CRITERIA FOR SOLVABILITY OF CERTAIN CONGRUENCES

JOSEPH B. MUSKAT

1. Lower case italics will denote rational integers, while lower case Greek letters will denote algebraic integers. The Law of Quadratic Reciprocity can be formulated as follows:

If p and q are distinct odd primes, then q is a quadratic residue (mod p) *if and only if* $(-1)^{(p-1)/2}p$ *is a quadratic residue* (mod q).

Let χ_p denote the non-principal quadratic character (mod p) and let ζ_p be a primitive pth root of unity. Then

$$(-1)^{(p-1)/2}p = \tau(\chi_p)^2, \qquad \text{where } \tau(\chi_p) = \sum_{n=1}^{p-1} \chi_p(n)\zeta_p^n.$$

This suggests the following generalization, due to N. C. Ankeny:

Let r be an odd prime. Let $Q(\zeta_r)$ denote the cyclotomic field obtained by adjoining a primitive rth root of unity ζ_r to the field of rationals Q. Let q be a prime different from r. If f is the smallest positive integer such that $q^f \equiv 1$ (mod r), *and $ef = r - 1$, then the ideal (q) is decomposed into $\mathfrak{Q}_1\mathfrak{Q}_2 \ldots \mathfrak{Q}_e$, where the $\mathfrak{Q}_j$ are prime ideals in $Q(\zeta_r)$.*

Let p be a prime $\equiv 1$ (mod r). *Let χ_p be a primitive rth power multiplicative character* (mod p). *Let*

$$\tau(\chi_p) = \sum_{n=1}^{p-1} \chi_p(n)\zeta_p^n.$$

$\tau(\chi_p)$ is called a Gaussian sum, or Lagrange's resolvent. Note that $\tau(\chi_p)^r \in Q(\zeta_r)$, but $\tau(\chi_p) \notin Q(\zeta_r)$.

Ankeny proved that

$$\tau(\chi_p)^{q^f-1} \equiv \chi_p(q)^{-f} \text{ (mod } q). \tag{1}$$

Consequently, if $\mathfrak{Q}$ is any one of the prime divisors of (q) in $Q(\zeta_r)$, q is an rth power (mod p) *if and only if $\tau(\chi_p)^r$ is an rth power residue in $Q(\zeta_r)/\mathfrak{Q}$; i.e.,*

$$\chi_p(q) = 1 \qquad \textit{if and only if } \tau(\chi_p)^r \equiv \beta^r \text{ (mod } \mathfrak{Q}) \tag{2}$$

for some $\beta \in Q(\zeta_r)$ (**1**, Theorem 2).

Received March 28, 1963. This research was supported in part 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, and in part by the National Science Foundation, Research Grant No. G11309. Reproduction in whole or in part is permitted for any purpose of the United States Government.

Let

$$\tau(\chi_p)^r = \sum_{j=1}^{r-1} b_j \zeta_r{}^j.$$

If $q \equiv 1 \pmod{r}$, then $Q(\zeta_r)/\mathfrak{Q}$ is the ground field of integers (mod q), since all the rth roots of unity are contained in the ground field. If h satisfies $h^r \equiv 1 \pmod{q}$, $h \not\equiv 1 \pmod{q}$, (2) becomes

$$\chi_p(q) = 1 \qquad \text{if and only if } \sum_{j=1}^{r-1} b_j h^j \text{ is an } r\text{th power (mod } q)$$

(1, Theorem B**)**.

If $q \not\equiv 1 \pmod{r}$, applying the reciprocity criterion necessitates working with congruences in algebraic number fields. There are, however, rational integral criteria which do not involve reciprocity. For example, let $q = 2$ and let r be a prime of form $2^t - 1$. Then, by (1),

$$\tau(\chi_p)^r \equiv \chi_p(2)^{-t} \pmod{2}.$$

This means that $\chi_p(2) = 1$ [2 is an rth power residue (mod p)] if and only if all the b_j are odd **(1**, pp. 1123–1124**)**. Otherwise just one of the b_j is odd, and knowing which b_j is odd enables one to determine easily the character of 2.

