SIGN AMBIGUITIES OF JACOBI SUMS

JOSEPH B. MUSKAT AND YUN-CHENG ZEE

Received October 16, 1972. This research was partially supported by National Science Foundation Grants GP2091, GP5308 and GP8973.

The Jacobi sums, which can be defined in terms of generalized Gaussian sums, occupy a central position in cyclotomy. It was conjectured that all the arithmetic relationships between Jacobi sums of a certain order can be derived from elementary properties of Gaussian sums and the formula of Davenport and Hasse. Four counterexamples were given previously; five new ones are given here. For each of the counterexamples there is a sign which cannot be determined by means of the abovementioned tools. But some information about the sign can be obtained from congruence conditions on coordinates of certain binary quadratic decompositions of primes.

1. Introduction. Let $p = ef + 1$ be a prime. Let g be a fixed primitive root of p. The Jacobi sum $R(m, n) = R_e(m, n)$ of order e is defined by

$$R(m, n) = \sum_{a=2}^{p-1} \exp\left[(m \operatorname{ind}_g a + n \operatorname{ind}_g (1 - a))2\pi i/e\right]. \tag{1.1}$$

The Jacobi sums are related to other character sums, including Gaussian sums (1.6), Jacobsthal sums [13], and Kloosterman sums [5]. They play an important role in several aspects of the theory of cyclotomy, including determination of cyclotomic numbers [6], [11] and residuacity criteria [7].

For any value of e there is the problem of determining the relationships between the various Jacobi sums of order e. Two Jacobi sums $R(m, n)$ and $R(m', n')$ will be said to be related linearly if there exist integers k and s such that $R(m, n) = u\beta^k\sigma_s R(m', n')$, $\beta = \exp(2\pi i/e)$, $u = \pm 1$, $(s, e) = 1$, where $\sigma_s : \beta \to \beta^s$ denotes the automorphism of $Q(\beta)$ mapping β into β^s. By calling $R(m, n)$ and $R(m', n')$ equivalent if and only if they are related linearly, we can divide the Jacobi sums of order e into equivalence classes. Then if all the linear relationships are known, the values of all the Jacobi sums of order e can be derived from a list of the values of a set of representatives for the Jacobi sums of order e, one representative from each equivalence class.

If e is prime, it suffices to use the elementary relationships $R(m, n) = R(m', n')$ if $m \equiv m' \pmod e$ and $n \equiv n' \pmod e$,

$$\sigma_s R(m, n) = R(sm, sn), \qquad (s, e) = 1, \tag{1.2}$$

and [2; (83)]

$$R(m, n) = R(n, m) = (-1)^{fn} R(-m - n, n). \tag{1.3}$$