Pacific Journal of Mathematics

CRITERION FOR rTH POWER RESIDUACITY

NESMITH CORNETT ANKENY

Vol. 10, No. 4 December 1960

CRITERION FOR rTH POWER RESIDUACITY

N. C. ANKENY

The Law of Quadratic Reciprocity in the rational integers states: If p, q are two distinct odd primes, then q is a square $(\bmod\, p)$ if and only if $(-1)^{(p-1)/2}p$ is a square $(\bmod\, q)$.

One of the classical generalizations of the law of reciprocity is of the following type. Let r be a fixed positive integer, $\phi(r)$ denotes the number of positive integers $\leqq r$ which are relatively prime to r; p, q are two distinct primes and $p \equiv 1 \pmod r$. Then can we find rational integers $a_1(p), a_2(p), \cdots, a_h(p)$ determined by p, such that q is an rth power $(\bmod\, p)$ if and only if $a_1(p), \cdots, a_h(p)$ satisfy certain conditions $(\bmod\, q)$.

The Law of Quadratic Reciprocity states that for $r = 2$, we may take $a_1(p) = (-1)^{(p-1)/2}p$.

Jacobi and Gauss solved this problem for $r = 3$ and $r = 4$, respectively. Mrs. E. Lehmer gave another solution recently [2].

In this paper I would like to develop the theory when r is a prime and $q \equiv 1 \pmod r$. I then show that q is an rth power $(\bmod\, p)$ if and only if a certain linear combination of $a_1(p), \cdots, a_{r-1}(p)$ is an rth power $(\bmod\, q)$. $a_1(p), \cdots, a_{r-1}(p)$ are determined by solving several simultaneous Diophantine equations. This determination appears mildly formidable and to make the actual numerical computations would certainly be so for a large r. (See Theorem B below.) Also given is a criterion for when r is an rth power $(\bmod\, p)$ in terms of a linear combination of $a_1(p), \cdots, a_{r-1}(p)$ $(\bmod\, r^2)$. (See Theorem A below.)

It is possible by the methods developed in this paper to eliminate the conditions that r is a prime and $q \equiv 1 \pmod r$. This would complicate the paper a great deal, and the cases given clearly indicate the underlying theory.

Consider the following Diophantine equations in the rational integers:

$$(1) \qquad r\sum_{j=1}^{r-1} X_j^2 - \left(\sum_{j=1}^{r-1} X_j\right)^2 = (r-1)p^{r-2}$$

$$(2) \qquad \textstyle\sum_1^{(1)} X_{j_1}X_{j_2} = \sum_i^{(1)} X_{j_1}X_{j_2} \qquad i = 2, \cdots, \dfrac{r-1}{2},$$

where $\sum_i^{(k)}$ denotes the sum over all $j_1, \cdots, j_{k+1} = 1, 2, \cdots, r-1$, with the condition $j_1 + \cdots + j_k - kj_{k+1} \equiv i \pmod r$.

Received April 24, 1959; in revised form January, 1960. This research was supported by the United States Air Force through the Air Force Office of Scientific Research of the Air Research and Development Command, under contract No. AF 18 (603)-90. Reproduction in whole or in part is permitted for any purpose of the United States Government.

(3) $$1 + \sum_{j=1}^{r-1} X_j \equiv \sum_{j=1}^{r-1} jX_j \equiv 0 \pmod{r}$$

(4) not all of the $X_j \equiv 0 \pmod{p}$ and

$$\sum\nolimits_i^{(k)} X_{j_1} \cdots X_{j_{k+1}} - \sum\nolimits_0^{(k)} X_{j_1} \cdots X_{j_{k+1}} \equiv 0 \pmod{p^{r-k-1}}$$

for $k = 2, \cdots, r-2$; $i = 1, 2, \cdots, r-1$.

We shall prove in § II that there exist exactly $r-1$ distinct integral solutions of the equations (1) through (4). In particular let $\{X_j = a_j, j = 1, \cdots, r-1\}$ be a solution. Then we prove that the $a_j(p) = a_j$ satisfy our residuacity criterion, namely

THEOREM A. *r is an rth power $\pmod{p}$ if and only if*

$$\sum_{j=1}^{r-1} ja_j + \frac{1}{2} ra_{r-1} \equiv 0 \pmod{r^2} .$$

THEOREM B. *If $q \equiv 1 \pmod{r}$ and h is any integer such that h^r is the least power of h which is $\equiv 1 \pmod{q}$, then q is an rth power $\pmod{q}$ if and only if $\sum_{j=1}^{r-1} a_j h^j$ is an rth power $\pmod{q}$.*

At the end of § II various special cases are considered.