If f is even, let $u = f/2$. $q^u \equiv -1 \pmod{r}$. The following, where applicable, enables one to find $\chi_p(q)$ with less computation than (1) requires.

THEOREM 1. $\tau(\chi_p)^{q^u+1} \equiv p\chi_p(q)^u \pmod{q}$.

Proof.

$$\begin{aligned}\tau(\chi_p)^{q^u} &= \left[\sum_{n=1}^{p-1} \chi_p(n)\zeta_p{}^n\right]^{q^u} \equiv \sum_{n=1}^{p-1} \chi_p(n)^{q^u}\zeta_p{}^{nq^u} \\ &\equiv \sum_{n=1}^{p-1} \chi_p(n)^{-1}\zeta_p{}^{nq^u} \equiv \chi_p(q^u) \sum_{n=1}^{p-1} \chi_p(nq^u)^{-1}\zeta_p{}^{nq^u} \\ &\equiv \chi_p(q)^u\tau(\chi_p{}^{-1}) \pmod{q}.\end{aligned}$$

Hence

$$\tau(\chi_p)^{q^u+1} \equiv \tau(\chi_p)\tau(\chi_p{}^{-1})\chi_p(q)^u \equiv p\chi_p(q)^u \pmod{q},$$

since $\tau(\chi_p)$ and $\tau(\chi_p{}^{-1})$ are complex conjugates with absolute value $\sqrt{p}$. This completes our proof.

If $q = 2$ and r is a prime of form $2^u + 1$, then

$$\tau(\chi_p)^r \equiv p\chi_p(2)^u \equiv \chi_p(2)^u \pmod{2}.$$

Hence $\chi_p(2) = 1$ if and only if all the b_j are odd. If $\chi_p(2) \neq 1$, just one of the b_j is odd.

If $q = 2$, $r = 11$, then $u = 5$. $\tau(\chi_p)^{33} \equiv p\chi_p(2)^5 \equiv \chi_p(2)^5 \pmod{2}$. So $\tau(\chi_p)^{11} \equiv \theta\chi_p(2)^9 \pmod{2}$, where θ is a cube root of unity (mod 2). Since the three cube roots of unity are

$1, \quad \zeta_{11} + \zeta_{11}^3 + \zeta_{11}^4 + \zeta_{11}^5 + \zeta_{11}^9, \quad$ and $\quad \zeta_{11}^2 + \zeta_{11}^6 + \zeta_{11}^7 + \zeta_{11}^8 + \zeta_{11}^{10}$,

$\chi_p(2) = 1$ if and only if $b_1 \equiv b_3 \equiv b_4 \equiv b_5 \equiv b_9 \pmod 2$, and $b_2 \equiv b_6 \equiv b_7 \equiv b_8 \equiv b_{10} \pmod 2$.

This method for ascertaining $\chi_p(2)$ can be generalized to other values of r.

For $q \equiv -1 \pmod r$ there is a rational integral criterion involving the trace of $\tau(\chi_p)^r$. This is derived in Section 2. Special criteria for $r = 5$, $q = 3, 7$, and for $r = 7$, $q = 3, 5$, are also presented.

Earlier authors have discovered rth power residue criteria, for $r = 3, 5$, and 7, which are related to the rational integral coefficients of the Jacobi function $\pi(\chi_p^1, \chi_p^1) = \tau(\chi_p)^2/\tau(\chi_p^2)$. Relations between Jacobi function criteria and those involving rth power Gaussian sums are explored in Section 3. A counter-example to an old conjecture is presented.

Although the simplest way to ascertain whether $\chi_p(q) = 1$ is to use Euler's criterion, the criteria in this paper are useful where the relevant Gaussian sums or Jacobi functions are available. Coefficients of rth power Gaussian sums for $r = 5$, $p \leqslant 14{,}431$; $r = 7$, $p \leqslant 10{,}781$; $r = 11$, $p \leqslant 10{,}627$ appear in **(6)**. Note that the tabulated coefficients are $a_j = b_j/p$, $j = 1, \ldots, r-1$. (The a_j, rather than the b_j, are used in **(1)** and **(6)**.) Tables of the Jacobi function for $r = 5$ can be found in **(8**, p. 229**)** for $p < 1000$ and in **(9**, pp. 256–262**)** for $1000 < p < 10{,}000$.

