Séminaire Delange-Pisot-Poitou.
Théorie des nombres

JOHN H. LOXTON

On the determination of Gauss sums

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 18, n° 2 (1976-1977), exp. n° 27, p. 1-12

<http://www.numdam.org/item?id=SDPP_1976-1977__18_2_A8_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
18e année, 1976/77, n° 27, 12 p.

23 mai 1977

ON THE DETERMINATION OF GAUSS SUMS

by John H. LOXTON

1. The quadratic Gauss sum.

The classical Gauss sum is the sum

$$\tau_2 = \sum'_{r \bmod p} \left(\frac{r}{p}\right) \xi^r ,$$

where p is an odd prime, $\left(\frac{r}{p}\right)$ is the Legendre symbol, that is the unique quadratic character mod p, $\xi = \exp(2\pi i/p)$ is a normalised p-th root of unity and the dash denotes summation over a reduced set of residues mod p. We see at once that

$$\tau_2^2 = (-1)^{(p-1)/2} p . \tag{1}$$

For,

$$\tau_2^2 = \sum'_{r,s \bmod p} \left(\frac{rs}{p}\right) \xi^{r+s} = \sum'_{t \bmod p} \left(\frac{t}{p}\right) \sum'_{s \bmod p} \xi^{s(t+1)} ,$$

by means of the substitution $r \equiv st \pmod p$, and the inner sum is $p-1$ if $t \equiv -1 \pmod p$ and -1 otherwise, which gives (1).

Thus, τ_2 is determined up to sign. The particular normalisation $\xi = \exp(2\pi i/p)$ makes τ_2 a definite complex number which GAUSS found by experiment to be given by the formula

$$\tau_2 = \begin{cases} p^{\frac{1}{2}} & \text{if } p \equiv 1 \pmod 4 \\ ip^{\frac{1}{2}} & \text{if } p \equiv -1 \pmod 4 , \end{cases} \tag{2}$$

where $p^{\frac{1}{2}}$ denotes the positive square root. Four years later, GAUSS [6] also gave a proof. The idea, which appears more clearly in a later proof of CAUCHY [3], is to consider the product

$$\sigma_2 = \prod_{r=1}^{(p-1)/2} (\xi^{2r-1} - \xi^{-2r+1}) .$$

Now,

$$\sigma_2^2 = (-1)^{(p-1)/2} \prod'_{r \bmod p} (\xi^r - \xi^{-r}) = (-1)^{(p-1)/2} p ,$$

since the product is just the value of the cyclotomic polynomial of order p at 1, so that

$$\sigma_2 = \pm \tau_2 . \tag{3}$$

In fact,

$$\sigma_2 = \tau_2 . \tag{4}$$

The difficult step is to settle the ambiguity of sign in (3) because, once that is done, the sign of σ_2 is easily determined by writing it in the form

$$\sigma_2 = (2i)^{(p-1)/2} \prod_{r=1}^{(p-1)/2} \sin 2\pi(2r - 1)/p ,$$

and simply counting the number of negative factors in the product. To prove (4), and so settle the determination of τ_2, we can use congruence considerations. The prime p is completely ramified in $Q(\xi)$ and, if $\lambda = 1 - \xi$, we have the prime ideal factorisation $[p] = [\lambda]^{p-1}$. Now, on the one hand, $(\frac{r}{p}) \equiv r^{(p-1)/2} \pmod p$, so

$$\tau_2 \equiv \sum_{r \bmod p} r^{(p-1)/2} (1 - \lambda)^r$$
$$= \sum_{s=0}^{(p-1)/2} (-\lambda)^s \sum_{r \bmod p} r^{(p-1)/2} \binom{r}{s} \pmod{\lambda^{(p+1)/2}} .$$

Here, we observe that $\sum_{r \bmod p} r^n$ is 0 or $-1 \pmod p$ according as $(p-1) | n$ or not, so that only the term $s = (p - 1)/2$ contributes to the sum. By Wilson's theorem, the result is

$$\tau_2 \equiv (\tfrac{p - 1}{2})! \, \lambda^{(p-1)/2} \pmod{\lambda^{(p+1)/2}} .$$

On the other hand, by similar arguments,

$$\xi^{2r-1} - \xi^{-2r+1} = - \xi^{-2r+1} \{1 - \xi^{2(2r - 1)}\} \equiv - 2(2r - 1)\lambda \pmod{\lambda^2} ,$$

so

$$\sigma_2 \equiv \prod_{r=1}^{(p-1)/2} \{- 2(2r - 1)\lambda\} \equiv (\tfrac{p - 1}{2})! \, \lambda^{(p-1)/2} \pmod{\lambda^{(p+1)/2}}$$

and this is enough to prove (4) (Cf. HASSE [8], section 20.5).