In particular, for $q = 2, r = 5$, then 2 is a quintic power $\pmod{p}$ if and only if $a_j \equiv a_{5-j} \pmod{2}, j = 1, 2$.

For $q = 2, r = 7$, then 2 is a 7th power $\pmod{p}$ if and only if $a_j \equiv 1 \pmod{2}$, $i = 1, \cdots, 6$.

Let $r = 3$. Then the solutions to the Diophantine equations (1) to (4) are (a_1, a_2) and (a_2, a_1), where

(5) $$p = a_1^2 - a_1 a_2 + a_2^2, a_1 \equiv a_2 \equiv 1 \pmod{3} .$$

Multiplying (5) by 4 and grouping terms gives

$$4p = (a_1 + a_2)^2 + 3(a_1 - a_2)^2 .$$

Let $L = -a_1 - a_2, M = (a_1 - a_2)/3$. This gives the representation which Lehmer employs:

$$4p = L^2 + 27M^2, L \equiv 1 \pmod{3} .$$

Theorem A states that 3 is a cubic residue $\pmod{p}$ if and only if $a_1 \equiv a_2 \pmod{9}$. This, in turn, is equivalent to M being divisible by 3, the condition quoted by Lehmer.

I. **Notation.** r denotes a prime number, ζ_r a primitive rth root of unity, Q the rational numbers, $Q(\zeta_r)$ the cyclotomic field over Q generated by ζ_r. For $j = 1, 2, \cdots, r-1$, σ_j are the automorphisms of $Q(\zeta_r)/Q$

such that $\sigma_j(\zeta_r) = \zeta_r^j$. $\sigma^{-1}(\zeta_r) = \zeta_r^{j'}$, where $jj' \equiv 1 \pmod r$. p denotes a positive rational prime $\equiv 1 \pmod r$, and $\chi_p = \chi$ will be any primitive rth power character $(\bmod\, p)$.

$$g(\chi) = \sum_{n=1}^{p-1} \chi(n)\zeta_p^n$$

will be the Gaussian sum associated with χ_p. $\langle\alpha\rangle$ denotes the fractional part of α; i.e., $\langle\alpha\rangle = \alpha - [\alpha]$.

LEMMA 1. (i) $|g(\chi^k)|^2 = p$,
(ii) $g(\chi)^k g(\chi^{-k}) \in Q(\zeta_r)$,
(iii) $g(\chi)^r \in Q(\zeta_r)$, and
(iv) $\sigma_k(g(\chi)^r) = g(\chi^k)^r$
for $k = 1, 2, \cdots, r - 1$.

Proof. (i) is the classical result about the absolute value of $g(\chi)$ and can easily be deduced from the definition of $g(\chi)$. (ii), (iii) and (iv) follow from Galois Theory using the relation $\sum_{n=1}^{p-1} \chi(n)\zeta_p^{nt} = \chi(t)^{-1}g(\chi)$ for any integer t prime to p.

LEMMA 2. *There exists a prime ideal* $\mathfrak{p}$ *in* $Q(\zeta_r)$ *dividing* p *such that* $(g(\chi^k)^r) = \sum_{j=1}^{r-1} \sigma_j^{-1} \mathfrak{p}^{r\langle kj/r\rangle}$.

Conversely, given any prime ideal $\mathfrak{p}_1$ *in* $Q(\zeta_r)$ *dividing* p, *there exists a* k *such that*

$$(g(\chi^k)^r) = \sum_{j=1}^{r-1} \sigma_j^{-1} \mathfrak{p}_1^j .$$

Proof. Lemma 2 is a result of Stickelberger. For a proof see Davenport and Hasse [1]. See especially the elegant proof on page 181–2. In $Q(\zeta_r)$, the ideal $(r) = (1 - \zeta_r)^{r-1}$,

LEMMA 3. $(1 - \zeta_r^t)(1 - \zeta_r)^{-1} \equiv t \pmod{(1 - \zeta_r)}$ and $r(1 - \zeta_r^t)^{-r+1} \equiv -1 \pmod{(1 - \zeta_r)}$ for $(t, r) = 1$.

