In this article, we prove that the sequence consisting of quadratic non-residues which are not primitive root modulo a prime $p$ obeys Poisson law whenever $\frac{p - 1}{2} - \phi(p - 1)$ is reasonably large as a function of $p$. To prove this, we count the number of $\ell$-tuples of quadratic non-residues which are not primitive roots mod $p$, thereby generalizing one of the results obtained in Gun et al. (Acta Arith, 129(4):325–333, 2007).
Distribution of a Subset of Non-residues Modulo $p$

R. Thangadurai and Veekesh Kumar

Dedicated to Professor V. Kumar Murty on his 60th birthday

Abstract In this article, we prove that the sequence consisting of quadratic non-residues which are not primitive root modulo a prime $p$ obeys Poisson law whenever $\frac{p - 1}{2} - \phi(p - 1)$ is reasonably large as a function of $p$. To prove this, we count the number of $\ell$-tuples of quadratic non-residues which are not primitive roots mod $p$, thereby generalizing one of the results obtained in Gun et al. (Acta Arith, 129(4):325–333, 2007, [9]).

Keywords Quadratic residues · Primitive roots · Finite fields

Mathematics Subject Classification Primary 11N69 · Secondary 11A07

1 Introduction

The values of the most arithmetic sequences are so fluctuating, it is of great interest to study the distribution and extract information using many randomness tests such as equidistribution, level spacing or pair correlation.

R. Thangadurai (✉) · V. Kumar
Harish-Chandra Research Institute, HBNI, Chhatnag Road, Jhunsi, Allahabad 211019, India
e-mail: thanga@hri.res.in

V. Kumar
e-mail: veekeshkumar@hri.res.in

© Springer Nature Switzerland AG 2018
Erdős and Kac [4] (see also [13, 14]) showed that the number of prime factors of integers up to \( x \) is normally distributed with mean \( \log \log x \) and standard deviation \( \sqrt{\log \log x} \).

The questions on the spacings between elements of arithmetic sequences, such as primes, quadratic residues, non-residues, primitive roots, integers that are co-prime to a given integer, values of binary quadratic forms, and the zeros of Riemann zeta function, are of great interest and have been studied in the literature.

Davenport [3] studied the spacing between consecutive quadratic residues modulo a prime \( p \). Then, Kurlberg and Rudnick [17], Granville and Kurlberg [7] and Kurlberg [16] studied the spacing between consecutive quadratic residues mod \( n \), where \( n \) is composite integer. Cobeli and Zaharescu [1] studied the spacing between consecutive primitive roots modulo a prime \( p \). Hooley [10–12] also considered the spacing between consecutive integers that are co-prime to an integer \( n \). Gallagher [5] investigated the spacing between consecutive primes, by assuming the Hardy–Littlewood prime \( k \)-tuple conjecture. Rudnick, Sarnak and Zaharescu [21] conjectured the distribution of spacing between the fractional parts of \( n^2 \alpha \) should obey the Poisson law and they proved some weaker result in this direction. Garaev, Luca and Shparlinski [6] obtained new information about the spacing between quadratic non-residues mod \( p \). In particular, they showed that there exists a positive integer \( n \ll p^{1/2+\epsilon} \), such that \( n! \) is a primitive root mod \( p \).

One can observe, from the known results, that almost all the arithmetic sequences obey Poisson law except for a few cases such as the zeros of the Riemann zeta function, where it is known to be normally distributed.

In this article, we shall study the arithmetic sequence which consists of quadratic non-residues which are not primitive roots modulo a prime \( p \). This particular type of residue was studied in [8, 9, 18, 19].

Since the number of quadratic non-residues modulo a prime \( p \) is \( (p-1)/2 \) and the number of primitive roots modulo \( p \) is \( \phi(p-1) \), where \( \phi \) is the Euler phi-function, we see that the number of quadratic non-residues which are not primitive roots modulo \( p \) is

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

Hence, \( k = 0 \) if and only if \( \frac{p-1}{2} = \phi(p-1) \) if and only if \( p = 2^m + 1 \) for some integer \( m \geq 1 \) if and only if \( p \) is a Fermat prime. Thus, in this article, we shall assume that any prime \( p \) means \( p \neq 2^m + 1 \) for any integer \( m \geq 1 \).

In order to understand the spacing between these particular residues modulo \( p \), we first enumerate these residues in the increasing order as \( 1 < \nu_1 < \nu_2 < \cdots < \nu_k < p \). Then, we see that the mean spacing of these residues is \( \frac{p-1}{k} \). We want to study how the elements \( \nu_i \)'s are placed in the interval \( (n, n+t] \) for some suitable real number \( t \geq 1 \) and for integer \( n \) with \( 0 < n < n+t \leq p \). We formulate this in terms of a random variable.
Let $X_t$ be a random variable $X_t : [1, p] \rightarrow \mathbb{R}$ defined by

$$X_t(n) = |\{\nu_i : \nu_i \in (n, n + t)\}|$$

for some real number $t$. One may ask the following natural question. For a given integer $\ell \geq 1$, what is the probability density function $P_t(X_t = \ell)$ for $X_t$ as $t \rightarrow \infty$ and for all large enough primes $p$?

