DISTRIBUTION OF RESIDUES MODULO p - II

F. LUCA AND R. THANGADURAI

On the occasion of 60th birthday of Prof. T. C. Vasudevan

Abstract. In this article, we shall study a problem of the following nature. Given a natural number $N \geq 2$, does there exist a positive integer $p_0(N)$ such that for every prime $p \geq p_0(N)$, there is $x \in (\mathbb{Z}/p\mathbb{Z})^*$ with $x, x+1, \cdots, x+N-1$ are all quadratic residues (respectively, quadratic non-residues) modulo p?. In 1928, Brauer [3] proved the existence of $p_0(N)$ for quadratic residues as well as quadratic non-residues mod p. In this article, we shall give an explicit bound for $p_0(N)$ for both the cases. Also, we study a related problem in this direction.

1. Introduction

For any prime number p, the distribution of residues modulo p has been of great interest to Number Theorists for many decades. The set of all non-zero residues modulo p can be divided into two classes, namely, the set of all quadratic residues (or squares) and quadratic non-residues (or non-squares) modulo p. In natural numbers, there are no consecutive squares as the difference of two consecutive squares is at least twice of the least one. In modulo p situation, one can expect a string of consecutive squares. In this article, we deal with the following question, first dealt by Brauer [3].

Question. For any given natural number $N \geq 2$, can we find an integer $p_0(N)$ such that for every prime $p \geq p_0(N)$, there exists an element $x \in (\mathbb{Z}/p\mathbb{Z})^*$ with $x, x+1, x+2, \cdots, x+N-1$ are all quadratic residues (respectively, quadratic non-residues) modulo p? If $p_0(N)$ exists, then can we find the explicit value?

In 1928, Brauer [3] answered the above question and proved the existence of $p_0(N)$ for quadratic residues and non-residues cases.

For a given prime p, the set of all non-residues modulo p can be, further, divided into two classes, namely, the set of all primitive roots (or generators of $(\mathbb{Z}/p\mathbb{Z})^*$) and non-residues which are not primitive roots modulo p.

In 1956, L. Carlitz [5] answered the above question for the set of all primitive roots modulo p and proved the existence of $p_0(N)$ in this case. This was independently proved by Szalay [25] and [26]. Recently, Gun *et al.* in [13], [14] and [19], answered the above question for the complementary case and gave an explicit value of $p_0(N)$ in that case.

It is worth to mention that Vegh [28], [29], [30] and [31] also, studied similar related problems for case of primitive roots modulo p.

Another related problem along this direction was considered by D. H. Lehmer and E. Lehmer [18] as follows.

Definition. Let $N \geq 2$ be an integer and p be a sufficiently large prime number. Define $r(N,p)$ (respectively $n(N,p)$) to be the least positive integer r such that

$$r, r+1, \cdots, r+N-1$$

are all quadratic residues (respectively, quadratic non-residues) mod p.

Define

$$\Gamma(N) = \limsup_{p\to\infty}\ r(N,p); \qquad \gamma(N) = \liminf_{p\to\infty}\ r(N,p)$$

and

$$\Delta(N) = \limsup_{p\to\infty} n(N,p); \qquad \delta(N) = \liminf_{p\to\infty} n(N,p).$$

In [18], they proved that $\Gamma(2) = 9$ and $\Gamma(N) = \infty$ for all $N \geq 3$. In this article, while surveying these results, we prove the upper bounds for $p_0(N)$ for the case of quadratic residues and non-residues modulo p. Also, we discuss the values of $\Delta(N), \gamma(N)$ and $\delta(N)$ for every $N \geq 2$.

2. Quadratic Residues modulo p

We shall start with the following theorem.

Theorem 1. *Let $N \geq 2$ be a given integer and $p(N)$ denote the least prime number which is $> N$. Then there are infinitely many primes p which are $\equiv 1 \pmod 4$ such that*

$$1, 2, \cdots, p(N)-1, -p(N)+1, -p(N)+2, \cdots, -1$$

all are quadratic residues modulo p.

Remark. The idea of the proof this theorem lies in the paper [22] of S. S. Pillai.

