Bull. Aust. Math. Soc. **99** (2019), 177–183
doi:10.1017/S0004972718001065

QUADRATIC NONRESIDUES AND NONPRIMITIVE ROOTS SATISFYING A COPRIMALITY CONDITION

JAITRA CHATTOPADHYAY, BIDISHA ROY✉, SUBHA SARKAR and R. THANGADURAI

(Received 20 August 2018; accepted 5 September 2018; first published online 12 November 2018)

Abstract

Let $q \geq 1$ be any integer and let $\epsilon \in [\frac{1}{11}, \frac{1}{2})$ be a given real number. We prove that for all primes p satisfying

$$p \equiv 1 \pmod{q}, \quad \log\log p > \frac{2\log 6.83}{1-2\epsilon} \quad \text{and} \quad \frac{\phi(p-1)}{p-1} \leq \frac{1}{2} - \epsilon,$$

there exists a quadratic nonresidue g which is not a primitive root modulo p such that $\gcd(g, (p-1)/q) = 1$.

2010 *Mathematics subject classification*: primary 11A07.

Keywords and phrases: distribution of nonresidues, primitive roots, fixed point discrete log problem.

1. Introduction

Let p be an odd prime number. There are exactly $(p-1)/2$ quadratic residues and the same number of nonresidues modulo p. Moreover, the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic (see [1]). A generator of this cyclic group is called a *primitive root* modulo p.

The distribution of quadratic residues, nonresidues and primitive roots is a fundamental area in number theory and has been of great interest to mathematicians for centuries. In 2010, Levin *et al.* [4] proved the existence of a primitive root satisfying a coprimality condition.

THEOREM 1.1. *For all prime numbers $p \geq 5$, there exists a primitive root g modulo p which satisfies the condition $\gcd(g, p-1) = 1$.*

Levin *et al.* [4] used this theorem to solve the fixed point discrete log problem that, for a given primitive root g in $(\mathbb{Z}/p\mathbb{Z})^*$, there exists an integer $t \in [1, p-1]$ such that $g^t \equiv t \pmod{p}$.

In this article, we deal with a similar problem for quadratic nonresidues which are not primitive roots (for further references on this related problem, see [2, 3, 5]). For notational convenience, we abbreviate 'quadratic nonresidue which is not a primitive root' as QNRNP. More precisely, we prove the following result.

© 2018 Australian Mathematical Publishing Association Inc.

https://doi.org/10.1017/S0004972718001065 Published online by Cambridge University Press

THEOREM 1.2. *Let $q \geq 1$ be an integer and $\epsilon \in [\frac{1}{11}, \frac{1}{2})$. Let p be a prime satisfying*

$$p \equiv 1 \pmod{q}, \quad \log\log p > \frac{2\log 6.83}{1-2\epsilon} \quad \text{and} \quad \frac{\phi(p-1)}{p-1} \leq \frac{1}{2} - \epsilon.$$

Then there exists an integer g satisfying $1 < g < p-1$ and $\gcd(g, (p-1)/q) = 1$ such that g is a QNRNP modulo p. In particular, when $q = 1$, there exists an integer g with $1 < g < p-1$ and $\gcd(g, p-1) = 1$ such that g is a QNRNP modulo p.

In the statement of Theorem 1.2, as usual, $\phi(n)$ is the Euler totient function. The third condition on p is quite natural. If $\phi(p-1) = \frac{1}{2}(p-1)$, then one can easily check that every nonresidue modulo p is a primitive root modulo p and if $\phi(p-1) < \frac{1}{2}(p-1)$ then there are nonresidues which are not primitive roots. The condition $\phi(p-1) \leq (\frac{1}{2} - \epsilon)(p-1)$ makes sure that $p-1$ has enough odd prime factors so that there is an abundance of QNRNP residues modulo p.

We can apply Theorem 1.2 to solve the fixed point discrete log problem for the cyclic subgroup generated by a QNRNP.

