Distribution of residues modulo \( p \)

by

S. Gun (Mississauga), Florian Luca (Morelia), P. Rath (Chennai), B. Sahu (Allahabad) and R. Thangadurai (Allahabad)

1. Introduction. The distribution of quadratic residues and non-residues modulo \( p \) has been of intrigue to the number theorists of the last several decades. Although Gauss’ celebrated Quadratic Reciprocity Law gives a beautiful criterion to decide whether a given number is a quadratic residue modulo \( p \) or not, it is still an open problem to find a small upper bound on the least quadratic non-residue mod \( p \) as a function of \( p \), at least when \( p \equiv 1 \) (mod 8). This is because for any given natural number \( N \) one can construct many primes \( p \equiv 1 \) (mod 8) having the first \( N \) positive integers as quadratic residue (see, for example, Theorem 3 below).

In 1928, Brauer [1] proved that for any given natural number \( N \) one can find \( N \) consecutive quadratic residues as well as \( N \) consecutive quadratic non-residues modulo \( p \) for all sufficiently large primes \( p \). Vegh, in a series of papers ([10]–[13]), studied the distribution of primitive roots modulo \( p \). He considered problems such as the existence of a consecutive pair of primitive roots modulo \( p \), or the existence of arbitrarily long arithmetic progressions of primitive roots modulo \( p^h \) whose common difference is also a primitive root mod \( p^h \), as well as the existence of a primitive root in a given sequence of the form \( g_1 + b, g_2 + b, \ldots, g_{\phi(p-1)} + b \), where \( b \) is any given integer and the \( g_i \)'s are all the primitive roots modulo \( p \).

In 1956, Carlitz [2] proved that for sufficiently large primes \( p \) one can find arbitrarily long strings of consecutive primitive roots modulo \( p \). This was independently proved by Szalay ([8] and [9]).

In [5], some of us studied the problem of the distribution of the non-primitive roots modulo \( p \). More precisely, we studied the distribution of the quadratic non-residues which are not primitive roots modulo \( p \). In the present paper, we improve upon [5] and prove results analogous to those of

2000 Mathematics Subject Classification: Primary 11N69; Secondary 11A07.
Key words and phrases: quadratic residues, primitive roots, finite fields.
Brauer and Szalay. Our main ingredients are some technical results due to Weil [14] or Davenport [4] and Szalay [9].

For convenience, we abbreviate the term “quadratic non-residue which is not a primitive root” to “QNRNP”. Note further that \( \phi(p - 1) = (p - 1)/2 \) if and only if \( p = 2^{2m} + 1 \) is a Fermat prime. In this case, the set of all QNRNP’s modulo \( p \) is empty, since the primitive roots coincide with the quadratic non-residues. Thus, throughout this paper we assume that \( p \) is not a Fermat prime. We prove the following theorems.

**Theorem 1.** Let \( \varepsilon \in (0, 1/2) \) be fixed and let \( N \) be any positive integer. Then for all primes \( p \geq \exp((2\varepsilon^{-1})^{8N}) \) satisfying

\[
\frac{\phi(p - 1)}{p - 1} \leq \frac{1}{2} - \varepsilon,
\]

we can find \( N \) consecutive QNRNP’s modulo \( p \).

Theorem 1 above generalizes the results of Brauer [1] and Gun et al. [5].

Given a prime number \( p \), we let

\[
k := \frac{p - 1}{2} - \phi(p - 1)
\]

denote the number of QNRNP’s modulo \( p \) and we write \( g_1 < \cdots < g_k \) for the increasing sequence of QNRNP’s.

**Corollary 1.** For any given \( \varepsilon \in (0, 1/2) \) and natural number \( N \), for all primes \( p \geq \exp((2\varepsilon^{-1})^{8N}) \) and satisfying \( \phi(p - 1)/(p - 1) \leq 1/2 - \varepsilon \), the sequence \( g_1 + N, g_2 + N, \ldots, g_k + N \) contains at least one QNRNP.

**Theorem 2.** There exists an absolute constant \( c_0 > 0 \) such that for almost all primes \( p \), there exists a string of

\[
N_p = \left\lceil c_0 \frac{\log p}{\log \log p} \right\rceil
\]

of quadratic non-residues which are not primitive roots.