Proof. Let $N \geq 2$ be a given integer. First we claim that *if $p = 4m+1$, then any divisor d of m is a quadratic residue modulo p.*

If a and b are quadratic residues mod p, then ab is a quadratic residue modulo p. Therefore, it is enough to prove the claim for any prime divisor of m.

Let q be a prime divisor of m. If $q = 2$, then $p \equiv 1 \pmod 8$. Therefore, by quadratic reciprocity law, we get,

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = 1.$$

Let q be an odd prime. Then, by the quadratic reciprocity law, we have

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = \left(\frac{1}{q}\right) = 1,$$

since $q|m$ and hence $p - 1 \equiv 0 \pmod{q}$. Thus, the claim follows.

Consider the sequence of positive integers

$$S := 4(N!) + 1, 2(4(N!)) + 1, 3(4(N!)) + 1, \cdots, k(4(N!)) + 1, \cdots.$$

Then the Dirichlet Prime Number Theorem predicts that there are infinitely many prime numbers q in this sequence S. For these primes, by the above claim, we see that $1, 2, \cdots, N$ are all quadratic residues.

Also, note that -1 is a quadratic residues modulo these primes q, as $q \equiv 1 \pmod{4}$. Therefore for these primes, $-1, -2, \cdots, -N$ are all quadratic residues modulo q.

Note that for any given N, the integers $N + 1, N + 2, \cdots, p(N) - 1$ are all composed of primes that are less than or equal to N. This is because, by the definition of $p(N)$, there is no prime in between $N + 1$ to $p(N) - 1$. Hence, by the above observation, every divisor of $N + 1, N + 2, \cdots, p(N) - 1$ is a quadratic residue modulo q. Hence, $N + 1, N + 2, \cdots, p(N) - 1$ are all quadratic residues modulo q. Thus, the theorem follows. $\square$

Remark. For any prime q satisfying Theorem 1, any quadratic non-residue modulo q lies between $p(N)$ and $-p(N)$ modulo q.

We give a new proof of the result of Brauer [3] with explicit value $p_0(N)$ as follows.

Theorem 2. *Let $N \geq 2$ be an integer. Then for every prime $p > \exp\left(2^{2^{2^{N^2+10}}}\right)$, we can find $x, x+1, x+2, \cdots, x+N-1$, for some $x \in (\mathbb{Z}/p\mathbb{Z})^*$, which are quadratic residues modulo p.*

The proof of Theorem 2 is an application of the celebrated Theorem of T. Gowers [11] which states as follows.

Theorem A. (T. Gowers, [11]) *Let $M \geq 2$ be any integer and $0 < \delta < 1$. Then whenever $L \geq L(M, \delta) = \exp\left(\delta^{2^{2^{M+9}}}\right)$, any subset $A \subset \{1, 2, \cdots, L\}$ with $|A| \geq \delta L$ contains an arithmetic progression of length M.*

Proof of Theorem 2. Let $N \geq 2$ be a given integer. Let p be any prime such that $p > \exp\left(2^{2^{2^{N^2+10}}}\right)$. Let A be denote the set of all quadratic residues modulo p.

Therefore, $|A| = \frac{p-1}{2}$. Put $L = p-1$, $\delta = \frac{1}{2}$ and $M = N^2+1$ in Theorem A. Clearly, by the hypothesis, L satisfies the conditions of Theorem A and hence there exists an arithmetic progression

$$a, a+d, a+2d, \cdots, a+N^2d$$

of length N^2+1 in A. That means, $a, a+d, a+2d, \cdots, a+N^2d$ are all quadratic residues modulo p.

If d is a quadratic residue modulo p, then so is d^{-1}. Thus, we get

$$ad^{-1}, ad^{-1}+1, \cdots, ad^{-1}+N^2$$

are all quadratic residues modulo p and we are done.