Some of the results in this paper are drawn from the author's dissertation **(5)**. The author wishes to express his appreciation to Professor N. C. Ankeny, M.I.T., for his guidance and assistance.

Thanks are also due to the Research Laboratory for Electronics, Department of Electrical Engineering, M.I.T., for permission to use the TX-0 computer to compute values of Jacobi functions.

2. If $q \equiv -1 \pmod r$, let $\mathfrak{Q}$ be a fixed prime ideal divisor of q in $Q(\zeta_r)$. $Q(\zeta_r)/\mathfrak{Q} = K$ is a quadratic extension of the field of integers (mod q).

Given any $\alpha \in K$, the only other element of K with the same trace and norm is α^q. α is an rth power if and only if α^q is. Thus for $q \equiv -1 \pmod r$ the reciprocity law can be given the following rational integral formulation: $\chi_p(q) = 1$ *if and only if* $\tau(\chi_p)^r$ *has the trace and norm of an* r*th power in* K.

If $p \equiv u^2 \pmod q$ for some u, the norm of $u^{-r}\tau(\chi_p)^r$ is equal to $p^{-r} \cdot p^r \equiv 1 \pmod q$. $u^{-r}\tau(\chi_p)^r$ is an rth power if and only if $\tau(\chi_p)^r$ is. Thus if p is a quadratic residue (mod q), $\chi_p(q) = 1$ if and only if $u^{-r}\tau(\chi_p)^r$ has the trace of an rth power in K whose norm is $\equiv 1 \pmod q$.

Let n be a fixed quadratic non-residue (mod q). If p is a quadratic non-residue (mod q), then $p \equiv v^2 n \pmod q$, for some v. The norm of $v^{-r}\tau(\chi_p)^r$ is

$$v^{-2r}p^r \equiv v^{-2r}v^{2r}n^r \equiv n^r \pmod q.$$

Hence if p is a quadratic non-residue (mod q), $\chi_p(q) = 1$ if and only if $v^{-r}\tau(\chi_p)^r$ has the trace of an rth power in K whose norm is $\equiv n^r \pmod q$. For each $q \equiv -1 \pmod r$, therefore, it suffices to tabulate the traces of all rth powers in K with

norms 1 and n^r. Then one ascertains whether the trace of $u^{-r}\tau(\chi_p)^r$ or $v^{-r}\tau(\chi_p)^r$ appears on the appropriate list.

There can be at most $2r$ elements in K whose rth powers have a given trace and a given norm. If β has norm n, then the elements $\beta, \beta\zeta_r, \beta\zeta_r^2, \ldots, \beta\zeta_r^{r-1}$, $\beta^q, \beta^q\zeta_r, \beta^q\zeta_r^2, \ldots, \beta^q\zeta_r^{r-1}$ are $2r$ distinct elements whose rth powers have the same norm n^r and the same trace $\beta^r + \beta^{rq}$. Since exactly $q+1$ of the elements of K have norm n and thus rth powers with norm n^r, exactly $(q+1)/2r$ trace values correspond to elements of K with norm n^r which are rth powers.

Similarly, $q+1$ of the elements of K have norm 1. Two of these, 1 and -1, are elements of the ground field. Since each is its own conjugate, the number of rth power trace values associated with quadratic residues (mod q), is one more than the number associated with quadratic non-residues (mod q). Thus, $1 + (q+1)/2r$ trace values correspond to rth powers in K with norm 1. (Two of these trace values are 2 and -2, corresponding to 1 and -1.)

α is an rth power if and only if $-\alpha$ is. They have the same norm, but traces of opposite sign. Thus if t is the trace of an rth power with a given norm, then so is $-t$. Note that if $q \equiv 1 \pmod 4$, $(q+1)/2r$ is odd, so that the trace value zero appears just on the quadratic non-residue list. If $q \equiv 3 \pmod 4$, $1 + (q+1)/2r$ is odd, so the trace value zero appears just on the quadratic residue list. (See Table I.)

