DISTRIBUTION OF QUADRATIC NON-RESIDUES WHICH ARE NOT PRIMITIVE ROOTS

S. GUN, B. RAMAKRISHNAN, B. SAHU AND R. THANGADURAI

Abstract. In this article, we shall study, using elementary and combinatorial methods, the distribution of quadratic non-residues which are not primitive roots modulo p^h or $2p^h$ for an odd prime p and $h \geq 1$ is an integer.

1. Introduction

Distribution of quadratic residues, non-residues and primitive roots modulo n for any positive integer n is one of the classical problems in Number Theory. In this article, by applying elementary and combinatorial methods, we shall study the distribution of quadratic non-residues which are not primitive roots modulo odd prime powers.

Let n be any positive integer and p be any odd prime number. We denote the additive cyclic group of order n by $\mathbb{Z}_n$. The multiplicative group modulo n is denoted by $\mathbb{Z}_n^*$ of order $\phi(n)$, the Euler phi function.

Definition 1.1. A *primitive root* g modulo n is a generator of $\mathbb{Z}_n^*$ whenever $\mathbb{Z}_n^*$ is cyclic.

A well-known result of C. F. Gauss says that $\mathbb{Z}_n^*$ has a primitive root g if and only if $n = 2, 4$ or p^h or $2p^h$ for any positive integer $h \geq 1$. Moreover, the number of primitive roots modulo these n's is equal to $\phi(\phi(n))$.

Definition 1.2. Let $n \geq 2$ and a be integers such that $(a, n) = 1$. If the quadratic congruence

$$x^2 \equiv a \pmod{n}$$

has an integer solution x, then a is called a *quadratic residue modulo* n. Otherwise, a is called a *quadratic non-residue modulo* n.

Whenever $\mathbb{Z}_n^*$ is cyclic and g is a primitive root modulo n, then $g^{2\ell-1}$ for $\ell = 1, 2 \cdots, \phi(n)/2$ are all the quadratic non-residue modulo n and $g^{2\ell}$ for $\ell = 0, 1, \cdots, \phi(n)/2 - 1$ are all the quadratic residue modulo n. Also, $g^{2\ell-1}$ for all $\ell = 1, 2, \cdots, \phi(n)/2$ such that $(2\ell - 1, \phi(n)) > 1$ are all the quadratic non-residues which are not primitive roots modulo n.

For a positive integer n, set

$$M(n) = \{g \in \mathbb{Z}_n^* \mid g \text{ is a primitive root modulo } n\}$$

2000 *Mathematics Subject Classification.* 11N69.

Key words and phrases. quadratic non-residues, primitive roots.

and

$$K(n) = \{a \in \mathbb{Z}_n^* \mid a \text{ is a quadratic non-residue modulo } n\}.$$

Note that $M(1) = K(1) = \emptyset$, $M(2) = \{1\}$, and $K(2) = \emptyset$. When $n \geq 3$, we know that $|K(n)| \geq \frac{\phi(n)}{2}$ and whenever $n = 2, 4$ or p^a or $2p^a$, we have $|K(n)| = \frac{\phi(n)}{2}$. Also, it can be easily seen that if $n \geq 3$, then

$$M(n) \subset K(n).$$

We shall denote a quadratic non-residue which is not a primitive root modulo n by QNRNP modulo n. Therefore, any $x \in K(n) \setminus M(n)$ is a QNRNP modulo n.

Recently, Křížek and Somer [2] proved that $M(n) = K(n)$ iff n is either a Fermat prime (primes of the form $2^{2^r} + 1$) or 4 or twice a Fermat prime. Moreover, they proved that for $n \geq 2$, $|M(n)| = |K(n)| - 1$ if and only if $n = 9$ or 18, or either n or $n/2$ is equal to a prime p, where $(p-1)/2$ is also an odd prime. They also proved that when $|M(n)| = |K(n)| - 1$, then $n - 1 \in K(n) \setminus M(n)$.

In this article, we shall prove the following theorems.