In this article, we prove that the probability density function $P_t(X_t = \ell)$ is Poisson as $t \rightarrow \infty$, when the random variable $X_t$ is restricted to the given interval $I$ of suitable length of $\mathbb{F}_p$ for all primes $p$ whose mean spacing is large enough. To prove this result, we apply the techniques employed in [1, 9] and on the way, this technique does generalize one of the main results of [9] in some sense.

2 Preliminaries

As we mentioned before, $p$ is assumed to be a prime number which is not of the form $2^m + 1$ for any integer $m$. The finite field with $p$ elements is denoted by $\mathbb{F}_p$, and its multiplicative group is denoted by $\mathbb{F}_p^*$, which is known to be a cyclic group.

An element $g \in \mathbb{F}_p^*$ is said to be a primitive root modulo $p$ if $g$ is a generator of the cyclic group $\mathbb{F}_p^*$. We abbreviate the term ‘quadratic non-residue which is not a primitive root mod $p$’ by ‘QNRNP’. Once we know a primitive root, say, $g$ modulo $p$, the QNRNPs are precisely the elements of the set

$$\{g^\ell : \ell = 1, 3, \ldots, (p - 2) \text{ and } (\ell, p - 1) > 1\}.$$

Let $I = \{M + 1, M + 2, \ldots, M + l\}$ be an interval in $\{1, 2, \ldots, p - 1\}$ for some integers $M \geq 0$ and $l \geq 1$. For any two disjoint subsets $\mathcal{A}$ and $\mathcal{B}$ of $\mathbb{F}_p$, we define

$$N(\mathcal{A}, \mathcal{B}) = N(\mathcal{A}, \mathcal{B}, p, I)$$

to be the cardinality of the subset $\mathcal{J}$ of $I$, containing all the elements $n \in I$ satisfying $n + a$ is a QNRNP for every $a \in \mathcal{A}$ and $n + b$ is not a QNRNP for every $b \in \mathcal{B}$. When $\mathcal{B} = \emptyset$, then we denote $N(\mathcal{A}, \emptyset)$ by $N(\mathcal{A})$.

First, heuristically, we compute the magnitude of $N(\mathcal{A}, \mathcal{B})$ as follows.

Among the $p - 1$ elements of $\mathbb{F}_p^*$, there is exactly $k = \left(\frac{p - 1}{2} - \phi(p - 1)\right)$ number of QNRNPs. Hence, for a given element $n \in \mathbb{F}_p^*$, the probability that $n + a$ being a QNRNP is $k/(p - 1)$ and the probability that $n + b$ not being QNRNP is $1 - k/(p - 1)$. Therefore, the probability that $n + a$ being a QNRNP and $n + b$ not being a QNRNP is

$$\left(\frac{k}{p - 1}\right) \left(1 - \frac{k}{p - 1}\right).$$
For a given \( n \in \mathbb{F}_p^* \), by assuming the independent nature of the elements \( n + a \) being a QNRNP and \( n + b \) not being a QNRNP for \( a \in A \) and for \( b \in B \), we see that the probability that \( n + a \) being QNRNP for all \( a \in A \) and \( n + b \) not being QNRNP for all \( b \in B \) is

\[
\left( \frac{k}{p-1} \right)^{|A|} \left( 1 - \frac{k}{p-1} \right)^{|B|}.
\]

Therefore, it is reasonable to expect

\[
N(A, B) \sim |I| \left( \frac{k}{p-1} \right)^{|A|} \left( 1 - \frac{k}{p-1} \right)^{|B|}.
\]

We prove this fact when \( p \) is sufficiently large.

Let \( \mu_{p-1} \) denote the multiplicative group of the set of all \((p - 1)\)th roots of unity in \( \mathbb{C} \). Then let \( \chi : \mathbb{F}_p^* \rightarrow \mu_{p-1} \) be an isomorphism of groups between \( \mathbb{F}_p^* \) and \( \mu_{p-1} \) such that the dual group of \( \mathbb{F}_p^* \) is generated by \( \chi \). Then it is easy to observe that \( \chi(g) \) is a \((p - 1)\)th primitive root of unity if and only if \( g \) is a primitive root modulo \( p \). Let \( \eta \) be a \((p - 1)\)th primitive root of unity, and let \( g \) be a primitive root modulo \( p \) such that \( \chi(g) = \eta \). Since \( \chi \) is a homomorphism, it follows that \( \chi(g^i) = \chi^i(g) = \eta^i \) for all integers \( i \). Hence, we get \( \chi(\kappa) = \eta^i \) with \( (i, p - 1) > 1 \) with some odd integer \( i \) if and only if \( \kappa \) is a QNRNP mod \( p \).

Let \( 0 \leq \ell \leq p - 2 \) be any integer. We define

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

where \( \eta \) is a primitive \((p - 1)\)th root of unity. Note that \( \beta_{\ell}(p - 1) \) is a complimentary sum of the well-known Ramanujan’s sum.

The following lemma computes the characteristic function for the residues QNRNPs.