There are a large number of proofs of (2) in the literature (Cf. CASSELS [2]). However, the one sketched above has been the most fruitful in suggesting extensions of the results for τ_2 to generalised Gauss sums.

2. Generalised Gauss sums.

A. Notation.

Let χ be a Dirichlet character with conductor q, say. If m is a multiple of q, then χ induces a character mod m which we denote by χ_m. The generalised Gauss sum is a sum of the shape

$$(5) \qquad \sum'_{r \bmod m} \chi_m(r) \exp(2\pi i a r/m) ,$$

where the sum is taken over a reduced set of residues mod m. Elementary manipulations rapidly enable us to express the sum (5) in terms of the primitive Gauss sum

$$\tau(\chi) = \sum'_{r \bmod q} \chi(r) \exp(2\pi i r/q)$$

(HASSE [8], Chapter 20, gives a systematic discussion). By means of the change of variable $s \equiv cr \pmod q$, we get the useful fact

$$(6) \qquad \sum_{r \bmod q} \chi(r) \exp(2\pi i c r/q) = \overline{\chi}(c) \sum_{r \bmod q} \chi(r) \exp(2\pi i r/q)$$

(this is actually valid when $(c , q) > 1$ because both sides are zero).

B. Prime power conductor.

Further reduction, via the Chinese remainder theorem, shows that we need only consider Gauss sums whose conductor is a prime power, p^ν say. ODONI [18] has shown that the case $\nu > 1$ can be completely settled. I illustrate the method, take p to be an odd prime and let χ be a primitive character mod p^ν with $\nu > 1$. Then $\chi(1 + p)$ must be a $p^{\nu-1}$-th root of unity, say

$$\chi(1 + p) = \exp(- 2\pi i a/p^{\nu-1}) .$$

In the Gauss sum $\tau(\chi)$, we write $r \equiv s(1 + tp^{\nu-1}) \pmod{p^\nu}$, giving

$$\tau(\chi) = \sum_{s \bmod p^{\nu-1}} \chi(s)\, \xi^s \sum_{t \bmod p} \chi(1 + tp^{\nu-1}) \exp(2\pi i s t/p) .$$

Now, $\chi(1 + tp^{\nu-1}) = \exp(- 2\pi i a t/p)$, so the inner sum is 0 unless $s \equiv a \pmod p$, whence

$$\tau(\chi) = p \sum_{s \bmod p^{\nu-1}, s \equiv a \pmod p} \chi(s)\, \xi^s$$

$$= p\, \chi(a)\, \xi^a \sum_{u \bmod p^{\nu-2}} \chi(1 + up)\, \xi^{aup} ,$$

where we have written $s \equiv a(1 + up) \pmod{p^{\nu-1}}$.

In particular, if $\nu = 2$, the last sum is trivial, and we get

$$\tau(\chi) = p\, \chi(a)\, \xi^a .$$

The formulae in the general case are more complicated, but still reasonably explicit.

C. Prime conductor.

There remains the problem of evaluating Gauss sums with odd prime conductor, p say. This subject remains rather mysterious, but we can make some general remarks. If χ, ψ are Dirichlet characters mod p, we define the Jacobi sum

$$\pi(\chi, \psi) = \sum_{r+s \equiv 1 \pmod p} \chi(r)\, \psi(s) . \tag{7}$$

If none of χ, ψ, $\chi\psi$ is the principal character mod p, then manipulation of the double sum for $\tau(\chi\psi)\, \pi(\chi, \psi)$ gives the identity

$$\pi(\chi, \psi) = \frac{\tau(\chi)\, \tau(\psi)}{\tau(\chi\psi)} . \tag{8}$$

Suppose now that the character χ has order k. Then

$$\tau(\chi)\, \tau(\chi) = \pi(\chi, \chi)\, \tau(\chi^2) ,$$

$$\tau(\chi)\, \tau(\chi^2) = \pi(\chi, \chi^2)\, \tau(\chi^3) ,$$

$$\tau(\chi)\, \tau(\chi^{k-1}) = \tau(\chi)\, \tau(\overline{\chi}) = \chi(- 1)\, |\tau(\chi)|^2 = \chi(- 1)\, p .$$

By telescoping these equations together, we get

$$\tau(\chi)^k = \chi(- 1)\, p\, \pi(\chi, \chi)\, \pi(\chi, \chi^2) \ldots \pi(\chi, \chi^{k-2}) ,$$

that is, $\tau(\chi)^k = \omega(\chi)$, say, is in $Q(\exp(2i\pi/k))$. We can regard this as the analogue of (1). The problem then is to determine which of the k-th roots of $\omega(\chi)$ is $\tau(\chi)$. Only the cases $k = 3$ and 4 have received much attention, and we shall examine them in the remainder of this report. Some remarks on larger values of k , mainly of an experimental nature, are made by LEHMER [13].

