. Math., t. 140, 1911, p. 252-265.

[30] STICKELBERGER (L.). - Über eine Verallgemeinerung der Kreisteilung, Math. Annalen, t. 37, 1890, p. 321-367.

[31] WHITEMAN (A. L.). - Cyclotomy and Jacobsthal sums, Amer. J. of Math., t. 74, 1952, p. 89-99.

[32] WHITEMAN (A. L.). - Finite Fourier series and equations in finite fields, Trans. Amer. math. Soc., t. 74, 1953, p. 78-98.

[33] WHITEMAN (A. L.). - The cyclotomic numbers of order ten, "Combinatorial analysis", p. 95-111. - Providence, American mathematical Society, 1960 (Proceedings of Symposia in applied Mathematics, 10).

[34] WHITEMAN (A. L.). - Theorems on Brewer and Jacobsthal sums, I, "Theory of numbers", p. 44-55. - Providence, American mathematical Society, 1965 (Proceedings of Symposia in pure Mathematics, 8).

[35] WHITEMAN (A. L.). - Theorems on Brewer and Jacobsthal sums, II, Michigan math. J., t. 12, 1965, p. 65-80.

[36] WILLIAMS (K. S.). - Elementary treatment of a quadratic partition of primes $p \equiv 1 \pmod 7$, Illinois J. of Math., t. 18, 1974, p. 608-621.

[37] YAMAMOTO (K.). - On a conjecture of Hasse concerning multiplicative relations of Gaussian sums, J. Combin. Theory, t. 1, 1966, p. 476-489.

[38] YAMAMOTO (K.). - On Jacobi sums and difference sets, J. Combin. Theory, t. 3, 1967, p. 146-181.

[39] ZEE (Y. C.). - The Jacobi sums of orders thirteen and sixty and related quadratic decompositions, Math. Z., t. 115, 1970, p. 259-272.

[40] ZEE (Y. C.). - The Jacobi sums of order twenty-two, Proc. Amer. math. Soc., t. 28, 1971, p. 25-31.

(Texte reçu le 22 avril 1975)

Philippe BARKAN
16 avenue Marie-Juliette
92250 LA GARENNE COLOMBES