**Lemma 2.1** (Gun et al. [9]) We have

\[
\frac{1}{p-1} \sum_{\ell=0}^{p-2} \beta_{\ell}(p - 1) \chi^\ell(n) = \begin{cases} 
1, & \text{if } n \text{ is a QNRNP;} \\
0, & \text{otherwise.}
\end{cases}
\]

**Lemma 2.2** (Gun et al. [9]) We have

\[
\sum_{\ell=0}^{p-1} |\beta_{\ell}(p - 1)| = 2^{\omega(p-1)} \phi(p - 1),
\]

where \( \omega(p - 1) \) denotes the number of distinct prime factors of \( p - 1 \).

The following lemma is standard and can be found in [20].
**Lemma 2.3** For all primes \( p \geq 5 \), we have

\[
\omega(p-1) < 1.4 \frac{\log p}{\log \log p}.
\]

The following theorem may be regarded as a generalization of Polya–Vinogradov theorem, and it is crucial for our main result.

**Theorem 2.1** (Cobeli and Zaharescu [1]) Let \( A = \{a_1, a_2, \ldots, a_r\} \) be a subset of \( \mathbb{F}_p \) and \( \chi \) be a generator of the dual group of \( \mathbb{F}_p^* \). Then, for any interval \( I \) of \( \mathbb{F}_p \), we have

\[
\left| \sum_{n \in I} \chi(n + a_1)\chi^2(n + a_2) \cdots \chi^r(n + a_r) \right| \leq 2r (\log p)\sqrt{p}.
\]

In this article, we prove the following theorems.

**Theorem 2.2** Let \( A \) and \( B \) be two disjoint subsets of \( \mathbb{F}_p \). Then

\[
\left| N(A, B) - |I| \left( \frac{k}{p-1} \right)^{|A|} \left( 1 - \frac{k}{p-1} \right)^{|B|} \right| \leq 2^{|B|+1+|A|+|B|}\omega(p-1) \]

\[
(\log p) \sqrt{p}.
\]

We need the following technical corollary for the main result.

**Corollary 2.1** Let \( \epsilon \) be a real number satisfying \( 0 < \epsilon < 1/4 \) and \( R \geq 1 \) be a natural number. Let \( p \) be a large prime such that

\[
k = \frac{p-1}{2} - \phi(p-1) \geq p^{1 - \frac{\epsilon}{4 + \epsilon}}.
\]

Let \( A \) and \( B \) be two disjoint subsets of \( \mathbb{F}_p \) such that \( R \leq |A| + |B| < \frac{R}{3} \log \log p \) and \( |A| = R \). Then, for all interval \( I \) of \( \mathbb{F}_p \) satisfying \( |I| \geq p^{1+\epsilon} \), we have

\[
N(A, B) = |I| \left( \frac{k}{p-1} \right)^{|A|} \left( 1 - \frac{k}{p-1} \right)^{|B|} \left( 1 + O \left( \frac{1}{p^{\epsilon/4}} \right) \right).
\]

In Sect. 4, we deduce from Corollary 2.1 to conclude that the sequence of QNRNPs obeys a Poisson law, when \( (p-1)/k \) is large enough.

Before we state the next corollary, we first note the following result.

**Lemma 2.4** Let \( \theta > 0 \) be a given real number, and let

\[
N(x, \theta) = \left\{ p \leq x : \frac{p-1}{k} \leq p^\theta \right\}
\]
be the number primes \( p \leq x \) such that \((p - 1)/k \leq p^\theta\). Then \( N(x, \theta) = \pi(x) + o(\pi(x)) \) for all large enough \( x \), where \( \pi(x) \) denotes the number of prime numbers \( p \leq x \).

**Proof** First note that

\[
\frac{p - 1}{k} \leq p^\theta \iff \frac{1}{p^\theta} \leq \frac{1}{2} - \frac{\phi(p - 1)}{p - 1}.
\]

Take any prime \( p \neq 2^n + 1 \), and let \( q \) be the least odd prime divisor of \( p - 1 \). Then,

\[
\phi(p - 1) = (p - 1) \prod_{r \mid (p - 1)} \left(1 - \frac{1}{r}\right) \leq (p - 1) \frac{1}{2} \left(1 - \frac{1}{q}\right),
\]

which is equivalent to

\[
\frac{\phi(p - 1)}{p - 1} \leq \frac{1}{2} \left(1 - \frac{1}{q}\right)
\]

and hence, we get

\[
\frac{1}{p^\theta} \leq \frac{1}{2} - \frac{1}{2} \left(1 - \frac{1}{q}\right) = \frac{1}{2q}.
\]

Thus, the prime \( p \) satisfying the condition \( p - 1 \leq kp^\theta \) implies that the least odd prime \( q \) of \( p - 1 \) satisfies \( q \leq (0.5)p^\theta \). Let \( M(x, \theta) \) denote the number of primes \( p \leq x \) such that every odd prime factor \( r \) of \( p - 1 \) satisfies \( r > (0.5)p^\theta \). Then, by sieve methods, it is known that

\[
M(x, \theta) \leq \pi(x^\theta) + \pi(x) \prod_{p \leq x^\theta} \left(1 - \frac{1}{p}\right) \leq \theta \frac{x}{\log^2 x},
\]

for all large enough \( x \), by Mertens’ formula. Therefore,

\[
N(x, \theta) \geq \pi(x) - M(x, \theta) - F(x) = \pi(x) + o(\pi(x)),
\]

where \( F(x) \) denotes the number of Fermat primes \( p \leq x \) which is at most

log log \( x \).

