Quadratic Non-Residues Versus Primitive Roots Modulo $p$

FLORIAN LUCA
Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58089, Morelia, Michoacán, México
fluca@matmor.unam.mx

IGOR E. SHPARLINSKI
Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au

R. THANGADURAI
Harish-Chandra Research Institute
Chhatnag Road, Jhunsi, Allahabad 211019, India
thanga@hri.res.in
Abstract

Given any $\varepsilon \in (0, 1/2)$ and any positive integer $s \geq 2$, we prove that for every prime

$$p \geq \max\{s^2(4/\varepsilon)^{2s}, s^{651s \log \log(10s)}\}$$

satisfying $\varphi(p-1)/(p-1) \leq 1/2 - \varepsilon$, where $\varphi(k)$ is the Euler function, there are $s$ consecutive quadratic non-residues which are not primitive roots modulo $p$.

Mathematics Subject Classification: 11A07, 11N35, 11N69

Key Words: quadratic residue, primitive root, sieve method

1 Introduction

For a prime $p$, we use $\mathcal{N}_p$ and $\mathcal{R}_p$ to denote the sets of quadratic nonresidues and primitive roots modulo $p$, respectively.

Both these sets have been extensively studied, although usually independently from each other (see [5, 6, 7] and references therein). Relatively less attention has been devoted to studying the set $\mathcal{S}_p = \mathcal{N}_p \setminus \mathcal{R}_p$, which is nevertheless an interesting object to study as $\mathcal{R}_p \subseteq \mathcal{N}_p$. We have

$$\#\mathcal{S}_p = \frac{p-1}{2} - \varphi(p-1),$$

where $\varphi(k)$ is the Euler function. In particular, $\mathcal{R}_p = \mathcal{N}_p$ if and only if $p = 2^{2^m} + 1$ is a Fermat prime. Thus, it is natural to expect that for primes $p$ for which $\#\mathcal{S}_p$ is large enough, that is, $\varphi(p-1)/(p-1)$ is not too close to 1/2, the elements of $\mathcal{S}_p$ have some uniformity of distribution properties.

In particular, it is shown in [2] that for any real $\varepsilon \in (0, 1/2)$ and any integer $s \geq 1$, for all primes

$$p \geq \exp \left((2/\varepsilon)^{8s}\right)$$

satisfying

$$\frac{\varphi(p-1)}{p-1} \leq \frac{1}{2} - \varepsilon,$$

the set $\mathcal{S}_p$ contains $s$ consecutive integers (see also [3]).
Here, we show that in fact the same property holds starting with significantly smaller primes. Alternatively, this means that for primes \( p \) satisfying (2), there are much longer strings of consecutive integers which all belong to \( S_p \).

We remark that it is quite possible that the method of [1] can be used to improve [2, Theorem 3].

2 Main Results

**Theorem 1.** Let \( \varepsilon \in (0, 1/2) \) be fixed and let \( s \geq 2 \) be an integer. If

\[
p \geq \max\{s^2(4/\varepsilon)^{2s}, s^{651s \log \log(10s)}\}
\]

is a prime satisfying

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

then there are \( s \) consecutive integers \( n, \ldots, n + s - 1 \) in \( S_p \).

We now immediately derive the following improvement of [2, Corollary 1].

**Corollary 1.** Let \( \varepsilon \in (0, 1/2) \) be fixed and let \( s \geq 2 \) be an integer. If

\[
p \geq \max\{s^2(4/\varepsilon)^{2s}, s^{651s \log \log(10s)}\}
\]

is a prime satisfying

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

then there are two elements \( a, b \in S_p \) with \( a - b = s \).

3 Proof

Let \( \psi(n) \) be the characteristic function of \( S_p \). It is enough to show that under the conditions of the theorem, we have

\[
W_s(p) > 0,
\]

where

\[
W_s(p) = \sum_{n=0}^{p-1} \prod_{j=1}^{s} \psi(n + j).
\]
As usual, we use $\omega(d)$ and $\mu(d)$ to denote the number of distinct prime factors and the Möbius function of $d$, respectively. For $d \mid p - 1$ we use $\psi_d(n)$ to denote the characteristic function of the set of $d$th power residues modulo $p$. Finally, we use $\eta(n)$ to denote the characteristic function of the set $\mathcal{R}_p$.