Suppose d is a quadratic non-residue modulo p. If there is $r \leq N$ such that r is a quadratic non-residue modulo p, then rd is a quadratic residue modulo p and so is $(rd)^{-1}$. Hence, we have a sub arithmetic progression

$$a+rd, a+2rd, \cdots, a+Nrd$$

all are quadratic residues modulo p with the difference rd is also a quadratic residue modulo p. Therefore, we get,

$$a(rd)^{-1}+1, a(rd)^{-1}+2, \cdots, a(rd)^{-1}+N$$

are all quadratic residue modulo p and we are done again.

If there is no $r \leq N$ such that r is a quadratic non-residue modulo p, then $1, 2, \cdots, N$ are quadratic residue modulo p and we have done. Thus the theorem follows. □

Theorem 3. (Lehmer and Lehmer, [18]) $\Gamma(2) = 9$ *and* $\Gamma(N) = \infty$ *for all* $N \geq 3$. *Also,* $\gamma(N) = 1$ *for all* $N \geq 2$.

Proof. First we shall prove that $\Gamma(2) \leq 9$. It is enough to prove that $r(2,p) \leq 9$ for every prime $p \geq 11$. If 10 is a quadratic non-residue mod p, then either 2 or 5 are quadratic residue mod p. Hence $(1,2)$ or $(4,5)$ are pairs of quadratic residues mod p. If 10 is a quadratic residue mod p, then $(9,10)$ is a pair of quadratic residue mod p. Also, this happens for all prime $p \geq 11$. Thus $\Gamma(2) \leq 9$. To see the equality, it is enough to prove that $r(2,p) = 9$ for infinitely many primes p. That is to prove that 10 is a quadratic residue modulo p for infinitely many primes p. However, this is, indeed, true. For instance (for the reference, see Chapter 7 in [8]), the primes $p \equiv 1 \pmod{40}$ for which 10 is a quadratic residue mod p and by Dirichlet's Prime Number Theorem, we have infinitely many such primes. Hence $\Gamma(2) = 9$ follows.

To prove $\Gamma(N) = \infty$, for all $N \geq 3$, it is enough to prove that $\Gamma(3) = \infty$, as if $\Gamma(M) = m < \infty$ for some $M > 3$, then it follows that $\Gamma(3) \leq m$. To prove

$\Gamma(3) = \infty$, it suffices to prove that for any given positive integer R, we have $r(3,p) \geq R$ for infinitely many primes p.

Let R be a given positive integer. Let $q_1, q_2, \cdots, q_m$ be all the primes $q \leq R$. By quadratic reciprocity law, we know that primes p for which q_i is a quadratic residue (respectively, quadratic non-residue) modulo p belong to the set (respectively, the different set) of arithmetic progressions of common difference $4q_i$. List those primes p for which q_i is a quadratic residue modulo p and $q_i \equiv 1 \pmod 3$ and those primes p for which q_j is a quadratic non-residue modulo p and $q_i \equiv -1 \pmod 3$. Combine the progressions of the first kind with those of the second kind. By Dirichlet's Prime Number Theorem, there are infinitely many primes p such that

$$\left(\frac{q}{p}\right) \equiv q \pmod 3 \qquad (q \neq 3, q \leq R).$$

Therefore, by the multiplicativity of the Legendre symbols, we conclude that

$$\left(\frac{m}{p}\right) \equiv m \pmod 3 \qquad (m \not\equiv 0 \pmod 3, m \leq R).$$

Among any three consecutive positive integers $\leq R$, there is an integer $m \equiv -1 \pmod 3$ and for which

$$\left(\frac{m}{p}\right) \equiv -1 \pmod 3 \implies \left(\frac{m}{p}\right) = -1.$$

Thus, we get $r(3,p) \geq R$.

To see, $\gamma(N) = 1$ for all $N \geq 2$, we apply Theorem 1. By Theorem 1, we have infinitely many primes for which $1, 2, \cdots, N$ are all quadratic residues modulo these primes. Therefore, $r(N,p) = 1$ for infinitely many primes p. Hence $\gamma(N) = 1$ for all $N \geq 2$. □

3. Quadratic Non-Residues modulo p

The proof of Theorem 2, in general, doesn't work, if we replace the quadratic residues by quadratic non-residues. By Theorem 1, it is clear that for infinitely many primes $p \equiv 1 \pmod 4$, the first quadratic non-residue r is $\geq p(N) > N$ for any given $N \geq 2$. Hence the proof of Theorem 2 doesn't work in this case. However, it does work for some cases as follows.