Proof. The first fact follows as

$$(1 - \zeta_r^t)(1 - \zeta_r)^{-1} = \sum_{j=0}^{t-1} \zeta_r^j \equiv \sum_{j=0}^{t-1} 1 \equiv t \pmod{(1 - \zeta_r)} .$$

The second follows from Wilson's Theorem as

$$\begin{aligned} r(1 - \zeta_r^t)^{-r+1} &= \Big(\prod_{j=1}^{r-1} (1 - \zeta_r^{jt})\Big)(1 - \zeta_r^t)^{-r+1} \\ &= \prod_{j=1}^{r-1} (1 - \zeta_r^{jt})(1 - \zeta_r^t)^{-1} \equiv (r - 1)! \equiv -1 \pmod{(1 - \zeta_r)} . \end{aligned}$$

THEOREM 1. *For any t not divisible by r,*

$$g(\chi^t)^r + 1 \equiv r(1 - \chi(r)^{-t}) \pmod{(1 - \zeta_r)^{r+1}} ,$$

and consequently, $\chi(r) = 1$ *if and only if*

$$g(\chi^t)^r + 1 \equiv 0 \pmod{(1 - \zeta_r)^{r+1}} .$$

Proof. As

$$g(\chi) = \sum_{n=1}^{p-1} \chi(n)\zeta_p^n ,$$

the binomial theorem yields

$$\begin{aligned} -g(\chi)^r &= \Big(-\sum_{n=1}^{p-1} \zeta_p^n + \sum_{n=1}^{p-1} (1 - \chi(n))\zeta_p^n\Big)^r = (1 + \sum_n (1 - \chi(n))\zeta_p^n)^r \\ &\equiv 1 + r \sum_n (1 - \chi(n))\zeta_p^n + \sum_n (1 - \chi(n))^r \zeta_p^{rn} \pmod{(1 - \zeta_r)^{r+1}} , \end{aligned}$$

as all other terms are divisible by at least $r(1 - \zeta_r)^2$. By Lemma 3, if $\chi(n) \neq 1$, $(1 - \chi(n))^{r-1} \equiv -r \pmod{(1 - \zeta_r)^r}$, and clearly, if $\chi(n) = 1$,

$$(1 - \chi(n))^r \equiv -r(1 - \chi(n)) \pmod{(1 - \zeta_r)^{r+1}} .$$

Thus,

$$\begin{aligned} -g(\chi)^r &\equiv 1 + r\Big(\sum_{n=1}^{p-1} (1 - \chi(n))\zeta_p^n - (1 - \chi(n))\zeta_p^{rn}\Big) \\ &\equiv 1 + r \sum_n (1 - \chi(n))\zeta_p^n - (1 - \chi(n)\chi(r)^{-1})\zeta_p^n \\ &\equiv 1 - r(1 - \chi(r)^{-1}) \sum_n \chi(n)\zeta_p^n \\ &\equiv 1 - r(1 - \chi(r)^{-1}) \sum_n \zeta_p^n \\ &\equiv 1 + r(1 - \chi(r)^{-1}) \pmod{(1 - \zeta_r)^{r+1}} . \end{aligned}$$

By (iv) of Lemma 1,

$$-g(\chi^t)^r = -\sigma_t(g(\chi)^r) \equiv 1 + r(1 - \chi(r)^{-t}) \pmod{(1 - \zeta_r)^{r+1}} ,$$

which completes the first statement of Theorem 1. The second statement in Theorem 1 then follows immediately.

Let q denote any positive rational prime other than r, f the least positive integer such that $q^f \equiv 1 \pmod{r}$, and $ef = r - 1$. Then in $Q(\zeta_r)$ the ideal $(q) = \mathfrak{A}_1\mathfrak{A}_2 \cdots \mathfrak{A}_e$, where the $\mathfrak{A}_j$ are prime ideals and

$$\operatorname*{Norm}_{Q(\zeta_r),Q} (\mathfrak{A}_j) = q^f . \tag{6}$$

In the following let $\mathfrak{A}$ be any of the e prime divisors $\mathfrak{A}_j$, $j = 1, \cdots, e$.