Clearly,

$$
\psi(n) = 1 - \psi_2(n) - \eta(n).
$$

Then, using the inclusion-exclusion principle, we see that for any integer $k \geq 1$, the following inequality holds:

$$
\eta(n) \leq 1 + \sum_{\nu=1}^{2k} \sum_{d \mid p-1, \omega(d) = \nu} \mu(d) \psi_d(n).
$$

Thus,

$$
\psi(n) \geq -\psi_2(n) - \sum_{\nu=1}^{2k} \sum_{d \mid p-1, \omega(d) = \nu} \mu(d) \psi_d(n). 
$$

On the other hand, $\psi_d(n)$ can be expressed via multiplicative characters of order $d$ as

$$
\psi_d(n) = \frac{1}{d} \sum_{\chi \equiv \chi_0} \chi(n) = \frac{1}{d} \sum_{\chi \equiv \chi_0, \chi \neq \chi_0} \chi(n), 
$$

where $\chi_0$ is the principal character and the summation is taken over all multiplicative characters $\chi$ whose order divides $d$ (see [5, Section 3.1]). Substituting (5) in (4), we derive

$$
\psi(n) \geq \vartheta_k(p) - \frac{1}{2} \left( \frac{n}{p} \right) - \sum_{\nu=1}^{2k} \sum_{d \mid p-1, \omega(d) = \nu} \frac{\mu(d)}{d} \sum_{\chi \equiv \chi_0, \chi \neq \chi_0} \chi(n),
$$

where $(n/p)$ is the Legendre symbol and

$$
\vartheta_k(p) = -\frac{1}{2} \sum_{\nu=1}^{2k} \sum_{d \mid p-1, \omega(d) = \nu} \frac{\mu(d)}{d}.
$$
Defining $\xi_d = 2$ if $d = 2$ and $\xi_d = 1$ otherwise, we can write (6) in a more compact form:

$$\psi(n) \geq \vartheta_k(p) - \sum_{\nu=1}^{2k} \sum_{\substack{d|p-1 \\omega(d) = \nu \\chi^d = \chi_0}} \frac{\mu(d)\xi_d}{d} \sum_{\substack{\chi \neq \chi_0}} \chi(n).$$

Therefore,

$$W_s(p) \geq \sum_{n=0}^{p-1} \prod_{j=1}^{s} \left( \vartheta_k(p) - \sum_{\nu_j=1}^{2k} \sum_{\substack{d_j|p-1 \\omega(d_j) = \nu_j \\chi_{d_j}^d = \chi_0}} \frac{\mu(d_j)\xi_{d_j}}{d_j} \sum_{\substack{\chi_j \neq \chi_0}} \chi_j(n+j) \right)$$

$$= p\vartheta_k(p)^s - \sum_{\mathcal{J} \subseteq \{1, \ldots, s\} \setminus \emptyset} \prod_{j \in \mathcal{J}} \frac{\mu(d_j)\xi_{d_j}}{d_j} \sum_{\substack{\{\nu_j\}_{j \in \mathcal{J}} \\chi_{d_j}^d = \chi_0 \\chi_j \neq \chi_0}} \prod_{j \in \mathcal{J}} \chi_j(n+j).$$

By the Weil bound (see [5, Theorem 11.23]), the absolute value of the inner sum is at most

$$\left| \sum_{n=0}^{p-1} \prod_{j \in \mathcal{J}} \chi_j(n+j) \right| \leq \#\mathcal{J} p^{1/2}.$$ 

