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

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

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

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

Let q be a prime distinct from r, belonging to the exponent $f \pmod r$. Then

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

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

$$\text{for some } \beta \in Q(\zeta_r) \ [1, \text{ Th. } 2] .$$

The following properties of the Gaussian sums are well known:
Assume $k \not\equiv 0 (\text{mod } r)$.

$$\tau(\chi^k)\tau(\chi^{-k}) = p \tag{2}$$

$$\tau(\chi^k) \notin Q(\zeta_r), \text{ but } \tau(\chi^k)^t/\tau(\chi^{kt}) \in Q(\zeta_r) .$$

In particular,

$$\tau(\chi^k)^r \in Q(\zeta_r) .$$

During the nineteenth century several people worked on special cases of the problem solved by Ankeny. C. G. J. Jacobi treated $r = 3$ in [3]. Using Cauchy's result that

$$\tau(\chi)^q/\tau(\chi^q) \equiv \chi(q)^{-q} (\text{mod } q), \qquad [6, \ p. 108]$$

T. Pepin showed that if $q \equiv \pm 1 (\text{mod } r)$, then $\chi(q) = 1$ if and only if $\tau(\chi)^r/\tau(\chi^2)^r$ is an rth power residue (mod q), ([6, pp. 117, 120]).

Define the Jacobi sums

$$\pi(\chi^a, \chi^b) = \sum_{n=2}^{p-1} \chi^a(n)\chi^b(1-n) = \sum_{j=0}^{r-1} c_j \zeta_r^j .$$

If r does not divide a, b, or $a + b$,

$$\pi(\chi^a, \chi^b) = \tau(\chi^a)\tau(\chi^b)/\tau(\chi^{a+b}) ,$$

so by (2)

$$\pi(\chi^a, \chi^b)\pi(\chi^{-a}, \chi^{-b}) = p . \tag{3}$$

(For information on Jacobi sums see [2, Ch. 20])

$\tau(\chi)^r$ can be expressed as a product of Jacobi sums, as follows:

$$\tau(\chi)^r = \tau(\chi)\tau(\chi^{r-1}) \prod_{j=1}^{r-2} \tau(\chi)\tau(\chi^j)/\tau(\chi^{j+1}) = p \prod_{j=1}^{r-2} \pi(\chi, \chi^j), \text{ by } (2) .$$

For $r = 3$, $\tau(\chi)^r = p\pi(\chi, \chi)$, so that knowing $\pi(\chi, \chi)$ gives complete information about reciprocity. For $r > 3$, however, it is often necessary to consider products of Jacobi sums. Some cases where $\pi(\chi, \chi)$ itself gives complete information about reciprocity are described in the following two theorems:

Notation. For brevity, let $\pi[t] = \pi(\chi^t, \chi^t)$. Let $\pi[1] = \sum_{j=0}^{r-1} c_j \zeta_r^j$. Then

$$\pi[t] = \sum_{j=0}^{r-1} c_j \zeta_r^{jt} .$$

Let 2 belong to the exponent $s (\text{mod } r)$.

LEMMA. $\pi[t]^{q^h} \equiv \pi[tq^h] (\text{mod } \mathfrak{q})$.

Proof.

$$\pi[t]^{q^h} = \left[\sum_{j=0}^{r-1} c_j \zeta_r^{jt}\right]^{q^h} \equiv \sum_{j=0}^{r-1} c_j^{q^h} \zeta_r^{jtq^h} \equiv \sum_{j=0}^{r-1} c_j \zeta_r^{jtq^h} \equiv \pi[tq^h] (\text{mod } q) .$$

THEOREM 1. *Assume* $2^{r-1} \not\equiv 1 (\text{mod } r^2)$. *If there exists an integer* u *such that* $q^u \equiv 2 (\text{mod } r)$, *then* $\tau(\chi)^r$ *is an* rth *power in* $Q(\zeta_r)/\mathfrak{q}$ *if and only if* $\pi(\chi, \chi)$ *is.*