3. The cubic Gauss sum.

A. Kummer's conjecture.

Let p be a prime with $p \equiv 1 \pmod 3$, and let $\omega = (-1 + \sqrt{-3})/2$ be a cube root of unity. By factorising p in $Q(\omega)$, we see that we can write

$$4p = a^2 + 27b^2 , \tag{9}$$

where a and b are rational integers determined uniquely by the additional requirements

$$a \equiv 1 \pmod 3 , \quad b > 0 .$$

Let $\varpi = (a + 3b\sqrt{-3})/2$ be one of the prime divisors of p in $Q(\omega)$, and define a cubic character on $Z[\omega]$ mod ϖ by

$$\chi(\alpha) \equiv \alpha^{(p-1)/3} \pmod{\varpi} .$$

This induces a character on Z mod p . The Kummer sum, or cubic Gauss sum, is

$$\tau_3 = \sum_{r \bmod p} \chi(r)\, \xi^r ,$$

where $\xi = \exp(2\pi i/p)$ as before. GAUSS [5], article 358, showed that

$$\tau_3^3 = p\varpi . \tag{10}$$

To prove this, we note that $\tau_3 \overline{\tau}_3 = p$ and

$$\tau_3^2 = \sum_{r,s \bmod p} \chi(rs)\, \xi^{r+s} = \sum_{s,t \bmod p} \chi(s^2 t)\, \xi^{s(t+1)}$$

$$= \overline{\tau}_3 \sum_{t \bmod p} \chi(t)\, \chi(t+1) = \overline{\tau}_3\, \alpha ,$$

say, so that $\tau_3^3 = p\alpha$, and α is one of the prime divisors of p in $Q(\omega)$. To identify α with ϖ , we observe that $\alpha \equiv 0 \pmod{\varpi}$, by calculating τ_3 modulo the prime divisor of ϖ in $Q(\omega, \xi)$, and that $\alpha \equiv -1 \pmod 3$, since

$$\tau_3^3 = p\alpha \equiv \sum\nolimits'_{r \bmod p} \xi^{3r} = -1 \pmod 3 .$$

(In fact, these remarks give another proof of the decomposition (9).)

From (10), τ_3 is determined up to a cube root of unity, and the problem apparently first pointed out by KUMMER [11] and V.-A. LEBESGUE [12] is to determine τ_3 itself. For a given prime p , there are just three possibilities, namely

$$|\arg \tau_3| < \pi/3 , \qquad \pi/3 < |\arg \tau_3| < 2\pi/3 , \qquad 2\pi/3 < |\arg \tau_3| < \pi .$$

KUMMER [11] investigated the 45 cases with $p < 500$ and found the relative frequencies 3 : 2 : 1 for these three possibilities. GOLDSTINE and von NEUMANN [7]

investigated $p < 10000$ and found these ratios to be $4 : 3 : 2$, which may be suggestive to a numerologist since $2 + 3 + 4 = 3^2$. However, LEHMER [13] and CASSELS [1] have extended the range of the experiments and report a continuing trend towards randomness. A propos of this, MORENO [17] has recently shown that the argument of τ_3^3 is uniformly distributed in the three intervals listed above. If we drop the normalisation $b > 0$ made above, and so define the Kummer sum mod ϖ for each first degree prime $\varpi \equiv -1 \pmod 3$ in $Q(\omega)$, then MORENO's observation is that the symbol $\exp(i\theta(\varpi)) = p^{-3/2}\,\tau_3^3$ is a Grossenchakter in $Q(\omega)$ and so, by the Hecke theory of L-functions,

$$\sum_{N\varpi \leqslant X} \exp(in\theta(\varpi)) = o\left(\frac{X}{\log X}\right)$$

as $X \longrightarrow \infty$, for each integer n, and this is equivalent to the uniform distribution of τ_3^3. There is now some theoretical evidence for the uniform distribution of τ_3, to be described in the next paragraph. However, these statistical results are almost certainly not the whole truth. The real goal should be a formula for τ_3 like Gauss's formula (1) for τ_2, but no-one has yet been able to guess what such a formula might be, let alone to prove one.