Since there are $d_j - 1$ multiplicative nonprincipal characters $\chi_j$ with $\chi_{d_j}^d = \chi_0$, we obtain

$$W_s(p) \geq p\vartheta_k(p)^s - p^{1/2} \sum_{\mathcal{J} \subseteq \{1, \ldots, s\} \setminus \emptyset} \vartheta_k(p)^s - \#\mathcal{J} \sum_{\substack{\{\nu_j\}_{j \in \mathcal{J}} \\chi_{d_j}^d = \chi_0 \\chi_j \neq \chi_0}} \prod_{j \in \mathcal{J}} \left( \omega(p-1) \right)$$

$$\geq p\vartheta_k(p)^s - p^{1/2} \sum_{\mathcal{J} \subseteq \{1, \ldots, s\} \setminus \emptyset} \vartheta_k(p)^s - \#\mathcal{J} \sum_{\substack{\{\nu_j\}_{j \in \mathcal{J}} \\chi_{d_j}^d = \chi_0 \\chi_j \neq \chi_0}} \prod_{j \in \mathcal{J}} \left( \omega(p-1) \right)$$

$$= p\vartheta_k(p)^s - p^{1/2} \sum_{\mathcal{J} \subseteq \{1, \ldots, s\} \setminus \emptyset} \vartheta_k(p)^s - \#\mathcal{J} \left( \sum_{\nu=1}^{2k} \left( \omega(p-1) \right) \right)^{\#\mathcal{J}}.$$
It is easy to verify that for any integer \( w \geq 2 \) we have
\[
\sum_{\nu=1}^{2k} \binom{w}{\nu} \leq w^{2k}.
\]

Therefore,
\[
W_s(p) \geq p \vartheta_k(p)^s - sp^{1/2} \sum_{\mathcal{J} \subseteq \{1,\ldots,s\}} \sum_{\mathcal{J} \neq \emptyset} \vartheta_k(p)^{s-\#\mathcal{J}} \omega(p-1)^{2k \#\mathcal{J}}
\]
\[
= p \vartheta_k(p)^s - sp^{1/2} \sum_{t=1}^{s} \binom{s}{t} \vartheta_k(p)^{s-t} \omega(p-1)^{2kt}.
\]

Since \( \vartheta_k(p)^{s-t} \leq \max\{\vartheta_k(p)^s, 1\} \), we finally derive
\[
W_s(p) \geq p \vartheta_k(p)^s - sp^{1/2} (\omega(p-1)^{2k} + 1)^s \max\{\vartheta_k(p)^s, 1\}. \tag{7}
\]

We now estimate \( \vartheta_k(p) \). We write
\[
\vartheta_k(p) = -\frac{1}{2} \sum_{d|p-1, d>1} \frac{\mu(d)}{d} + \sum_{\nu \geq 2k} \sum_{d|p-1, \omega(d)=\nu} \frac{\mu(d)}{d}
\]
\[
= -\frac{1}{2} \sum_{\ell \text{ prime}} \left( \prod_{d|p-1, \ell \text{ prime}} \left( 1 - \frac{1}{\ell} \right) - 1 \right) + \sum_{\nu \geq 2k} \sum_{d|p-1, \omega(d)=\nu} \frac{\mu(d)}{d}
\]
\[
= \frac{1}{2} \sum_{\ell \text{ prime}} \left( \prod_{d|p-1, \ell \text{ prime}} \left( 1 - \frac{1}{\ell} \right) + \sum_{\nu \geq 2k} \sum_{d|p-1, \omega(d)=\nu} \frac{\mu(d)}{d}
\]
\[
= \frac{1}{2} \varphi(p-1) + \frac{p-1}{p-1} + \sum_{\nu \geq 2k} \sum_{d|p-1, \omega(d)=\nu} \frac{\mu(d)}{d}.
\]