Proof. By an identity attributed to Cauchy, [6, p. 112]

$$\begin{aligned} \tau(\chi)^{2^{s}-1} &= \pi[1]^{2^{s-1}} \pi[2]^{2^{s-2}} \pi[4]^{2^{s-3}} \cdots \pi[2^{s-2}]^2 \pi[2^{s-1}] \\ &= \prod_{j=0}^{s-1} \pi[2^j]^{2^{s-j-1}} = \prod_{j=0}^{s-1} \pi[q^{uj}]^{2^{s-j-1}} \\ &= \beta^r \prod_{j=0}^{s-1} \pi[q^{uj}]^{q^{u(s-j-1)}} , \quad \text{for some } \beta \in Q(\zeta_r) . \qquad (4) \end{aligned}$$

To the jth factor of the product in (4) apply the lemma with $t = 1$ and $h = uj$:

$$\begin{aligned} \tau(\chi)^{2^{s}-1} &\equiv \beta^r \prod_{j=0}^{s-1} \pi[q^0]^{q^{u(s-1)}} \equiv \beta^r \pi[1]^{sq^{u(s-1)}} \\ &\equiv \gamma^r \pi[1] 2^{s-1} s (\text{mod } q), \quad \text{for some } \gamma \in Q(\zeta_r) . \end{aligned}$$

Since $r^2 \nmid 2^{r-1} - 1, r \nmid (2^s - 1)/r$. Also, $r \nmid 2^{s-1}s$. It follows that $\tau(\chi)^r$ is an rth power in $Q(\zeta_r)/\mathfrak{q}$ if and only if $\pi(\chi, \chi)$ is.

EXAMPLE. $r = 7, q = 3. \quad s = 3, u = 2.$

$$\begin{aligned} \tau(\chi)^7 = \pi[1]^4 \pi[2]^2 \pi[4] &= \beta^7 \pi[1]^{3^4} \pi[3^2]^{3^2} \pi[3^4]^{3^0} \\ &\equiv \beta^7 [\pi[1]^{3^4}]^3 \equiv \beta^7 \pi[1]^{3^4 \cdot 3} (\text{mod } 3) . \end{aligned}$$

(A different treatment of the example was given in [5, *p.* 351].)

THEOREM 2. *Assume* $2^{r-1} \not\equiv 1 (\text{mod } r^2)$, $r > 3$, *and* $s \equiv 2 (\text{mod } 4)$. *If there exists an integer* v *such that* $q^v \equiv 4 (\text{mod } r)$, *then* $\tau(\chi)^r$ *is an* rth *power in* $Q(\zeta_r)/\mathfrak{q}$ *if and only if* $\pi(\chi, \chi)$ *is.*

Proof.

$$\tau(\chi)^{2^{s}-1} = \prod_{j=0}^{s/2-1} \pi[2^{2j}]^{2^{s-1-2j}} \pi[2^{2j+1}]^{2^{s-2-2j}}$$

$$= \prod_{j=0}^{s/2-1} \pi[q^{vj}]^{2^{s-1-2j}} \pi[2q^{vj}]^{2^{s-2-2j}}$$

$$(5) \qquad = \beta^r \prod_{j=0}^{s/2-1} \pi[q^{vj}]^{2q^{v(s/2-1-j)}} \pi[2q^{vj}]^{q^{v(s/2-1-j)}} ,$$

for some $\beta \in Q(\zeta_r)$,

$$(6) \qquad \equiv \beta^r [\pi[q^0]^{2q^{v(s/2-1)}} \pi[2q^0]^{q^{v(s/2-1)}}]^{s/2} (\mathrm{mod}\ q),$$

by applying the Lemma with $h = vj$ and $t = 1$, then 2, to the jth factor of (5). Now apply the Lemma to the second factor of (6) with $t = 2$, $h = v(s-2)/4$:

$$\begin{aligned}\tau(\chi)^{2^{s-1}} &\equiv \beta^r [\pi[1]^{2q^{v(s/2-1)}} \pi[2q^{v(s-2)/4}]^{q^{v(s-2)/4}}]^{s/2} \\ &\equiv \beta^r [\pi[1]^{2q^{v(s/2-1)}} \pi[2 \cdot 4^{(s-2)/4}]^{q^{v(s-2)/4}}]^{s/2} \\ &\equiv \gamma^r [\pi[1]^{2^{s-1}} \pi[2^{s/2}]^{2^{s/2-1}}]^{s/2} ,\end{aligned}$$

for some $\gamma \in Q(\zeta_r)$,

$$\equiv \gamma^r [\pi[1]^{2^{s-1}} \pi[-1]^{2^{s/2-1}}]^{s/2} (\mathrm{mod}\ q) .$$

By (3)

$$\tau(\chi)^{2^{s-1}} \equiv \gamma^r [p^{2^{s/2-1}} \pi[1]^{2^{s-1} - 2^{s/2-1}}]^{s/2} (\mathrm{mod}\ q) .$$

Since $r > 3$, $q \not\equiv 1 (\mathrm{mod}\ r)$, so p is an rth power in $Q(\zeta_r)/\mathfrak{q}$.

$$2^{s-1} - 2^{s/2-1} \equiv 1 (\mathrm{mod}\ r), \text{ so}$$
$$\tau(\chi)^{2^{s-1}} \equiv \delta^r \pi[1]^{s/2} (\mathrm{mod}\ \mathfrak{q}) ,$$

for some $\delta \in Q(\zeta_r)$. $r \nmid (2^s - 1)/r$, $r \nmid s/2$, and the theorem follows.

In Theorem 3 of [5] the above results were proved for the following values of q, under the restriction $2^{r-1} \not\equiv 1 (\mathrm{mod}\ r^2)$:

(a) $q \equiv 2 (\mathrm{mod}\ r)$.

(b) $r > 3$, $q \equiv -2 (\mathrm{mod}\ r)$.

Part (a) is included in Theorem 1. Part (b) has three cases:

If s is odd, $(-2)^{s+1} = 2^s \cdot 2 \equiv 2 (\mathrm{mod}\ r)$. Theorem 1 applies, with $u = s + 1$.

If $s \equiv 2 (\mathrm{mod}\ 4)$, $(-2)^2 = 4$. Theorem 2 applies, with $v = 2$.

If $s \equiv 0 (\mathrm{mod}\ 4)$, $(-2)^{s/2+1} = -(2)^{s/2}(2) \equiv 2 (\mathrm{mod}\ r)$. Theorem 1 applies, with $u = s/2 + 1$.

For certain small values of q and r it is possible to characterize when $\chi(q) = 1$ in terms of the coefficients of $\pi[1]$ (mod p). Pepin gave the following three (the first not quite correctly).

Let $r = 5$. $\chi(3) = 1$ if and only if $c_1 \equiv c_4$ (mod 3) and

$$c_2 \equiv c_3 (\mathrm{mod}\ 3) \ [6,\ p. 132] .$$

Let $r = 7$. $\chi(3) = 1$ if and only if $c_1 \equiv c_2 \equiv c_4$ (mod 3) and

$$c_3 \equiv c_5 \equiv c_6 (\bmod 3) \ [6, \text{ pp. } 145\text{-}146] .$$

$\chi(2) = 1$ if and only if c_0 is odd [6, p. 122] .

Analogous criteria for $r = 5$, $q = 7$ and $r = 7$, $q = 5$ can be found in [5, p. 349].

A more general result, which yields only a sufficient condition, however, was suggested by Emma Lehmer [4], who proved it for $r = 5$.

THEOREM 3: *Assume* $2^{r-1} \not\equiv 1 (\bmod r^2)$, *and* $r > 3$. *Let* g *be a primitive root, modulo* r. *If* $c_g \equiv c_{g^3} \equiv c_{g^5} \equiv \cdots \equiv c_{g^{r-2}} (\bmod q)$ *and* $c_{g^2} \equiv c_{g^4} \equiv c_{g^6} \equiv \cdots \equiv c_1 (\bmod q)$, *then* q *is an* rth *power residue* $(\bmod p)$.