Computing the rth power trace values (by hand) is laborious. The following algorithm reduces this computation to a minimum.

Let ζ_r and $\zeta_r' = \zeta_r^q$ be a basis for K. Let $x\zeta_r + y\zeta_r'$ have rth power norm 1 (or n^r). Compute its rth power trace. Call it t. Then a sequence of elementary computations gives all the other elements of K whose rth powers have norm 1 (or n^r) and trace t or $-t$. Redundant computation of t or $-t$ can thus be avoided.

The algorithm depends upon the following theorem. The proof presented here is due to N. C. Ankeny. $S(\theta)$ will denote the trace of θ.

THEOREM 2. *If* $\alpha = x\zeta_r + y_1\zeta_r'$, $\beta = x\zeta_r + y_2\zeta_r'$, $y_1 \neq y_2$, *and* α *and* β *have the same norm, then* $S(\alpha^r) + S(\beta^r) \equiv 0 \pmod q$.

Proof. Since α and β have the same norm, there exists $\lambda \in K$ such that $\alpha = \beta\lambda^{q-1}$.

$$(\beta\lambda^{q-1} - \beta)^{r(q-1)} = (\alpha - \beta)^{r(q-1)} = [(y_1 - y_2)\zeta_r']^{r(q-1)} = 1.$$

Thus

$$\begin{aligned}\beta^{-r(q-1)} &= (\lambda^{q-1} - 1)^{r(q-1)} = [(\lambda^{q-1} - 1)^q/(\lambda^{q-1} - 1)]^r \\ &= [(\lambda^{1-q} - 1)/(\lambda^{q-1} - 1)]^r = -\lambda^{r(1-q)}.\end{aligned}$$

Hence $\lambda^{r(1-q)} = -\beta^{r(1-q)}$. Also, $\lambda^{r(q-1)} = -\beta^{r(q-1)}$. Then

$$\begin{aligned}S(\alpha^r) + S(\beta^r) &= \alpha^r + \alpha^{rq} + \beta^r + \beta^{rq} \\ &= \beta^r\lambda^{r(q-1)} + \beta^{rq}\lambda^{r(1-q)} + \beta^r + \beta^{rq} \\ &= -\beta^{r+r(q-1)} - \beta^{rq+r(1-q)} + \beta^r + \beta^{rq} \\ &= -\beta^{rq} - \beta^r + \beta^r + \beta^{rq} = 0.\end{aligned}$$

If $(x\zeta_r + y\zeta_r')^r$ has norm 1 or n^r, let m denote the norm of $x\zeta_r + y\zeta_r'$; i.e., $(x\zeta_r + y\zeta_r')(x\zeta_r' + y\zeta_r) = m$, or

$$x^2 + y^2 + (\zeta_r^2 + \zeta_r'^2)xy = m. \tag{3}$$

Step 1 of algorithm: Set $x = 0$. Go to step 3.

Step 2: Increase x by 1. If the new value of x has appeared in a previously generated cycle, go to Step 2.

Step 3: For this value of x, does (3), as a congruence (mod q), have roots? If not, go to Step 2.

Step 4: Generate a cycle of values, as follows: Set $x = z_0$, and let the two roots of (3) be z_{-1} and z_1. If $x = z_1$, then $y = z_0$ is a root of (3), by symmetry. Call the other root z_2. Again by symmetry, if $x = z_2$, $y = z_1$ is a root. Call the other root z_3. Continuing this process generates a *cycle*. It is shown in **(5**, pp. 30–35**)** that $z_0 + z_r \equiv 0 \pmod{q}$, so that the cycle has period $2r$.

Step 5: Compute the rth power trace value t (or $-t$) for the cycle. If all the rth power trace values for the list have been found, stop. Otherwise, go to Step 2.

