Metadata of the chapter that will be visualized in SpringerLink

Book Title	Geometry, Algebra, Number Theory, and Their Information Technology Applications
Series Title	
Chapter Title	Distribution of a Subset of Non-residues Modulo ***p***
Copyright Year	2018
Copyright HolderName	Springer Nature Switzerland AG

Corresponding Author	Family Name	**Thangadurai**
	Particle	
	Given Name	**R.**
	Prefix	
	Suffix	
	Role	
	Division	
	Organization	Harish-Chandra Research Institute, HBNI
	Address	Chhatnag Road, Jhunsi, Allahabad, 211019, India
	Email	thanga@hri.res.in
Author	Family Name	**Kumar**
	Particle	
	Given Name	**Veekesh**
	Prefix	
	Suffix	
	Role	
	Division	
	Organization	Harish-Chandra Research Institute, HBNI
	Address	Chhatnag Road, Jhunsi, Allahabad, 211019, India
	Email	veekeshkumar@hri.res.in

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 ℓ-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, [illegible]).

Keywords (separated by '-')	Quadratic residues - Primitive roots - Finite fields
Mathematics Subject Classification (separated by '-')	Primary 11N69 - Secondary 11A07

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 ℓ-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

A. Akbary and S. Gun (eds.), *Geometry, Algebra, Number Theory, and Their Information Technology Applications*, Springer Proceedings in Mathematics & Statistics 251, https://doi.org/10.1007/978-3-319-97379-1_20

435589_1_En_20_Chapter ☑ TYPESET ☐ DISK ☐ LE ☑ CP Disp.:24/7/2018 Pages: 16 Layout: T1-Standard

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-residue 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 ϕ 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 $\dfrac{p-1}{k}$. We want to study how the elements ν_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 $X_t : [1, p] \to \mathbb{R}$ 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 $t \to \infty$ 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 $t \to \infty$, when the random variable X_t is restricted to the given interval $\mathcal{I}$ 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

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

Let $\mathcal{I} = \{M+1, M+2, \ldots, M+l\}$ 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

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

to be the cardinality of the subset $\mathcal{J}$ of $\mathcal{I}$, containing all the elements $n \in \mathcal{I}$ 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

$$\left(\frac{k}{p-1}\right)\left(1 - \frac{k}{p-1}\right).$$

435589_1_En_20_Chapter ☑ TYPESET ☐ DISK ☐ LE ☑ CP Disp.:24/7/2018 Pages: 16 Layout: T1-Standard

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 $a \in \mathcal{A}$ and for $b \in \mathcal{B}$, we see that the probability that $n + a$ being QNRNP for all $a \in \mathcal{A}$ and $n + b$ not being QNRNP for all $b \in \mathcal{B}$ is

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

Therefore, it is reasonable to expect

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

We prove this fact when p is sufficiently large.

Let μ_{p-1} denote the multiplicative group of the set of all $(p-1)$th roots of unity in $\mathbb{C}$. Then let $\chi : \mathbb{F}_p^* \to \mu_{p-1}$ be an isomorphism of groups between $\mathbb{F}_p^*$ and μ_{p-1} such that the dual group of $\mathbb{F}_p^*$ is generated by χ. 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 η be a $(p-1)$th primitive root of unity, and let g be a primitive root modulo p such that $\chi(g) = \eta$. Since χ 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 κ is a QNRNP mod p.

Let $0 \le \ell \le p-2$ be any integer. We define

$$\beta_\ell(p-1) = \sum_{\substack{1 \le i \le p-1 \\ i \ \text{ odd}, \ (i, p-1) > 1}} \left(\eta^i\right)^\ell,$$

where η 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*

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

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].

435589_1_En_20_Chapter ✓ TYPESET DISK LE ✓ CP Disp.:24/7/2018 Pages: 16 Layout: T1-Standard

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 $\mathcal{A} = \{a_1, a_2, \ldots, a_r\}$ be a subset of $\mathbb{F}_p$ and χ be a generator of the dual group of $\mathbb{F}_p^*$. Then, for any interval $\mathcal{I}$ of $\mathbb{F}_p$, we have*

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

In this article, we prove the following theorems.

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

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

We need the following technical corollary for the main result.