The following corollary is a generalization of one of the main results in [9], and by Lemma 2.4, the following result is true for almost all the prime numbers.

**Corollary 2.2** Let \( R \geq 1 \) be any integer, and let \( \mathcal{A} = \{a_1, a_2, \ldots, a_R\} \) be a subset of integers. Let \( \epsilon > 0 \) be a given real number. Let \( p \geq p_{\epsilon, R} \) be a sufficiently large prime number satisfying \( \frac{p - 1}{k} \leq p^{\epsilon/(3R)} \) for some computable constant \( p_{\epsilon, R} \) which depends only on \( \epsilon \) and \( R \). Then, for any interval \( \mathcal{I} \subset \mathbb{F}_p^* \) of cardinality \( |\mathcal{I}| > p^{\frac{1}{2} + \epsilon} \)
contains an element \( n \in \mathcal{I} \) such that \( n + a \) is a QNRNP for any \( a \in \mathcal{A} \).
3 Proof of Theorem 2.2

We prove the theorem in two cases as follows.

**Case 1.** \( B = \emptyset \).

In this case, we have \(|B| = 0\). Therefore, we need to estimate the quantity \( N(A, B) = N(A, \emptyset) = N(A) \).

Let \(|A| = s\). By Lemma 2.1, we see that

\[
N(A) = \sum_{n \in I} \left\{ \prod_{a \in A} \left[ \frac{1}{p-1} \sum_{\ell=0}^{p-2} \beta_{\ell}(p-1) \chi^\ell(n+a) \right] \right\}
\]

\[
= \left( \frac{1}{p-1} \right)^{|A|} \sum_{n \in I} \left\{ \prod_{a \in A} \left[ k + \sum_{\ell=1}^{p-2} \beta_{\ell}(p-1) \chi^\ell(n+a) \right] \right\}
\]

\[
= |I| \left( \frac{k}{p-1} \right)^{|A|} + \frac{M}{(p-1)^{|A|}},
\]

where

\[
M = \sum_{0 \leq l_1, l_2, \ldots, l_\ell \leq p-2} \left[ s \prod_{j=1}^s \beta_{l_j}(p-1) \right] \sum_{n \in I} \left[ \prod_{j=1}^s \chi_{l_j}^j(n+a_j) \right].
\]

In order to finish the proof of this case, we have to estimate \( M \). Now, we write \( M = D + C \), where

\[
C = \sum_{1 \leq l_1, l_2, \ldots, l_\ell \leq p-2} \left[ s \prod_{j=1}^s \beta_{l_j}(p-1) \right] \sum_{n \in I} \left[ \prod_{j=1}^s \chi_{l_j}^j(n+a_j) \right]
\]

and \( D \) 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 \( l_j \) is zero, then exactly two of the \( l_j \)'s are 0, etc., up to when just one of the \( l_j \)'s is nonzero.

Now, we look at the sum corresponding to the case when exactly \( j \) of the \( \ell_j \)'s are equal to zero. This means that \( s - j \) of the \( \ell_j \)'s are nonzero. The corresponding sum is

\[
D_j = k^j \sum_{0 \leq r_1, \ldots, r_{s-j} \leq p-2} \left[ \prod_{b=1}^{s-j} \beta_{r_b}(p-1) \right] \sum_{n \in I} \left[ \prod_{b=1}^{s-j} \chi_{r_b}^b(n+a_b) \right].
\]

When we take the absolute value of this summand, we get
Thus, by Theorem 2.1 and Lemma 2.2, we get

\[ |D_j| \leq k^j \sum_{0<r_1,\ldots,r_{s-j} \leq p-2} \prod_{b=1}^{s-j} |\beta_{r_b}(p-1)| \sum_{n \in I} \left( \prod_{b=1}^{s-j} \chi_{r_b}^t(n + a_b) \right) \]

\[ \leq k^j \left( \sum_{l=0}^{p-2} |\beta_l(p-1)| \right)^{s-j} \sum_{n \in I} \left( \prod_{b=1}^{s-j} \chi_{r_b}^t(n + a_b) \right). \]

This inequality holds for all \( j = 1, 2, \ldots, s-2 \). When \( j = s-1 \), we get

\[ |D_{s-1}| \leq k^{s-1} 2^{\omega(p-1)} \phi(p-1) s (\log p) \sqrt{p}. \]

The term \( C \) in \( M \) can also be estimated as above, and we get

\[ |C| \leq \left( 2^{\omega(p-1)} \phi(p-1) \right)^s s (\log p) \sqrt{p}. \]