THEOREM 2. *Let q, p, and r be distinct.*

Then

$$g(\chi)^{q^f-1} \equiv \chi(q)^{-f} \pmod{q} . \tag{7}$$

Consequently $\chi(q) = 1$ *if and only if*

$$g(\chi)^r \equiv \beta^r \pmod{\mathfrak{A}} \text{ for some } \beta \in Q(\zeta_r) . \tag{8}$$

Proof.
$$\begin{aligned} g(\chi)^{q^f} &= \Big(\sum_{n=1}^{p-1} \chi(n)\zeta_p^n\Big)^{q^f} \\ &\equiv \sum_{n=1}^{p-1} \chi(n)^{q^f} \zeta_p^{nq^f} \pmod{q} \\ &\equiv \sum_n \chi(n)\zeta_p^{nq^f} \pmod{q}, \text{ as } r \mid q^f - 1 , \\ &\equiv \chi(q)^{-f} g(\chi) \pmod{q} . \end{aligned}$$

Multiplying both sides of the above congruence by $\overline{g(\chi)}$, and noting (i) of Lemma 1, yields

$$p g(\chi)^{q^f-1} \equiv \chi(q)^{-f} p \pmod{q} \text{ or } g(\chi)^{q^f-1} \equiv \chi(q)^{-f} \pmod{q} ,$$

as p and q are distinct primes. Hence, we have proved (7).

Note that as $r \mid q^f - 1$, (7) becomes a congruence in $Q(\zeta_r)$. As $f \mid r - 1$, $(f, r) = 1$, we have by (7) that $\chi(q) = 1$ if and only if $g(\chi)^{q^f-1} \equiv 1 \pmod{\mathfrak{A}}$.

(Note that $1 - \zeta_r^t \not\equiv 0 \pmod{\mathfrak{A}}$ unless $\zeta_r^t = 1$.)

If $g(\chi)^r \equiv \beta^r \pmod{\mathfrak{A}}$ for some $\beta \in Q(\zeta_r)$, then

$$g(\chi)^{q^f-1} \equiv \beta^{q^f-1} \equiv 1 \pmod{\mathfrak{A}}$$

by (6).

Conversely, if $g(\chi)^{q^f-1} \equiv 1 \pmod{\mathfrak{A}}$ then $(g(\chi)^r)^{(q^f-1)/r} \equiv 1 \pmod{\mathfrak{A}}$. By Lemma 1, $g(\chi)^r \in Q(\zeta_r)$. By (6) this implies $g(\chi)^r \equiv \beta^r \pmod{\mathfrak{A}}$. (Euler's Criterion for rth powers.)

In the above argument we must bear in mind that $g(\chi) \notin Q(\zeta_r)$.

II. In the last section we have developed a criterion for rth power residuacity in $Q(\zeta_r)$. From this we derive a criterion in the rational numbers Q, which is the purpose of Theorems A and B.

First let us assume that there is a rational integral solution $X_j = a_j$ of equations (1), (2), (3) and (4). In $Q(\zeta_r)$ define the algebraic integer $\alpha = \sum_{j=1}^{r-1} a_j \zeta_r^j$. We shall prove that α satisfies

$$| \sigma_k(\alpha) |^2 = p^{r-2} , \qquad k = 1, 2, \cdots, r - 1 . \tag{9}$$

$$(p\alpha)^k \sigma_k(p\alpha)^{-1} \tag{10}$$

is also an algebraic integer in $Q(\zeta_r)$, for $k = 1, 2, \cdots, r - 1$.

To prove (9) we note that

$$\begin{aligned} |\alpha|^2 &= \Big(\sum_j a_j\zeta_r^j\Big)\Big(\sum_i a_i\zeta^{r-i}\Big) \\ &= \sum_{j,i} a_j a_i \zeta_r^{j-i} \\ &= \sum_{j=1}^{r-1} a_j^2 + \sum_{i=1}^{r-1}\big(\textstyle\sum_i^{(1)} a_{j_1}a_{j_2}\big)\zeta_r^i \,. \end{aligned}$$

