Abstract. In this paper, if prime \( p \equiv 3 \pmod{4} \) is sufficiently large then we prove an upper bound on the number of occurrences of any arbitrary pattern of quadratic residues and nonresidues of length \( k \) as \( k \) tends to \( \lceil \log_2 p \rceil \). As an immediate consequence, it proves that, there exist a constant \( c \) such that, the least nonresidue for such primes is at most \( c \lceil \log_2 p \rceil \).

1. Introduction

An integer \( r \) is called a quadratic residue modulo prime \( p \), if there exists an integer \( x \) such that
\[
x^2 \equiv r \pmod{p}.
\]
Otherwise, \( r \) is called a nonresidue modulo \( p \).

There are two interesting problems which dominate the theory of distribution of quadratic residues and nonresidues.

(1) If \( R \) (resp. \( N \)) is the maximum length of consecutive quadratic residues (resp. nonresidues) modulo \( p \), then what is \( R \) (resp. \( N \))? 

(2) For each prime \( p \), let \( n(p) \) denote the least natural number that is not a quadratic residue modulo \( p \). Then what is \( n(p) \)?

Much of the effort has been devoted to answer the second problem. Gauss proved the first nontrivial bound on this problem: he proved that if \( p \equiv 1 \pmod{8} \), then the least nonresidue is less than \( 2\sqrt{p} + 1 \).

Vinogradov [20] established the asymptotic bound
\[
n(p) \ll p^{\frac{1}{2}+\epsilon} \log^2 p
\]
for all primes and made the following conjecture.

Conjecture 1.1. For any fixed \( \epsilon > 0 \), we have \( n(p) \ll p^\epsilon \).

In 1942, Linnik [11] proved that, this conjecture follows from the Generalised Riemann Hypothesis (GRH). In 1952, Ankeny [1] improved the bound further to \( n(p) \ll \log^2 p \). However the conjecture remains open unconditionally.

In 1957, Burgess [3] proved that \( n(p) \ll p^{\frac{1}{2}+\epsilon} \) without assuming GRH. Till today this remains to be the best known bound.

On the other hand, in 1990, Graham and Ringrose [5] proved that, for infinitely many primes \( n(p) \geq c \log p \).

Recently, Tao [17], connected one of the standard conjectures in sieve theory called the Elliot-Halberstam conjecture by proving Elliot-Halberstam conjecture implies Vinogradov’s conjecture. For more details on Conjecture 1.1, refer to Tao [16].

In 1992, by exploring some combinatorial implications of Weil’s bound on character sums, Peralta [12] proved the following.

2010 Mathematics Subject Classification. 11A07, 11B75.
Theorem 1.2. The number of occurrences of arbitrary patterns of quadratic residues and nonresidues of length $k$ in $\mathbb{Z}_p$ is in the range $\frac{p^2}{8} \pm k(3 + \sqrt{p})$

In this paper, by using purely combinatorial arguments, we discuss about the number of occurrences of patterns of length $k$ for primes $p \equiv 3 \pmod{4}$. As an immediate consequence, we prove that, there exists a constant $c$ such that $n(p) \leq c\lceil \log_2 p \rceil$. This proves beyond Vinogradov’s conjecture.

In the next section, we discuss about the number of occurrences of all possible patterns of quadratic residues and nonresidues of length 2 and 3 for primes $p \equiv 3 \pmod{4}$.

2. Preliminaries

For a prime $p$, $\mathbb{Z}_p$ denote the group of integers modulo prime $p$.

Let $a, a+d, a+2d, \ldots, a+(k-1)d$ be a $k$–arithmetic progression with the common difference $d$, where $a+id \in \mathbb{Z}_p \setminus \{0\}$ for all $0 \leq i \leq k-1$. We say that, the above arithmetic progression is a $k$–arithmetic progression of quadratic residues if for every $i$, $a+id$ is a quadratic residue. Similarly, if $a+id$ is a nonresidue for every $i$ then we say that it is $k$–arithmetic progression of nonresidues. We also define, the following.

Let $a, a+1, a+2, \ldots, a+(k-1)$ be $k$–consecutive nonzero elements of $\mathbb{Z}_p$. Then we define

$$\text{Pattern of length } k = \begin{cases} a+i & \text{is quadratic residue for all } i \\ a+i & \text{is nonresidue for all } i \\ a+i & \text{is quadratic residue for some } i \text{ and nonresidue for other } i \end{cases}$$

Also, we define, two arithmetic progressions $a, a+d, a+2d, \ldots, a+(k-1)d$ and $b, b+d, b+2d, \ldots, b+(k-1)d$ to be the same if $a+id$ and $b+id$ are simultaneously quadratic residues or nonresidues for $0 \leq i \leq k-1$.