Corollary 2.1 *Let ϵ 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*

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

Let $\mathcal{A}$ and $\mathcal{B}$ be two disjoint subsets of $\mathbb{F}_p$ such that $R \leq |\mathcal{A}| + |\mathcal{B}| < \frac{\epsilon}{3} \log \log p$ and $|\mathcal{A}| = R$. Then, for all interval $\mathcal{I}$ of $\mathbb{F}_p$ satisfying $|\mathcal{I}| \geq p^{\frac{3}{4}+\epsilon}$, we have

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

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*

$$N(x, \theta) = \left| \left\{ p \leq x \ : \ \frac{p-1}{k} \leq p^{\theta} \right\} \right|$$

435589_1_En_20_Chapter ☑ TYPESET ☐ DISK ☐ LE ☑ CP Disp.:24/7/2018 Pages: 16 Layout: T1-Standard

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 $p \neq 2^m + 1$, and let q be the least odd prime divisor of $p-1$. Then,

$$\phi(p-1) = (p-1) \prod_{r|(p-1)} \left(1 - \frac{1}{r}\right) \leq (p-1)\frac{1}{2}\left(1 - \frac{1}{q}\right),$$

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 $\log\log x$. $\square$

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 $\dfrac{p-1}{k} \leq p^{\epsilon/(3R)}$ for some computable constant $p_{\epsilon,R}$ which depends only on ϵ 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. $\mathcal{B} = \emptyset$.

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

Let $|\mathcal{A}| = s$. By Lemma 2.1, we see that

$$\begin{aligned} N(\mathcal{A}) &= \sum_{n\in\mathcal{I}} \left\{ \prod_{a\in\mathcal{A}} \left[\frac{1}{p-1} \sum_{\ell=0}^{p-2} \beta_\ell(p-1)\chi^\ell(n+a) \right] \right\} \\ &= \left(\frac{1}{p-1} \right)^{|\mathcal{A}|} \sum_{n\in\mathcal{I}} \left\{ \prod_{a\in\mathcal{A}} \left[k + \sum_{\ell=1}^{p-2} \beta_\ell(p-1)\chi^\ell(n+a) \right] \right\} \\ &= |\mathcal{I}| \left(\frac{k}{p-1} \right)^{|\mathcal{A}|} + \frac{M}{(p-1)^{|\mathcal{A}|}}, \end{aligned}$$

where

$$M = \sum_{\substack{0\le l_1,l_2,\ldots,l_s\le p-2 \\ (l_1,\ldots,l_s)\neq \mathbf{0}}} \left[\prod_{j=1}^{s} \beta_{l_j}(p-1) \right] \sum_{n\in\mathcal{I}} \left[\prod_{a\in\mathcal{A}} \chi^{l_j}(n+a) \right].$$

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

$$C = \sum_{1\le l_1,l_2,\ldots,l_s\le p-2} \left[\prod_{j=1}^{s} \beta_{l_j}(p-1) \right] \sum_{n\in\mathcal{I}} \left[\prod_{j=1}^{s} \chi^{l_j}(n+a_j) \right]$$

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_i is zero, then exactly two of the l_i's are 0, etc., up to when just one of the l_i's is nonzero.

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

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

When we take the absolute value of this summand, we get

435589_1_En_20_Chapter ✓ TYPESET DISK LE ✓ CP Disp.:24/7/2018 Pages: 16 Layout: T1-Standard

$$
\begin{aligned}
|D_j| &\le k^j \sum_{0<r_1,\ldots,r_{s-j}\le p-2} \prod_{b=1}^{s-j} |\beta_{r_b}(p-1)| \left| \sum_{n\in\mathcal{I}} \left(\prod_{b=1}^{s-j} \chi^{r_b}(n+a_b) \right) \right| \\
&\le k^j \left(\sum_{\ell=0}^{p-2} |\beta_\ell(p-1)| \right)^{s-j} \left| \sum_{n\in\mathcal{I}} \left(\prod_{b=1}^{s-j} \chi^{r_b}(n+a_b) \right) \right|.
\end{aligned}
$$

Thus, by Theorem 2.1 and Lemma 2.2, we get

$$
\begin{aligned}
|D_j| &< k^j \left(2^{\omega(p-1)}\phi(p-1)\right)^{s-j} \left(2(s-j)(\log p)\sqrt{p}\right) \\
&< 2sk^j \left(2^{\omega(p-1)}\phi(p-1)\right)^{s-j} (\log p)\sqrt{p}.
\end{aligned}
$$