B. Application of some ideas from the theory of automorphic functions.

In several papers, for example [9] and [10], KUBOTA has indicated a method for obtaining some asymptotic results on the distribution of Gauss sums. For Kummer sums, this arises as follows. Let $\left(\frac{a}{b}\right)_3$ be the cubic residue symbol in $Q(\omega)$, and set $\Gamma = \{ \gamma \text{ in } SL_2(Z[\omega]) \; ; \; \gamma \equiv I \pmod 3 \}$.

For $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in Γ, define

$$\psi(\gamma) = \left(\frac{c}{a}\right)_3 \text{ if } c \neq 0, \qquad \psi(\gamma) = 1 \text{ if } c = 0.$$

By using the law of cubic reciprocity, we find that ψ is a character on Γ. The group Γ acts discontinuously on the upper half-space $H = C \times R_+^{\times}$ as follows. We represent a point $u = (z, v)$ in H by the matrix

$$u = \begin{pmatrix} z & -v \\ v & \overline{z} \end{pmatrix}$$

and, for w in C, we write

$$\tilde{w} = \begin{pmatrix} w & 0 \\ 0 & \overline{w} \end{pmatrix}.$$

Then the action of Γ on H is given by

$$\gamma(u) = (\tilde{a}u + \tilde{b})(\tilde{c}u + \tilde{d})^{-1}, \qquad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Following SELBERG, we introduce the Eisenstein series corresponding to the cusp ∞:

$$E(u, s) = \sum_{\gamma \text{ in} \Gamma_\infty \backslash \Gamma} \overline{\psi(\gamma)}\, v(\gamma(w))^s \qquad (\mathrm{re}\ s > 2),$$

where $\Gamma_\infty = \{\gamma \text{ in } \Gamma \ ; \ \gamma^\infty = \infty\}$ and, for $u = (z \ , \ v)$ in H, we have written $v = v(u)$. It follows from Selberg's general theory [21] that $E(u \ , \ s)$ has a meromorphic continuation to the whole s-plane. If we complement $E(u \ , \ s)$ by three further Eisenstein series corresponding to the remaining inequivalent essential cusps, then there is a functional equation connecting s and $2 - s$. On forming the Fourier expansion of $E(u \ , \ s)$ with respect to Γ_∞, we find that the coefficients are Dirichlet series satisfying similar functional equations and whose coefficients are Kummer sums. The theory shows that these Dirichlet series are regular in the half-plane $\text{re } s > 4/3$. In particular, the regularity at $s = 3/2$ together with a well-known tauberian theorem gives

$$\sum_{\text{Norm}\alpha \leqslant X} \tau_3/|\tau_3| = o(X) \qquad (X \longrightarrow \infty)$$

(In the sum, α runs through all integers $\equiv 1 \pmod 3$ in $\mathbb{Z}[\omega]$ and τ_3 is the Kummer sum mod α defined by

$$\tau_3 = \sum_{r \bmod \alpha} \left(\frac{r}{\alpha}\right)_3 \exp\{\pi i \text{tr}(r/\alpha)\} \ .)$$

The theory has recently been reworked and refurbished in the cubic case by PATTERSON [19]. He shows inter alia that if we take Kummer sums mod α for any integer $\alpha \equiv 1 \pmod 3$ in $\mathbb{Z}[\omega]$, then indeed their arguments are uniformly distributed round the circle. Moreover, theory and experiment suggest the asymptotic formula

$$\sum_{p \leqslant X} \text{re}\{\tau_3/|\tau_3|\} \sim \frac{(2\pi)^{2/3}}{5\Gamma(2/3)} \frac{X^{5/6}}{\log X} \qquad (X \longrightarrow \infty) \ .$$

This formula comes from an attempt to apply the Hardy-Littlewood circle method, but the contributions from the minor arcs cannot at present be satisfactorily estimated. The same difficulty obstructs the proof of the assertion, almost certainly true, that the argument of τ_3, as p runs through the primes congruent to $1 \pmod 3$, is uniformly distributed round the circle.

C. An elementary product related to the Kummer sum.

I turn now to two attempts to construct cubic analogues to the product σ_2. The first idea goes back to CAUCHY [3]. We choose a rational integer q with $q \equiv \omega \pmod{\varpi}$ and a third set $\mathfrak{S}$ of residues mod p, that is $\mathfrak{S}$ consists of $(p - 1)/3$ rational integers and the numbers r, qr, $q^2 r$ (r in $\mathfrak{S}$) form a reduced set of residues mod p. Set

$$\sigma_3 = \prod_{r \text{ in } \mathfrak{S}} (\xi^r + \omega\xi^{qr} + \omega^2 \xi^{q^2 r}) \ .$$

