A CHARACTERISTIC PROPERTY OF QUADRATIC RESIDUES

JOHN B. KELLY

1. Introduction. Let $p$ be an odd prime. We denote by $R_p$ the set of quadratic residues (mod $p$), by $N_p$ the set of quadratic nonresidues, and by $r_i, i = 1, 2, \ldots, (p-1)/2,$ and $n_j, j = 1, 2, \ldots, (p-1)/2,$ the elements of $R_p$ and $N_p,$ respectively. We shall indicate by $r+N_p$ the set of all residues (mod $p$) obtained by adding the (fixed) quadratic residue, $r,$ to the various elements of $N_p.$ A similar significance attaches to such expressions as $r+R_p,$ $n+R_p,$ and $n+N_p.$

The following two theorems are well known.

**Theorem 1.** Let $p$ be of the form $4k+1,$ $r$ an arbitrary quadratic residue, $n$ an arbitrary nonresidue. The sets $r+N_p$ and $n+R_p$ consist of $k$ quadratic residues and $k$ quadratic nonresidues.

**Theorem 2.** Let $p$ be of the form $4k-1,$ $r$ an arbitrary quadratic residue, $n$ an arbitrary nonresidue. The sets $r+N_p$ and $n+R_p$ consist of $0,$ $k-1$ quadratic residues, and $k-1$ nonresidues.

One may ask whether or not the “equidistribution” property mentioned in Theorems 1 and 2 actually characterizes the quadratic residues among subsets of $(p-1)/2$ nonzero elements of the cyclic group of order $p.$ It is also natural to inquire whether or not there exist subsets with this property when we replace the prime modulus, $p,$ by a composite modulus, $n.$ These questions are answered by the two theorems which follow.

**Theorem 3.** Let $m$ be an integer of the form $4k+1.$ Let the least positive residues mod $m$ be divided into two mutually exclusive classes of $2k$ elements each. Call these classes $A$ and $B.$ Suppose that $A$ and $B$ may be chosen so that:

(a) $1 \in A.$

(b) For every choice of $a^* \in A,$ the set $a^*+B$ contains $k$ elements of $A$ and $k$ elements of $B.$

(c) For every choice of $b^* \in B,$ the set $b^*+A$ contains $k$ elements of $A$ and $k$ elements of $B.$

Then:

(1) $m$ is a prime.

(2) $A$ consists of the quadratic residues mod $m$ and $B$ consists of the quadratic nonresidues mod $m.$

Presented to the Society, December 29, 1953; received by the editors March 7, 1953.
Theorem 4. Let \( m \) be an integer of the form \( 4k - 1 \). Let the \( 4k - 2 \) least positive residues mod \( m \) be divided into two mutually exclusive classes of \( 2k - 1 \) elements each. Call these classes \( A \) and \( B \). Suppose that \( A \) and \( B \) may be chosen so that:

(a') \( 1 \in A \).

(b') For every choice of \( a^* \in A \), the set \( a^* + B \) contains \( 0, k - 1 \) elements of \( A \), and \( k - 1 \) elements of \( B \).

Then:

(1') \( m \) is a prime.

(2') \( A \) consists of the quadratic residues mod \( m \) and \( B \) consists of the quadratic nonresidues mod \( m \).

Hypothesis (b) of Theorem 3 implies:

(d) If \( a \not\in A \), then \( m - a \in A \);

while hypothesis (b') of Theorem 4 implies:

(d') If \( a \not\in A \), then \( m - a \not\in B \); in other words, \( B = -A \).

The analogue, (c'), of (c), is an immediate consequence of (b') and (d').

It is of some interest to observe that the hypotheses of Theorems 3 and 4 involve only the additive group (mod \( m \)) whereas the conclusion involves the multiplicative group. This is not overly surprising, perhaps, when one recalls that the multiplicative group (mod \( m \)) is isomorphic to the group of automorphisms of the additive group (mod \( m \)).

The main part of this paper, §3, is concerned with the proof of Theorem 3. The proof of Theorem 4 so closely parallels the proof of Theorem 3 that we have not included it. For the sake of completeness, we have given a proof of Theorem 1 in §2, inasmuch as neither this theorem nor Theorem 2 is explicitly stated in readily available sources. Again, since the proof of Theorem 2 so closely resembles that of Theorem 1, we have seen fit to omit it.

We conclude with some remarks (§4) on the extension of our results to finite fields, and on some work of Perron closely related to ours.