We may also combine our theorems with the above-mentioned results of Brauer and Szalay and infer that if \( \varepsilon \in (0, 1/2) \) and \( N \) are fixed, then for each sufficiently large prime \( p \) with \( \phi(p - 1)/(p - 1) < 1/2 - \varepsilon \), there exist \( N \) consecutive quadratic residues, \( N \) consecutive primitive roots, as well as \( N \) consecutive quadratic non-residues which furthermore are not primitive roots. In fact, we can even arrange the quadratic residues to be the first \( N \) quadratic residues.

**Theorem 3.** For every positive integer \( N \) there are infinitely many primes \( p \) for which \( 1, \ldots, N \) are quadratic residues modulo \( p \), and there exist both a string of \( N \) consecutive QNRNP’s as well as a string of \( N \) consecutive primitive roots. The smallest such prime can be chosen to be \( < \exp(\exp(c_1 N^2)) \), where \( c_1 > 0 \) is an absolute constant.
2. Preliminaries. Unless otherwise specified, \( p \) denotes a sufficiently large prime number. We denote the group of residues modulo \( p \) by \( \mathbb{Z}_p \) and the multiplicative group of \( \mathbb{Z}_p \) by \( \mathbb{Z}_p^* \).

An element \( \zeta \in \mathbb{Z}_p^* \) is said to be a primitive root modulo \( p \) if \( \zeta \) is a generator of \( \mathbb{Z}_p^* \). Once we know a primitive root modulo \( p \), the QNRNP’s are precisely the elements of the set

\[
\{\zeta^l : l = 1, 3, \ldots, p-2 \text{ and } (l, p-1) > 1\}.
\]

Consider a non-principal character \( \chi : \mathbb{Z}_p^* \rightarrow \mu_{p-1} \), where \( \mu_{p-1} \) denotes the group of \((p-1)\)th roots of unity. Then it is easy to observe that \( \chi(\zeta) \) is a primitive \((p-1)\)th root of unity if and only if \( \zeta \) is a primitive root mod \( p \).

Let \( \eta \) be a primitive \((p-1)\)th root of unity and assume that \( \chi(\zeta) = \eta \). Since \( \chi \) is a homomorphism, it follows that \( \chi(\zeta^i) = \chi^i(\zeta) = \eta^i \). Hence, by the above observation, it is clear that \( \chi(\kappa) = \eta^i \) with \((i, p-1) > 1\) with some odd \( i \) if and only if \( \kappa \) is a QNRNP mod \( p \).

Let \( l \) be any non-negative integer. We define

\[
\beta_l(p-1) = \sum_{1 \leq i \leq p-1 \atop i \text{ odd}, (i, p-1) > 1} (\eta^i)^l.
\]

**Lemma 1.** For \( 0 < l < p-1 \), we have

\[
\beta_l(p-1) = -\alpha_l(p-1),
\]

where \( \alpha_l(p-1) \) is the sum of the \( l \)th powers of the primitive \((p-1)\)th roots of unity.

**Proof.** Observing that

\[
\sum_{i=0}^{p-2} \eta^i = 0 = \sum_{i=0}^{(p-3)/2} \eta^{2i},
\]

we get the desired result. 

Let

\[
\chi_1, \chi_2 = \chi_1^2, \ldots, \chi_{p-2} = \chi_1^{p-2}, \chi_0 = \chi_1^{p-1}
\]

be all the multiplicative characters modulo \( p \) with the convention \( \chi_l(0) = 0 \) for all \( l = 0, 1, \ldots, p-2 \).

**Lemma 2.** We have

\[
\sum_{l=0}^{p-2} \beta_l(p-1)\chi_l(x) = \begin{cases} 
  p - 1 & \text{if } x \text{ is a QNRNP}, \\
  0 & \text{otherwise}.
\end{cases}
\]
Proof. When \( x \equiv 0 \pmod{p} \), the statement is obvious. We assume that \( x \not\equiv 0 \pmod{p} \). Let \( \eta \) be a primitive \((p-1)\)th root of unity. Consider
\[
\eta^{i_1}, \eta^{i_2}, \ldots, \eta^{i_k},
\]
where \( 1 < i_1 < \cdots < i_k \), and \((i_j, p-1) > 1\) and \( i_j \) is odd for all \( j = 1, \ldots, k \).