This is not yet quite satisfactory since σ_3 depends on the particular choice of the third set $\mathfrak{S}$. However, by Wilson's theorem

$$(\prod_{r \text{ in } \mathfrak{S}} r)^3 \equiv -1 \pmod{\varpi} \ ,$$

so we have

(11) $$\prod_{r \text{ in } \mathfrak{S}} r \equiv -\Omega \pmod{\varpi}$$

for some cube root Ω of unity. We therefore consider the normalised product

$$P_3 = \Omega \sigma_3 ,$$

which is independent of the choice of $\mathfrak{S}$. It is easy to see that a typical automorphism $\xi \longrightarrow \xi^t$ of $Q(\omega, \xi)/Q(\omega)$ sends P_3 to $\overline{\chi}(t) P_3$, that is P_3 transforms in the same way as the Gauss sum τ_3. So we have $P_3 = \alpha\tau_3$ for some integer α in $Q(\omega)$. This idea was rediscovered by RESHETUKHA [20], and he found, by experiment, the curious fact that for all primes $p < 6000$, the number P_3^3 lies in the upper half-plane. (Of course, this observation depends on the normalisation of ϖ, which we have taken to lie in the upper half-plane.) This turned out to be not quite the right conjecture since more exact calculations suggested that

(12) $$\arg(-\varpi P_3^3) = O(p^{-\frac{1}{2}+\varepsilon}) \qquad (p \longrightarrow \infty) .$$

In view of (10), we can consider (12) to be an analogue of the elementary equation $\sigma_2^2 = \tau_2^2$ in the quadratic case (Cf. (3)). In fact, (12) is true, so it is only natural to ask whether the present situation contains an analogue of the deeper equation (4). On the basis of numerical evidence from the primes $p < 5000$, I make the following conjecture :

CONJECTURE 1 [15]. - $\arg(-\chi(3)\, \tau_3\, P_3) \longrightarrow 0$ as $p \longrightarrow \infty$.

Observe, incidentally, that because of our normalisation, $\chi(3) = \omega^{-b}$ is an elementary quantity. The proof of (12), asserted above is a somewhat more elaborate version of the argument sketched in paragraph 4.B (See [14] and the correction noted in [15]). Unfortunately, this analysis is not adequate for dealing with the product P_3 itself.

D. A non-elementary product.

Another product related to the Kummer sum has been proposed by CASSELS [2]. The elliptic curve $y^2 = 4x^3 - 1$ is parametrised over C by the Weierstrass elliptic functions $x = \wp(z)$, $y = \wp'(z)$ with periods $\theta\, Z[\omega]$, where $\theta = 3.0599\ldots$ is the smallest real period. From the equation for the ϖ-division points on the curve, we find

$$\prod_{r=1}^{p-1} \wp\left(\frac{\theta r}{\varpi}\right) = \frac{1}{\varpi^2} .$$

Let $\mathfrak{S}$ be a third set of residues mod ϖ as before, and set

$$P = \Omega^{-1} \prod_{r \text{ in } \mathfrak{S}} \wp\left(\frac{\theta r}{\varpi}\right) ,$$

where Ω is the normalising cube root of unity given by (11). Then $P^3 = 1/\varpi^2$, using the complex multiplication $\wp(\omega z) = \omega\, \wp(z)$ on the curve, and from (10),

$$\tau_3 = \varepsilon p^{1/3} \varpi P ,$$

where ε is one of the cube roots of unity. CASSELS gives the following conjecture for the determination of ε, valid by computation for $p < 5000$:

CONJECTURE 2 [2]. - $\tau_3 = p^{1/3}\,\varpi P$.

The conjecture can be put into an equivalent form which may be amenable to a p-adic attack along the lines of the proof of (4) in section 1. Such an approach leads to a problem about points of finite order on the elliptic curve $y^2 = 4x^3 - 1$ over a field of characteristic p, but does not at the moment seem to be tractable.

4. The quartic Gauss sum.

A. A conjecture for the value of the Gauss sum.

Let p be a prime with $p \equiv 1 \pmod 4$. Then we can write $p = a^2 + b^2$ where a and b are rational integers determined uniquely by the normalisations

$$a \equiv 1 \pmod 4 , \qquad b \equiv -\left(\frac{p-1}{2}\right)! \, a \pmod p .$$