2. Proof of Theorem 1. Let \( p = 4k + 1 \). Consider the set, \( H_p \), of all expressions of the form \( r_i + n_j, i = 1, 2, \ldots, (p - 1)/2, j = 1, 2, \ldots, (p - 1)/2 \). We show that all nonzero residues are represented equally often in \( H_p \). (0 is not represented, since \( r \in R_p \) implies \( p - r \in R_p \) when \( p \equiv 1 \) (mod 4).) To every representation of 1, \( 1 = r + n \), corresponds a unique representation of \( g \), \( g = r' + n' \), where \( r' = gr \) and \( n' = gn \) when \( g \) is a quadratic residue and \( r' = gn, n' = gr \) when \( g \) is a nonresidue. Conversely, to every representation of \( g \), \( g = r' + n' \), cor-
responds a unique representation of \(1, 1 = r + n\), where \(r = g^{-1}r', n = g^{-1}n'\) when \(g\) is a quadratic residue and \(r = g^{-1}n', n = g^{-1}r'\) when \(g\) is a nonresidue. Thus a one-to-one correspondence exists between the representations of 1 and the representations of any other nonzero residue. Hence \(H_p\) contains as many representations of quadratic residues as of nonresidues.

Suppose now that the set \(1 + N_p\) contained more (fewer) quadratic residues than nonresidues. Then the set \(r_i + N_p = r_i(1 + r_i^{-1}N_p) = r_i(1 + N_p)\) would also contain more (fewer) quadratic residues than nonresidues. Consequently \(H_p = \cup_i (r_i + N_p)\) would contain more (fewer) quadratic residues than nonresidues, a contradiction.

It follows that the set \(1 + N_p\) contains as many quadratic residues as nonresidues; the sets \(r_i + N_p = r_i(1 + N_p)\) and \(n_j + R_p = n_j(1 + N_p)\) also have this property.

3. Proof of Theorem 3. Theorem 3 is considerably more difficult to prove than Theorem 1, even though it may be regarded as a converse of Theorem 1. We shall discuss the reason for this situation in §4. Our principal tool is cyclotomy.

We define the symbol

\[
\{l, A\} \quad \left(\begin{array}{c} m \\
\end{array}\right)
\]

as follows:

\[
\begin{align*}
\{l, A\} \quad \left(\begin{array}{c} m \\
\end{array}\right) &= 1, \quad l \equiv l' \pmod{m}, \quad l' \in A; \\
\{l, A\} \quad \left(\begin{array}{c} m \\
\end{array}\right) &= -1, \quad l \equiv l' \pmod{m}, \quad l' \in B; \\
\{l, A\} \quad \left(\begin{array}{c} m \\
\end{array}\right) &= 0, \quad l \equiv 0 \pmod{m}.
\end{align*}
\]

It follows from (b), (c), and (d) that

\[
\begin{align*}
\text{(e)} \quad \sum_{j \in A} \left\{\frac{n - j, A}{m}\right\} &= -1 - \left\{\frac{n, A}{m}\right\} \quad , \quad n \not\equiv 0 \pmod{m}; \\
\text{(f)} \quad \sum_{j \in A} \left\{\frac{n - j, A}{m}\right\} &= \frac{m - 1}{2}, \quad n \equiv 0 \pmod{m}.
\end{align*}
\]
Let $\omega$ be any algebraic integer with the properties
\[(g) \quad \omega^m = 1; \quad \omega \neq 1.\]

Let
\[(h) \quad \alpha(\omega, A) = \sum_{n=0}^{m-1} \binom{n}{m} \omega^n,\]
and
\[(i) \quad \beta(\omega, A) = \sum_{j \in A} \omega^j.\]

Then, using (e), (f), and (g), we have
\[
\alpha(\omega, A)\beta(\omega, A) = \sum_{j \in A} \sum_{n=0}^{m-1} \binom{n}{m} \omega^{n+j} = \sum_{n=1}^{m} \omega^n \sum_{j \in A} \binom{n-j}{m}
\]
\[
= \frac{m-1}{2} + \sum_{n=1}^{m-1} \frac{-1 - \binom{n}{m}}{2} \omega^n
\]
\[
= -\frac{\alpha(\omega, A)}{2} + \frac{m}{2}.
\]

Hence $\alpha(\omega, A)(2\beta(\omega, A) + 1) = m$. But $2\beta(\omega, A) + 1 = 2\beta(\omega, A) + 1 - \sum_{j=0}^{m-1} \omega^j = \alpha(\omega, A)$.