In this section, for a given prime $p \equiv 3 \pmod{4}$, we find the exact number of occurrences of all possible patterns of length 2 and 3 in $\mathbb{Z}_p$.

Let $r$ and $n$ be the quadratic residue and the nonresidue respectively. Following are the set of all possible patterns of length 2 and 3.

\[
\begin{array}{cccccccc}
rt & nr & nn & rnr & rrr & rrr & rnr & nnn
\end{array}
\]

Definition 2.1. [18] A $k$–element subset $D$ of a finite group $(G, \ast)$ of order $v$ is called a $(v, k, \lambda)$ difference set in $G$ provided that the multiset $\{d_1 \ast d_2^{-1} : d_1, d_2 \in D, d_1 \neq d_2\}$ contains each nonidentity element of $G$ exactly $\lambda$ times.

A difference set $D$ in an additive group $G$ is called a skew Hadamard difference set if and only if $G$ is the disjoint union of $D, -D, \{0\}$.

Note 2.2. If $p \equiv 3 \pmod{4}$, then the set of all quadratic residues of $\mathbb{Z}_p$ forms a skew Hadamard difference set (SHDS) with $\lambda = \frac{p-3}{4}$. Therefore, there are exactly $\frac{p-3}{4}$ number of 2–arithmetic progressions of quadratic residues with common difference $d$ for every $d \in \mathbb{Z}_p \setminus \{0\}$.

From the above note, we can see that, the number of 2-arithmetic progressions of quadratic residues is exactly $\frac{p-3}{4}$.

In 2016 [15], we have proved the following.

Theorem 2.3. [15] For $p \equiv 3 \pmod{4}$ the number of 3–arithmetic progressions of quadratic residues with common difference $d$ is exactly $\lfloor \frac{p-3}{8} \rfloor$ for every $d \in \mathbb{Z}_p \setminus \{0\}$.
Note 2.4. We know that, for any given prime \( p \equiv 3(\text{mod } 4) \), if \( x \) is a quadratic residue then \(-x\) is nonresidue.

Therefore, the number of 2—arithmetic progressions, 3—arithmetic progressions of nonresidues with common difference \( d \) for every \( d \in \mathbb{Z}_p\setminus\{0\} \) are \( \frac{p-3}{4} \), \( \left\lfloor \frac{p-3}{8} \right\rfloor \) respectively.

From above Theorem 2.3, Note 2.2 and Note 2.4, we have the following.

**Corollary 2.5.** For \( p \equiv 3 \pmod{4} \) the number of occurences of any pattern of length 3 is either \( \left\lfloor \frac{p-3}{8} \right\rfloor \) or \( \left\lceil \frac{p-3}{8} \right\rceil \).

**Proof.** Since the number of occurences of patterns of the type \( rrr \) is \( \left\lfloor \frac{p-3}{8} \right\rfloor \), from Note 2.2, we can see that, the number of occurences of patterns of the type \( rnr \) and \( rrn \) are \( \left\lceil \frac{p-3}{8} \right\rceil \). From Note 2.4, the number of occurences of patterns of type \( nnn, nrr \) are \( \left\lfloor \frac{p-3}{8} \right\rfloor \) and the number of occurences of patterns of type \( nnr, nrn \) are \( \left\lceil \frac{p-3}{8} \right\rceil \). \( \square \)

Similarly, one can prove the following.

**Corollary 2.6.** For \( p \equiv 3 \pmod{4} \) the number of occurences of any pattern of length 2 is either \( \frac{p-3}{4} \) or \( \frac{p-3}{4}+1 \).

In the next section, we discuss about the number of occurences of arbitrary patterns of length \( k > 3 \).

3. **Main results**

In this section, we prove that, if \( p \) is large enough then there exists a constant \( c \) such that the number of occurences of any pattern of length \( k \) is at most \( c \) as \( k \) tends to \( \lceil \log_2 p \rceil \).

We know that there are \( 2^k \) number of patterns of length \( k \). Let us classify all the possible patterns of length \( k \) into four types and each of size \( 2^{k-2} \) as follows.

1. Patterns starts with quadratic residue and ends with quadratic residue.
2. Patterns starts with quadratic residue and ends with nonresidue.
3. Patterns starts with nonresidue and ends with quadratic residue.
4. Patterns starts with nonresidue and ends with nonresidue.

From Note 2.4, the number of occurences of all patterns of type 3 and 4 is immediate if we know the number of occurences of all patterns of type 1 and 2.

Now, we discuss about the number of occurences of patterns of type 1 and same argument is valid for type 2 as well.

Let \( \left\lfloor \frac{p}{2^k} \right\rfloor = \left\lceil \frac{p}{2^k} \right\rceil \). Consider all possible patterns of type 1 with length \( k \). Since we do not know the exact number of occurences of patterns of length \( k \geq 4 \), let us assume that, the number of occurences of a pattern be \( \left( \frac{p}{2^k} \right) + e(i, k) \), where, \( 1 \leq i \leq 2^{k-2} \) and \( e(i, k) \in \mathbb{Z} \) for every \( i \) and \( k \).