COROLLARY 1.3. *Let $\epsilon \in [\frac{1}{11}, \frac{1}{2})$. Let p be a prime satisfying*

$$\log\log p > \frac{2\log 6.83}{1-2\epsilon} \quad \text{and} \quad \frac{\phi(p-1)}{p-1} \leq \frac{1}{2} - \epsilon.$$

Then there are a QNRNP g and an integer $x \in [1, p-1]$ such that x is a QNRNP and $g^x \equiv x \pmod{p}$.

In [4], Theorem 1.1 is proved first for all large primes and verified for small primes by computation. However, such computations are cumbersome in the case of Theorem 1.2 because of the extra parameters.

2. Preliminaries

Let μ_{p-1} stand for the multiplicative group of $(p-1)$th roots of unity. Let $g \in \{1, \ldots, p-1\}$ be a primitive root modulo p and let $\chi : (\mathbb{Z}/p\mathbb{Z})^* \to \mu_{p-1}$ be a character modulo p such that χ is a generator of the dual group of $(\mathbb{Z}/p\mathbb{Z})^*$. Let ℓ be an integer with $0 \leq \ell \leq p-2$. Then $\chi_\ell = \chi^\ell$ is a character modulo p and χ_0 is the principal character.

Suppose that $\chi(g) = \eta$. Since χ is a generator of the dual group of $(\mathbb{Z}/p\mathbb{Z})^*$ and g is a primitive root modulo p, it follows that η is a primitive $(p-1)$th root of unity.

Following [2], we define $\beta_\ell(p-1)$ and the Ramanujan sums $\alpha_\ell(p-1)$ by

$$\beta_\ell(p-1) = \sum_{\substack{1 \leq i \leq p-1 \\ i \text{ odd}, (i,p-1)>1}} (\eta^i)^\ell \quad \text{and} \quad \alpha_\ell(p-1) = \sum_{\substack{1 \leq i \leq p-1 \\ (i,p-1)=1}} (\eta^i)^\ell.$$

Now we list some basic results, which will be useful for the proof of Theorem 1.2.

LEMMA 2.1 [2]. *For all integers ℓ with $0 < \ell < p-1$,*

$$\beta_\ell(p-1) = -\alpha_\ell(p-1).$$

https://doi.org/10.1017/S0004972718001065 Published online by Cambridge University Press

Lemma 2.2 ([2], characteristic function for QNRNP). *For any $x \in (\mathbb{Z}/p\mathbb{Z})^*$,*

$$\sum_{\ell=0}^{p-2} \beta_\ell(p-1)\chi_\ell(x) = \begin{cases} p-1 & \text{if } x \text{ is a QNRNP,} \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 2.3. (1) [6] *Let $\omega(n)$ denote the number of distinct prime divisors of n. For all primes $p \geq 5$,*

$$\omega(p-1) \leq 1.385 \frac{\log p}{\log\log p}.$$

(2) [1] *Let $\mu(n)$ denote the Möbius function. Then*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1. \end{cases}$$

(3) [7] *For any odd prime p and any divisor q of $p-1$,*

$$\sum_{d|(p-1)/q} |\mu(d)| = 2^{\omega((p-1)/q)}.$$

Lemma 2.4 [7]. *The Ramanujan sums satisfy*

$$\sum_{\ell=1}^{p-2} |\alpha_\ell(p-1)| = 2^{\omega(p-1)}\phi(p-1).$$

Finally, the following result is a standard theorem to estimate a character sum over an interval (see, for example, [1]).

Theorem 2.5 (Pólya–Vinogradov). *Let p be any odd prime and χ be a nonprincipal character modulo p. Then, for any integers M, N with $0 \leq M < N \leq p-1$,*

$$\left| \sum_{m=M}^{N} \chi(m) \right| \leq \sqrt{p}\log p.$$

3. Proof of Theorem 1.2

Suppose that the integer $q \geq 1$ and $\epsilon \in [\frac{1}{11}, \frac{1}{2})$ are given. We consider all primes $p \equiv 1 \pmod q$ with $\phi(p-1) \leq (\frac{1}{2} - \epsilon)(p-1)$. By Dirichlet's prime number theorem, there are infinitely many such primes.

