THE RECKONING OF CERTAIN QUARTIC AND OCTIC GAUSS SUMS

by BRUCE C. BERNDT and S. CHOWLA

(Received 2 February, 1976)

In this brief note, we evaluate certain quartic and octic Gauss sums with the use of theorems on fourth and eighth power difference sets. We recall that a subset H of a finite (additive) abelian group G is said to be a difference set of G [5, p. 64] if for some fixed natural number λ, every nonzero element of G can be written as a difference of two elements of H in exactly λ ways.

Throughout the paper, p designates an odd prime. An evaluation of general quartic Gauss sums for $p \equiv 1 \pmod 4$ can be found in Hasse's book [3, pp. 490–493]. R. J. Evans and the first named author [1] have explicitly evaluated general octic Gauss sums for $p \equiv 1 \pmod 8$. Unfortunately, only a special class of Gauss sums can be evaluated by the method of this note, but we feel that the method's brevity and simplicity are worth noting.

For $m \in \{4, 8\}$ and $p \equiv 1 \pmod m$, let

$$S_m(p) = \sum_r e^{2\pi i r/p},$$

where the sum is over the $(p-1)/m$ distinct mth power residues $(\operatorname{mod} p)$.

THEOREM 1. *Assume that* $p = 4b^2+1$, *where* b *is odd. Then*

$$S_4(p) = \frac{\sqrt{p}-1}{4} \pm \frac{i}{2}\sqrt{\frac{p+\sqrt{p}}{2}}.$$

Proof. For the primes under consideration, the latter named author [2], [5, p. 92] has shown that the $(p-1)/4$ quartic residues modulo p form a difference set. Hence,

$$S_4(p)\overline{S_4(p)} = \sum_r e^{2\pi i r/p} \sum_r e^{-2\pi i r/p} = \frac{p-1}{4} + \frac{p-5}{16}\sum_{n=1}^{p-1} e^{2\pi i n/p} = \frac{3p+1}{16}. \tag{1}$$

For the number of terms in the product at the far left side of (1) is $\{(p-1)/4\}^2$, and so, since the $(p-1)/4$ quartic residues $(\operatorname{mod} p)$ form a difference set, a simple calculation shows that each integer n, $1 \leqq n \leqq p-1$, must occur precisely $(p-5)/16$ times. Since $p \equiv 5 \pmod 8$, -1 is a quadratic residue but a quartic nonresidue modulo p. Thus, if $r_1, \ldots, r_k$, $k = (p-1)/4$, denote a complete set of quartic residues modulo p, then $\pm r_1, \ldots, \pm r_k$ represent the quadratic residues modulo p. Thus, letting r run through the distinct quadratic residues modulo p, we have

$$S_4(p) + \overline{S_4(p)} = \sum_r e^{2\pi i r/p} = \tfrac{1}{2}(\sqrt{p}-1), \tag{2}$$

where we have used the well-known evaluation of quadratic Gauss sums [3, p. 115]. Solving (1) and (2) simultaneously for $S_4(p)$, we obtain the desired result.

THEOREM 2. *Assume that $p = 4b^2+9$, where b is odd. Then*

$$S_4(p) = \frac{\sqrt{p}-1}{4} \pm \frac{i}{2}\sqrt{\frac{p-3\sqrt{p}}{2}}.$$

Proof. By a theorem of E. Lehmer [4], [5, p. 92], for the primes under consideration, the $(p-1)/4$ quartic residues and zero form a difference set. Hence,

$$(S_4(p)+1)(\overline{S_4(p)}+1) = \frac{p+3}{4} + \frac{p+3}{16}\sum_{n=1}^{p-1} e^{2\pi i n/p} = \frac{3p+9}{16}. \tag{3}$$

By the same argument as in the previous proof, (2) again holds. Solving (2) and (3) simultaneously for $S_4(p)$, we complete the proof of the theorem.

THEOREM 3. *Assume that $p = 8b^2+1$, where b is odd, and that $p = 64c^2+9$, where c is odd. Then*

$$S_8(p) = \tfrac{1}{4}\left\{\frac{\sqrt{p}-1}{2} + \varepsilon\sqrt{\frac{p+3\sqrt{p}}{2}} \pm \sqrt{(\sqrt{p}-1)\left\{\varepsilon\sqrt{\frac{p+3\sqrt{p}}{2}}-\sqrt{p}\right\}}\right\},$$

where $\varepsilon = \pm 1$.

Proof. By a theorem of E. Lehmer [4], for the primes considered here, the $(p-1)/8$ octic residues modulo p form a difference set. Hence,

$$S_8(p)\overline{S_8(p)} = \frac{p-1}{8} + \frac{p-9}{64}\sum_{n=1}^{p-1} e^{2\pi i n/p} = \frac{7p+1}{64}. \tag{4}$$

Since $p \equiv 9 \pmod{16}$, -1 is a quartic residue but an octic nonresidue modulo p. Hence, arguing as in the proof of Theorem 1, we find that

$$S_8(p)+\overline{S_8(p)} = S_4(p). \tag{5}$$

However by [3, pp. 490–493], [1],

$$S_4(p) = \frac{\sqrt{p}-1}{4} + \varepsilon\tfrac{1}{2}\sqrt{\frac{p+3\sqrt{p}}{2}}, \tag{6}$$

where $\varepsilon = \pm 1$. Substituting (6) into (5) and then solving (4) and (5) simultaneously, we reach the desired result.

E. Lehmer [4] has also determined necessary and sufficient conditions for zero and the eighth powers modulo p to form a difference set. By using the ideas in the proofs of Theorems 2 and 3, we may also evaluate octic Gauss sums for these primes.

In [1], the opposite tack is taken from that presented here; the theory of Gauss sums is used to prove theorems on difference sets.

REFERENCES

1. Bruce C. Berndt and Ronald J. Evans, manuscript in preparation.
2. S. Chowla, A property of biquadratic residues, *Proc. Nat. Acad. Sci. India, Sect. A* **14** (1944), 45–46.
3. Helmut Hasse, *Vorlesungen über Zahlentheorie* (Springer-Verlag, 1964).
4. E. Lehmer, On residue difference sets, *Canad. J. Math.* **5** (1953), 425–432.
5. Henry B. Mann, *Addition theorems* (Wiley, 1965).

UNIVERSITY OF ILLINOIS
URBANA
ILLINOIS 61801
U.S.A.

INSTITUTE FOR ADVANCED STUDY
PRINCETON
NEW JERSEY 08540
U.S.A.

PRINTED IN GREAT BRITAIN BY ROBERT MACLEHOSE AND CO. LTD
PRINTERS TO THE UNIVERSITY OF GLASGOW