Let $\varpi = a + ib$ be one of the prime divisors of p in $Q(i)$ and define a quartic character χ on Z mod p by

$$\chi(\alpha) \equiv \alpha^{(p-1)/4} \pmod{\varpi} .$$

The quartic Gauss sum is

$$\tau_4 = \sum_{r=1}^{p-1} \chi(r)\, \xi^r ,$$

where $\xi = \exp(2\pi i/p)$, as before. In this case, we have

$$\tau_4^2 = - p^{\frac{1}{2}}\, \varpi . \tag{14}$$

To see this, we compute

$$\tau_4^2 = \sum_{t=1}^{p-1} \chi(t) \sum_{s=1}^{p-1} \left(\frac{s}{p}\right) \xi^{s(t+1)} = p^{\frac{1}{2}} \sum_{t=1}^{p-1} \chi(t) \left(\frac{t+1}{p}\right) = p^{\frac{1}{2}}\, \alpha ,$$

say. Put $\alpha = A + iB$. Now $\alpha \equiv 0 \pmod{\varpi}$, $\alpha \equiv 1 \pmod 2$ and

$$A = \sum_{s=1}^{(p-1)/2} \left(\frac{s}{p}\right)\left(\frac{s^2+1}{p}\right) = \sum_{s=1}^{(p-1)/2} \left(\frac{s}{p}\right)\left\{\left(\frac{s^2+1}{p}\right) - 1\right\} = \left(\frac{q}{p}\right) \sum_{s=1}^{(p-1)/2} \left(\frac{s}{p}\right)\left\{\left(\frac{s^2-1}{p}\right) - 1\right\}$$

where q satisfies $q^2 \equiv -1 \pmod p$ and the last step results on replacing s by qs in the sum. The above is congruent mod 4 to

$$\left(\frac{q}{p}\right) \sum_{s=1}^{(p-1)/2} \left\{\left(\frac{s^2-1}{p}\right) - 1\right\} = -\left(\frac{q}{p}\right) \frac{p+1}{2} \equiv -1 \pmod 4 ,$$

so, finally, $\alpha = -\varpi$. This argument also gives the congruence

$$a \equiv -\frac{1}{2} \binom{(p-1)/2}{(p-1)/4} \pmod p . \tag{15}$$

Again, τ_4 is determined up to sign. Computations for $p < 5000$ indicate the following conjecture :

CONJECTURE 3 [15]. - $\tau_4 = i\,\chi(2i)\,(\frac{2|b|}{|a|})\,p^{1/4}\,\varpi^{1/2}$.

Here, $\varpi^{1/2}$ denotes the principal square root, and $p^{1/4}$ denotes the positive fourth root. In addition, we remark that $\chi(2) = i^{b/2}$ and $\chi(i) = i^{(p-1)/4}$. The simplicity of the formula is rather unexpected.

B. Reformulation of the conjecture in terms of an elementary product.

We can reformulate the conjecture in terms of a trigonometric product along the lines of conjecture 1 ; this will serve to explain how the conjecture was found. A naive approach, similar to that in paragraph 3.C, leads us to examine the product

$$\sigma_4 = \prod_{r \text{ in } \mathfrak{S}} (\xi^r + i\xi^{qr} - \xi^{-r} - i\xi^{-qr}) ,$$

where q is a rational integer with $q \equiv i \pmod{\varpi}$, that is $q \equiv -(\frac{p-1}{2})! \pmod{p}$, and $\mathfrak{S}$ is a fourth set of residues mod p . To fix the notation, we choose $\mathfrak{S}$ so that the absolutely least residues mod p of r and qr for each r in $\mathfrak{S}$ are positive. It is easy to see that replacing ξ by ξ^t with $1 \leqslant t \leqslant p-1$ takes σ_4 to $\overline{\chi}(t)\,\sigma_4$. In particular, if we replace ξ by ξ^a and then by ξ^{aq} in σ_4 and multiply the resulting expressions together, observing that $(\frac{a}{p}) = 1$ by (15), we get

$$\sigma_4^2 = 2^{(p-1)/2}\,(-i)^{(p-1)/4} \prod_{r=1}^{(p-1)/2} (\sin\frac{2\pi ar}{p} + i \sin\frac{2\pi br}{p}) .$$

It is convenient to put

$$P_4 = \prod_{r=1}^{(p-1)/2} (\sin\frac{2\pi ar}{p} + i \sin\frac{2\pi br}{p}) .$$

Now, we have $\sigma_4 = \alpha\tau_4$ for some integer α in $Q(i)$, so as a first step we might seek some connection between σ_4^2 and τ_4^2 , that is, between P_4 and ϖ . Again, experiments do not reveal quite what we expect, but rather that $\arg(\varpi P_4^2) \to 0$ as $p \to \infty$. Now that we know what to look for, it becomes possible to prove that

$$\arg((\frac{2|b|}{|a|})\,\varpi^{\frac{1}{2}}\,P_4) = O(p^{-1+\varepsilon}) \tag{16}$$

as $p \to \infty$ for any $\varepsilon > 0$. We can therefore give an equivalent form of conjecture 3 :

CONJECTURE 4 [15]. - $\arg(-i\,\chi(2i)\,\tau_4\,P_4) \longrightarrow 0$ as $p \to \infty$.