By (2) all of the coefficients of ζ_r^i are equal, since for any i, the sums corresponding to i and $r-i$ are identical. Thus

$$\begin{aligned} |\alpha|^2 &= \sum_j a_j^2 - \textstyle\sum_1^{(1)} a_{j_1}a_{j_2} \\ &= \sum_j a_j^2 - (r-1)^{-1}\sum_{i=1}^{r-1}\textstyle\sum_i^{(1)} a_{j_1}a_{j_2} \\ &= r(r-1)^{-1}\sum_j a_j^2 - (r-1)^{-1}\sum_{i=0}^{r-1}\textstyle\sum_i^{(1)} a_{j_1}a_{j_2} \\ &= r(r-1)^{-1}\sum_{j=1}^{r-1} a_j^2 - (r-1)^{-1}\Big(\sum_{j=1}^{r} a_j\Big)^2 \\ &= p^{r-2} \end{aligned}$$

by (1). Similarly $|\sigma_k(\alpha)|^2 = p^{r-2}$. Thus (1) and (2) imply (9).

Let k be a fixed integer $2 \leqq k \leqq r-1$. Then

$$\begin{aligned} (p\alpha)^k\sigma_k(p\alpha)^{-1} &= p^{k-1}\alpha^k\sigma_k(\alpha)^{-1} \\ &= p^{k-1}\alpha^k\sigma_{-k}(\alpha)\,|\,\sigma_k(\alpha)\,|^{-2} \\ &= p^{-r+k+1}\alpha^k\sigma_{-k}(\alpha) \end{aligned} \tag{11}$$

by (10). Now

$$\begin{aligned} \alpha^k\sigma_{-k}(\alpha) &= \big(\textstyle\sum a_j\zeta_r^j\big)^k\big(\textstyle\sum a_j\zeta_r^{-jk}\big) \\ &= \sum_{i=0}^{r-1}\big(\textstyle\sum_i^{(k)} a_{j_1}\cdots a_{j_{k+1}}\big)\zeta_r^i \\ &= \sum_{i=1}^{r-1}\big(\textstyle\sum_i^{(k)} - \sum_0^{(k)}\big)\zeta_r^i \,. \end{aligned} \tag{12}$$

Condition (4) implies that each coefficient of ζ_r^i in (12) is divisible by p^{r-k-1}. Placing this information in (11) states that $(p\alpha)^k\sigma_k(p\alpha)^{-1}$ is an integer; thus proving (10).

(4) also tells us that p, but not p^2, divides $p\alpha$, as not all the coefficients of ζ_r^j in $\alpha = \sum_{j=1}^{r-1} a_j\zeta_r^j$ are divisible by p.

If we restate the above facts in terms of ideals, we have that $(p\alpha)$ is an integral ideal in $Q(\zeta_r)$ divisible only by the prime ideals which divide p.

There exists one prime ideal, say $\mathfrak{p}$, dividing p, which divides $p\alpha$ but $\mathfrak{p}^2$ does not divide $p\alpha$. All other prime factors of p in $Q(\zeta_r)$ are of the form $\sigma_i^{-1}\mathfrak{p}$. Hence,

$$(13)\qquad (p\alpha) = \sum_{i=1}^{r-1} \sigma_i^{-1}\mathfrak{p}^{d_i} \text{ where } d_1 = 1, d_i > 0\ .$$

By (9)

$$\begin{aligned}(p\alpha)(\sigma_{-1}(p\alpha)) &= (p^2\,|\,\alpha\,|^2) = p^r \\ &= \Bigl(\prod_i \sigma_i^{-1}\mathfrak{p}^{d_i}\Bigr)\Bigl(\prod_i \sigma_{-1}\sigma_i^{-1}\mathfrak{p}^{d_i}\Bigr) \\ &= \prod_i \sigma_i^{-1}\mathfrak{p}^{d_i+d_{r-i}}\end{aligned}$$

or

$$(14)\qquad d_i + d_{r-i} = r\ .$$

By (10), $(p\alpha)^k\sigma_k(p\alpha)^{-1}$ is integral, or

$$\begin{aligned}(p\alpha)^k(\sigma_k(p\alpha))^{-1} &= \prod_i \sigma_i^{-1}\mathfrak{p}^{d_ik} \prod_i \sigma_k\sigma_i^{-1}\mathfrak{p}^{-d_i} \\ &= \prod \sigma_i^{-1}\mathfrak{p}^{d_ik-d_{ik}}\end{aligned}$$

is an integral ideal. (The index of d_{ik} is interpreted mod r.) Hence, $kd_i \geqq d_{ik}$.