Without loss of generality, let

\[
(3.1) \quad \underbrace{(\frac{p}{2^k}) + (\frac{p}{2^k}) + ... + (\frac{p}{2^k})}_{2^{k-2} \text{ terms}} = \frac{p-3}{4}.
\]

From (3.1) and Note 2.2, we can see that,

\[
(3.2) \quad \sum_{i=1}^{2^{k-2}} e(i, k) = 0.
\]
Now we prove the following.

**Lemma 3.1.** If \( e(i, k) \) is zero for every \( i, k \) then \( \left( \frac{p}{2^k} \right) \) is at most 1 as \( k \) tends to \( \lceil \log_2 p \rceil \).

**Proof.** Let the number of occurrences of a pattern be \( \left( \frac{p}{2^k} \right) + e(i,k) \), where, \( 1 \leq i \leq 2^{k-2} \) and \( e(i, k) \in \mathbb{Z} \) for every \( i \) and \( k \). If \( e(i, k) \) is zero for every \( i, k \), then \( \left( \frac{p}{2^k} \right) \leq 1 \) as \( k \) tends to \( \lceil \log_2 p \rceil \). \( \square \)

**Lemma 3.2.** If \( e(i, k) \) is nonzero then it must be governed by a rule.

**Proof.** Let \( k \) be \( (p_1p_2...p_s)n+1 \), where, \( p_1, p_2, ..., p_s \) are distinct primes such that \( n \) and \( s \) are positive integers. Then for any arbitrary pattern (type 1) of length \( k \), there are arithmetic progressions of lengths \( (p_2p_3...p_s)n+1 \), \((p_1p_3...p_s)n+1 \), ..., \((p_1p_2...p_{s-1})n+1 \) with common differences \( p_1, p_2, ..., p_s \) respectively.

Corresponding to each \( j, \ 1 \leq j \leq s \), let us divide \( 2^{k-2} \) patterns into \( 2(p_1...p_{j-1}p_{j+1}...p_s)n-1 \) groups. In each group there are exactly \( 2^{k-[(p_1...p_{j-1}p_{j+1}...p_s)n+1]} \) patterns such that arithmetic progressions with common difference \( p_j \) are same.

Let \( j \) be fixed. For every \( 1 \leq i \leq 2^{k-2} \), there exists \( 1 \leq m \leq 2(p_1...p_{j-1}p_{j+1}...p_s)n-1 \) and \( 1 \leq n \leq 2^{k-[(p_1...p_{j-1}p_{j+1}...p_s)n+1]} \) such that \( e(i, k) = e(m_n, k)_j \). Therefore,

\[
\sum_{n=1}^{2^{k-[(p_1...p_{j-1}p_{j+1}...p_s)n+1]}} \left[ \left( \frac{p}{2^k} \right) + e(m_n, k)_j \right] = \left( \frac{p}{2(p_1...p_{j-1}p_{j+1}...p_s)n+1} \right) + e(m, [(p_1...p_{j-1}p_{j+1}...p_s)n+1]).
\]

Let

\[
\left[ \left( \frac{p}{2^k} \right) + r_1 \right] + \left[ \left( \frac{p}{2^k} \right) + r_2 \right] + ... + \left[ \left( \frac{p}{2^k} \right) + r_n \right] = \left( \frac{p}{2(p_1...p_{j-1}p_{j+1}...p_s)n+1} \right),
\]

where, \( r_i \) can choose either 0, 1 or -1 and \( r_j \) need not be equal to \( r_j \) for every \( 1 \leq i \leq j \leq 2^{k-[(p_1...p_{j-1}p_{j+1}...p_s)n+1]} \). Hence, for a fixed \( j, m \),

\[
\sum_{n=1}^{2^{k-[(p_1...p_{j-1}p_{j+1}...p_s)n+1]}} [e(m_n, k)_j + r_n] = e(m, [(p_1...p_{j-1}p_{j+1}...p_s)n+1]).
\]

One can also see that, patterns shuffles across different groups for different \( j \). Therefore, if \( s \) is large enough then \( e(i, k) \) can’t be chosen randomly. Hence, if \( e(i, k) \) is nonzero then for every \( i, k \) it must be defined by a rule. \( \square \)

**Remark 3.3.** We know that, \( \left( \frac{p}{2^k} \right) \) is at most 1 as \( k \) tends to \( \lceil \log_2 p \rceil \). Hence for every \( 1 \leq i \leq 2^{k-2}, e(i, k) \) must be greater than \(-1\).

Now, we prove the following.