Thus $\alpha^2(\omega, A) = m$ and
\[(j) \quad \alpha(\omega, A) = \pm \sqrt{m}.
\]

Since the quadratic residues of a prime $p \equiv 1 \pmod{4}$ have, according to Theorem 1, the properties (a), (b), (c), and (d), it follows that
\[(k) \quad \sum_{n=0}^{p-1} \left\lfloor \frac{n}{p} \right\rfloor \omega^n = \pm \sqrt{p},
\]
where
\[
\left[ \frac{n}{p} \right]
\]
is the Legendre symbol and $\omega$ is a primitive $p$th root of unity. Actually the indeterminacy of sign may be eliminated, but this requires a deeper analysis than is necessary for the proof of our theorem.

It is obvious that
\[(l) \quad \alpha(\omega, A) = -\alpha(\omega, B).\]
We prove now that \( m \) is a prime. If \( m \) is neither a square nor a power of a prime, we obtain a contradiction fairly readily. For in this case we may put \( m = p^t Q \) where \( p \) is a prime, \((p, Q) = 1\), and \( Q \) is not a square. If we let \( \omega = e^{2 \pi i/p} \), a comparison of (h) and (j) reveals that the field \( R(\omega) \) contains quadratic irrationalities other than \((\pm p)^{1/2}\), which is impossible.

Case 1. \( m \) is a square. We may put \( m = p^{2t} Q^2 \), where \( p \) is a prime and \((p, Q) = 1\). Let \( \omega = e^{2 \pi i/p} \) and

\[
r_j^{(1)} = \sum_{i \equiv j \pmod p} \left\{ i, A \right\}.
\]

Then

\[
\alpha(\omega, A) = \sum_{j=0}^{p-1} r_j^{(1)} \omega^j.
\]

Since \( 1 = -\sum_{j=1}^{p-1} \omega^j \), we have

\[
\alpha(\omega, A) = \sum_{j=1}^{p-1} (r_j^{(1)} - r_0^{(1)}) \omega^j.
\]

It follows from (j) that

\[
\sum_{j=1}^{p-1} (r_j^{(1)} - r_0^{(1)}) \omega^j = \pm p^t Q = \pm p^t Q \sum_{j=1}^{p-1} \omega^j.
\]

The irreducibility of the cyclotomic polynomial entails the linear independence of \( \omega, \omega^2, \omega^3, \ldots, \omega^{p-1} \), over the rational field.

Hence either

\[
r_j^{(1)} - r_0^{(1)} = p^t Q, \quad j = 1, 2, 3, \ldots, p - 1,
\]

or

\[
r_j^{(1)} - r_0^{(1)} = -p^t Q, \quad j = 1, 2, 3, \ldots, p - 1.
\]

Now

\[
\sum_{j=0}^{p-1} r_j^{(1)} = \sum_{n=1}^{m} \left\{ n, A \right\} = 0.
\]

Thus \( p r_0^{(1)} \pm p^t Q (p - 1) = 0 \), whence \( r_0^{(1)} = \pm p^{t-1} Q (p - 1) \), and \( r_j^{(1)} = \pm p^{t-1} Q, j = 1, 2, \ldots, p - 1 \). In particular

\[
r_1^{(1)} = \pm p^{t-1} Q.
\]

Now let \( \omega = e^{2 \pi i/p^2} \) and
\[ r_j^{(2)} = \sum_{i=j \,(\text{mod} \, p^2)}^{p^2-1} \left\{ \frac{i}{m} \right\}, \quad j = 0, 1, 2, \ldots, p^2 - 1. \]

Then

\[ \alpha(\omega, A) = \sum_{n=-\infty}^{\infty} \left\{ \frac{n}{m} \right\} \omega^n = \sum_{j=0}^{p^2-1} r_j^{(2)} \omega^j. \]

Using

\[ 1 = -\omega^p - \omega^{2p} - \cdots - \omega^{p^2-p}, \]

\[ \omega = -\omega^{p+1} - \omega^{2p+1} - \cdots - \omega^{p^2-p+1}, \]

\[ \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots, \]

\[ \omega^{p-1} = -\omega^{2p-1} - \omega^{3p-1} - \cdots - \omega^{p^2-1}, \]

and observing that each power of \( \omega \) from \( \omega^p \) to \( \omega^{p^2-1} \) occurs just once on the right-hand side in this scheme, we find that

\[ \alpha(\omega, A) = \sum_{j=0}^{p^2-1} (r_j^{(2)} - r_{k(j)}^{(2)}) \omega^j \]

where \( k(j) \equiv j \,(\text{mod} \, p) \), \( k(j) = 0, 1, 2, \ldots, p-1 \). It follows from \( j \) that \( \sum_{j=0}^{p^2-1} (r_j^{(2)} - r_{k(j)}^{(2)}) \omega^j = \pm p^i Q = \pm p^i Q \sum_{i=0}^{p^2-1} \omega^i. \) The irreducibility of the cyclotomic polynomial of order \( p^2 \) entails the linear independence of \( \omega^p, \omega^{p+1}, \omega^{p+2}, \ldots, \omega^{p^2-1} \) over the rational field. Hence

\[ r_j^{(2)} - r_{k(j)}^{(2)} = 0, \quad \text{if} \ j \neq 0 \,(\text{mod} \, p). \]