Adding up all the above estimates for \( |D_j| \) and \( |C| \), we get

\[ \frac{|M|}{(p-1)^s} \leq 2s \frac{\log p \sqrt{p}}{(p-1)^s} s \sum_{j=0}^{s-1} \binom{s}{j} k^j \left( 2^{\omega(p-1)} \phi(p-1) \right)^{s-j} \]

\[ < 2s \log p \sqrt{p} \left( \frac{2^{\omega(p-1)} \phi(p-1)}{p-1} + \frac{k}{p-1} \right)^s \]

\[ < 2s 2^{\omega(p-1)} (\log p) \sqrt{p}, \]

where we have used the fact that \( \frac{2^{\omega(p-1)} \phi(p-1)}{p-1} + \frac{k}{p-1} < 2^{\omega(p-1)} \). Hence, we arrive at

\[ \left| N(\mathcal{A}) - |I| \left( \frac{k}{p-1} \right)^{|\mathcal{A}|} \right| \leq 2|\mathcal{A}|(\log p) \sqrt{p} 2^{|\mathcal{A}| \omega(p-1)}, \]

which satisfies the result when \( \mathcal{B} = \emptyset \).

**Case 2.** \( \mathcal{B} \neq \emptyset \).

For every natural number \( n \), we define

\[ \delta(n) := \frac{1}{p-1} \sum_{\ell=0}^{p-2} \beta_{\ell}(p-1) \chi_{\ell}^t(n). \]
Then, by Lemma 2.1, we get

$$\delta(n) = \begin{cases} 
1, & \text{if } n \text{ is a QNRNP,} \\
0, & \text{otherwise.} 
\end{cases}$$

Using this characteristic function $\delta(n)$ and a well-known formula,

$$\prod_{n \in B} (1 - x_n) = \sum_{C \subset B} (-1)^{|C|} \prod_{n \in C} x_n,$$

we shall write $N(A, B)$ as follows:

$$N(A, B) = \sum_{n \in I} \prod_{a \in A} \delta(n + a) \prod_{b \in B} (1 - \delta(n + b))$$

$$= \sum_{n \in I} \prod_{a \in A} \delta(n + a) \sum_{C \subset B} (-1)^{|C|} \prod_{c \in C} \delta(n + c)$$

$$= \sum_{C \subset B} (-1)^{|C|} \prod_{n \in I} \delta(n + d)$$

$$= \sum_{C \subset B} (-1)^{|C|} N(A \cup C, \emptyset).$$

By Case 1, for any subset $C \subset B$, we get

$$N(A \cup C, \emptyset) = |I| \left( \frac{k}{p - 1} \right)^{|A \cup C|} + \theta_C 2 |A \cup C| (\log p) \sqrt{p} 2^{|A \cup C| \omega(p - 1)},$$

for some real number $\theta_C$ satisfying $|\theta_C| \leq 1$. Therefore,

$$N(A, B) = \sum_{C \subset B} (-1)^{|C|} |I| \left( \frac{k}{p - 1} \right)^{|A \cup C|} + \sum_{C \subset B} (-1)^{|C|} |C| \theta_C 2 |A \cup C| (\log p) \sqrt{p} 2^{|A \cup C| \omega(p - 1)}.$$

Since $A \cap B = \emptyset$, we see that $|A \cup C| = |A| + |C|$ for any subset $C$ of $B$. Therefore, we get

$$\sum_{C \subset B} (-1)^{|C|} |I| \left( \frac{k}{p - 1} \right)^{|A \cup C|} = |I| \left( \frac{k}{p - 1} \right)^{|A|} \sum_{C \subset B} (-1)^{|C|} \left( \frac{k}{p - 1} \right)^{|C|}$$

$$= |I| \left( \frac{k}{p - 1} \right)^{|A|} \left( 1 - \frac{k}{p - 1} \right)^{|B|}.$$
Hence,
\[
N(A, B) = |\mathcal{I}| \left( \frac{k}{p-1} \right)^{|A|} \left( 1 - \frac{k}{p-1} \right)^{|B|} \leq \sum_{\mathcal{C} \subset \mathcal{B}} 2^{|\mathcal{A} \cup \mathcal{C}|} (\log p)^{2|\mathcal{A} \cup \mathcal{C}|(p-1)} \leq 2^{|\mathcal{B}|+1} |\mathcal{A} \cup \mathcal{B}| (\log p)^{2|\mathcal{A} \cup \mathcal{B}|(p-1)}.
\]

This proves this case and hence the theorem. 

4 Proof of Corollary 2.1

Let \( \epsilon > 0 \) be a given real number and \( R \geq 1 \) be a given natural number. Assume that \( p \) is a large prime such that
\[
k = \frac{p - 1}{2} - \phi(p-1) \geq p^{1 - \frac{1}{\log p}}.
\]

Let \( I \) be a given interval in \( \mathbb{F}_p \) of cardinality \( |I| \geq p^{\frac{3}{4} + \epsilon} \). Let \( A \) and \( B \) be two disjoint subsets of \( \mathbb{F}_p \) such that \( |A| + |B| \leq \frac{1}{3} \log p \) and \( |A| = R \).