**Lemma 3.4.** As \( k \) tends to \( \lceil \log_2 p \rceil \) for some \( i \) if \( e(i, k) \) is any arbitrary positive function of \( p \) then there exists \( l \neq i \) such that \( e(l, k) \) is a negative function of \( p \).

**Proof.** As \( k \) tends to \( \lceil \log_2 p \rceil \), suppose that, \( e(i, k) \) be any arbitrary positive function of \( p \), say \( f(p) \). Then from (3.2) and Remark 3.3 there exist \( j_1, j_2, ..., j_{f(p)} \) such that \( e(j_r, k) = -1 \) for every \( 1 \leq r \leq f(p) \).

But according to Lemma 3.2, \( e(i, k) \) can’t be chosen randomly. It must be governed by a rule and there exists no rule which satisfy the above condition. Therefore, there exists \( l \neq i \) such that \( e(l, k) \) must be a negative function of \( p \). \( \square \)

From Lemma 3.1, Lemma 3.2 and Lemma 3.4 we have the following.
Theorem 3.5. If $p$ is sufficiently large then there exists a constant $c$ such that the number of occurrences of patterns of length $k$ as $k$ tends to $\lceil \log_2 p \rceil$ at most $c$.

For $p \equiv 3 \pmod{4}$, from the above theorem, we have the following.

Corollary 3.6. If $p$ is sufficiently large then $n(p) \leq c\lceil \log_2 p \rceil$.

The above corollary proves beyond Vinogradov’s conjecture.

References

[1] N. C. Ankeny, The least quadratic nonresidue, Ann. of Math. (2) 55 (1952), 65–72.
[2] A. Brauer, Über die Verteilung der Poten zenreste, Math. Z. 35 (1932) 39–50.
[3] D. A. Burgess, The distribution of quadratic residues and non-residues, Mathematika 4 (1957) 106–112.
[4] H. Davenport, P. Erdős, The distribution of quadratic and higher residues, Publ. Math. Debrecen 2 (1952) 252–265.
[5] S. W. Graham and C. J. Ringrose, Lower bounds for least quadratic non-residues, 269-309 in Analytic number theory (Allerton Park, IL, 1989), edited by B. C. Berndt et al., Progr. Math. 85 Birkhauser, Boston, 1990. MR 92d:11108Zbl 0719.11006
[6] A. Granville, Smooth numbers: computational number theory and beyond, Algorithmic number theory 44 (2008), 267-323.
[7] R. K. Guy, Unsolved Problems in Number Theory, Springer, New York, 1994, pp. 372–373.
[8] R. H. Hudson, On sequences of consecutive quadratic nonresidues, Journal of Number Theory 3 (1971) 178–181.
[9] R. H. Hudson, On a conjecture of Issai Schur, J. Reine Angew. Math. 289 (1977) 215–220.
[10] P. Hummel, On consecutive quadratic non-residues: a conjecture of Issai Schur, Journal of Number Theory 103 (2003) 257–266.
[11] U. V. Linnik, A remark on the least quadratic non-residue, C. R.(Doklady)Acad.Sci. URSS(N.S.) 36 (1942), 119–120.
[12] Rene Peralta, On the distribution of quadratic residues and nonresidues modulo prime a number, Mathematics of Computation 58 (178) (1992), 433-440.
[13] O. Perron, Bemerkungen über die Verteilung der quadratischen Reste, Mathematische Zeitschrift 56 (1952) 122–130.
[14] G. Pólya, Über die Verteilung der quadratischen Reste und Nichtreste, Nachr. Akad. Wm. Göttingen. Math. Phys. Kl. (1918) 30-36.
[15] Shivarajkumar, Beyond Schur’s conjecture, Amer. Math. Monthly 123 (2016) 64–67.
[16] Terence Tao, The least quadratic nonresidue and the square root barrier, https://terrytao.wordpress.com/2009/08/18 the-least-quadratic-nonresidue-and-the-square-root-barrier/
[17] Terence Tao, The Elliott–Halberstam conjecture implies the Vinogradov least quadratic nonresidue conjecture, Algebra and Number Theory 9 (2015) 1005–1034.
[18] J H Van Lint and R M Wilson, A course in Combinatorics, Cambridge University Press Second edition.
[19] I. Vinogradov, Über die Verteilung der quadratischen Reste und Nichtreste, J. Sot. Phys. Math. Univ. Permi. 2 (1919) 1–14.
[20] I. Vinogradov, Selected works. With a biography by K. K. Mardzhanishvili. Translated from the Russian by Naidu Psv. Translation edited by Yu. A. Bakhturin. Springer-Verlag Berlin, 1985.
[21] I. Vinogradov, On a general theorem concerning the distribution of the residues and nonresidues of powers, Trans. American Math. Soc. 29 (1927), 209-217.

Department of Mathematics, The National Institute of Engineering, Mysuru, India.
Email address: shivarajmacs@gmail.com