Theorem 1.1. *Let r and h be any positive integers. Let $n = p^h$ or $2p^h$ for any odd prime p. Then $|M(n)| = |K(n)| - 2^r$ if and only if n is either (i) p or $2p$ whenever $p = 2^{r+1}q + 1$ with q is also a prime or (ii) p^2 or $2p^2$ whenever $p = 2^{r+1} + 1$ is a Fermat prime. In this case, the set $K(n) \setminus M(n)$ is nothing but the set of all generators of the unique cyclic subgroup H of order 2^{r+1} of $\mathbb{Z}_n^*$.*

When p is not a Fermat prime, then it is clear from the above discussion that $\nu := |K(p) \setminus M(p)| = \frac{p-1}{2} - \phi(p-1) > 0$. When $\nu \geq 2$, the natural question is that whether does there exist any consecutive pair of QNRNP modulo p? From Theorem 1.1, we know that $\nu = 2$ for all primes $p = 4q + 1$ where q is also a prime number.

Theorem 1.2. *Let p be a prime such that $p = 4q + 1$ where q is also a prime. Then there does not exist a pair of consecutive QNRNP modulo p.*

In contrast to Theorem 1.2, we shall prove the following.

Theorem 1.3. *Let p be any odd prime such that $\frac{\phi(p-1)}{p-1} < \frac{1}{6}$. Then there exists a pair of consecutive QNRNP modulo p.*

In the following theorem, we shall address a weaker question than Theorem 1.3; but works for arbitrary length k.

Theorem 1.4. *Let $q > 1$ be any odd integer and $k > 1, h \geq 1$ be integers. Then there exists a positive integer $N = N(q, k)$ depending only on q and k such that for every prime $p > N$ and $p \equiv 1 \pmod{q}$, we have an arithmetic progression of length k whose terms are QNRNP modulo n, where $n = p^h$ or $2p^h$. Moreover, we can choose the common difference to be a QNRNP modulo n, whenever $n = p^h$.*

2. Preliminaries

In this section, we shall prove some preliminary lemmas which will be useful for proving our theorems.

Proposition 2.1. *Let h be any positive integer and let $n = p^h$ or $2p^h$ for any odd prime p. Then any integer g is a primitive root modulo n if and only if*

$$g^{\phi(n)/q} \not\equiv 1 \pmod{n}$$

for every prime divisor q of $\phi(n)$.

Proof. Proof is straight forward and we omit the proof. □

The following proposition gives a criterion for QNRNP modulo n whenever $n = p^h$ or $2p^h$.

Proposition 2.2. *Let h be any positive integer. Let n be any positive integer of the form p^h or $2p^h$ where p is an odd prime. Then an integer a is a QNRNP modulo n if and only if for some odd divisor $q > 1$ of $\phi(n)$, we have,*

$$a^{\phi(n)/2q} \equiv -1 \pmod{n}.$$

Proof. Suppose a is a QNRNP modulo n. Then,

$$a^{\phi(n)/2} \equiv -1 \pmod{n}.$$

If n is a Fermat prime or twice a Fermat prime, then we know that every non-residue is a primitive root modulo n. Therefore, by the assumption, n is not such a number. Thus there exists an odd integer $q > 1$ which divides $\phi(n)$. Since a is not a primitive root modulo n, by Proposition 2.1, there exists an odd prime q_1 dividing q satisfying

$$a^{\phi(n)/q_1} \equiv 1 \pmod{n}.$$

Therefore, by taking the square-root of $a^{\phi(n)/q_1}$ modulo n, we see that

$$a^{\phi(n)/2q_1} \equiv \pm 1 \pmod{n}.$$

If

$$a^{\phi(n)/2q_1} \equiv 1 \pmod{n},$$

then by taking the q_1-th power both the sides, it follows that a is quadratic residue modulo p, a contradiction. Hence, we get $a^{\phi(n)/2q_1} \equiv -1 \pmod{n}$.