Claim 1. We have
\[
2^{|B|+1+(|A|+|B|)\omega(p-1)}(|A| + |B|)(\log p)^{2|\mathcal{A} \cup \mathcal{B}|(p-1)} \leq p^{\frac{1}{2} + \frac{\epsilon}{2}}.
\]

Note that by Lemma 2.3, we see that
\[
|B| + 1 + (|A + B|)\omega(p-1) \leq \frac{\epsilon}{3} \left( \log \log p + \frac{3}{\epsilon} + (\log \log p)(1.4) \frac{\log p}{\log \log p} \right)
\]
\[
\leq \frac{(1.5) \epsilon}{3} \log p = \frac{\epsilon}{2} \log p.
\]

Therefore,
\[
2^{|B|+1+(|A|+|B|)\omega(p-1)}(|A| + |B|)(\log p)^{2|\mathcal{A} \cup \mathcal{B}|(p-1)} \leq p^{\frac{(\log 2)\epsilon}{3} (\log \log p)(\log p)^{2|\mathcal{A} \cup \mathcal{B}|(p-1)} \leq p^{\frac{1}{2} + \frac{\epsilon}{2}},
\]
as \( \log 2 \leq 0.7 \). This proves Claim 1.

By Theorem 2.2 and Claim 1, we get
\[
N(A, B) = |\mathcal{I}| \left( \frac{k}{p-1} \right)^{|A|} \left( 1 - \frac{k}{p-1} \right)^{|B|} + O \left( \frac{p^{\frac{1}{2} + \frac{\epsilon}{2}}}{|\mathcal{I}| \left( \frac{k}{p-1} \right)^{|A|} \left( 1 - \frac{k}{p-1} \right)^{|B|}} \right).
\]
Therefore, we need to estimate the quantity

\[
\kappa := \left( p^{\frac{k}{2} + \frac{1}{2}} \right) / \left[ |\mathcal{I}| \left( \frac{k}{p-1} \right)^{|A|} \left( 1 - \frac{k}{p-1} \right)^{|B|} \right] = \frac{p^{\frac{k}{2} + \frac{1}{2}} (p-1)^{|A|}}{|\mathcal{I}| \left( 1 - \frac{k}{p-1} \right)^{|B|}}.
\]

Since \( k = \frac{p-1}{2} - \phi(p-1) \) and hence,

\[
1 - \frac{k}{p-1} = \frac{1}{2} + \frac{\phi(p-1)}{p-1} \geq \frac{1}{2},
\]

we see that

\[
\left( 1 - \frac{k}{p-1} \right)^{|B|} \geq \frac{1}{2^{(\epsilon/4) \log \log p}} = (\log p)^{-\epsilon \log 2/3}.
\]

Since \(|\mathcal{I}| \geq p^{\frac{k}{4} + \epsilon}\), we get

\[
\kappa \leq \frac{p^{\frac{k}{2} + \frac{1}{2}} (p-1)^R \left( \log p \right)^{(\epsilon(\log 2))/3}}{p^{\frac{k}{4} + \epsilon}} \cdot \frac{(p-1)^R \left( \log p \right)^{(\epsilon(\log 2))/3}}{p^{\frac{k}{4} + \frac{1}{2}}}
\]

Therefore, by the hypothesis that \( k \geq p^{1-(\epsilon+1)/(4(R+1))} \), we see that

\[
\kappa \leq \frac{1}{p^{\epsilon/4}}
\]

and hence the corollary.

\[\square\]

## 5 Proof of Corollary 2.2

Given that \( R \geq 1 \) is an integer and \( \epsilon > 0 \) is a given real number. Let \( p \) be a prime number satisfying \( \frac{p-1}{k} \leq p^{1/(3R)} \). Let \( \mathcal{A} = \{a_1, a_2, \ldots, a_R\} \) and \( B = \emptyset \) be subsets of \( \mathbb{F}_p \) in Theorem 2.2. Then \(|\mathcal{A}| + |\mathcal{B}| = R\).

Suppose \( \mathcal{I} \) be any interval in \( \mathbb{F}_p^* \) satisfying \( |\mathcal{I}| \geq p^{\frac{k}{4}} \). Therefore, by Theorem 2.2, we have

\[
\left| N(\mathcal{A}) - |\mathcal{I}| \left( \frac{k}{p-1} \right)^R \right| \leq 2^{R^{3/2} (p-1)} R (\log p)^{3/2}.
\]
The inequality is equivalent to
\[
\left| \frac{N(A)}{|I|^{\delta R}} - 1 \right| \leq 2^{R\omega(p-1)+1} \delta^{-R} R \frac{(\log p) \sqrt{p}}{|I|},
\]
where \( \delta = k/(p - 1) \).

In order to finish the proof of the corollary, we need to prove that \( N(A) \neq 0 \). That is, it is enough to prove that the quantity \( \left| \frac{N(A)}{|I|^{\delta R}} - 1 \right| < 1 \) and hence by the above inequality, it is enough to prove that \( 2^{R\omega(p-1)+1} \delta^{-R} R \frac{(\log p) \sqrt{p}}{|I|} < 1 \).