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

$$
|D_{s-1}| \le k^{s-1} 2^{\omega(p-1)} \phi(p-1) s (\log p)\sqrt{p}.
$$

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

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

Adding up all the above estimates for $|D_j|$ and $|C|$, we get

$$
\begin{aligned}
\frac{|M|}{(p-1)^s} &\le 2s \frac{\log p\sqrt{p}}{(p-1)^s} \sum_{j=0}^{s-1} \binom{s}{j} k^j \left(2^{\omega(p-1)}\phi(p-1)\right)^{s-j} \\
&< 2s \log p\sqrt{p} \left(2^{\omega(p-1)} \frac{\phi(p-1)}{p-1} + \frac{k}{p-1} \right)^s \\
&< 2s 2^{s\omega(p-1)} (\log p)\sqrt{p},
\end{aligned}
$$

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

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

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

Case 2. $\mathcal{B} \neq \emptyset$.

For every natural number n, we define

$$
\delta(n) := \frac{1}{p-1} \sum_{\ell=0}^{p-2} \beta_\ell(p-1)\chi^\ell(n).
$$

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,

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

we shall write $N(\mathcal{A}, \mathcal{B})$ as follows:

$$\begin{aligned} N(\mathcal{A}, \mathcal{B}) &= \sum_{n \in \mathcal{I}} \prod_{a \in \mathcal{A}} \delta(n+a) \prod_{b \in \mathcal{B}} (1 - \delta(n+b)) \\ &= \sum_{n \in \mathcal{I}} \prod_{a \in \mathcal{A}} \delta(n+a) \sum_{\mathcal{C} \subset \mathcal{B}} (-1)^{|\mathcal{C}|} \prod_{c \in \mathcal{C}} \delta(n+c) \\ &= \sum_{\mathcal{C} \subset \mathcal{B}} (-1)^{|\mathcal{C}|} \sum_{n \in \mathcal{I}} \prod_{d \in \mathcal{A} \cup \mathcal{C}} \delta(n+d) \\ &= \sum_{\mathcal{C} \subset \mathcal{B}} (-1)^{|\mathcal{C}|} N(\mathcal{A} \cup \mathcal{C}, \emptyset). \end{aligned}$$

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

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

for some real number $\theta_{\mathcal{C}}$ satisfying $|\theta_{\mathcal{C}}| \leq 1$. Therefore,

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

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

$$\begin{aligned} \sum_{\mathcal{C} \subset \mathcal{B}} (-1)^{|\mathcal{C}|} |\mathcal{I}| \left(\frac{k}{p-1} \right)^{|\mathcal{A} \cup \mathcal{C}|} &= |\mathcal{I}| \left(\frac{k}{p-1} \right)^{|\mathcal{A}|} \sum_{\mathcal{C} \subset \mathcal{B}} (-1)^{|\mathcal{C}|} \left(\frac{k}{p-1} \right)^{|\mathcal{C}|} \\ &= |\mathcal{I}| \left(\frac{k}{p-1} \right)^{|\mathcal{A}|} \left(1 - \frac{k}{p-1} \right)^{|\mathcal{B}|}. \end{aligned}$$

435589_1_En_20_Chapter ✓ TYPESET DISK LE ✓ CP Disp.:24/7/2018 Pages: 16 Layout: T1-Standard

Hence,

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

This proves this case and hence the theorem. □

4 Proof of Corollary 2.1

Let $\epsilon > 0$ be a given real number and $R \ge 1$ be a given natural number. Assume that p is a large prime such that

$$k = \frac{p-1}{2} - \phi(p-1) \ge p^{1-\frac{\epsilon+1}{4(R+1)}}.$$

Let $\mathcal{I}$ be a given interval in $\mathbb{F}_p$ of cardinality $|\mathcal{I}| \ge p^{\frac{3}{4}+\epsilon}$. Let $\mathcal{A}$ and $\mathcal{B}$ be two disjoint subsets of $\mathbb{F}_p$ such that $|\mathcal{A}|+|\mathcal{B}| \le \frac{\epsilon}{3}\log\log p$ and $|\mathcal{A}| = R$.