For the converse, let a be an integer satisfying

$$a^{\phi(n)/2q} \equiv -1 \pmod{n}, \tag{1}$$

where $q > 1$ is an odd divisor of $\phi(n)$. Then by squaring both the sides of (1), we conclude by Proposition 2.1 that a cannot be a primitive root modulo n. By taking the q-th power both sides of (1), we see that the right hand side of the congruence is still -1 as q is odd and hence we conclude that a is a quadratic non-residue modulo n. Thus the proposition follows. □

Corollary 2.2.1. *Let p be a prime. Suppose p is not a Fermat prime and 4 divides $p-1$. If a is a QNRNP modulo p, then $\pm a^{(p-1)/4q}$ is a square-root of -1 modulo p for some odd divisor q of $p-1$.*

Proof. By Lemma 2.2, it follows that there exists an odd divisor q of $p-1$ such that $a^{(p-1)/2q} \equiv -1 \pmod{p}$. Since 4 divides $p-1$, it is clear that $(a^{(p-1)/4q})^2 \equiv -1 \pmod{p}$ and hence the result. □

Lemma 2.3. (Křížek and Somer, [2]) *Let m be an odd positive integer. Then $|K(2m)| = |K(m)|$ and $|M(2m)| = |M(m)|$.*

Theorem 2.4 (Brauer, [1]) *Let r, k and s be positive integers. Then there exists a positive integer $N = N(r,k,s)$ depending only on r, k and s such that for any partition of the set*

$$\{1, 2, \cdots, N\} = C_1 \cup C_2 \cup \cdots \cup C_r$$

into r-classes, we have positive integers $a, a+d, \cdots, a+(k-1)d \leq N$ and $sd \leq N$ lie in only one of the C_i's.

Using Theorem 2.4, Brauer [1] proved that for all large enough primes p, one can find arbitrary long sequence of consecutive quadratic residues (resp. non-residues) modulo p. Also, in a series of papers, E. Vegh [3], [4], [5], [6] and [7] studied the distribution of primitive roots modulo p^h or $2p^h$.

3. Proof of Theorem 1.1

Lemma 3.1. *Let h and r be any positive integers. Let $n = p^h$ or $2p^h$ for any odd prime p. Then $|M(n)| = |K(n)| - 2^r$ if and only if n is either (i) p or $2p$ whenever $p = 2^{r+1}q + 1$ with q is also a prime or (ii) p^2 or $2p^2$ whenever $p = 2^{r+1} + 1$ is a Fermat prime.*

Proof. In the view of Lemma 2.3, it is enough to assume that $n = p^h$. Let $p = 2^\ell q + 1$ where ℓ, q are positive integers such that $2 \not| q$.

Case (i) $(h = 1)$

In this case, we have,

$$|M(p)| = \phi(p-1) = 2^{\ell-1}\phi(q)$$

and

$$|K(p)| - 2^r = \frac{\phi(p)}{2} - 2^r = \frac{p-1}{2} - 2^r = 2^{\ell-1}q - 2^r.$$

Hence, $|M(p)| = |K(p)| - 2^r$ would imply

$$2^{\ell-1}\phi(q) = 2^{\ell-1}q - 2^r \Longrightarrow \ell - 1 = r$$

and $\phi(q) = q - 1$. Since the positive integer q satisfies $\phi(q) = q - 1$, q must be a prime number. Therefore, those primes p satisfies the hypothesis are of the form $2^{r+1}q + 1$ where q is also a prime number.

Case (ii) $(h \geq 2)$

In this case, we have,

$$\begin{aligned} |M(p^h)| &= \phi(\phi(p^h)) = \phi(p^{h-1}(p-1)) = \phi(p^{h-1})\phi(p-1) \\ &= p^{h-2}(p-1)\phi(p-1) = p^{h-2}2^\ell q 2^{\ell-1}\phi(q) = 2^{2\ell-1}q\phi(q)p^{h-2}. \end{aligned}$$

Now,

$$|K(p^h)| = \frac{\phi(p^h)}{2} = \frac{p^{h-1}(p-1)}{2} = p^{h-1}2^{\ell-1}q.$$

Therefore, $|M(p^h)| = |K(p^h)| - 2^r$ implies

$$2^{2\ell-1}q\phi(q)p^{h-2} \quad = \quad p^{h-1}2^{\ell-1}q - 2^r$$

and hence we get, $\ell - 1 = r$ and $q = 1$. Thus we have, $2^{r+1}p^{h-2} = p^{h-1} - 1$ which would imply h cannot be greater than 2. If $h = 2$, then we have $p = 2^{r+1} + 1$. That is, if $h \geq 2$, then the only integers n satisfies the hypothesis are p^2 where p is a Fermat prime.