For all z_n in the cycle, $z_n\zeta_r + z_{n+1}\zeta_r'$ and $z_n\zeta_r + z_{n-1}\zeta_r'$ have norm m, since (z_n, z_{n+1}) and (z_n, z_{n-1}) satisfy (3). By symmetry and Theorem 2,

$$\begin{aligned} S((z_0\zeta_r + z_{-1}\zeta_r')^r) &= -S((z_0\zeta_r + z_1\zeta_r')^r) = -S((z_1\zeta_r + z_0\zeta_r')^r) \\ &= S((z_1\zeta_r + z_2\zeta_r')^r) = S((z_2\zeta_r + z_1\zeta_r')^r) = -S((z_2\zeta_r + z_3\zeta_r')^r) \\ &= -S((z_3\zeta_r + z_2\zeta_r')^r) = S((z_3\zeta_r + z_4\zeta_r')^r) = S((z_4\zeta_r + z_3\zeta_r')^r) = \ldots . \end{aligned}$$

Thus all the rth power trace values are the same except for sign. The $4r$ pairs $(z_n, z_{n\pm1})$, $n = 0, 1, 2, \ldots, 2r - 1$, are distinct (so that all the elements in K having norm m and rth power trace $\pm t$ have been exhausted) except for two cases. In one, which always occurs on the quadratic residue list, the cycle contains $x = 0$, $y = \pm 1$, and entries with $x = y$. Each pair occurs twice in the cycle. The rth power trace values are 2 and -2. In the other case, the cycle contains values of x for which the two roots of (3) are equal and entries with $x + y \equiv 0 \pmod{q}$. Each pair occurs twice in the cycle and the rth power trace value is zero.

Table I contains rth power trace values for several values of $q \equiv -1 \pmod{r}$, $r = 5, 7, 11$.

If both q and r are small, one could list all the b_j combinations (mod q) and determine which correspond to rth powers in $Q(\zeta_r)/\mathfrak{Q}$.

$$\sum_{j=1}^{r-1} b_j \zeta_r^{\,j}$$

is an rth power in $Q(\zeta_r)/\mathfrak{Q}$ if and only if its image

$$\sum_{j=1}^{r-1} b_j \zeta_r^{\,kj}, \qquad 1 \leqslant k \leqslant r - 1,$$

under the automorphism $\zeta_r \to \zeta_r^{\,k}$, is an rth power. The same holds for

https://doi.org/10.4153/CJM-1964-034-5 Published online by Cambridge University Press

TABLE I

TABLE OF RESIDUE CLASSES (mod q) FOR THE TRACE OF $u^{-r}\tau(\chi_p)^r$ OR $v^{-r}\tau(\chi_p)^r$ IF AND ONLY IF p IS AN rTH POWER RESIDUE (mod q)

	$p \pmod q$		
q	Quadratic residue	Quadratic non-residue	n
	$r = 5$		
19	0, ±2	±8	2
29	±1, ±2	0, ±3	2
59	0, ±1, ±2, ±11	±8, ±11, ±19	2
79	0, ±2, ±9, ±13, ±25	±2, ±13, ±31, ±39	3
89	±1, ±2, ±12, ±36, ±41	0, ±6, ±27, ±38, ±44	3
109	±2, ±19, ±28, ±32, ±41, ±44	0, ±1, ±13, ±20, ±28, ±52	2
139	0, ±2, ±5, ±23, ±29, ±37, ±46, ±54	±2, ±8, ±11, ±29, ±39, ±47, ±54	2
149	±1, ±2, ±8, ±21, ±32, ±40, ±41, ±62	0, ±17, ±29, ±42, ±49, ±52, ±55, ±66	2
179	0, ±1, ±2, ±6, ±19, ±34, ±46, ±76, ±80, ±82	±8, ±13, ±16, ±19, ±29, ±72, ±73, ±80, ±87	2
199	0, ±2, ±8, ±20, ±61, ±62, ±67, ±72, ±81, ±90, ±93	±1, ±2, ±18, ±30, ±37, ±38, ±42, ±79, ±92, ±95	3
	$r = 7$		
13	±2	0,	2
41	±1, ±2	0, ±1	3
83	0, ±1, ±2, ±13	±13, ±16, ±29	2
97	±2, ±25, ±30, ±41	0, ±23, ±27, ±34	5
139	0, ±2, ±30, ±56, ±63, ±64	±13, ±14, ±16, ±49, ±64	2
167	0, ±1, ±2, ±8, ±13, ±21, ±62	±6, ±17, ±55, ±58, ±64, ±72	5
181	±2, ±32, ±45, ±53, ±64, ±69, ±89	0, ±8, ±13, ±20, ±22, ±62, ±88	2
	$r = 11$		
43	0, ±2	±21	2
109	±2, ±10, ±11	0, ±27, ±30	2
131	0, ±1, ±2, ±38	±5, ±62, ±64	2
197	±1, ±2, ±6, ±28, ±34	0, ±31, ±38, ±49, ±69	2