As $d_1 = 1$, $k \geqq d_k$ for $k = 2, 3, \cdots, r-2$. By (14) this yields that $d_k = k$. By Lemma 2, we arrive at the fact that in terms of ideals

$$(15)\qquad (p\alpha) = (g(\chi^t)^r) \text{ for some } 1 \leqq t < r\ .$$

In proving (15) we have used (1), (2) and (4). We wish to prove that $p\alpha = g(\chi^t)^r$. To do this we now utilize (3). By (15) we have that for some unit $\eta \in Q(\zeta_r)$, $g(\chi^t)^r = \eta p\alpha$, or

$$(16)\qquad g(\chi^{tk})^r = \sigma_k(\eta p\alpha) = \sigma_k(\eta)\sigma_k(p\alpha)\ .$$

Taking the absolute value of both sides of (16) and utilizing (i) of Lemma 1 and (9) gives $p^r = |\,\sigma_k(\eta)\,|^2p^r$, or $|\,\sigma_k(\eta)\,|^2 = 1$. By a Theorem of Dirichlet on units (See [3] Theorem IV 9, A pp. 174), any unit which has all of its conjugates with absolute value 1 is then a root of unity. As $\eta \in Q(\zeta_r)$, $\eta = \pm\zeta_r^s$.

Now

$$\begin{aligned}\alpha = \sum_{j=1}^{r} a_j\zeta_r^j &= \sum_j a_j - \sum_j a_j(1-\zeta_r^j) \\ &\equiv \sum_j a_j - \sum_j ja_j(1-\zeta_r) \pmod{(1-\zeta_r)^2}\ ,\end{aligned}$$

by Lemma 3. As $p \equiv 1 \pmod{r}$, $p \equiv 1 \pmod{(1-\zeta_r)^2}$. By (3),

$$1 + \sum_j a_j \equiv \sum_j ja_j \equiv 0 \pmod{r}\ .$$

Hence, $p\alpha \equiv -1 \pmod{(1-\zeta_r)^2}$. By Theorem 1, $g(\chi^t)^r \equiv -1 \pmod{1-\zeta_r)^2}$. Therefore, $\eta \equiv 1 \pmod{(1-\zeta_r)^2}$. But $\eta = \pm\zeta_r^s \equiv \pm(1+s(1-\zeta_r)) \pmod{(1-\zeta_r)^2}$; i.e., $s \equiv 0 \pmod{r}$ and the $+$ sign holds. Hence, $\eta = 1$.

Therefore, if the a_j are any integral solution of (1), (2), (3) and (4), there exists an integer $1 \leqq t \leqq r-1$ such that

$$p\sum_{j=1}^{r-1} a_j \zeta_r^j = g(\chi^t)^r . \tag{17}$$

Conversely, given any integer t, $1 \leqq t \leqq r-1$, and writing

$$g(\chi^t)^r = p\sum_{j=1}^{r-1} a_j \zeta_r^j ,$$

we can prove that the a_j are rational integers which satisfy (1), (2), (3), and (4). The proof is merely reversing the above steps we used in proving (17). By Lemma 2 the prime factorizations of $(g(\chi^s)^r)$ and $(g(\chi^t)^r)$, $1 \leqq s < t \leqq r-1$, are distinct, and thus $g(\chi^s)^r \neq g(\chi^t)^r$. Hence, we have shown that there are precisely $r-1$ rational integral solutions of (1), (2), (3), and (4).

We are now in a position to prove Theorems A and B. First for Theorem A.

Let a_j be an integral solution of (1) through (4). Then we have shown that $p\sum_{j=1}^{r-1} a_j\zeta_r^j = g(\chi^t)^r$ for some integer t relatively prime to r. By Theorem 1, the above states that $\chi(r) = 1$ if and only if $p\sum_j a_j\zeta_r^j \equiv -1 \pmod{(1-\zeta_r)^{r+1}}$.

