J. W. S. Cassels

On the determination of generalized Gauss sums

Archivum Mathematicum, Vol. 5 (1969), No. 2, 79--84

Persistent URL: http://dml.cz/dmlcz/104683

ON THE DETERMINATION OF GENERALIZED GAUSS SUMS

By J. W. S. CASSELS

To Professor O. BORŮVKA for his 70th birthday

(Received February 12, 1969)

The sums with which we are concerned are of the type

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

where $p > 2$ is a rational prime, ξ is a primitive p-th root of unity and χ is a character on the multiplicative group of integers modulo p.

The ordinary Gauss sum τ_2 is the special case in which $\chi = \chi_2$ is the quadratic residue character. It is easy to see that

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

When p is normalized analytically, say

$$\xi = \mathrm{e}^{2\pi i/p}, \tag{3}$$

Gauss [2] proved that

$$\begin{cases} \tau_2 = p^{1/2}\, [p \equiv 1 \pmod 4], \\ \tau_2 = ip^{1/2}\, [p \equiv 3 \pmod 4] \end{cases} \tag{4}$$

where $p^{1/2}$ is the positive square root, a result which he had conjectured many years previously from the numerical evidence [...demonstrationem rigorosam huius elegantissimi theorematis, per plures annos olim variis modis incassum tentatum, tandemque per considerationes singulares satisque subtiles feliciter perfectam... proferamus. They could write in those days!]

When χ is a character of order 3, which is possible only when $p \equiv 1$ (modulo 6), an expression for τ^3 was given already by Gauss [1]. Kummer [4, 5] considered the problem of determining τ with the normalization (3) and computed τ for the primes $p \equiv 1 \pmod 6$ less than 500. No rule comparable to (4) emerged but Kummer made a conjecture of a statistical nature. For any given p, there holds precisely one of the three possibilities

$$\begin{cases} \text{(I)} & |\arg \tau| < \pi/3 \\ \text{(II)} & \pi/3 < |\arg \tau| < 2\pi/3, \\ \text{(III)} & 2\pi/3 < |\arg \tau| < \pi \end{cases} \tag{5}$$

where the many-valued function arg is normalized by

$$|\arg \tau| < \pi. \tag{6}$$

Kummer conjectured that the three cases (5) occur with asymptotic frequencies proportional to $3:2:1$. More extensive calculations by J. von Neumann and Goldstine [8] and by E. Lehmer [6] threw doubt on this conjecture. Recently A. I. Vinogradov has published a proof [9] that the three possibilities (I), (II) and (III) occur with equal asymptotic frequencies, but I understand that there are some doubts as to the correctness of the argument. The corresponding problem for quartic residues has also been discussed [3, 6], but the evidence is less complete.

The actual computation of Kummer's τ from its definition is, of course, a lengthy and tedious business. Since τ^3 is known, it is, however, enough to estimate $\arg \tau$ with an error of less than $\pi/3$. Kummer [5] showed how to do this fairly simply given the values of the three sums

$$\sum_{\chi(n)=1} \frac{1}{n^2}, \quad \sum_{\chi(n)=\omega} \frac{1}{n^2}, \quad \sum_{\chi(n)=\omega^2} \frac{1}{n^2},$$

where ω, ω^2 are the complex cube roots of 1. The argument is reproduced in Mathews [7]. The object of this little note is to show that there is a much simpler procedure which does not require even the evaluation of reciprocals. It will be clear that the argument can be extended to any generalized Gauss sum τ. At the end of the note we present further numerical evidence about Kummer's conjecture which was obtained in this way.