$$\sum_{j=1}^{r-1} tb_j\zeta_r^{kj}, \qquad 1 \leqslant k \leqslant r-1, 1 \leqslant t \leqslant q-1, q \not\equiv 1 \pmod r).$$

It suffices, therefore, to examine one of these elements. We shall take the element ("representative") whose coefficients, juxtaposed, give the smallest number.

Since the product of $\tau(\chi_p)^r$ and its complex conjugate $\tau(\chi_p{}^{-1})^r$ is p^r, a rational integer,

$$\sum_{j=1}^{r-2} b_j b_{j+1} = \sum_{j=1}^{r-1} b_j b_{j+k}, \qquad k = 2, \ldots, (r-1)/2, \tag{4}$$

where $b_{n+r} = b_n$, $b_r = 0$ **(1**, p. 1115**)**. It is therefore necessary to consider only those sets which satisfy (4) as congruences (mod q).

https://doi.org/10.4153/CJM-1964-034-5 Published online by Cambridge University Press

This approach was used for the following four cases: $r = 5$, $q = 3, 7$; $r = 7$, $q = 3, 5$. The rth power representatives were determined by using Theorem 1. The juxtaposed coefficients of the representatives are presented in Table II.

TABLE II

REPRESENTATIVES OF SETS WHICH SATISFY (4) (mod q)

	Quadratic residues (mod q)			Quadratic non-residues (mod q)		
	rth powers	Not rth powers		rth powers	Not rth powers	
$q = 3$ $r = 5$	1111	0001		1221	0121	
$q = 3$ $r = 7$	111111 112122	000001	010112	001011	001101	010111
$q = 5$ $r = 7$	011413 111111 112122	000001 010114 010242 012322 114241	010112 010231 010433 113321	001011 013434 114144	001101 010113 013223 014331 112323	010111 012124 013341 014412
$q = 7$ $r = 5$	0001 1111	0125 1136 1241	0163 1152	0141 1661	0132 1143 1351	0154 1165

The following conclusions are apparent from Table II:

(5) 3 *is a fifth power* (mod p) *if and only if* $b_1 \equiv b_4 \pmod 3$ *and* $b_2 \equiv b_3 \pmod 3$.

(6) 3 *is a seventh power* (mod p) *if and only if* $b_1 \equiv b_2 \equiv b_4 \pmod 3$ *and* $b_3 \equiv b_5 \equiv b_6 \pmod 3$.

(7) 5 *is a seventh power* (mod p) *if and only if either* $b_1 \equiv b_2 \equiv b_4 \pmod 5$ *and* $b_3 \equiv b_5 \equiv b_6 \pmod 5$ *or* $b_1 + b_2 + b_4 \equiv b_3 + b_5 + b_6 \equiv 0 \pmod 5$.

(8) 7 *is a fifth power* (mod p) *if and only if the following is satisfied*:

Define $b_0 = 0$. *If* p *is a quadratic residue* (mod q), *four of the five* b_j *are congruent to each other* (mod 7). *If* p *is a quadratic non-residue* (mod q), *there are two pairs of congruent coefficients* (mod 7).