The expression
\[
1 + \eta^{i_1} \chi_1(x) + (\eta^{i_1})^2 \chi_2(x) + \cdots + (\eta^{i_1})^{p-2} \chi_{p-2}(x)
\]
has the value \( p-1 \) if \((\chi_1(x))^{-1} = \eta^{i_1}\) and zero otherwise whenever \( x \not\equiv 0 \). Thus, giving \( l \) the values \( 1, \ldots, k \) and adding up the above resulting expressions we get
\[
\beta_0(p-1)\chi_0(x) + \cdots + \beta_{p-2}(p-1)\chi_{p-2}(x) = \begin{cases} p-1 & \text{if } x \text{ is a QNRNP,} \\ 0 & \text{otherwise,} \end{cases}
\]
which completes the proof of the lemma. \( \blacksquare \)

The following deep theorem of Weil [14] is of central importance in the proofs of Theorems 1 and 2.

**Theorem 4.** For any integer \( l \) satisfying \( 2 \leq l < p \) and for any non-principal characters \( \chi_1, \ldots, \chi_l \) and distinct \( a_1, \ldots, a_l \in \mathbb{Z}_p \), we have
\[
\left| \sum_{x=1}^{p} \chi_1(x+a_1)\chi_2(x+a_2)\cdots\chi_l(x+a_l) \right| \leq (l-1)\sqrt{p}.
\]

For \( l = 2 \), Davenport [3] was the first one to prove the above bound. Note also that when \( l = 1 \), the sum is 0.

For a positive integer \( m \), we write \( \omega(m) \) for the number of distinct prime factors of \( m \). The next result is due to Szalay [8].

**Lemma 3.** We have
\[
\sum_{l=0}^{p-2} |\alpha_l(p-1)| = 2^{\omega(p-1)}\phi(p-1).
\]

**3. Proof of Theorem 1.** Let \( M(p, N) \) denote the number of consecutive QNRNP’s modulo \( p \) of length \( N \) in \( \mathbb{Z}_p^* \). We start with the following technical lemma.

**Lemma 4.** For any prime \( p \) and any positive integer \( N \), we have
\[
\left| M(p, N) - p \left( \frac{k}{p-1} \right)^N \right| \leq 2N2^{N\omega(p-1)}\sqrt{p}.
\]
Proof. First note that $\beta_0(p - 1) = k$. Clearly, by Lemma 2, we have

$$M(p, N) = \sum_{x=1}^{p-N} \left\{ \prod_{j=0}^{N-1} \left[ \frac{1}{p-1} \sum_{l=0}^{p-2} \beta_l(p - 1)\chi_l(x + j) \right] \right\}$$

$$= \sum_{x=1}^{p} \left\{ \prod_{j=0}^{N-1} \left[ \frac{1}{p-1} \sum_{l=0}^{p-2} \beta_l(p - 1)\chi_l(x + j) \right] \right\}$$

$$= (p - 1)^{-N} \sum_{x=1}^{p} \left\{ \prod_{j=0}^{N-1} \left[ k + \sum_{l=1}^{p-2} \beta_l(p - 1)\chi_l(x + j) \right] \right\}$$

$$= p \left( \frac{k}{p-1} \right)^N + \frac{A}{(p-1)^N},$$

where

$$A = \sum_{0 \leq l_1, \ldots, l_N \leq p-2 \atop (l_1, \ldots, l_N) \neq 0} \left[ \prod_{j=1}^{N} \beta_{l_j}(p - 1) \right] \sum_{x=1}^{p-N} \left[ \prod_{j=1}^{N} \chi_{l_j}(x + j - 1) \right].$$

In order to finish the proof of Lemma 4, we have to estimate $A$. So, we rewrite it as $A = B + C$, where

$$C = \sum_{1 \leq l_1, \ldots, l_N \leq p-2} \left[ \prod_{j=1}^{N} \beta_{l_j}(p - 1) \right] \sum_{x=1}^{p-N} \left[ \prod_{j=1}^{N} \chi_{l_j}(x + j - 1) \right],$$

and $B$ is the similar summation with at least one (but not all) of the $l_j$’s equal to zero. We further separate each sum over the set for which exactly one of the $l_i$’s is zero, then exactly two of the $l_i$’s are 0, etc., up to when just one of the $l_i$’s is non-zero.