Claim 1. We have

$$2^{|\mathcal{B}|+1+(|\mathcal{A}|+|\mathcal{B}|)\omega(p-1)}(|\mathcal{A}|+|\mathcal{B}|)(\log p)\sqrt{p} \le p^{\frac{1}{2}+\frac{\epsilon}{2}}.$$

Note that by Lemma 2.3, we see that

$$|\mathcal{B}|+1+(|\mathcal{A}+\mathcal{B}|)\omega(p-1) \le \frac{\epsilon}{3}\left(\log\log p + \frac{3}{\epsilon} + (\log\log p)(1.4)\frac{\log p}{\log\log p}\right)$$
$$\le \frac{(1.5)\epsilon}{3}\log p = \frac{\epsilon}{2}\log p.$$

Therefore,

$$2^{|\mathcal{B}|+1+(|\mathcal{A}|+|\mathcal{B}|)\omega(p-1)}(|\mathcal{A}|+|\mathcal{B}|)(\log p)\sqrt{p} \le p^{\frac{(\log 2)\epsilon}{2}}\frac{\epsilon}{3}(\log\log p)(\log p)\sqrt{p} \le p^{\frac{1}{2}+\frac{\epsilon}{2}},$$

as $\log 2 \le 0.7$. This proves Claim 1.

By Theorem 2.2 and Claim 1, we get

$$N(\mathcal{A},\mathcal{B}) = |\mathcal{I}|\left(\frac{k}{p-1}\right)^{|\mathcal{A}|}\left(1-\frac{k}{p-1}\right)^{|\mathcal{B}|}$$
$$+\, O\left(\left[p^{\frac{1}{2}+\frac{\epsilon}{2}}\right] \Big/ \left[|\mathcal{I}|\left(\frac{k}{p-1}\right)^{|\mathcal{A}|}\left(1-\frac{k}{p-1}\right)^{|\mathcal{B}|}\right]\right).$$

Therefore, we need to estimate the quantity

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

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

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

Since $|\mathcal{I}| \geq p^{\frac{3}{4}+\epsilon}$, we get

$$\begin{aligned} \kappa &\leq \frac{p^{\frac{1}{2}+\frac{\epsilon}{2}} \left(\frac{p-1}{k}\right)^{R} (\log p)^{(\epsilon(\log 2))/3}}{p^{\frac{3}{4}+\epsilon}} \\ &\leq \frac{\left(\frac{p-1}{k}\right)^{R} (\log p)^{(\epsilon(\log 2))/3}}{p^{\frac{1}{4}+\frac{\epsilon}{2}}}. \end{aligned}$$

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. □

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 $\dfrac{p-1}{k} \leq p^{\epsilon/(3R)}$. Let $\mathcal{A} = \{a_1, a_2, \ldots, a_R\}$ and $\mathcal{B} = \emptyset$ 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 $|\mathcal{I}| \geq p^{\epsilon+\frac{1}{2}}$. Therefore, by Theorem 2.2, we have

$$\left| N(\mathcal{A}) - |\mathcal{I}| \left(\frac{k}{p-1}\right)^{R} \right| \leq 2^{R\omega(p-1)+1} R(\log p)\sqrt{p}.$$

435589_1_En_20_Chapter ✓ TYPESET DISK LE ✓ CP Disp.:24/7/2018 Pages: 16 Layout: T1-Standard

The inequality is equivalent to

$$\left|\frac{N(\mathcal{A})}{|\mathcal{I}|\delta^R} - 1\right| \leq 2^{R\omega(p-1)+1}\delta^{-R} R \frac{(\log p)\sqrt{p}}{|\mathcal{I}|},$$

where $\delta = k/(p-1)$.

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

Since, by Lemma 2.3, we have $\omega(p-1) < 1.4 \log p / \log\log p$, we see that

$$R2^{R\omega(p-1)+1}(\log p) \leq 2^{2R(\log p)/\log\log p} = p^{(R\log 4)/\log\log p};$$

and since $R(\log 4)/(\log\log p) \to 0$ as $p \to \infty$, we get

$$R2^{R\omega(p-1)+1}(\log p) \leq p^{\frac{\epsilon}{2}}.$$

By hypothesis, we have $(p-1)/k \leq p^{\epsilon/3R}$. By putting together both the estimates, we see that