To prove (16), we proceed as follows. Write

$$F(t) = \sin\frac{2\pi at}{p} + i \sin\frac{2\pi bt}{p} ,$$

and define $G(t)$ to be a continuous branch of the argument of $F(t)$ for $0 \leqslant t \leqslant p/2$, normalised so that $G(p/4) = 0$. Observe that

$$G(\tfrac{p}{2} - t) = - G(t) \quad (0 < t < \tfrac{p}{2}) , \qquad G(0+) = \arg \varpi - 2k\pi ,$$

for some integer k . Now, by a version of the Euler-MacLaurin sum formula,

$$\arg P_4 \equiv \sum_{r=1}^{(p-1)/2} G(r) = \int_0^{p/2} G(t)\, dt - \tfrac{1}{2} G(0+) + R \pmod{2\pi}$$

with an appropriate error term R . By taking advantage of some fortuitous cancelletation, we can show that $R = O(p^{-1+\varepsilon})$ for any $\varepsilon > 0$, so we have

$$\arg P_4 = - \tfrac{1}{2} \arg \varpi + k\pi + O(p^{-1+\varepsilon}) .$$

In order to compute k , we define the n-th branch of $\arg F(t)$ to correspond to the range $-\pi + 2n\pi < \arg F(t) \leqslant \pi + 2n\pi$. Now k is just the change in branch number of $\arg F(t)$ as t goes from 0 to $p/4$. But $\arg F(t)$ changes branch when $\sin(2\pi bt/p) = 0$ and $\sin(2\pi at/p) < 0$, so $k \bmod 2$ is the number of integers ℓ with $0 < \ell < |b|/2$ and $\sin(\pi a\ell/|b|) < 0$. If we assume for the moment that a and b are positive, then we get

$$k \equiv [\tfrac{2b}{a}] - [\tfrac{b}{a}] + [\tfrac{4b}{a}] - [\tfrac{3b}{a}] + \ldots + [\tfrac{(a-1)b}{2a}] - [\tfrac{(a-3)b}{2a}] \equiv \sum_{\ell=1}^{(a-1)/2} [\tfrac{\ell b}{a}] \pmod{2} ,$$

so in this case, $(-1)^k = (\frac{2|b|}{|\cdot|})$. An identical calculation shows that this result continues to hold for any disposition of the signs of a and b . This proves our assertion.

C. Concluding remarks.

McGETTRICK [16] has found an analogue of Cassels'conjecture 2 for the quartic case. Set

$$\theta = 4 \int_0^1 \frac{dt}{\sqrt{(1 - t^4}} = \frac{\Gamma(1/4)^2}{\sqrt{2\pi}}$$

and let $\varphi(z)$ be the lemniscate function, that is the solution of $\varphi'(z)^2 = 1 - \varphi(z)^4$ with $\varphi(z/4) = 1$. Thus $\varphi(z)$ is a doubly periodic function with period lattice $\theta\, \mathbb{Z}[i]$ and has the complex multiplication $\varphi(iz) = i\, \varphi(z)$. In the course of proving quartic reciprocity, EISENSTEIN [4] showed that the product of the ϖ-division points of $\varphi(z)$ is

$$\prod_{r \bmod \varpi} \varphi(\tfrac{r\theta}{\varpi}) = (-1)^{(p-1)/4}\, \varpi .$$

Consequently, if we set

$$P = \prod_{r=1}^{(p-1)/2} \varphi(\tfrac{r\theta}{\varpi}) ,$$

then $P^2 = (-1)^{(p-1)/4}\, \varpi$. Comparing this with (14), we have $\tau_4\, P = \varepsilon p^{1/4}\, \varpi$ for some fourth root ε of unity. On the basis of computation for $p < 5700$, ε is given as follows :

CONJECTURE 5 (after McGETTRICK [16]). - $\tau_4\, P = - \overline{\chi}(-2)\, \varpi p^{1/4}$.