Recalling the assumption of the theorem, we obtain
\[
\frac{1}{2} + \sum_{\nu \geq 2k} \sum_{d|p-1, \omega(d)=\nu} \frac{\mu(d)}{d} \geq \vartheta_k(p) \geq \varepsilon + \sum_{\nu \geq 2k} \sum_{d|p-1, \omega(d)=\nu} \frac{\mu(d)}{d}. \tag{8}
\]
Furthermore,

\[
\left| \sum_{\nu \geq 2k} \sum_{\ell \mid p-1 \atop \omega(d)=\nu} \frac{\mu(d)}{d} \right| \leq \sum_{\nu \geq 2k} \sum_{\ell \mid p-1 \atop \omega(d)=\nu} \frac{1}{d} \leq \sum_{\nu \geq 2k} \frac{1}{\nu!} \rho(p)^\nu.
\]

where

\[
\rho(p) = \sum_{\ell \mid p-1 \atop \ell \text{ prime}} \frac{1}{\ell}.
\]

We now assume that

\[
k \geq e \rho(p). \tag{9}
\]

Then, by the inequality

\[
\nu! \geq (\nu/e)^\nu, \tag{10}
\]

we have

\[
\sum_{\nu \geq 2k} \frac{1}{\nu!} \rho(p)^\nu \leq \sum_{\nu \geq 2k} \left( \frac{\rho(p)}{\nu} \right)^\nu \leq \sum_{\nu \geq 2k} 2^{-\nu} = 2^{1 - 2k + 1} \leq \frac{\varepsilon}{2}.
\]

Thus, we see from (8) that with the choice (9), we have

\[
1 \geq \vartheta_k(p) \geq \frac{\varepsilon}{2}.
\]

Using also the trivial bound \( \omega(p-1)^{2k} + 1 \leq 2\omega(p-1)^{2k} \), we get that (7) simplifies to

\[
W_s(p) \geq p \left( \frac{\varepsilon}{2} \right)^s - s2^{s}p^{1/2}\omega(p-1)^{2ks}.
\]

Hence, in order for (3) to hold, it is enough to have

\[
p^{1/2} > s \left( \frac{4\omega(p-1)^{2k}}{\varepsilon} \right)^s. \tag{11}
\]

If \( \omega(p-1)^{2k} \leq 4/\varepsilon \), then it suffices that

\[
p^{1/2} \geq s \left( \frac{4}{\varepsilon} \right)^s,
\]
or, equivalently, that
\[ p > s^2 \left( \frac{4}{\varepsilon} \right)^{2s} \]
holds.
Assume now that \( \omega(p - 1)^{2k} \geq 4/\varepsilon \). Hence, it suffices that the inequality
\[ p^{1/2} > s\omega(p - 1)^{4ks} \]
holds. We use the inequality
\[ \omega(p - 1) < 1.4 \frac{\log p}{\log \log p} \]
which is valid for all primes \( p \geq 5 \) (see, for example, [8]). Since also \( s \leq 2^s \leq 2^{ks} \) holds for all \( s \geq 1 \) and \( k \geq 1 \), it suffices that
\[ p^{1/2} > \left( \frac{2^{1/4} \cdot 1.4 \log p}{\log \log p} \right)^{4ks} \].

Since
\[ p \geq s^{651 s \log \log (10s)} \geq 2^{1302 \log \log 20} \tag{12} \]
we get that \( \log \log p > 6.89 > 2^{1/4} \cdot 1.4 \). Therefore it suffices that
\[ \log p > 8ks \log \log p. \]

It now follows easily from the estimates in [9] that the inequality
\[ \rho(p) = \sum_{\ell \text{ prime}} \frac{1}{\ell} < \log \log \log p + 1 \]
holds for all primes \( p \geq 20 \). Thus, taking \( k = \lfloor e\rho(p) \rfloor \) to satisfy (9), it is enough to guarantee that
\[ \log p > 8es(\log \log p + 1 + 1/e) \log \log p. \tag{13} \]

By (12), we have that \( \log p > 100 \). For \( t > 100 \), the function
\[ t \mapsto \frac{t}{(\log \log t + 1 + 1/e) \log t} \]
8
is increasing. It remains to verify that
\[ \frac{\log P_0(s)}{(\log \log \log P_0(s) + 1 + 1/e) \log \log P_0(s)} > 8\varepsilon, \]
where
\[ P_0(s) = s^{651s \log \log(10s)} \]
for all \( s \geq 2 \), which indeed holds and finishes the proof of Theorem 1.

References