Thus

\[ r_1^{(2)} = r_{p+1}^{(2)} = r_{2p+1}^{(2)} = \cdots = r_{p^2-p+1}^{(2)}. \]

Now \( r_1^{(2)} = \sum_{i=0}^{p^2-1} r_i^{(2)} = \omega r_1^{(2)}. \) From \( m \) we obtain

\[ r_1^{(2)} = \pm p^{t-2} Q. \]

We continue this procedure, defining \( r_j^{(3)}, r_j^{(4)}, \ldots, r_j^{(h)}, \ldots \) in an obvious way, putting successively \( \omega = e^{2\pi i / p^3}, \omega = e^{2\pi i / p^4}, \ldots, \omega = e^{2\pi i / p^h}, \ldots \) in \( h \), and using the irreducibility of the cyclotomic polynomials of orders \( p^3, p^4, \ldots, p^h, \ldots \) to obtain the formula

\[ r_1^{(h)} = \pm p^{t-h} Q, \quad h \leq 2t. \]

It is permissible to take \( h = t+1 \), for \( t+1 \leq 2t \), so that \( \omega = e^{2\pi i / p^{t+1}} \) is an \( m \)th root of unity. But then \( h \) implies that \( r_1^{(t+1)} \) is not an integer, a contradiction.
Case 2. $m$ is a power of a prime. Even powers of primes have been covered in Case 1, so that we may suppose $m = p^{2t+1}$, $p \equiv 1 \pmod{4}$, $t \geq 1$. Let $\omega = e^{2\pi i/p}$ and

$$r_j^{(1)} = \sum_{i \equiv j \pmod{m}} \left\{ \frac{i}{m} \right\}. $$

Then, just as in Case 1 we have

$$\alpha(\omega, A) = \sum_{n=0}^{m-1} \left\{ \frac{n}{A} \right\} \omega^n = \sum_{j=0}^{p-1} r_j^{(1)} \omega^j = \sum_{j=1}^{p-1} (r_j^{(1)} - r_0^{(1)}) \omega^j,$$

whence, from (j),

$$\sum_{j=1}^{p-1} (r_j^{(1)} - r_0^{(1)}) \omega^j = \pm p^t p^{1/2}.$$

But from (k) there follows

$$p^t \sum_{j=1}^{p-1} \left[ \frac{j}{p} \right] \omega^j = \pm p^t p^{1/2},$$

so that

$$\sum_{j=1}^{p-1} (r_j^{(1)} - r_0^{(1)}) \omega^j = \pm \sum_{j=1}^{p-1} p^t \left[ \frac{j}{p} \right] \omega^j.$$

The linear independence of $\omega, \omega^2, \ldots, \omega^{p-1}$ over the rational field implies that either

$$r_j^{(1)} - r_0^{(1)} = p^t \left[ \frac{j}{p} \right], \quad j = 1, 2, \ldots, p - 1,$$

or

$$r_j^{(1)} - r_0^{(1)} = -p^t \left[ \frac{j}{p} \right], \quad j = 1, 2, \ldots, p - 1.$$

In either case,

$$\sum_{j=0}^{p-1} r_j^{(1)} = \pm p r_0^{(1)} \pm p^t \sum_{j=1}^{p-1} \left[ \frac{j}{p} \right] = pr_0^{(1)}.$$

As before, $\sum_{j=0}^{p-1} r_j^{(1)} = 0$. Hence $r_0^{(1)} = 0$ and

$$r_1^{(1)} = \pm p^t.$$

Now let $\omega = e^{2\pi i/p^2}$. Let
Then, as before,

\[
\sum_{j=0}^{p^2-1} r_j^{(2)} \omega^j = \sum_{j=p}^{p^2-1} (r_j^{(2)} - r_{k(j)}^{(2)}) \omega^j = \pm p^{t + 1/2},
\]

where \( k(j) \equiv j \pmod{p} \) and \( k(j) = 0, 1, 2, \ldots, p-1 \). But from (k) there follows

\[
\omega^p \sum_{j=1}^{p-1} \left[ \frac{l}{p} \right] \omega^j = \pm \omega^{p+1/2},
\]

whence

\[
\sum_{j=p}^{p^2-1} (r_j^{(2)} - r_{k(j)}^{(2)}) \omega^j = \pm \sum_{l=1}^{p-1} p^t \left[ \frac{l}{p} \right] \omega^l.
\]