Theorem 4. *Let $N \geq 2$ be an integer. Then for every prime p which is $\equiv \pm 3 \pmod 8$ and $p > \exp\left(2^{2^{2^{2N+10}}}\right)$, we can find $x \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $x, x+1, x+2, \cdots, x+N-1$ are all quadratic non-residues modulo p.*

Proof. Proceeding as in the proof of Theorem 2 for $p \equiv \pm 3 \pmod 8$ and A equal to the set of all quadratic non-residues mod p, we get an arithmetic progression

$$a, a+d, a+2d, \cdots, a+2Nd$$

each of which is quadratic non-residue modulo p.

If d is a quadratic residue modulo p, then so is d^{-1}. Hence, we get

$$ad^{-1}, ad^{-1}+1, ad^{-1}+2, \cdots, ad^{-1}+N$$

are all quadratic non-residues modulo p.

Suppose d is a quadratic non-residue modulo p. When $p \equiv \pm 3 \pmod 8$, we know that 2 is a quadratic non-residue modulo p. Hence $2d$ is a quadratic non-residue modulo p. Thus, we get,

$$a(2d)^{-1}+1, a(2d)^{-1}+2, \cdots, a(2d)^{-1}+N$$

are all quadratic residues modulo p. Therefore, the result follows. □

To generalize the idea of the proof of Theorem 4, we need the following lemmas. Though the following lemma is well-known, for the sake of completeness, we include the proof here. To prove the proposition, we need the following theorem.

Let $n > 1$ be an integer and m be an integer such that $1 \leq m \leq n$ and $(m, n) = 1$. Let $\pi(x, n, m)$ be denote the number of primes $p \leq x$ and $p \equiv m \pmod n$ and $\phi(n)$ denote the Euler Phi-function which counts the number of integers m with $1 \leq m \leq n$ and $(m, n) = 1$. Then Siegel-Walfisz theorem states as follows.

Siegel-Walfisz Theorem. (see e.g., [23], Satz 4.8.3) *For any $A > 1$, we have*

$$\pi(x, n, m) = \frac{\pi(x)}{\phi(n)} + O\left(\frac{x}{(\log x)^A}\right)$$

holds for all large enough x.

Proposition 5. *Let $n > 1$ be any integer which is not a perfect square of an integer. Then, for all large enough x, we have,*

$$\sum_{p \leq x} \left(\frac{n}{p}\right) = o(\pi(x)),$$

where $\pi(x)$ counts the number of primes upto x.

Proof. Define a map

$$\chi : (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \{\pm 1\}$$

by

$$\chi(m) = \left(\frac{n}{m}\right) \text{ for every } 1 \leq m \leq n, \ (m, n) = 1,$$

where $\left(\frac{n}{m}\right)$ is the Kronecker symbol. Note that when $m = 1$, we define $\chi(1) = 1$. By the multiplicativity of the Kronecker symbol, it is clear that χ is a character modulo n. Hence, by the orthogonality relation, we get

$$\sum_{\substack{1 \le m \le n \\ (m,n)=1}} \chi(m) = 0.$$

For simplicity, we define,

$$\sum_{m \pmod{n}^*} := \sum_{\substack{1 \le m \le n \\ (m,n)=1}} .$$

Now, consider

$$\sum_{p \le x} \left(\frac{n}{p}\right) = \sum_{\ell \pmod{n}^*} \sum_{\substack{p \equiv \ell \pmod{n} \\ p \le x}} \left(\frac{n}{\ell}\right) = \sum_{\ell \pmod{n}^*} \sum_{\substack{p \equiv \ell \pmod{n} \\ p \le x}} \chi(\ell).$$