Define b_s, $s = 0, 1, \cdots, r-2$, by $b_0 = -pa_{r-1}$, $b_s = p(a_s - a_{r-1})$, $s = 1, 2, \cdots, r-2$. Then

$$p\sum_{j=1}^{r-1} a_j\zeta_r^j = \sum_{s=0}^{r-2} b_s\zeta_r^s .$$

Further let

$$C_i = (-1)^i \sum_{s=i}^{r-2} \binom{s}{i} b_s ,$$

where $\binom{s}{i}$ is the binomial coefficient. Then

$$\begin{aligned} p\sum_{j=1}^{r-1} a_j\zeta_r^j &= \sum_{s=0}^{r-2} b_s\zeta_r^s = \sum_s b_s(1-(1-\zeta_r))^s \\ &= \sum_s b_s \sum_{i=0}^{s} (-1)^i\binom{s}{i}(1-\zeta_r)^i \\ &= \sum_{i=0}^{r-2} C_i(1-\zeta_r)^i . \end{aligned}$$

The first statement in Theorem 1 states that $g(\chi^t)^r + 1 \equiv 0 \pmod{(1-\zeta_r)^r}$. Hence,

$$\begin{aligned} \sum_{i=0}^{r-2} C_i(1-\zeta_r)^i + 1 &\equiv (C_0+1) + \sum_{i=1}^{r-2} C_i(1-\zeta_r)^i \\ &\equiv 0 \pmod{(1-\zeta_r)^r} \end{aligned}$$

This implies that $C_0 + 1 \equiv 0 \pmod{r^2}$. Hence,

$$\sum_{i=0}^{r-2} C_i(1 - \zeta_r)^i \equiv C_1(1 - \zeta_r) \pmod{(1 - \zeta_r)^{r+1}}$$

or that $\chi(r) = 1$ if and only if

$$C_1 \equiv 0 \pmod{r^2} . \tag{18}$$

Now

$$\begin{aligned} C_1 &= (-1)\sum_{s=1}^{r-2} \binom{s}{1} b_s = -\sum_{s=1}^{r-2} s b_s \\ &= -p \sum_{s=1}^{r-2} s(a_s - a_{r-1}) \\ &= -p \sum_{s=1}^{r-2} s a_s + \frac{1}{2} p(r-2)(r-1)a_{r-1} \\ &\equiv -p\left(\sum_{s=1}^{r-1} s a_s + \frac{1}{2} r a_{r-1}\right) \pmod{r^2} . \end{aligned} \tag{19}$$

Equations (18) and (19) complete the proof of Theorem A.

Theorem B is also derived immediately from Theorem 2. If $q \equiv 1 \pmod{r}$, q a positive rational prime, then in $Q(\zeta_r)$, $(q) = \mathfrak{A}_1\mathfrak{A}_2 \cdots \mathfrak{A}_{r-1}$, where $\mathfrak{A}_j$ are prime ideals and $\mathrm{Norm}_{Q(\zeta_r), Q}\, \mathfrak{A}_j = q$.

We may take $0, 1, 2, \cdots, q - 1$ as a set of residues $(\mathrm{mod}\ \mathfrak{A}_1)$. Hence, as $1 - \zeta_r^t \not\equiv 0 \pmod{\mathfrak{A}_1}$, unless $\zeta_r^t = 1$, $\zeta_r \equiv h \pmod{\mathfrak{A}_1}$, where h is a rational integer such that $h^r \equiv 1 \pmod{q}$.

Thus by Theorem 2, $\chi(q) = 1$ if and only if there is a $\beta \in Q(\zeta_r)$ such that $g(\chi^t)^r = p \sum_j a_j \zeta_r^j \equiv p \sum_j a_j h^j \equiv \beta^r \pmod{\mathfrak{A}_1}$.

We may take $\beta = b \in Q$ by the above remarks.

Hence, $\chi_p(q) = 1$ if and only if $\chi_q(p \sum_j a_j h^j) = 1$ where χ_q is a primitive rth power character $(\mathrm{mod}\ q)$.

If we had chosen another h_1 whose order was $r \pmod{q}$, then $h_1 \equiv h^t \pmod{\mathfrak{A}_1}$, and

$$p \sum_j a_j h_1^t \equiv p \sum_j a_j \zeta_r^{jt} \equiv g(\chi^t)^r \pmod{\mathfrak{A}_1} .$$

Thus, any h whose order $(\mathrm{mod}\ q)$ is r works equally well in Theorem B.

There are several special cases one can derive when $q \not\equiv 1 \pmod{r}$, in particular, when $q = 2$, and $r = 5, 7$.

