PACIFIC JOURNAL OF MATHEMATICS
Vol. 20, No. 2, 1967

RECIPROCITY AND JACOBI SUMS

JOSEPH B. MUSKAT

Recently N. C. Ankeny derived a law of rth power reciprocity, where r is an odd prime:

q is an rth power residue, modulo $p \equiv 1 \pmod r$, if and only if the rth power of the Gaussian sum (or Lagrange resolvent) $\tau(\chi)$, which depends upon p and r, is an rth power in $GF(q^f)$, where q belongs to the exponent $f \pmod r$.

$\tau(\chi)^r$ can be written as the product of algebraic integers known as Jacobi sums. Conditions in which the reciprocity criterion can be expressed in terms of a single Jacobi sum are presented in this paper.

That the law of prime power reciprocity is a generalization of the law of quadratic reciprocity is suggested by the following formulation of the latter:

If p and q are distinct odd primes, then q is a quadratic residue $(\text{mod } p)$ if and only if $(-1)^{(p-1)/2}p = \tau(\psi)^2$ is a quadratic residue $(\text{mod } q)$. Here ψ denotes the nonprincipal quadratic character modulo p (the Legendre symbol) and

$$\tau(\psi) = \sum_{n=1}^{p-1} \psi(n)e^{2\pi in/p}$$

is a Gaussian sum.

A complete statement of Ankeny's result is the following:

Let r be an odd prime. $Q(\zeta_r)$ will denote the cyclotomic field obtained by adjoining $\zeta_r = e^{2\pi i/r}$ to the field of rationals Q.

Let p be a prime $\equiv 1 (\text{mod } r)$. Let χ denote a fixed primitive rth power multiplicative character $(\text{mod } p)$. Define the Gaussian sum

$$\tau(\chi^k) = \sum_{n=1}^{p-1} \chi^k(n)e^{2\pi in/p}, \qquad r \nmid k .$$

Let q be a prime distinct from r, belonging to the exponent $f (\text{mod } r)$. Then

$$\tau(\chi)^{q^f-1} = [\tau(\chi)^r]^{(q^f-1)/r} \equiv \chi(q)^{-f} \qquad (\text{mod } q) .$$

Consequently, if $\mathfrak{q}$ is any one of the prime ideal divisors of the ideal (q) in $Q(\zeta_r)$, q is an rth power $(\text{mod } p)$ if and only if $\tau(\chi)^r$ is an rth power in $Q(\zeta_r)/\mathfrak{q}$, a field of q^f elements; i.e.,

$$(1) \qquad \chi(q) = 1 \text{ if and only if } \tau(\chi)^r \equiv \beta^r (\text{mod } \mathfrak{q})$$