By interchanging the summation, we get,

$$\sum_{p \le x} \left(\frac{n}{p}\right) = \sum_{\ell \pmod{n}^*} \chi(\ell) \pi(x, n; \ell),$$

where $\pi(x, n, \ell)$ denotes the number of primes $p \equiv \ell \pmod{n}$ and $p \le x$. Walfisz's Theorem implies that for any fixed integer $A > 1$, we have

$$\pi(x, n, \ell) = \frac{\pi(x)}{\phi(n)} + O\left(\frac{x}{(\log x)^A}\right)$$

for every large enough x. Therefore, we get,

$$\sum_{p \le x} \left(\frac{n}{p}\right) = \frac{\pi(x)}{\phi(n)} \sum_{\ell \pmod{n}^*} \chi(\ell) + O\left(\frac{\phi(n)x}{(\log x)^A}\right).$$

By the orthogonality relation, we, further, get,

$$\sum_{p \le x} \left(\frac{n}{p}\right) = O\left(\frac{\phi(n)x}{(\log x)^A}\right) = o(\pi(x)).$$

Hence the lemma. □

Corollary 6. *For any integer $s \ge 2$ which is not a perfect square of an integer, then there are infinitely many primes p for which s is a quadratic non-residue modulo p.*

Proof. If there are only finitely many primes, say, $p_1, p_2, \cdots, p_r$ for which s is a quadratic non-residue, then for any $x > p_r$

$$\sum_{\substack{p \le x \\ p \ne p_i}} \left(\frac{s}{p}\right) = \pi(x) - r \ne o(\pi(x))$$

a contradiction to Proposition 5. Hence, there are infinitely many primes p for which s is a quadratic non-residue modulo p. □

Remark. Since 3 is a quadratic non-residue modulo p for every prime $p \equiv \pm 5 \pmod{12}$, we see that *for every prime* $p \equiv \pm 5 \pmod{12}$ *and* $p > \exp\left(2^{2^{2^{3N+10}}}\right)$, *we can find* $x \in (\mathbb{Z}/p\mathbb{Z})^*$ *such that* $x, x+1, \cdots, x+N-1$ *are quadratic non-residue modulo these primes.* More generally, let $f(N)$ denotes an increasing function of N. Then we can find infinitely many primes satisfying $p > \exp\left(2^{2^{2^{sf(N)+10}}}\right)$ where $2 \leq s \leq f(N)$ is not a perfect square of an integer and s is a quadratic non-residue for these primes (by Corollary 6). Then these primes satisfy the conclusion of Theorem 3.

Theorem 7. $\Delta(N) = \infty$ *for all* $N \geq 2$.

Proof. Theorem 1 implies that there is a sequence of primes $p_1, p_2, \cdots, p_r, \cdots$, for which $n(N, p_i) \geq N$ for all i. Therefore $\Delta(N) \geq p(N)$ (the smallest prime $p > N$) for all $N \geq 2$. However, the least quadratic non-residue modulo p (denoted by $g(p)$) satisfies $g(p) \geq (\log p)(\log\log\log p)$ (this result is due to Graham and Ringrose [10]) for infinitely many primes p. Therefore, $n(N,p) \geq (\log p)(\log\log p)$ for infinitely many primes p and consequently, we get, $\Delta(N) = \infty$. □

Regarding $\delta(N)$, first we prove that $\delta(2) = 2$. For that we need to prove 2 and 3 are quadratic non-residues modulo p for infinitely many primes p. In [12], Gupta and Murty proved, using sieve theory, that

$$\#\left\{p \leq x : p-1 = 2q \text{ or } 2q_1q_2, \left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = -1\right\} \geq \frac{cx}{\log^2 x}$$

for some $c > 0$. Therefore, by taking $x \to \infty$, we get there are infinitely many primes p for which $2, 3$ are quadratic non-residues mod p. Thus, $\delta(2) = 2$ follows.

When $N = 3$, we can prove that $\delta(3) = 5$. Clearly, $\delta(3) \geq 5$, because, 1 and 4 are perfect squares. For the upper bound, we need to prove $5, 6, 7$ are quadratic non-residues modulo p for infinitely many primes p. This has been achieved in [4]. Hence, $\delta(3) = 5$.

