130 (2005) MATHEMATICA BOHEMICA No. 4, 387–396

DISTRIBUTION OF QUADRATIC NON-RESIDUES WHICH ARE NOT PRIMITIVE ROOTS

S. Gun, B. Ramakrishnan, B. Sahu, R. Thangadurai, India

(Received February 24, 2005)

Abstract. In this article we 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 $h \geqslant 1$ an integer.

MSC 2000: 11N69

Keywords: quadratic non-residues, primitive roots, Fermat numbers

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 will study the distribution of quadratic non-residues which are not primitive roots modulo odd prime powers.

Let n be any positive integer and p 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 $\varphi(n)$, 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 prime number p and a positive integer $h \geqslant 1$. Moreover, the number of primitive roots modulo these n's is equal to $\varphi(\varphi(n))$.

Definition 1.2. Let $n \geqslant 2$ 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^{2l-1} for $l = 1, 2, \ldots, \varphi(n)/2$ are all the quadratic non-residues modulo n and g^{2l} for $l = 0, 1, \ldots, \varphi(n)/2 - 1$ are all the quadratic residues modulo n. Also, g^{2l-1} for all $l = 1, 2, \ldots, \varphi(n)/2$ such that $(2l-1, \varphi(n)) > 1$ are all the quadratic non-residues which are not primitive roots modulo n.

For a positive integer n, set

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

and

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

Note that $M(1) = K(1) = \emptyset$, $M(2) = \{1\}$ and $K(2) = \emptyset$. When $n \geqslant 3$, we know that $|K(n)| \geqslant \varphi(n)/2$ and whenever $n = 2, 4$ or p^a or $2p^a$, we have $|K(n)| = \varphi(n)/2$. Also, it can be easily seen that if $n \geqslant 3$, 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 $n \geqslant 2$, $|M(n)| = |K(n)| - 1$ 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 will prove the following theorems.

Theorem 1.1. *Let r and h be any positive integers. Let $n = p^h$ or $2p^h$ for an 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 $\nu := |K(p) \setminus M(p)| = (p-1)/2 - \varphi(p-1) > 0$. When $\nu \geqslant 2$, a natural question is whether there exists 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 exists no pair of consecutive QNRNP modulo p.*

In contrast to Theorem 1.2, we will prove the following

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

In the next theorem, we will address a weaker question than Theorem 1.3; however, it works for an arbitrary length k.

Theorem 1.4. *Let $q > 1$ be any odd integer and $k > 1, h \geqslant 1$ 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 four theorems.

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

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

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

Proof. We omit the proof as it is straightforward. □

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 $\varphi(n)$ we have*

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

Proof. Suppose a is a QNRNP modulo n. Then

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

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 $\varphi(n)$. Since a is not a primitive root modulo n, by Proposition 2.1 there exists an odd prime q_1 dividing q and satisfying

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

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

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

If

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

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

Conversely, let a be an integer satisfying

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

where $q > 1$ is an odd divisor of $\varphi(n)$. 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 of 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 2.3. *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 2.4 (Křížek and Somer, [2]). *Let $m \geqslant 3$ be an odd positive integer. Then $|K(2m)| = |K(m)|$ and $|M(2m)| = |M(m)|$.*

Theorem 2.5 (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*

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

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

Using Theorem 2.5, Brauer [1] proved that for all primes p large enough, one can find an arbitrary long sequence of consecutive quadratic residues (or non-residues) modulo p. Also, in a series of papers, E. Vegh [3], [4], [5], [6], [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 an 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 being also a prime or* (ii) *p^2 or $2p^2$ whenever $p = 2^{r+1} + 1$ is a Fermat prime.*

Proof. In view of Lemma 2.4, it is enough to assume that $n = p^h$. Let $p = 2^l q + 1$ where l, q are positive integers such that $2 \nmid q$.

Case (i) ($h = 1$). We have

$$|M(p)| = \varphi(\varphi(p)) = 2^{l-1}\varphi(q)$$

and

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

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

$$2^{l-1}\varphi(q) = 2^{l-1}q - 2^r \Longrightarrow l - 1 = r$$

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

Case (ii) ($h \geqslant 2$). We have

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

Now,

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

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

$$2^{2l-1}q\varphi(q)p^{h-2} = p^{h-1}2^{l-1}q - 2^r$$

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

The converse is trivial to establish. $\square$

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

Case (i) ($n = p$ or $2p$, where $p = 2^{r+1}q+1$ is prime and 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 $l > 1$ of $\varphi(n)$ that satisfies

$$g^{\varphi(n)/2l} \equiv -1 \pmod{n}.$$

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

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

Let H be the unique cyclic subgroup of $\mathbb{Z}_n^*$. Then $g \in H$ with order of g being 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 $\varphi(n)$ satisfying

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

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}. $\square$

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. Let a and $a + 1$ be QNRNP modulo p. Therefore, by Proposition 2.2, we have