Since, by Lemma 2.3, we have \( \omega(p - 1) < 1.4 \log p / \log \log p \), we see that \( R^{2^{R\omega(p-1)+1} \delta^{-R} R} (\log p) \sqrt{p} \leq p^{\frac{1}{2} + \frac{k}{6}} \).

By hypothesis, we have \( (p - 1)/k \leq p^{c/3R} \). By putting together both the estimates, we see that
\[
2^{R\omega(p-1)+1} \delta^{-R} R \frac{(\log p) \sqrt{p}}{|I|} < p^{\frac{1}{2} + \frac{k}{6}} \sqrt{p} \frac{\sqrt{p}}{|I|} = p^{\frac{1}{2} + \frac{k}{6}} < 1,
\]
as \( |I| \geq p^{\frac{1}{2} + \epsilon} \). Hence, we conclude that \( N(A) \neq 0 \) which means that there exists an \( n \in \mathcal{I} \) such that \( n + a \) is a QNRNP for any \( a \in A \).

\( \square \)

6 The Poisson Distribution of QNRNPs

Let \( p \) be a prime number and \( k = \frac{p - 1}{2} - \phi(p - 1) \) such that \( (p - 1)/k \) is reasonably large enough. For a positive real number \( t \), we define a random variable \( X_t \) which is a function \( X_t : [1, p] \to \mathbb{R} \) and defined by
\[
X_t(n) = |\{ \nu : \nu \in (n, n + t) \text{ and } \nu \text{ is a QNRNP} \}|.
\]
Clearly, \( X_t(n) \) takes values 0, 1, 2, \ldots

For a given interval \( \mathcal{I} \) of \( \mathbb{F}_p \) and a natural number \( \ell \geq 1 \), we compute the probability density function \( P_t(X_t = \ell) \) by restricting \( X_t \) to \( \mathcal{I} \). Note that if \( t < \ell \), then, clearly, we see that \( P_t(X_t = \ell) = 0 \), as the interval \( (n, n + t) \) contains at most \( \ell - 1 \) integers. Hence, we assume that \( t \geq \ell \).
By definition, we can write $P_t(X_t = \ell)$ as follows:

$$P_t(X_t = \ell) = \frac{1}{|I|} \sum_{C \subset \{1, 2, \ldots, [t]\} \atop |C| = \ell} N(C, C'),$$

where $C'$ is the set of integers from $[1, t]$ which are not in $C$.

Let $\epsilon$ be a given real number with $0 < \epsilon < 1/4$. We choose primes $p$ satisfying

$$k = \frac{p - 1}{2} - \phi(p - 1) \geq p^{1 - \frac{\epsilon^3 + \epsilon}{\log p}}.$$  

Take any interval $I$ of $\mathbb{R}_p$ with $|I| \geq p^{3/4 + \epsilon}$ and $\ell < \frac{\epsilon}{3} \log \log p$. With this, we shall compute $P_t(X_t = \ell)$. By Corollary 2.1, we have

$$P_t(X_t = \ell) = \frac{1}{|I|} \sum_{C \subset \{1, 2, \ldots, [t]\} \atop |C| = \ell} |I| \left(\frac{k}{p - 1}\right)^{|C|} \left(1 - \frac{k}{p - 1}\right)^{|C'|} \left(1 + O\left(\frac{1}{p^{\epsilon/4}}\right)\right)$$

$$= \sum_{C \subset \{1, 2, \ldots, [t]\} \atop |C| = \ell} \left(\frac{k}{p - 1}\right)^{|C|} \left(1 - \frac{k}{p - 1}\right)^{|C'|} \left(1 + O\left(\frac{1}{p^{\epsilon/4}}\right)\right)$$

$$= \left(\frac{k}{p - 1}\right)^{\ell} \left(1 - \frac{k}{p - 1}\right)^{|t| - \ell} \left(1 + O\left(\frac{1}{p^{\epsilon/4}}\right)\right)$$

$$= \left(\frac{k}{p - 1}\right)^{\ell} \left(1 - \frac{k}{p - 1}\right)^{|t| - \ell} \left(1 + O\left(\frac{1}{p^{\epsilon/4}}\right)\right)$$

$$= \left(\frac{k}{p - 1}\right)^{\ell} \left(1 - \frac{k}{p - 1}\right)^{|t| - \ell} \left(1 + O\left(\frac{1}{p^{\epsilon/4}}\right)\right)$$

We write $t = [t] + \{t\}$, where $[t]$ denotes the integral part of $t$ and $\{t\}$ denotes the fractional part of $t$. Since

$$[t](|t| - 1) \cdots (|t| - \ell + 1) = (t - \{t\})(t - \{t\} - 1) \cdots (t - \ell + 1 - \{t\})$$

$$= t(t - 1) \cdots (t - \ell + 1) \prod_{i=0}^{\ell-1} \left(1 - \frac{\{t\}}{t - i}\right)$$

$$= t(t - 1) \cdots (t - \ell + 1) \left(1 + O\left(\frac{1}{t}\right)\right)^{\ell}.$$