Now, we look at the sum corresponding to the case when exactly $j$ of the $l_i$’s are equal to zero. This means that $N - j$ of the $l_i$’s are non-zero. The corresponding sum is

$$B_j = k^j \sum_{0 < r_1, \ldots, r_{N-j} \leq p-2} \left[ \prod_{b=1}^{N-j} \beta_{r_b}(p - 1) \right] \left[ \sum_{x=1}^{p-N-j} \left( \prod_{b=1}^{N-j} \chi_{r_b}(x + m_b) \right) + E \right],$$

where $E$ is the sum of some $(p - 1)$th roots of unity and in the summation at most $N$ terms occur. When we take the absolute value of this summand,
we get

$$|B_j| \leq k^j \sum_{0 < r_1, \ldots, r_{N-j} \leq p-2} \prod_{b=1}^{N-j} |\beta_{rb}(p-1)| \left( \left| \sum_{x=1}^{p} \left( \prod_{b=1}^{N-j} \chi_{rb}(x + m_b) \right) \right| + N \right)$$

$$\leq k^j \left( \sum_{l=0}^{p-2} |\beta_l(p-1)| \right)^{N-j} \left( \left| \sum_{x=1}^{p} \left( \prod_{b=1}^{N-j} \chi_{rb}(x + m_b) \right) \right| + N \right).$$

Notice now that $|\beta_l(p-1)| = |\alpha_l(p-1)|$ for all $l = 1, \ldots, p-2$, and $|\beta_0(p-1)| = k$, while $|\alpha_0(p-1)| = \phi(p-1)$. Thus, by Theorem 4 and Lemma 3, we get

$$|B_j| < k^j (2^{\omega(p-1)} \phi(p-1))^{N-j} ((N - j - 1)\sqrt{p} + N)$$

$$< 2Nk^j (2^{\omega(p-1)} \phi(p-1))^{N-j} \sqrt{p}.$$ 

This inequality holds for all $j = 1, \ldots, N-2$. When $j = N-1$, we get

$$|B_{N-1}| \leq k^{N-1} 2^{\omega(p-1)} \phi(p-1) N.$$ 

The term $C$ in $A$ can also be estimated as above and we get for it

$$|C| \leq (2^{\omega(p-1)} \phi(p-1))^N (N - 1) \sqrt{p}.$$ 

So, we see that inequality (1) holds when $j = N-1$ as well. Adding up all the above estimates for $|B_j|$ and $|C|$, we get

$$\frac{A}{(p-1)^N} \leq 2N \sqrt{p} \sum_{j=0}^{N-1} \binom{N}{j} k^j (2^{\omega(p-1)} \phi(p-1))^{N-j}$$

$$< 2N \sqrt{p} \left( 2^{\omega(p-1)} \phi(p-1) \frac{p-1}{p} + \frac{k}{p-1} \right)^N$$

$$< 2N 2^{N \omega(p-1)} \sqrt{p},$$

where we used the fact that $2^{\omega(p-1)} \phi(p-1)/(p-1) + k/(p-1) < 2^{\omega(p-1)}$. This finishes the proof of the lemma.

**Proof of Theorem 1.** We assume that $N \geq 4$. From the definition of $k$, it is easy to observe that

$$\frac{k}{p-1} = \frac{1}{2} - \frac{\phi(p-1)}{p-1} \geq \varepsilon.$$ 

Lemma 4 above tells us now that

$$p \varepsilon^N - M(p, N) \leq \left| M(p, N) - p \left( \frac{k}{p-1} \right)^N \right| \leq 2N 2^{N \omega(p-1)} \sqrt{p}.$$ 