The linear independence of \( \omega^p, \omega^{p+1}, \ldots, \omega^{p^2-1} \) over the rational field implies that

\[
r_j^{(2)} - r_{k(j)}^{(2)} = 0, \quad \text{if } j \not\equiv 0 \pmod{p}.
\]

Hence

\[
r_1^{(2)} = r_{p+1}^{(2)} = r_{2p+1}^{(2)} = \cdots = r_{p^2-p+1}^{(2)}.
\]

Now \( r_1^{(2)} = \sum_{i=0}^{p-1} r_{ip+1}^{(2)} = p r_1^{(2)} \). From (p) we obtain

\[
(r^{(2)}) = \pm p^{t-1}.
\]

Just as with Case 1 we may continue this procedure to obtain the formula

\[
(r^{(h)}) = \pm p^{t-h+1}, \quad h \leq 2t + 1.
\]

In (r) it is permissible to take \( h = t+2 \), since \( t+2 \leq 2t+1 \) if \( t \geq 1 \). Again, (r) implies that \( r_1^{(h)} \) is not an integer, a contradiction.

We have thus shown that \( m \) is a prime. We shall denote this prime by \( p \). The proof of (2) is almost immediate. Suppose there were two distinct splittings of the nonzero residues mod \( p \) with the properties described in the statement of the theorem. Call the corresponding pairs of sets \( A, B \) and \( A', B' \). It follows from (j) that either \( \alpha(\omega, A) = \alpha(\omega, A') \) or \( \alpha(\omega, A) = \alpha(\omega, B') \). But, looking at (h) we see that either of these equations would contradict the linear independence of \( \omega, \omega^2, \omega^3, \ldots, \omega^{p-1} \) over the rational field.
4. **Finite fields.** Our proof of Theorem 1 used nothing more than the fact that the residues mod \( p \) form a finite field. Hence Theorems 1 and 2 have obvious analogues for the Galois fields \( GF(p^n) \). The analogue of Theorem 1 will hold if \( p^n \equiv 1 \pmod{4} \); otherwise the analogue of Theorem 2 will hold.

We show, by means of a counter-example, that the expected analogues of Theorems 3 and 4 do not hold for finite fields in general. That is, there exist splittings of the nonzero elements of \( GF(p^n) \) other than the splitting into squares and nonsquares which have the equidistribution property.

Consider the finite field, \( GF(3^2) \), generated over the field of residues \( \pmod{3} \) by a solution, \( X \), of the irreducible equation \( X^2 + 1 = 0 \). The square elements of \( GF(3^2) \) are then 1, 2, \( \lambda \), and \( 2\lambda \); the nonsquares are 1+\( \lambda \), 1+2\( \lambda \), 2+\( \lambda \) and 2+2\( \lambda \). One can readily verify, however, that the splitting \((1, 2, 1+\lambda, 2+2\lambda), (\lambda, 2\lambda, 1+2\lambda, 2+\lambda)\) also has the equidistribution property.

These considerations indicate that in proving parts 2 and 2' of Theorems 3 and 4, we must use more than the fact that the residues \( \pmod{p} \) form a finite field. Our use of cyclotomy is, from this point of view, not unnatural.

Perron [1] has proved theorems which may be derived from Theorems 1 and 2 if one regards zero as a quadratic residue. Thus, for \( p = 4k - 1 \), he has shown that if \( A \) is the set of quadratic residues, \( \pmod{p} \), including zero, and if \( a \) is any residue prime to \( p \), the set \( a + A \) consists of \( k \) residues and \( k \) nonresidues. This is also true of the set \( A' \) consisting of 0 and the quadratic nonresidues \( \pmod{p} \). It would be interesting to know whether or not the sets \( A \) and \( A' \) are the only sets with \( 2k \) elements which have this property. Without substantial modification our method will not yield an answer to this question. An example given by Perron for the case \( m = 15 \) shows, however, that the complete analogue of Theorem 4 is false; that is, the existence of sets with this property for an arbitrary modulus does not force this modulus to be a prime.

**Reference**


*Michigan State College*