$$2^{R\omega(p-1)+1}\delta^{-R} R \frac{(\log p)\sqrt{p}}{|\mathcal{I}|} \leq p^{\frac{\epsilon}{2}} p^{\frac{\epsilon}{3}} \frac{\sqrt{p}}{|\mathcal{I}|} = \frac{p^{\frac{1}{2}+\frac{5\epsilon}{6}}}{|\mathcal{I}|} < 1,$$

as $|\mathcal{I}| \geq p^{\frac{1}{2}+\epsilon}$. Hence, we conclude that $N(\mathcal{A}) \neq 0$ which means that there exists an $n \in \mathcal{I}$ such that $n + a$ is a QNRNP for any $a \in \mathcal{A}$. $\square$

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:

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

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

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

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

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

$$\begin{aligned}
P_t(X_t = \ell) &= \frac{1}{|\mathcal{I}|} \sum_{\substack{\mathcal{C} \subset \{1,2,\ldots,[t]\} \\ |\mathcal{C}|=\ell}} |\mathcal{I}| \left(\frac{k}{p-1}\right)^{|\mathcal{C}|} \left(1 - \frac{k}{p-1}\right)^{|\mathcal{C}'|} \left(1 + O\left(\frac{1}{p^{\epsilon/4}}\right)\right) \\
&= \sum_{\substack{\mathcal{C} \subset \{1,2,\ldots,[t]\} \\ |\mathcal{C}|=\ell}} \left(\frac{k}{p-1}\right)^{\ell} \left(1 - \frac{k}{p-1}\right)^{[t]-\ell} \left(1 + O\left(\frac{1}{p^{\epsilon/4}}\right)\right) \\
&= \left(\frac{k}{p-1}\right)^{\ell} \left(1 - \frac{k}{p-1}\right)^{[t]-\ell} \left(\sum_{\substack{\mathcal{C} \subset \{1,2,\ldots,[t]\} \\ |\mathcal{C}|=\ell}} 1 \right) \left(1 + O\left(\frac{1}{p^{\epsilon/4}}\right)\right) \\
&= \left(\frac{k}{p-1}\right)^{\ell} \left(1 - \frac{k}{p-1}\right)^{[t]-\ell} \binom{[t]}{\ell} \left(1 + O\left(\frac{1}{p^{\epsilon/4}}\right)\right) \\
&= \frac{[t]([t]-1)\cdots([t]-\ell+1)}{\ell!} \left(\frac{k}{p-1}\right)^{\ell} \frac{\left(1 - \frac{k}{p-1}\right)^{[t]}}{\left(1 - \frac{k}{p-1}\right)^{\ell}} \left(1 + O\left(\frac{1}{p^{\epsilon/4}}\right)\right).
\end{aligned}$$

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

$$\begin{aligned}
[t]([t]-1)\cdots([t]-\ell+1) &= (t - \{t\})(t - \{t\} - 1)\cdots(t - \ell + 1 - \{t\}) \\
&= t(t-1)\ldots(t-\ell+1) \prod_{i=0}^{\ell-1} \left(1 - \frac{\{t\}}{t-i}\right) \\
&= t(t-1)\ldots(t-\ell+1) \left(1 + O\left(\frac{1}{t}\right)\right)^{\ell}.
\end{aligned}$$

Since $\ell \leq t$, we see that

435589_1_En_20_Chapter ✓ TYPESET ☐ DISK ☐ LE ✓ CP Disp.:24/7/2018 Pages: 16 Layout: T1-Standard

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

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

$$\begin{aligned}
P_t(X_t=\ell) &= \frac{t(t-1)\cdots(t-\ell+1)(1+O(\ell/t))}{\ell!}\left(\frac{k}{p-1}\right)^{\ell}\frac{\left(1-\frac{k}{p-1}\right)^{t}}{\left(1-\frac{k}{p-1}\right)^{\{t\}+\ell}}\left(1+O\left(\frac{1}{p^{\epsilon/4}}\right)\right)\\
&= \left(t\frac{k}{p-1}\right)^{\ell}\frac{1}{\ell!}\left(1-\frac{k}{p-1}\right)^{t}\left(1+O\left(\frac{\ell}{t}\right)\right)\left(1-\frac{k}{p-1}\right)^{-\{t\}-\ell}\left(1+O\left(\frac{1}{p^{\epsilon/4}}\right)\right)\\
&= \left(t\frac{k}{p-1}\right)^{\ell}\frac{1}{\ell!}e^{-\frac{tk}{p-1}}\left(1+O\left(\frac{\ell}{t}\right)\right)\left(1-\frac{k}{p-1}\right)^{-\{t\}-\ell}\left(1+O\left(\frac{1}{p^{\epsilon/4}}\right)\right).
\end{aligned}$$