In general, we can prove $\delta(N) \geq \left(\left[\frac{N-1}{2}\right] + 1\right)^2 + 1$. For, note that for a given integer $N \geq 2$, the least positive integer m_N satisfying $m_N^2 < N < (m_N+1)^2$ is $m_N = [(N-1)/2] + 1$. Therefore, $n(N,p) \geq m_N^2 + 1$ for all but possibly finitely many primes p. Hence $\delta(N) \geq \left(\left[\frac{N-1}{2}\right] + 1\right)^2 + 1$.

In the case of primitive roots modulo p, as we mentioned in the introduction, Carlitz [5] and Szalay [25] and [26] proved the existence of $p_0(N)$. In [14] and

[19], we proved the existence of $p_0(N)$ for the case of non-residues which are not the primitive roots modulo p. Also we proved an upper bound for $p_0(N)$. In fact, in [19], we proved the following result which improves the result in [14].

Theorem B. *Let $\varepsilon \in (0, 1/2)$ be fixed and let $N \geq 2$ be an integer. If*

$$p \geq \max\{N^2(4/\varepsilon)^{2N}, N^{651N \log\log(10N)}\}$$

is a prime satisfying

$$\frac{\phi(p-1)}{p-1} \leq \frac{1}{2} - \varepsilon,$$

then there are N consecutive integers $n, \ldots, n+N-1$ that are quadratic non-residues but not primitive roots modulo p.

It is also possible to give a bound similar to Theorem B for $p_o(N)$ for the primitive root mod p case.

In 1976, Hausman [15] proved the existence of p_o such that for every prime $p \geq p_o$, there exists an integer $g \leq p-1$ and $(g, p-1) = 1$ such that g is a primitive root modulo p. Recently, R. Thangadurai [27] proved that $p_0 \leq e^{110.8} \sim 1.318 \times 10^{48}$.

4. Related problem

Another related question is as follows. For a given non-empty subset $S = \{a_1, a_2, \ldots, a_\ell\}$ of $\mathbb{Z}$, can we find infinitely many primes p such that every element of S is a quadratic residue (respectively, non-residue) modulo p? If yes, what is the density of such primes for a given subset S?

In 1968, M. Fried [9] answered that there are infinitely many primes p for which a is a quadratic residue modulo p for every $a \in S$. Also, he provided a necessary and sufficient condition for a to be a quadratic non-residue modulo p for every $a \in S$. More recently, S. Wright [32] and [33] also studied this qualitative problem.

For a given prime p, the set of all quadratic non-residue modulo p is a disjoint union of the set of all generators g of $(\mathbb{Z}/p\mathbb{Z})^*$ (which are called primitive roots modulo p) and the complement set contains all the non-residues which are not primitive roots modulo p.

A set P of prime numbers is said to have the *relative density* ε with $0 \leq \varepsilon \leq 1$, if

$$\varepsilon = \lim_{x\to\infty} \frac{|P \cap [1, x]|}{\pi(x)}$$

exits. Also, the following numbers count some special subsets of S.

(i) Let α_S denote the number of subsets T of S, including the empty one, such that $|T|$ is even and $\prod_{s\in T} s = m^2$ for some integer m; hence, $\alpha_S \geq 1$ for every S.

(ii) Let β_S denote the number of subsets T of S such that $|T|$ is odd and $\prod_{s\in T} s = m^2$ for some integer m.

Then the following theorems were proved by R. Balasubramanian, F. Luca and R. Thangadurai [2].

Theorem 8. ([2], 2010) *The relative density of the set of prime numbers p for which a is a quadratic residue modulo p for every $a \in S$ is*

$$\frac{\alpha_S + \beta_S}{2^\ell}.$$

Theorem 9. ([2], 2010) *We have, $\beta_S = 0$ if and only if the density of the set of primes p for which a is a quadratic non-residue modulo p for every $a \in S$ is*

$$\frac{\alpha_S}{2^\ell}.$$

We shall present the proof of Theorem 8 and Theorem 9 follows similarly.