Proof. Let $\lambda = \sum_{j=0}^{\frac{r-3}{2}} \zeta_r^{g^{2j}}$, $\mu = \sum_{j=0}^{\frac{r-3}{2}} \zeta_r^{g^{2j+1}}$

$$\pi[1] = \sum_{j=0}^{r-1} c_j \zeta_r^j = \sum_{j=1}^{r-1} (c_j - c_0) \zeta_r^j \equiv (c_1 - c_0)\lambda + (c_g - c_0)\mu (\bmod q).$$

Similarly,

$$\pi[g] \equiv (c_1 - c_0)\mu + (c_g - c_0)\lambda (\bmod q) .$$

If 2 is a quadratic residue, modulo r,

$$\begin{aligned} \tau(\chi)^{2^s-1} &= \prod_{j=0}^{s-1} \pi[2^j]^{2^{s-j-1}} \equiv \prod_{j=0}^{s-1} [(c_1 - c_0)\lambda + (c_g - c_0)\mu]^{2^{s-j-1}} \\ &\equiv [(c_1 - c_0)\lambda + (c_g - c_0)\mu]^{2^s-1} (\bmod q) . \end{aligned}$$

If 2 is a quadratic nonresidue, modulo r,

$$\begin{aligned} \tau(\chi)^{2^s-1} &= \prod_{j=0}^{s/2-1} \pi[2^{2j}]^{2^{s-1-2j}} \pi[2^{2j+1}]^{2^{s-2-2j}} \\ &\equiv [(c_1 - c_0)\lambda + (c_g - c_0)\mu]^{2(2^s-1)/3} [(c_1 - c_0)\mu + (c_g - c_0)\lambda]^{(2^s-1)/3} \\ &\quad (\bmod q) . \end{aligned}$$

In both cases $\tau(\chi)^{2^s-1}$ has been shown to be an rth power in $Q(\zeta_r)/\mathfrak{q}$. Since $r \nmid (2^s - 1)/r$, $\tau(\chi)^r$ is an rth power in $Q(\zeta_r)/\mathfrak{q}$, and applying (1) yields the theorem.

COROLLARY. *Assume* $2^{r-1} \not\equiv 1 (\bmod r^2)$. *If* $c_1 \equiv c_2 \equiv \cdots \equiv c_{r-1}$ $(\bmod q)$, *then* q *is an* r*th power residue* $(\bmod p)$.

Proof. If $r > 3$, apply Theorem 3. If $r = 3$, $\tau(\chi)^3 \equiv (c_0 - c_1)^3$ $(\bmod q)$.

A computation by John Brillhart shows that 1093 and 3511 are the only primes r less than 2^{24} for which $2^{r-1} \equiv 1 (\bmod r^2)$.

BIBLIOGRAPHY

1. Nesmith C. Ankeny, *Criterion for* rth *power residuacity*, Pacific J. Math. **10** (1960), 1115-1124.

2. H. Hasse, *Vorlesungen über Zahlentheorie*, 2nd ed., Springer Verlag, Berlin 1964.

3. C. G. J. Jacobi, *De Residuis Cubicis Commentatio Numerosa*, Journal für die reine und angewandte Mathematik **2** (1827), 66-69.

4. Emma Lehmer, *Artiads characterized*, Journal of Mathematical Analysis and Applications **15** (1966), 118-131.

5. Joseph B. Muskat, *Criteria for solvability of certain congruences*, Canad. J. Math. **16** (1964), 343-352.

6. T. Pepin *Memoire sur les lois de réciprocité relatives aux résidues de puissances*, Pontificia accademia delle scienze, Atti **31** (1877), 40-148.

Received January 19, 1966. This research was sponsored in part by the National Science Foundation under Research Grant GP-2091.