Converse is trivial to establish. □

Proof of Theorem 1.1. Given that $|M(n)| = |K(n)| - 2^r$. By Lemma 3.1, we have two cases.

Case (i) ($n = p$ or $2p$ where $p = 2^{r+1}q + 1$ where q is also a prime)

Let $g \in K(n) \setminus M(n)$ be an arbitrary element. Then g is a quadratic non-residue modulo n; but not a primitive root modulo n. Therefore by Proposition 2.2, we know that there exists an odd divisor $\ell > 1$ of $\phi(n)$ satisfies

$$g^{\frac{\phi(n)}{2\ell}} \equiv -1 \pmod{n}.$$

Since $\phi(n) = p - 1 = 2^{r+1}q$ where q is the only odd divisor of $\phi(n)$, we must have $\ell = q$. Therefore,

$$g^{\frac{p-1}{2q}} \equiv -1 \pmod{n} \Rightarrow g^{2^r} \equiv -1 \pmod{n} \Rightarrow g^{2^{r+1}} \equiv 1 \pmod{n}.$$

Let H be the unique cyclic subgroup of $\mathbb{Z}_n^*$. Then $g \in H$ with order of g is 2^{r+1}. Hence as g is arbitrary, $K(n) \setminus M(n)$ is the set of all generators of H.

Case (ii) ($n = p^2$ or $2p^2$ where $p = 2^{r+1} + 1$ is a prime and $r + 1$ is a power of 2)

Let $g \in K(n) \setminus M(n)$. Then by Proposition 2.2, we know that there exists an odd divisor q of $\phi(n)$ satisfying

$$g^{\frac{\phi(n)}{2q}} = g^{\frac{p(p-1)}{2p}} = g^{2^r} \equiv -1 \pmod{n}$$

and hence $g^{2^{r+1}} \equiv 1 \pmod{n}$. Thus, $g \in H$ where H is the unique subgroup of $\mathbb{Z}_n^*$ of order 2^{r+1}. □

4. Proof of Theorem 1.2

Lemma 4.1. *Let p be a prime such that $p = 4q + 1$ where q is also a prime. If $(a, a + 1)$ is a pair of QNRNP modulo p, then $a \equiv -1/2 \pmod{p}$.*

Proof. Given that a and $a + 1$ are QNRNP modulo p. Therefore, by Proposition 2.2, we have

$$a^{\frac{p-1}{2q}} = a^2 \equiv -1 \pmod{p} \text{ and } (a + 1)^{\frac{p-1}{2q}} = (a + 1)^2 \equiv -1 \pmod{p}.$$

That is, $(a + 1)^2 = a^2 + 2a + 1 \equiv 2a \equiv -1 \pmod{p}$. Hence the result. □

Proof of Theorem 1.2. By Lemma 3.1, we know that for these primes, there are exactly two QNRNP modulo p. Suppose we assume that these two QNRNP modulo p are consecutive pair, say, $(a, a + 1)$. Then by Lemma 4.1, we get, $a \equiv -1/2 \pmod{p}$. To end the proof, we shall, indeed, show that a is a primitive root modulo

p and we arrive at a contradiction. To prove a is a primitive root, we have to prove that the order of $a = -1/2$ in $\mathbb{Z}_p^*$ is $p-1$. Since the order of -1 is 2 and the order of 2 is equal to the order of $1/2$, it is enough to prove that 2 is a primitive root modulo p. By Proposition 2.1, we have to prove that $2^{\frac{p-1}{m}} \not\equiv 1 \pmod{p}$ for every prime divisor m of $p-1$. In this case, we have $m = 2$ and $m = q$. If $m = q$, then $(p-1)/q = 4$ and so $16 = 2^4 \not\equiv 1 \pmod{p}$, as $p = 4q+1$. Hence, it is enough to prove that $2^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$. Indeed, by the quadratic reciprocity law, we know $2^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ and hence the theorem. $\square$

5. Proof of Theorem 1.3

Lemma 5.1. *Let $p > 3$ be a prime such that $p \neq 2^l + 1$. Let ν be denote the total number of QNRNP modulo p. Then exactly $(\nu-1)/2$ number of QNRNP modulo p are followed by quadratic non-residue modulo p whenever $p = 2m+1$ where $m > 1$ is an odd integer; Otherwise, exactly half of QNRNP modulo p is followed by a quadratic non-residue modulo p.*

Proof. First note that $\nu = (p-1)/2 - \phi(p-1)$ is odd if and only if $(p-1)/2$ is odd if and only if $p = 2m+1$ where $m > 1$ is an odd integer.