If $q = 2$, $r = 5$, then in $Q(\zeta_r)$, 2 remains a prime because 2^4 is the least power of 2 congruent to 1 (mod 5). One can easily compute that the only elements in $Q(\zeta_5)$ which are fifth powers (mod 2) are $1 = -\sum_{j=1}^4 \zeta_5^j$, $\zeta_5 + \zeta_5^{-1}$, and $\zeta_5^2 + \zeta_5^{-2} \pmod{2}$. Hence, for $r = 5$, $\chi_p(2) = 1$ if and only if $a_j \equiv a_{5-j} \pmod{2}$.

For $q = 2$, $r = 7$, then $2^3 \equiv 1 \pmod{7}$. Hence, in $Q(\zeta_7)$, $(2) = \mathfrak{A}_1\mathfrak{A}_2$ where $\mathrm{Norm}\, \mathfrak{A}_i = 8$. For $\alpha \equiv \beta^7 \pmod{\mathfrak{A}_1}$, $\beta \not\equiv 0 \pmod{\mathfrak{A}_1}$, and $\beta \in Q(\zeta_7)$

implies $\alpha \equiv 1 \pmod{\mathfrak{A}_1}$. Hence, for $r = 7$, $\chi_p(2) = 1$ if and only if $a_j \equiv 1 \pmod 2$ for $j = 1, \cdots, 6$.

One could easily generalize this to the case when $r = 2^s - 1$. Then $\chi_p(2) = 1$ if and only if $a_j \equiv 1 \pmod 2$ for $j = 1, \cdots, r-1$.

BIBLIOGRAPHY

1. H. Davenport and H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen,* Journal für die reine und angewandte Mathematik, Band CLXXII, (1935), 151-182.

2. E. Lehmer, *Criteria for cubic and quartic residuacity,* Mathematika, **5**, Part 1, (1958), 20-29.

3. H. Weyl, *Algebraic Theory of Numbers,* Annals of Mathematical Studies, Princeton University Press, 1940.

PACIFIC JOURNAL OF MATHEMATICS

EDITORS

DAVID GILBARG
Stanford University
Stanford, California

F. H. BROWNELL
University of Washington
Seattle 5, Washington

A. L. WHITEMAN
University of Southern California
Los Angeles 7, California

L. J. PAIGE
University of California
Los Angeles 24, California

ASSOCIATE EDITORS

E. F. BECKENBACH
T. M. CHERRY
D. DERRY
E. HEWITT
A. HORN
L. NACHBIN
M. OHTSUKA
H. L. ROYDEN
M. M. SCHIFFER
E. SPANIER
E. G. STRAUS
F. WOLF

SUPPORTING INSTITUTIONS

UNIVERSITY OF BRITISH COLUMBIA
CALIFORNIA INSTITUTE OF TECHNOLOGY
UNIVERSITY OF CALIFORNIA
MONTANA STATE UNIVERSITY
UNIVERSITY OF NEVADA
NEW MEXICO STATE UNIVERSITY
OREGON STATE COLLEGE
UNIVERSITY OF OREGON
OSAKA UNIVERSITY
UNIVERSITY OF SOUTHERN CALIFORNIA
STANFORD UNIVERSITY
UNIVERSITY OF TOKYO
UNIVERSITY OF UTAH
WASHINGTON STATE COLLEGE
UNIVERSITY OF WASHINGTON

* * *

AMERICAN MATHEMATICAL SOCIETY
CALIFORNIA RESEARCH CORPORATION
HUGHES AIRCRAFT COMPANY
SPACE TECHNOLOGY LABORATORIES
NAVAL ORDNANCE TEST STATION

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be typewritten (double spaced), and the author should keep a complete copy. Manuscripts may be sent to any one of the four editors. All other communications to the editors should be addressed to the managing editor, L. J. Paige at the University of California, Los Angeles 24, California.

50 reprints per author of each article are furnished free of charge; additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is published quarterly, in March, June, September, and December. The price per volume (4 numbers) is $12.00; single issues, $3.50. Back numbers are available. Special price to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: $4.00 per volume; single issues, $1.25.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 2120 Oxford Street, Berkeley 4, California.

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), No. 6, 2-chome, Fujimi-cho, Chiyoda-ku, Tokyo, Japan.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.

Pacific Journal of Mathematics

Vol. 10, No. 4 December, 1960