Proof of Theorem 8. Let $\mathcal{P}(S)$ be the set of all distinct prime factors of $a_1a_2\cdots a_\ell$. Clearly, $|\mathcal{P}(S)|$ is finite. Let $x > 1$ be a real number. Consider the following counting function

$$S_x = \frac{1}{2^\ell} \sum_{\substack{p\leq x \\ p\notin\mathcal{P}(S)}} \left(1 + \left(\frac{a_1}{p}\right)\right)\cdots\left(1 + \left(\frac{a_\ell}{p}\right)\right).$$

Since the Legendre symbol is completely multiplicative, $\left(\frac{a_i}{p}\right)\left(\frac{a_j}{p}\right) = \left(\frac{a_ia_j}{p}\right)$, we see that

$$S_x = \frac{1}{2^\ell} \sum_{\substack{p\leq x \\ p\notin\mathcal{P}(S)}} \sum_{\substack{0\leq b_i\leq 1 \\ n=a_1^{b_1}\cdots a_\ell^{b_\ell}}} \left(\frac{n}{p}\right) = \sum_{\substack{0\leq b_i\leq 1 \\ n=a_1^{b_1}\cdots a_\ell^{b_\ell}}} \frac{1}{2^\ell} \sum_{\substack{p\leq x \\ p\notin\mathcal{P}(S)}} \left(\frac{n}{p}\right).$$

Note that if n is a perfect square, then $\left(\frac{n}{p}\right) = 1$ for each $p \notin \mathcal{P}(S)$. Thus, for these $\alpha_S + \beta_S$ values of n, the inner sum is

$$\frac{1}{2^\ell} \sum_{\substack{p\leq x \\ p\notin\mathcal{P}(S)}} \left(\frac{n}{p}\right) = \frac{1}{2^\ell}(\pi(x) - |\mathcal{P}(S)|).$$

For the remaining values of n (i.e., when n is not a perfect square), we apply Proposition 5 to get

$$\frac{1}{2^\ell} \sum_{\substack{p \le x \\ p \notin \mathcal{P}(S)}} \left(\frac{n}{p}\right) = o(\pi(x)) \qquad \text{as} \quad x \to \infty.$$

Therefore,

$$S_x = \frac{1}{2^\ell}(\alpha_S + \beta_S)(\pi(x) - |\mathcal{P}(S)|) + o(\pi(x))$$

and hence

$$\frac{S_x}{\pi(x)} = \frac{\alpha_S + \beta_S}{2^\ell}\left(1 - \frac{|\mathcal{P}(S)|}{\pi(x)}\right) + o(1).$$

Since $|\mathcal{P}(S)|$ is a finite number and it is elementary to see that as $x \to \infty$, $\pi(x) \to \infty$, we get

$$\lim_{x \to \infty} \frac{S_x}{\pi(x)} = \frac{\alpha_S + \beta_S}{2^\ell}.$$

This completes the proof of Theorem 8. □

This can be applied to the quadratic non-residue case as well. Take

$$S_x = \frac{1}{2^\ell} \sum_{\substack{p \le x \\ p \notin \mathcal{P}(S)}} \left(1 - \left(\frac{a_1}{p}\right)\right) \cdots \left(1 - \left(\frac{a_\ell}{p}\right)\right)$$

and proceed as in the proof of Theorem 8. This yields Theorem 9.

For a given prime p, the set of all quadratic non-residue modulo p is a disjoint union of the set of all generators g of $(\mathbb{Z}/p\mathbb{Z})^*$ (which are called primitive roots modulo p) and the complement set contains all the non-residues which are not primitive roots modulo p.

In 1927, E. Artin [1] conjectured the following;

Artin's primitive root conjecture. Let $g \neq \pm 1$ be a square-free integer. Then there are infinitely many primes p such that g is a primitive root modulo p.