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 λ; 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

1. C. Cobeli and A. Zaharescu, On the distribution of primitive roots mod p, *Acta Arith.* **83** (2) (1998), 143–153.
2. C. Cobeli, M. Vâjâitu, and A. Zaharescu, Distribution of gaps between the inverses mod q, *Proc. Edinb. Math. Soc.* (2) **46** (1) (2003), 185–203.
3. H. Davenport, On the distribution of quadratic residues (mod p). *J. London Math. Soc.* **6** (1931), 49–54, ibid. **8** (1933), 46–52.
4. P. Erdős and M. Kac, The Gaussian law of errors in the theory of additive number theoretic functions, *Amer. J. Math.* **62** (1940), 738–742.
5. P. X. Gallagher, On the distribution of primes in short intervals, *Mathematika* **23** (1976), 4–9.
6. M. Z. Garaev, F. Luca and I. E. Shparlinski, Character sums and congruences with $n!$, *Trans. Amer. Math. Soc.* **356** (2004), 5089–5102.
7. A. Granville and P. Kurlberg, Poisson statistics via the chinese remainder theorem, *Adv. Math.* **218** (2008), no. 6, 2013–2042.
8. S. Gun, B. Ramakrishnan, B. Sahu and R. Thangadurai, Distribution of quadratic non-residues which are not primitive roots, *Math. Bohem.* **130** (4) (2005), 387–396.
9. S. Gun, F. Luca, P. Rath, B. Sahu and R. Thangadurai, Distribution of residues modulo p, *Acta Arithmetica* **129** (4) (2007), 325–333.
10. C. Hooley, On the difference of consecutive numbers prime to n - I, *Acta Arith.* **8** (1962/63), 343–34.

11. C. Hooley, On the difference between consecutive numbers prime to n - II, *Publ. Math. Debrecen* **12** (1965), 39–49.
12. C. Hooley, On the difference between consecutive numbers prime to n - III, *Math. Z.* **90** (1965), 355–364.
13. R. Khan, On the distribution of $\omega(n)$, *Anatomy of integers, 199–207, CRM Proc. Lecture Notes* **46**, *Amer. Math. Soc., Providence, RI*, 2008.
14. R. Khan, Spacing between integers having typically many prime factors, *Canad. Math. Bull.* **53** (1) (2010), 102–117.
15. P. Kurlberg, The distribution of spacings between quadratic residues - II, *Israel J. Math.* **120** (2000) part A, 205–224.
16. P. Kurlberg, Poisson spacing statistics for value sets of polynomials, *Int. J. Number Theory* **5** (3) (2009), 489–513.
17. P. Kurlberg and Z. Rudnick, The distribution of spacings between quadratic residues, *Duke Math. J.* **100** (1999), no. 2, 211–242.
18. F. Luca and R. Thangadurai, Distribution of residues modulo p - II, *Number Theory, 51–62, Ramanujan Math. Soc. Lect. Notes Ser.* **15**, *Ramanujan Math. Soc., Mysore*, 2011.
19. F. Luca, I. E. Shparlinski and R. Thangadurai, Quadratic non-residues versus primitive roots modulo p, *J. Ramanujan Math. Soc.* **23** (1) (2008), 97–104.
20. G. Robin, Estimation de la fonction de Tchebyshef θ sur le k-iéme nombre premier et grandes valeurs de la fonction $\omega(n)$ nombre de diviseurs premiers de n, *Acta Arith.* **42** (1983), 367–389.
21. Z. Rudnick, P. Sarnak and A. Zaharescu, The distribution of spacing between the fractional parts of $n^2\alpha$, *Invent. Math.* **145** (1) (2001), 37–57.

Author Queries

Chapter 20

Query Refs.	Details Required	Author's response
AQ1	References [2, 15] are given in list but not cited in text. Please cite in text or delete from list.	

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.

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