Theorem. *Let $p > 2$ be a rational prime, let*

$$\xi = e^{2\pi i/p} \tag{7}$$

and denote by χ a character on the multiplicative group mod p such that

$$\chi(-1) = 1 \tag{8}$$

but which is not the principal character (i.e. not identically 1). Write

$$\tau = \sum_{r=1}^{p-1} \chi(r)\, \xi^r \tag{9}$$

and

$$T = \sum r(r-p)\, \chi(r). \tag{10}$$

Then

$$|\arg (T/\tau)| \leqq \arcsin\left(\frac{\pi^2}{6} - 1\right) < \pi/4. \tag{11}$$

We require a simple lemma.

Lemma. *Suppose that*

(12) $$0 \leqq r < p.$$

Then

(13) $$\psi(r) \text{ (say) } = \sum_{s=1}^{p-1} \frac{\xi^{rs}}{1 - \xi^{-s}} = -r + \frac{1}{2}(p-1)$$

and

(14) $$\varphi(r) \text{ (say) } = \sum_{s=1}^{p-1} \frac{\xi^{rs}}{\xi^s + \xi^{-s} - 2} = \frac{1}{2} r(p-r) - (p^2-1)/12.$$

Proof. We have

$$\psi(r) - \psi(r-1) = \sum_{s=1}^{p-1} \xi^{rs} = \begin{cases} p-1 \text{ if } & r \equiv 0 \pmod p \\ -1 \text{ otherwise} & \end{cases}$$

and

$$\sum_{r \bmod p} \psi(r) = \sum_{s=1}^{p-1} \frac{1}{1-\xi^{-s}} \sum_{r \bmod p} \xi^{rs} = 0.$$

This determines the $\psi(r)$ uniquely and so gives (13). Similarly

$$\varphi(r+1) - \varphi(r) = \psi(r),$$

and

$$\sum_{r \bmod p} \varphi(r) = 0:$$

which gives (14). This completes the proof of the lemma.

Now we prove the theorem. Since $\sum \chi(r) = 0$, we have

$$\frac{1}{2} T = \frac{1}{2} \sum_r r(r-p)\, \chi(r) = -\sum_r \varphi(r)\, \chi(r) =$$

$$= \sum_{s=1}^{p-1} \frac{(-1)}{\xi^s + \xi^{-s} - 2} \sum_r \chi(r)\, \xi^{rs}$$

by (14). But

$$\chi(s) \sum_r \chi(r)\, \xi^{rs} = \sum_r \chi(rs)\, \xi^{rs} = \tau,$$

and so

(15) $$T = 2\tau R,$$

where

(16) $$R = \sum_{s=1}^{p-1} \frac{-\bar{\chi}(s)}{\xi^s + \xi^{-s} - 2}.$$

Here

(17) $$\xi^s + \xi^{-s} - 2 = -4 \sin^2 (s\pi/p) < 0,$$

and so

$$| R | \leqq \sum \frac{-1}{\xi^s + \xi^{-s} - 2} = -\varphi(0) = (p^2 - 1)/12 < p^2/12.$$

By (8) and (17) the contribution of the terms with $s = 1, p - 1$ to the right hand side of (16) is

$$R_0 \text{ (say)} = \frac{1}{2 \sin^2 \pi/p} > \frac{p^2}{2\pi^2}.$$

Hence

$$| \arg R | \leqq \arc\sin ((| R | - R_0)/R_0) < \arc\sin \left(\frac{\pi^2}{6} - 1\right).$$

Thus (11) follows from (15): which concludes the proof of the theorem.

In order to explain the application of the Theorem to Kummer's problem we require some more details about the relevant τ. Suppose that p is a positive rational prime $\equiv 1 \pmod 6$. Then

$$4p = l^2 + 27m^2 \tag{18}$$

for integers l, m, which are uniquely normalized by the conditions

$$l \equiv 1 \pmod 3), \qquad m > 0. \tag{19}$$

Further, $p = P\bar{P}$ in the Eisenstein field $Q((-3)^{1/2})$, where

$$P = \frac{1}{2}(l + m(-3)^{1/2}).$$

We distinguish one of the two characters of order 3 modulo p by the condition

$$\chi(r) \equiv r^{(p-1)/3} \pmod P. \tag{20}$$

With this normalization we have

$$\tau^3 = pP \tag{21}$$

(cf. Gauss [1] art. 358, or e. g. Mathews [7], Hasse [3]).