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

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 that these two QNRNP modulo p are a consecutive pair, say, $(a, a + 1)$. Then by Lemma 4.1, we get $a \equiv -1/2 \pmod{p}$. To complete the proof, we shall 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 $2^{(p-1)/m} \not\equiv 1 \pmod{p}$ 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 $2^{(p-1)/2} \not\equiv 1 \pmod{p}$. Indeed, by the quadratic reciprocity law, we know that $2^{(p-1)/2} \equiv -1 \pmod{p}$ and hence the theorem follows. □

5. Proof of Theorem 1.3

Lemma 5.1. *Let $p > 3$ be a prime such that $p \neq 2^l + 1$. Let ν denote the total number of QNRNP modulo p. Then exactly $(\nu - 1)/2$ QNRNP modulo p are followed by a 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 $\nu = (p - 1)/2 - \varphi(p - 1)$ 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 $1 < l \leqslant p - 2$, $(l, p - 1) > 1$ and $\Phi_1 = g^l$. Therefore, $\Phi_2 = g^{p-1-l}$ 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, $g^{p-1-r} \equiv \Phi_1 = g^l \pmod p$. Then $p-1-r \equiv l \pmod p$. Since $1 < p-1-r \leqslant p-2$, it is clear that $p-1-r = l$, which would imply $p-1-l = r$ and therefore, we get $\chi = g^r \equiv g^{p-1-l} = \Phi_2 \pmod p$, 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 $\varphi_1 \equiv \Phi_2 \pmod p$ if and only if $l \equiv p-1-l \pmod{p-1}$, which would imply $l = (p-1)/2$, as $1 < l < p-2$. 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 $\varphi(p-1) < (p-1)/6$. If possible, we will assume that there is no pair of consecutive QNRNP modulo p. Let $k = (p-1)/2 - \varphi(p-1)$. Therefore, clearly, $k > (p-1)/2 - (p-1)/6 = (p-1)/3$. By Lemma 5.1, we know that exactly half of QNRNP modulo p are followed by a quadratic non-residue modulo p. This implies that $k/2 \geqslant (p-1)/6$ QNRNP modulo p are followed by primitive roots modulo p. Since there are at most $(p-1)/6 - 1$ 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 $r = 2q$ and $s = 1$ in Theorem 2.5. We get a natural number $N = N(q,k)$ depending only on q and k such that for any r-partitioning of the set $\{1, 2, \dots, N\}$, we have positive integers $a, a+d, a+2d, \dots, a+(k-1)d$ and d which are less than or equal to N and are 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 $j; 1 \leqslant j \leqslant p-1$, there exists a unique integer $\lambda_j; 1 \leqslant \lambda_j \leqslant p^{h-1}(p-1)$ satisfying $g^{\lambda_j} \equiv j \pmod{p^h}$.

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

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

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

Since $p-1 \geqslant N$, there exists an arithmetic progression of length k, say $a, a+d, \dots, a+(k-1)d$, together with its common difference d lying in C_τ for some

$\tau = 1, 2, \ldots, r$. By the definition of our partition, we have

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

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

$$\tau_0 \equiv \tau_1 \equiv \ldots \equiv \tau_k \equiv \tau \pmod{r}.$$

Since τ_i's run through a single residue class modulo r, we can as well assume, if necessary applying 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

$$\tau_0 + \kappa \equiv \tau_1 + \kappa \equiv \ldots \equiv \tau_k + \kappa \equiv \kappa \pmod{r}.$$

Since κ is an odd integer and τ_i's are even integers, we get that $\tau_i + \kappa$ 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

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

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 the case when $n = p^h$ and we leave it to the reader. □

Before we conclude this section, we wish to raise the following open questions.

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

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

Acknowledgments. We are thankful to Professor M. Křížek for sending us his paper [2]. We thank the referee for making some useful comments. Also, we are grateful to Professor D. Rohrlich for pointing out an error in the previous version of this paper.

References

[1] *A. Brauer*: Über Sequenzen von Potenzresten. Sitzungsberichte Akad. Berlin (1928), 9–16. (In German.)
[2] *M. Křížek, L. Somer*: A necessary and sufficient condition for the primality of Fermat numbers. Math. Bohem. *126* (2001), 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*: Arithmetic progressions of primitive roots of a prime 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*: Arithmetic progressions of primitive roots of a prime III. J. Reine Angew. Math. *256* (1972), 130–137.

Authors' addresses: *S. Gun*, *B. Ramakrishnan*, *B. Sahu*, *R. Thangadurai*, School of Mathematics, Harish Chandra Research Institute, Chhatnag Road, Jhusi, 211019 Allahabad, India, e-mail: `sanoli@mri.ernet.in`, `ramki@mri.ernet.in`, `sahu@mri.ernet.in`, `thanga@mri.ernet.in`.