The above chain of inequalities obviously implies that $M(p, N) > 0$ if

$$\sqrt{p} \varepsilon^N > 2N 2^{N \omega(p-1)}.$$
This last inequality is satisfied if
\[
\log p > 2 \log(2N) + 2N(\omega(p-1) \log 2 + \log(\varepsilon^{-1})).
\]
For \( p > 4 \cdot 10^6 \), we have \( \omega(p-1) < 2 \log p / \log \log p \). Thus, for such values of \( p \), the right hand side above is bounded above by
\[
2 \log(2N) + \frac{4N \log 2}{\log \log p} \log p + 2N \log(\varepsilon^{-1}),
\]
and so the desired inequality holds provided that
\[
\left( 1 - \frac{4N \log 2}{\log \log p} \right) \log p > 2 \log(2N) + 2N \log(\varepsilon^{-1}).
\]
When \( p > \exp(2^{8N}) \), the factor appearing in parenthesis on the left hand side of the last inequality above is \( \geq 1/2 \). Note that since \( N \geq 1 \), we have \( \exp(2^{8N}) > 4 \cdot 10^6 \), so the inequality \( \omega(p-1) < 2 \log p / \log \log p \) is indeed satisfied for such values of \( p \). Thus, in this range for \( p \) it suffices that
\[
\log x - \log \log x > 2 \log(2N) + 2N((1 + 2\delta) \log 2 + \log(2 \log \log x)).
\]
The above inequality is satisfied if we choose
\[
N = \left\lfloor c_3 \frac{\log x}{\log \log x} \right\rfloor,
\]
where we can take \( c_3 \) to be a positive constant \( < 1/(2 \log 2) \), provided that afterwards \( \delta \) is chosen to be small enough and \( x \) is then chosen to be sufficiently large. This completes the proof of the theorem.
5. Proof of Theorem 3. First we prove that there exist infinitely many primes $p$ for which $1, \ldots, N$ are all quadratic residues modulo $p$ for any given natural number $N$. For each prime $q \geq 5$ let $a_q \pmod{q}$ be a quadratic residue modulo $q$ such that $a_q > 1$ and put $a_3 = 1$. Let $p$ be a prime congruent to $1$ modulo $8$ and to $a_q$ modulo $q$ for all odd primes $q \leq N$. Then, by Quadratic Reciprocity, \[
mid \quad \left( \frac{q}{p} \right) = \left( \frac{p}{q} \right) = \left( \frac{a_q}{q} \right) = 1\] whenever $q \leq N$ is an odd prime. Furthermore, $\left( \frac{2}{p} \right) = 1$ because $p \equiv 1 \pmod{8}$. Using the multiplicativity property of the Legendre symbol, we find that $\left( \frac{a_q}{q} \right) = 1$ whenever $a$ is a positive integer whose all prime factors are $\leq N$. In particular, the first $N$ positive integers are quadratic residues modulo $p$. Note that $3 | (p - 1)$, and from the argument used in the proof of Theorem 2, it follows that we may take $\varepsilon = 1/6$. Furthermore, $p - 1$ is not divisible by any prime $q \in [5, \ldots, N]$. By the Chinese remainder theorem, the system of congruences $p \equiv 1 \pmod{8}$ and $p \equiv a_q \pmod{q}$ for all odd primes $q \leq N$ has a solution $p_0 \pmod{P}$, where $P = 4 \prod q \leq N q = \exp(O(N))$. There are infinitely many primes in this progression. Now the argument from the proof of Theorem 1 shows that such $p$ can be chosen on the scale of $x = \exp(12^8N)$. The only problem that might worry us is the existence of primes in the arithmetic progression $p_0 \pmod{P}$ on the scale of $x$. But note that $P = \exp(O(N)) = (\log x)^{\omega(1)}$, so the Siegel–Walfisz theorem, for example, tells us that the interval $[x, 2x]$ contains $(1 + o(1))\pi(x)/\phi(P)$ primes $p \equiv p_0 \pmod{P}$ (in particular, at least one of them), which finishes the argument.

6. Final remarks. Let $N \neq 1$ be any square-free natural number. Then it is well-known that $N$ is a quadratic non-residue modulo $p$ for infinitely many primes $p$. The analogous result for primitive roots is known as Artin’s Primitive Root Conjecture. In 1967, Hooley [6] proved this conjecture subject to the assumption of the generalized Riemann hypothesis. Interestingly, it is not even known whether 2 is a primitive root modulo infinitely many primes. For more details, we refer to the article by Ram Murty [7]. Finally, in Theorem 1, it would be of interest to obtain a constant $M$ which depends only on the natural number $N$ and not on $\varepsilon$.

Acknowledgments. We are grateful to Prof. Ram Murty for going through our work. This work was started when the first and the third authors were at Harish-Chandra Research Institute. The second author was supported in part by grants PAPIIT IN104505, SEP-CONACyT 46755 and a Guggenheim Fellowship.
References