To determine τ we have thus only to decide on the correct cube root on the right hand side of (21). This is done by evaluating T in (10) and picking the cube root whose argument is nearest the argument of T. A check against systematic errors is provided by the inequality (11). In fact, the largest observed value of

$$| \arg (T/\tau) |$$

was (0.21) $(2\pi/3)$ at $p = 102397$.

Using the Cambridge computer TITAN, I tabulated τ for the primes in various intervals. In Table 1 the first column gives the beginning p_0 of the interval over which the count is carried out, the second column gives the number of primes $p \equiv 1 \pmod 6$ in the interval, and the three remaining columns give the number of primes in each of the three classes (I), (II), (III) of the classification (5). The first two rows are due to Kummer [4, 5] and von Neumann and Goldstine [8] respectively and were confirmed by my calculations. The third row differs from the count

Table 1

p_0	n	(I)	(II)	(III)
0	45	24	14	7
0	611	272	201	138
0	1 000	438	322	240
0	1 259	552	416	291
25 000	192	83	69	40
30 000	119	49	40	30
100 000	165	49	68	48

Table 2

form	n	(I)	(II)	(III)
$\frac{1}{4}(l^2 + 27),\ l > 0$ $l \equiv 1 \pmod 6$	39	13	13	13
$l_1^2 + 27,\ l_1 > 0$ $l_1 \equiv 2 \pmod 3$	24	8	9	7

of E. Lehmer [6] who gives 438, 321 and 241 for the distribution of the first thousand primes into classes. The total numbers of primes in the remaining rows are irregular because the program was set to run for predetermined periods.

In the hope of detecting some sort of regularity I also computed τ for the first 39 primes of the form $\frac{1}{4}(l^2 + 27)$, $l > 0$, $l \equiv 1 \pmod 6$ (from 7 to 88513) and for the first 24 primes of the form $l_2 + 27$, $l_1 > 0$, $l_1 \equiv 2 \pmod 3$ (from 31 to 131071) (i.e. in each case as far as my rather amateur program would run in 5 minutes). The subdivision into classes is given in Table 2.

I thank the Director of the Cambridge University Mathematical Laboratory for making the necessary machine time available.

REFERENCES

[1] C. F. Gauss, Disquisitiones Arithmeticae (Lipsiae, 1801) (= Werke, Bd. 1).

[2] C. F. Gauss, Summatio quarundarum serierum singularium. Commentationes societatis regiae scientiarum Gottingensis recentiores 1 (MDCCCXI). (= Werke, Bd. 2, 9—45).

[3] H. Hasse, Vorlesungen über Zahlentheorie. (2. Auflage, Berlin, 1964).

[4] E. E. Kummer, Eine Aufgabe betreffend die Theorie der cubischen Reste. J. reine angew. Math. *23* (1842), 285—286.

[5] E. E. Kummer, De residuis cubicis disquisitiones nonnullae analyticae. J. reine angew. Math. *32* (1846), 341—359.

[6] E. Lehmer, On the location of Gauss sums. Mathematics of Computation *10* (1956), 194—202.

[7] G. B. Mathews, Theory of Numbers. (Cambridge, Deighton Bell, 1892).

[8] J. von Neumann and H. H. Goldstine. A numerical study of a conjecture by Kummer. Mathematics of Computation *7* (1953), 133—134.

[9] А. И. Виноградов. О кубической сумме Гаусса. Известия Акад. Наук СССР (сер. мат.) *31* (1967), 123—148 (*added in proof:* but see also *33* 1969), 455).

Department of Pure Mathematics and Mathematical Statistics, 16 Mill Lane,
Cambridge
U.K.