Let Φ_1 be a QNRNP modulo p. Let g be a fixed primitive root modulo p. Then there exists an odd integer ℓ satisfying $1 < \ell \leq p-2$, $(\ell, p-1) > 1$ and $\Phi_1 = g^\ell$. Therefore, $\Phi_2 = g^{p-1-\ell}$ is also a QNRNP modulo p. Then we have,

$$\Phi_1(1 + \Phi_2) = \Phi_1 + \Phi_1\Phi_2 \equiv \Phi_1 + 1 \pmod{p}.$$

This implies Φ_2+1 is a quadratic residue modulo p if and only if Φ_1+1 is a quadratic non-residue modulo p. Therefore, to complete the proof of this lemma, it is enough to show that if $\chi = g^r$ is a QNRNP modulo p and $\chi \not\equiv \Phi_1, \Phi_2 \pmod{p}$, then $g^{p-1-r} \not\equiv \Phi_1, \Phi_2 \pmod{p}$. Suppose not, that is, $g^{p-1-r} \equiv \Phi_1 = g^\ell \pmod{p}$. Then, $p-1-r \equiv \ell \pmod{p}$. Since $1 < p-1-r \leq p-2$, it is clear that $p-1-r = \ell$ which would imply $p-1-\ell = r$ and therefore we get $\chi = g^r \equiv g^{p-1-\ell} = \Phi_2 \pmod{p}$, a contradiction and hence $g^{p-1-r} \not\equiv \Phi_2 \pmod{p}$. Similarly, we have $g^{p-1-r} \not\equiv \Phi_1 \pmod{p}$. Note that $\phi_1 \equiv \Phi_2 \pmod{p}$ if and only if $\ell \equiv p-1-\ell \pmod{p-1}$ which would imply $\ell = (p-1)/2$, as $1 < \ell < p-2$. Since ℓ is odd, this happens precisely when $p = 2m+1$ where $m > 1$ is an odd integer. Hence the lemma. $\square$

Proof of Theorem 1.3. Let p be any prime such that $\phi(p-1) < (p-1)/6$. If possible, we shall assume that there is no pair of consecutive QNRNP modulo p. Let $k = \frac{p-1}{2} - \phi(p-1)$. Therefore, clearly, $k > \frac{p-1}{2} - \frac{p-1}{6} = \frac{p-1}{3}$. By Lemma 5.1, we know that exactly half of QNRNP modulo p followed by a quadratic non-residue modulo p. This implies, $k/2 \geq (p-1)/6$ number of QNRNP modulo p followed by primitive roots modulo p. Since there there are utmost $(p-1)/6 - 1$ primitive roots available, it follows that there exists a QNRNP modulo p followed by a QNRNP modulo p. $\square$

6. Proof of Theorem 1.4

Given that $q > 1$ is an odd integer and $k > 1$ is an integer. Put $r = 2q, k = k$ and $s = 1$ in Theorem 2.4. We get a natural number $N = N(q, k)$ depending only on q and k such that for any r-partitioning of the set $\{1, 2, \cdots, N\}$, we have positive integers $a, a+d, a+2d, \cdots, a+(k-1)d$ and d which are less than or equal to N and lying in exactly one of the classes.

Choose a prime $p > N$ such that $p \equiv 1 \pmod q$. By Dirichlet's prime number theorem on arithmetic progression, such a prime p exists and there are infinitely many such primes. Let g be a fixed primitive root modulo p^h. Note that for each $j; 1 \leq j \leq p-1$, there exists a unique integer $\lambda_j; 1 \leq \lambda_j \leq p^{h-1}(p-1)$ satisfying $g^{\lambda_j} \equiv j \pmod{p^h}$.