As remarked in paragraph 3.D, there is a p-adic reformulation of the conjecture

involving the ϖ- and $\bar{\varpi}$-division points on the elliptic curve $y^2 = 1 - x^4$. There is also another possible p-adic approach to conjectures 3 and 5 using ideas of YAMAMOTO [22]. He starts with the Kronecker class number formula

$$p^{1/2}\ \varepsilon^{-h} = \prod_{(\frac{r}{p})=1} (\xi^r - 1)\ ,$$

where h is the class number and ε is the fundamental unit of $Q(\sqrt{p})$. The product has a canonical square root and, by comparing signs, we find that

$$p^{1/4}\ \varepsilon^{-h/2} = i^{((p-1)/2)^2}\ \overline{\chi}(-2i) \prod_{r \text{ in } R} (\xi^{2r} - \xi^{-2r})\ ,$$

where R is the set of quadratic residues in the set $\{1, 2, \ldots, (p-1)/2\}$. Using this and some further lemmas from YAMAMOTO, we can reduce conjecture 3 p-adically, giving yet another conjecture involving h and quantities connected with the simple continued fraction expansion of $\sqrt{p}$.

REFERENCES

[1] CASSELS (J. W. S.). - On the determination of generalised Gauss sums, Archiv. Math., Brno, t. 5, 1969, p. 79-84.

[2] CASSELS (J. W. S.). - On Kummer sums, Proc. London math. Soc., Series 3, t. 21, 1970, p. 19-27.

[3] CAUCHY (A). - Méthode simple et nouvelle pour la détermination complète des sommes alternées formées avec les racines primitives des équations binômes, J. de Math. pures et appl., Série 1, t. 5, 1840, p. 154-168.

[4] EISENSTEIN (G.). - Beitrage zur Theorie der elliptischen Functionen, I : Ableitung des biquadratischen Fundamentaltheorems aus der Theorie der Lemniskatenfunctionen, nebst Bemerkungen zu den Transformationsformeln, J. reine und angew. Math., t. 30, 1846, p. 185-210.

[5] GAUSS (C. F.). - Disquisitiones Arithmeticae.-Lipsiae, G. Fleischer, 1801.

[6] GAUSS (C. F.). - Summatio quarundarum serierum singularium, Commentationes societatis regiae Gottingensis recentiores, Band 1, 1811.

[7] GOLDSTINE (H.) and von NEUMANN (J.). - A numerical study of a conjecture of Kummer, Math. of Comp., t. 7, 1953, p. 133-134.

[8] HASSE (H.). - Vorlesungen über Zahlentheorie. 2nd ed. — Berlin, Springer-Verlag, 1964.

[9] KUBOTA (T.). - On a special kind of Dirichlet series, J. Math. Soc. Japan, t. 20, 1968, p. 193-207.

[10] KUBOTA (T.). - Some results concerning reciprocity law and real automorphic functions, "1969 Number theory institute", p. 382-395. - Providence, American mathematical Society, 1971 (Proceedings of Symposia in pure Mathematics, 20).

[11] KUMMER (E. E.). - De residuis cubicis disquisitiones nonnullae analyticae, J. reine und angew. Math., t. 32, 1846, p. 341-359.

[12] LEBESGUE (V.-A.). - Sommation de quelques séries, J. de Math. pures et appl., Série 1, t. 5, 1840, p. 42-71.

[13] LEHMER (E.). - On the location of Gauss sums, Math. of Comp., t. 10, 1956, p. 194-202.

[14] LOXTON (J. H.). - Products related to Gauss sums, J. reine und angew. Math., t. 268/269, 1974, p. 53-67.

[15] LOXTON (J. H.). - Some conjectures concerning Gauss sums, J. reine und angew. Math. (to appear).

[16] McGETTRICK (A. D.). - On the biquadratic Gauss sum, Proc. Camb. phil. Soc., t. 71, 1972, p. 79-83.

[17] MORENO (C. J.). - Sur le problème de Kummer, Enseign. Math., t. 20, 1974, p. 45-51.

[18] ODONI (R. K.). - On Gauss sums (mod p^n) , $n \geqslant 2$, Bull. London math. Soc., t. 5, 1973, p. 325-327.

[19] PATTERSON (S. J.). - A cubic analogue of the theta series, J. reine und angew. Math. (to appear).

[20] RESHETUKHA (I. V.). - A problem in the theory of cubic sums, Mat. Zametki, t. 7, 1970, p. 469-476.

[21] SELBERG (A.). - Discontinuous groups and harmonic analysis, "Proceedings of the international Congress of mathematicians [1962. Stockholm]", p. 177-189. - Djursholm, Institut Mittag-Leffler, 1963.

[22] YAMAMOTO (K.). - On Gaussian sums with biquadratic residue characters, J. reine und angew. Math., t. 219, 1965, p. 200-213.

(Texte reçu le 3 juin 1977)

John H. LOXTON
School of Mathematics
University of New South Wales
KENSINGTON, Sydney, NSW 2033
(Australie)