Since $\ell \leq t$, we see that
\[ \left(1 + \left(\frac{1}{t}\right)\right)^\ell = \left(1 + O\left(\frac{\ell}{t}\right)\right), \]

and note that, when \( t \to \infty \), the above quantity is close to 1. Now, consider

\[ P_t(X_t = \ell) = \frac{(t - 1) \cdots (t - \ell + 1)(1 + O(\ell/t))}{\ell!} \left(1 - \frac{k}{p - 1}\right)^t \left(1 - \frac{k}{p - 1}\right)^{\ell - t} \left(1 + O\left(\frac{1}{p^{3/4}}\right)\right) \]

Now, we run through the sequence of primes \( p \) and the sequence of \( t \), both tend to infinity, such that \( \lambda = tk/(p - 1) \) remains constant. This is possible because \( k/(p - 1) \) tends to 0, as \( p \to \infty \) and also we have \( t \to \infty \). This shows that asymptotically the probability density function \( P_t(X_t = \ell) \) of the random variable \( X_t \) obey Poisson law with parameter \( \lambda \); that is,

\[ P_t(X_t = \ell) \sim e^{-\lambda} \frac{\lambda^\ell}{\ell!}. \]

Acknowledgements We are grateful to the referee for going through the article meticulously and suggesting many useful changes and pointing out Lemma 2.4 to make the article better readable.

References

Distribution of a Subset of Non-residues Modulo $p$


## Author Queries

### Chapter 20

<table>
<thead>
<tr>
<th>Query Refs.</th>
<th>Details Required</th>
<th>Author’s response</th>
</tr>
</thead>
<tbody>
<tr>
<td>AQ1</td>
<td>References [2, 15] are given in list but not cited in text. Please cite in text or delete from list.</td>
<td></td>
</tr>
</tbody>
</table>
# MARKED PROOF

**Please correct and return this set**

Please use the proof correction marks shown below for all alterations and corrections. If you wish to return your proof by fax you should ensure that all amendments are written clearly in dark ink and are made well within the page margins.

<table>
<thead>
<tr>
<th>Instruction to printer</th>
<th>Textual mark</th>
<th>Marginal mark</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leave unchanged</td>
<td>... under matter to remain</td>
<td>[ ] New matter followed by [ ] or [ ]</td>
</tr>
<tr>
<td>Insert in text the matter indicated in the margin</td>
<td>/ through single character, rule or underline or / through all characters to be deleted</td>
<td>[ ] or [ ]</td>
</tr>
<tr>
<td>Delete</td>
<td></td>
<td>[ ] new character / or [ ] new characters /</td>
</tr>
<tr>
<td>Substitute character or substitute part of one or more word(s)</td>
<td>/ through letter / through characters</td>
<td></td>
</tr>
<tr>
<td>Change to italics</td>
<td>— under matter to be changed</td>
<td></td>
</tr>
<tr>
<td>Change to capitals</td>
<td>— under matter to be changed</td>
<td></td>
</tr>
<tr>
<td>Change to small capitals</td>
<td>— under matter to be changed</td>
<td></td>
</tr>
<tr>
<td>Change to bold type</td>
<td>— under matter to be changed</td>
<td></td>
</tr>
<tr>
<td>Change to bold italic</td>
<td>— under matter to be changed</td>
<td></td>
</tr>
<tr>
<td>Change to lower case</td>
<td>Encircle matter to be changed</td>
<td></td>
</tr>
<tr>
<td>Change italic to upright type</td>
<td>(As above)</td>
<td></td>
</tr>
<tr>
<td>Change bold to non-bold type</td>
<td>(As above)</td>
<td></td>
</tr>
<tr>
<td>Insert ‘superior’ character</td>
<td>/ through character or [ ] where required</td>
<td>[ ] or [ ] under character e.g. [ ] or [ ]</td>
</tr>
<tr>
<td>Insert ‘inferior’ character</td>
<td>(As above)</td>
<td>[ ] over character e.g. [ ]</td>
</tr>
<tr>
<td>Insert full stop</td>
<td>(As above)</td>
<td></td>
</tr>
<tr>
<td>Insert comma</td>
<td>(As above)</td>
<td>[ ] or [ ] and/or [ ] or [ ]</td>
</tr>
<tr>
<td>Insert single quotation marks</td>
<td>(As above)</td>
<td>[ ] or [ ] and/or [ ] or [ ]</td>
</tr>
<tr>
<td>Insert double quotation marks</td>
<td>(As above)</td>
<td>[ ] or [ ] and/or [ ] or [ ]</td>
</tr>
<tr>
<td>Insert hyphen</td>
<td>(As above)</td>
<td></td>
</tr>
<tr>
<td>Start new paragraph</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>No new paragraph</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>Transpose</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Close up</td>
<td>linking [ ] characters</td>
<td></td>
</tr>
<tr>
<td>Insert or substitute space between characters or words</td>
<td>/ through character or [ ] where required</td>
<td></td>
</tr>
</tbody>
</table>
| Reduce space between characters or words | between characters or words affected | [ ] }