We partition the set $\{1, 2, \cdots, p-1\}$ into $r = 2q$ parts as follows.

$$\{1, 2, \cdots, p-1\} = C_1 \cup C_2 \cup \cdots \cup C_r$$

by $j \in C_i$ if and only if $\lambda_j \equiv i \pmod r$.

Since $p - 1 \geq N$, there exists an arithmetic progression of length k, say $a, a+d, \cdots, a+(k-1)d$ together with its common difference d lying in C_τ for some $\tau = 1, 2, \cdots, r$. By the definition of our partition, we have

$$a + id \equiv g^{\tau_i} \pmod{p^h} \text{ and } d \equiv g^{\tau_k} \pmod{p^h},$$

where $\tau_i \in \{1, 2, \cdots, p-1\}$ for each $i = 0, 1, \cdots, k$, satisfying

$$\tau_0 \equiv \tau_1 \equiv \cdots \equiv \tau_k \equiv \tau \pmod r.$$

Since τ_i's run through single residue class modulo r, we can as well assume, if necessary by a suitable translation, that $\tau \equiv 0 \pmod r$. Now, choose an integer κ such that $\kappa \equiv 1 \pmod 2$ and $\kappa \equiv 0 \pmod q$. Then we see that

$$\tau_0 + \kappa \equiv \tau_1 + \kappa \equiv \cdots \equiv \tau_k + \kappa \equiv \kappa \pmod r.$$

Since κ is an odd integer and τ_i's are even integers, we get, $\tau_i + \kappa$ are odd integers together with $\tau_i + \kappa \equiv 0 \pmod q$. Therefore, q divides the $\gcd(\tau_i + \kappa, p-1)$. Putting $a_0 \equiv g^\kappa \pmod{p^h}$, we get,

$$a_0 a, a_0 a + a_0 d, \cdots, a_0 a + (k-1) a_0 d, a_0 d$$

are QNRNP p^h.

If g is an odd integer, then g is also a primitive root modulo $2p^h$. If g is an even integer, then put $g' = g + p^h$ which is an odd integer and hence it is a primitive root modulo $2p^h$. Now the proof is similar to case when $n = p^h$ and we leave it to the readers. □

Before we conclude this section, we shall raise the following questions.

(1) Can Theorems 1.4 be true for all large enough primes p?

(2) What is the general property of the set of all positive integers satisfying $M(n) = K(n) - m$ for any given positive integer $m \neq 1, 2^r$?

Acknowledgment. We are thankful to Professor M. Křížek for sending his paper [2]. Also, we are grateful to Professor D. Rohrlich pointing out an error in the previous version of this paper.

References

[1] A. Brauer, Űber Sequenzen von Potenzresten, *Sitzungsberichte der Preubischen Akademie der Wissenschaften*, (1928), 9-16.

[2] M. Křížek, L. Somer, A necessary and sufficient condition for the primality of Fermat numbers, *Math. Bohem.,* **126** (2001), no. 3, 541-549.

[3] E. Vegh, Pairs of consecutive primitive roots modulo a prime, *Proc. Amer. Math. Soc.*, **19** (1968), 1169-1170.

[4] E. Vegh, Primitive roots modulo a prime as consecutive terms of an arithmetic progression, *J. Reine Angew. Math.*, **235** (1969), 185-188.

[5] E. Vegh, Primitive roots modulo a prime as consecutive terms of an arithmetic progression - II, *J. Reine Angew. Math.*, **244** (1970), 108-111.

[6] E. Vegh, A note on the distribution of the primitive roots of a prime, *J. Number Theory*, **3** (1971), 13-18.

[7] E. Vegh, Primitive roots modulo a prime as consecutive terms of an arithmetic progression - III, *J. Reine Angew. Math.*, **256** (1972), 130-137.

School of Mathematics, Harish Chandra Research Institute, Chhatnag Road, Jhusi, Allahabad - 211019, India.

E-mail address, S. Gun: `sanoli@mri.ernet.in`

E-mail address, B. Ramakrishnan: `ramki@mri.ernet.in`

E-mail address, B. Sahu: `sahu@mri.ernet.in`

E-mail address, R. Thangadurai: `thanga@mri.ernet.in`