By Lemma 2.2, for any integer m,

$$f(m) := \frac{1}{p-1} \sum_{\ell=0}^{p-2} \beta_\ell(p-1)\chi_\ell(m) = \begin{cases} 1 & \text{if } m \text{ is a QNRNP,} \\ 0 & \text{otherwise.} \end{cases}$$

Set

$$N_p := \sum_{\substack{m=1 \\ (m,(p-1)/q)=1}}^{p-1} f(m).$$

https://doi.org/10.1017/S0004972718001065 Published online by Cambridge University Press

Then N_p counts the number of QNRNPs in $\{1, \dots, p-1\}$ which are relatively prime to $(p-1)/q$. To prove Theorem 1.2, it suffices to prove that $N_p \geq 1$ for all the primes p under consideration (that is, with $p \equiv 1 \pmod{q}$ and $\phi(p-1) \leq (\frac{1}{2} - \epsilon)(p-1)$) which satisfy $\log\log p > 2\log 6.83/(1-2\epsilon)$. Therefore, we consider

$$\begin{aligned} N_p &= \sum_{\substack{m=1 \\ (m,(p-1)/q)=1}}^{p-1} f(m) = \frac{1}{p-1} \sum_{\substack{m=1 \\ (m,(p-1)/q)=1}}^{p-1} \sum_{\ell=0}^{p-2} \beta_\ell(p-1)\chi_\ell(m) \\ &= \frac{1}{p-1} \sum_{\ell=0}^{p-2} \beta_\ell(p-1) \sum_{\substack{m=1 \\ (m,(p-1)/q)=1}}^{p-1} \chi_\ell(m) \\ &= \frac{1}{p-1}\left(\beta_0(p-1)q\phi\left(\frac{p-1}{q}\right) + \sum_{\ell=1}^{p-2} \beta_\ell(p-1) \sum_{\substack{m=1 \\ (m,(p-1)/q)=1}}^{p-1} \chi_\ell(m)\right), \end{aligned}$$

where we have used the fact that the number of integers m in $\{1, \dots, p-1\}$ such that $(m, (p-1)/q) = 1$ is $q\phi((p-1)/q)$. Let us define

$$E_p := N_p - \frac{1}{p-1}\beta_0(p-1)q\phi\left(\frac{p-1}{q}\right) = \frac{1}{p-1} \sum_{\ell=1}^{p-2} \beta_\ell(p-1) \sum_{\substack{m=1 \\ (m,(p-1)/q)=1}}^{p-1} \chi_\ell(m).$$

In order to prove that $N_p \geq 1$, we need to get an upper bound for E_p. We consider the two sums in the expression for E_p separately. For a given integer ℓ with $1 \leq \ell \leq p-2$,

$$\begin{aligned} \sum_{\substack{m=1 \\ (m,(p-1)/q)=1}}^{p-1} \chi_\ell(m) &= \sum_{m=1}^{p-1} \chi_\ell(m) \sum_{d \mid (m,(p-1)/q)} \mu(d) = \sum_{d \mid (p-1)/q} \mu(d) \sum_{t=1}^{(p-1)/d} \chi_\ell(d)\chi_\ell(t) \\ &= \sum_{d \mid (p-1)/q} \mu(d)\chi_\ell(d) \sum_{t=1}^{(p-1)/d} \chi_\ell(t) \end{aligned}$$

by Lemma 2.3(2). Hence, by Theorem 2.5 and Lemma 2.3(3),

$$\left| \sum_{\substack{m=1 \\ (m,(p-1)/q)=1}}^{p-1} \chi_\ell(m) \right| \leq \sum_{d \mid (p-1)/q} |\mu(d)| \left| \sum_{t=1}^{(p-1)/d} \chi_\ell(t) \right| \leq 2^{\omega((p-1)/q)} \sqrt{p} \log p.$$