3. Define the Jacobi function

$$\pi(\chi_p{}^i, \chi_p{}^j) = \tau(\chi_p{}^i)\tau(\chi_p{}^j)/\tau(\chi_p{}^{i+j}), \qquad i, j, i + j \not\equiv 0 \pmod r.$$

Let $\pi\ (i, j)$ denote $\pi(\chi_p{}^i, \chi_p{}^j)$.

https://doi.org/10.4153/CJM-1964-034-5 Published online by Cambridge University Press

$$(9) \qquad \pi(i,j) = \sum_{n=1}^{p-1} \chi_p{}^i(n)\chi_p{}^j(1-n) \in Q(\zeta_r) \qquad \textbf{(3, } p. \text{ 152)}.$$

This relation is used to compute Jacobi functions. Given the Jacobi functions, one can compute the rth power Gaussian sums, as

$$\tau(\chi_p)^r = p \prod_{j=1}^{r-2} \pi(1,j) \qquad \textbf{(3, } p. \text{ 152)}.$$

Reciprocity criteria can be formulated in terms of Jacobi functions. The simplest cases are described by the following theorem.

THEOREM 3. (*a*) *If* $q \equiv 2 \pmod r$ *and* $2^{r-1} \not\equiv 1 \pmod{r^2}$, *then* $\chi_p(q) = 1$ *if and only if* $\pi(1,1)$ *is an* rth *power in* $Q(\zeta_r)/\mathfrak{Q}$.

(*b*) *If* $q \equiv -2 \pmod r$, $r > 3$, *and* $2^{r-1} \not\equiv 1 \pmod{r^2}$, *then* $\chi_p(q) = 1$ *if and only if* $\pi(1,1)$ *is an* rth *power in* $Q(\zeta_r)/\mathfrak{Q}$.

Note. The restriction $2^{r-1} \not\equiv 1 \pmod{r^2}$ excludes only $r = 1093$ and $r = 3511$ out of all the primes less than 500,000 **(4)**.

Proof of (*a*).

$$\tau(\chi_p)^q = \left[\sum_{n=1}^{p-1} \chi_p(n)\zeta_p{}^n\right]^q \equiv \sum_{n=1}^{p-1} \chi_p(n)^q\zeta_p{}^{nq}$$

$$\equiv \chi_p(q)^{-q} \sum_{n=1}^{p-1} \chi_p(nq)^q\zeta_p{}^{nq} \equiv \chi_p(q)^{-q}\tau(\chi_p{}^q)$$

$$\equiv \chi_p(q)^{-2}\tau(\chi_p{}^2) \pmod q.$$

Hence

$$\chi_p(q)^{-2} \equiv \tau(\chi_p)^q/\tau(\chi_p{}^2) \equiv \tau(\chi_p)^{q-2}\tau(\chi_p)^2/\tau(\chi_p{}^2)$$
$$\equiv \tau(\chi_p)^{q-2}\pi(1,1) \pmod q.$$

Let f be the least positive integer such that $q^f \equiv 1 \pmod r$. Raise both sides of the congruence to the $(q^f-1)/r$ power:

$$\tau(\chi_p)^{(q-2)(q^f-1)/r}\pi(1,1)^{(q^f-1)/r} \equiv \chi_p(q)^{-2(q^f-1)/r} \pmod q.$$

Let $q = hr + 2$. Then

$$q^f - 1 = (hr+2)^f - 1 \equiv 2^{f-1}frh + 2^f - 1 \equiv 2^{-1}frh + 2^f - 1 \pmod{r^2},$$

since $2^f \equiv q^f \equiv 1 \pmod r$. Then

$$\tau(\chi_p)^{h(q^f-1)}\pi(1,1)^{(q^f-1)/r} \equiv \chi_p(q)^{-fh-2(2^f-1)/r} \pmod q.$$

Applying (1) gives

$$\chi_p(q)^{-fh}\pi(1,1)^{(q^f-1)/r} \equiv \chi_p(q)^{-fh-2(2^f-1)/r} \pmod q,$$

or

$$\pi(1,1)^{(q^f-1)/r} \equiv \chi_p(q)^{-2(2^f-1)/r} \pmod q.$$

https://doi.org/10.4153/CJM-1964-034-5 Published online by Cambridge University Press

Since r^2 does not divide $2^{r-1} - 1$, it does not divide $2^f - 1$. Since

$$\pi(1, 1) \in Q(\zeta_r)/\mathfrak{Q},$$

which contains q^f elements, the theorem follows.