Also, by Lemmas 2.1 and 2.4,

$$\left| \sum_{\ell=1}^{p-2} \beta_\ell(p-1) \right| \leq \sum_{\ell=1}^{p-2} |\beta_\ell(p-1)| \leq \sum_{\ell=0}^{p-2} |\alpha_\ell(p-1)| = 2^{\omega(p-1)}\phi(p-1).$$

https://doi.org/10.1017/S0004972718001065 Published online by Cambridge University Press

Using the last two estimates,

$$|E_p| = \left|N_p - \frac{1}{p-1}\beta_0(p-1)q\phi\left(\frac{p-1}{q}\right)\right| \le \frac{1}{p-1}\sum_{\ell=1}^{p-2}|\beta_\ell(p-1)|\left|\sum_{\substack{m=1\\(m,(p-1)/q)=1}}^{p-1}\chi_\ell(m)\right|$$

$$\le 2^{\omega((p-1)/q)+\omega(p-1)}\frac{\phi(p-1)}{p-1}\sqrt{p}\log p. \tag{3.1}$$

Observe that (3.1) implies that

$$-2^{\omega((p-1)/q)+\omega(p-1)}\frac{\phi(p-1)}{p-1}\sqrt{p}\log p \le N_p - \frac{q\phi((p-1)/q)}{(p-1)}\beta_0(p-1),$$

which is equivalent to

$$N_p \ge \frac{\phi((p-1)/q)}{(p-1)/q}\beta_0(p-1) - 2^{\omega((p-1)/q)+\omega(p-1)}\frac{\phi(p-1)}{p-1}\sqrt{p}\log p.$$

Thus, to establish $N_p > 0$, it is enough to show that

$$\frac{\phi((p-1)/q)}{(p-1)/q}\beta_0(p-1) - 2^{\omega((p-1)/q)+\omega(p-1)}\frac{\phi(p-1)}{p-1}\sqrt{p}\log p > 0,$$

which is equivalent to showing that

$$\beta_0(p-1) > 2^{\omega((p-1)/q)+\omega(p-1)}\frac{\phi(p-1)}{q\phi((p-1)/q)}\sqrt{p}\log p. \tag{3.2}$$

Now it is clear that

$$\phi(p-1) \le q\phi\left(\frac{p-1}{q}\right) \iff \frac{\phi(p-1)}{q\phi((p-1)/q)} \le 1. \tag{3.3}$$

Since $\omega((p-1)/q) \le \omega(p-1)$, by (3.2) and (3.3), it is enough to prove that

$$\beta_0(p-1) > 4^{\omega(p-1)}\sqrt{p}\log p \tag{3.4}$$

for primes p satisfying $\log\log p > 2\log 6.83/(1-2\epsilon)$ and $\phi(p-1) \le (\frac{1}{2}-\epsilon)(p-1)$.

Let p be such a prime. Then

$$p^{1-2\epsilon} > p^{2\log 6.83/\log\log p}. \tag{3.5}$$

By Lemma 2.3(1),

$$\omega(p-1) \le 1.385\frac{\log p}{\log\log p}.$$

Therefore,

$$4^{\omega(p-1)} \le 4^{1.385\log p/\log\log p} \le 6.83^{\log p/\log\log p} = p^{\log 6.83/\log\log p}.$$

Hence, from (3.5),

$$p^{1-2\epsilon} > 4^{2\omega(p-1)} \iff p^{1-\epsilon}(\log p) > 4^{\omega(p-1)}\sqrt{p}\log p.$$

https://doi.org/10.1017/S0004972718001065 Published online by Cambridge University Press

In order to prove (3.4), it is enough to show that

$$\beta_0(p-1) > p^{1-\epsilon}\log p \tag{3.6}$$

for all primes p satisfying $\log\log p > 2\log 6.83/(1-2\epsilon)$ and $\phi(p-1) \le (\frac{1}{2}-\epsilon)(p-1)$. Note that the condition

$$\frac{\phi(p-1)}{p-1} \le \frac{1}{2} - \epsilon \iff \epsilon(p-1) \le \frac{p-1}{2} - \phi(p-1) = \beta_0(p-1).$$

Therefore, to prove (3.6), it is enough to prove that $\epsilon(p-1) \ge p^{1-\epsilon}\log p$ for all primes p with $\log\log p > 2\log 6.83/(1-2\epsilon)$.

Write $\epsilon = 1/c$. Since $\epsilon \in [\frac{1}{11}, \frac{1}{2})$, the real number c satisfies $2 < c \le 11$. Now

$$\log\log p > \frac{\log 6.83}{\frac{1}{2}-\epsilon} > 3.84 \times 1.22 > 4.68 \quad \text{and} \quad \log p > e^{4.68} > 107.7.$$

To achieve $\epsilon(p-1) \ge p^{1-\epsilon}\log p$ for all primes p with $\log\log p > 2\log 6.83/(1-2\epsilon)$, it is enough to prove that

$$\frac{p}{1.1} > \frac{1}{\epsilon}p^{1-\epsilon}\log p \iff p > (1.1c)^c(\log p)^c \iff \log p > c\log(1.1c) + c\log\log p.$$

Note that $e^x/x \ge 22$ for all $x \ge 4.68$. By applying this with $x = \log\log p$, we see that $\log p > 2c\log\log p$ for $2 < c \le 11$. Hence, it is enough to prove that

$$\log p > c\log(1.1) + c\log c + \frac{\log p}{2} \iff \log p > 2c\log(1.1) + 2c\log c.$$

Since $c \le 11$,

$$2c\log(1.1) + 2c\log c \le 22\log(1.1) + 22\log 11 \le 54.86 < 107.7 < \log p.$$

Thus, the inequality in (3.6) is true. This completes the proof of the theorem.

4. Proof of Corollary 1.3

By Theorem 1.2, there is a QNRNP x modulo p satisfying $x \in [1, p-1]$ and $\gcd(x, p-1) = 1$. Let y be the multiplicative inverse of x modulo $p-1$. Put $g = x^y$. Then note that g is also a QNRNP modulo p and $g^x \equiv x^{xy} \equiv x \pmod{p}$.

Acknowledgement

We are thankful to the referee for pointing out a lacuna in the previous version and for suggesting important references.

References

[1] T. M. Apostol, *Introduction to Analytic Number Theory*, Undergraduate Texts in Mathematics (Springer, New York, 1976).

https://doi.org/10.1017/S0004972718001065 Published online by Cambridge University Press

[2] S. Gun, F. Luca, P. Rath, B. Sahu and R. Thangadurai, 'Distribution of residues modulo p', *Acta Arith.* **129**(4) (2007), 325–333.
[3] T. Jarso and T. Trudgian, 'Quadratic non-residues that are not primitive roots', *Math. Comp.*, to appear, doi:10.1090/mcom/3378.
[4] M. Levin, C. Pomerance and K. Soundararajan, 'Fixed points for discrete logarithms', in: *Algorithmic Number Theory*, Lecture Notes in Computer Science, 6197 (Springer, Berlin, 2010), 6–15.
[5] F. Luca, I. E. Shparlinski and R. Thangadurai, 'Quadratic non-residue versus primitive roots modulo p', *J. Ramanujan Math. Soc.* **23**(1) (2008), 97–104.
[6] J. Sándor, D. S. Mitrinović and B. Crstici, *Handbook on Number Theory I* (Springer, Dordrecht, 2001).
[7] M. Szalay, 'On the distribution of the primitive roots mod p', *Mat. Lapok* **21** (1970), 357–362 (in Hungarian).

JAITRA CHATTOPADHYAY, Harish-Chandra Research Institute, HBNI,
Chhatnag Road, Jhunsi, Allahabad-211019, India
e-mail: jaitrachattopadhyay@hri.res.in

BIDISHA ROY, Harish-Chandra Research Institute, HBNI,
Chhatnag Road, Jhunsi, Allahabad-211019, India
e-mail: bidisharoy@hri.res.in

SUBHA SARKAR, Harish-Chandra Research Institute, HBNI,
Chhatnag Road, Jhunsi, Allahabad-211019, India
e-mail: subhasarkar@hri.res.in

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

https://doi.org/10.1017/S0004972718001065 Published online by Cambridge University Press