The proof of (b) is similar.

Let

$$\pi(1, 1) = \sum_{j=1}^{r-1} d_j \zeta_r^j.$$

Then

$$\pi(k, k) = \sum_{j=1}^{r-1} d_j \zeta_r^{jk}.$$

Pepin showed that $\chi_p(2) = 1$ if and only if all the d_j, $j = 1, \ldots, r-1$, are odd **(7)**. Specifically, $\pi(j, j) \equiv \chi_p^{-2j}(2) \pmod 2$. This is an easy consequence of (9). We have

$$\pi(k, k)^q = \left[\sum_{j=1}^{r-1} d_j \zeta_r^{jk}\right]^q \equiv \sum_{j=1}^{r-1} d_j \zeta_r^{jkq} \equiv \pi(kq, kq) \pmod q. \tag{10}$$

Since the product of $\pi(1, 1)$ and its complex conjugate is p, a rational integer,

$$\sum_{j=1}^{r-2} d_j d_{j+1} = \sum_{j=1}^{r-1} d_j d_{j+k}, \qquad k = 2, \ldots, \tfrac{1}{2}(r-1),$$

where $d_{r+n} = d_n$, $d_r = 0$. Table II is therefore applicable to the d_j also.

It follows from Theorem 3 that (5), (7), and (8) hold if the b_j are replaced by d_j. (6) also holds if the d_j replace the b_j:

$$\begin{aligned}
\tau(\chi_p)^7 &= \tau(\chi_p)^8/\tau(\chi_p^2)^4 \cdot \tau(\chi_p^2)^4/\tau(\chi_p^4)^2 \cdot \tau(\chi_p^4)^2/\tau(\chi_p) \\
&= \pi(1, 1)^4 \pi(2, 2)^2 \pi(4, 4) \\
&\equiv \pi(1, 1) \pi(3, 3) \pi(2, 2)^2 \pi(4, 4), \qquad \text{by (10)}, \\
&\equiv p\pi(5, 5)^3 \pi(2, 2)^2 \\
&\equiv p^3 \pi(5, 5) \equiv p\pi(5, 5) \pmod 3.
\end{aligned}$$

These criteria for $q = 3$, $r = 5, 7$, were given by Pepin **(7)**.

Bickmore suggested the following generalization **(2**, p. 35**)**: 3 *is an* rth *power residue* (mod p) *if and only if all the* d_j *whose subscripts are quadratic residues* (mod r) *are congruent to each other* (mod 3) *and all the other* d_j *are congruent to each other* (mod 3). This is incorrect. 3 is an 11th power residue (mod 683). But the d_j, $j = 1, \ldots, 10$, as generated by the primitive root $g = 5$, are 6, 10, 22, 16, 12, 7, 14, -6, 16, 12.

References

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

2. C. E. Bickmore, *On the numerical factors of $a^n - 1$ (Second notice)*, Messenger Math., *26* (1896), 1–38.
3. H. Davenport and H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen*, J. reine angew. Math., *172* (1935), 151–182.
4. H. Riesel, *Note on the congruence $a^{p-1} \equiv 1 \pmod{p^2}$*, Math. of Comp., *18* (1964), 149–150.
5. J. B. Muskat, *Criteria for prime power residuacity*, Doctoral Dissertation, M.I.T. (1961).
6. ——— *On certain prime power congruences*, Abh. Math. Sem. Univ. Hamburg, *26* (1963), 102–110.
7. T. Pepin, *Mémoire sur les lois de réciprocité relatives aux résidues de puissances*, Pontif. accad. sci., Rome, *31* (1877), 40–148.
8. H. W. Lloyd Tanner, *On the binomial equation $x^p - 1 = 0$: quinquesection*, Proc. Lond. Math. Soc., *18* (1887), 214–234.
9. ——— *On complex primes formed with the fifth roots of unity*, Proc. Lond. Math. Soc., *24* (1893), 223–272.

University of Pittsburgh