Note that it is not even known that for a given square-free integer, $g \neq \pm 1$, there exists a prime p such that g is a primitive root modulo p. The above Artin's conjecture asks for the existence infinitely many such primes. In 1967, Hooley [17] proved this conjecture assuming the (as yet) unresolved genearlized Riemann hypothesis for Dedekind zeta functions of certain number fields. In 1983, R. Gupta and M. R. Murty [12] made the first breakthrough by showing the following: given three prime numbers a, b, c, then at least one of the thirteen numbers

$$\left\{ac^2, a^3b^2, a^2b, b^3c, b^2c, a^2c^3, ab^3, a^3bc^2, bc^3, a^2b^3c, a^3c, ab^2c^3, abc\right\}$$

is a primitive root modulo p for infinitely many primes p. Then later Heath-Brown [16] proved that $\{a, b, c\}$ one is primitive root modulo p for infinitely many primes p. Similarly, using the method of Hooley, in 1976, K. R. Matthews [20] found a necessary and sufficient condition for a to be primitive root modulo p for every $a \in S$, under unproved hypothesis.

Analogue question for a non-residue which is not a primitive root modulo a prime is relatively easier to handle. For example, in [21] it is proved that for a given g which is not a perfect square of an integer, there are infinitely many primes p for which g is a quadratic non-residue but not a primitive root modulo p, using the arithmetic of certain number fields. Of course computing the density of such primes is not done yet.

References

[1] E. Artin, Collected Papers, Addison-Wesley, 1965.

[2] R. Balasubramanian, F. Luca and R. Thangadurai, On the exact degree of $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \cdots, \sqrt{a_\ell})$ over $\mathbb{Q}$, To appear in: *Proc. Amer. Math. Soc.*, (2010).

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

[4] R. Balasubramanian, F. Luca and R. Thangadurai, *Finite set and quadratic non-residues modulo p*, Preprint, 2009.

[5] L. Carlitz, Sets of primitive roots, *Compositio Math.*, **13** (1956), 65-70.

[6] H. Davenport, On the distribution of quadratic residues (mod p), *J. London Math. Soc.*, **6** (1931), 49-54.

[7] H. Davenport, On the distribution of quadratic residues (mod p), *J. London Math. Soc.*, **8** (1933), 46-52.

[8] J. Esmonde and M. Ram Murty, Problems in Algebraic Number Theory, Graduate Texts in Mathematics, 190. Springer-Verlag, New York, 1999.

[9] M. Fried, Arithmetical properties of value sets of polynomials, *Acta Arith.*, **15** (1968/69), 91-115.

[10] S. W. Graham and C. J. Ringrose, Lower bounds for least quadratic non residues. Analytic number theory (Allerton Park, IL, 1989), 269–309, Progr. Math., 85, Birkhäuser Boston, Boston, MA, 1990.

[11] W. T. Gowers, A new proof of Szemerédi's theorem. *Geom. Funct. Anal*, **11** (2001), no. 3, 465–588.

[12] R. Gupta and M. Ram Murty, A remark on Artin's conjecture, *Invent. Math.*, **78** (1984), 127-130.

[13] S. Gun, B. Ramakrishnan, B. Sahu and R. Thangadurai, Distribution of Quadratic non-residues which are not primitive roots, *Math. Bohem.*, **130** (2005), no. 4, 387-396.

[14] S. Gun, F. Luca, P. Rath, B. Sahu and R. Thangadurai, Distribution of residues modulo p, *Acta Arith.*, **129.4** (2007), 325-333.

[15] M. Hausman, Primitive roots satisfying a coprime condition, *Amer. Math. Monthly,* **83** (1976) 720-723.

[16] D. R. Heath-Brown, Artin's conjecture for primitive roots, *Quart. J. Math. Oxford*, (2) **37** (1986), 27-38.

[17] C. Hooley, On Artin's conjecture, *J. Reine. Angew. Math.*, **225** (1967), 209-220.

[18] D. H. Lehmer and E. Lehmer, On runs of residues, *Proc. Amer. Math. Soc.* **13**, No. 1 (1962), 102-106
[19] F. Luca, I. E. Shparlinski and R. Thangadurai, Quadratic non-residue verses primitive roots modulo p, *J. Ramanujan Math. Soc.*, **23** (2008), no. 1, 97–104.
[20] K. R. Matthews, A generalisation of Artin's conjecture for primitive roots, *Acta Arith.*, **XXIX** (1976), 113-146.
[21] P. Moree and R. Thangadurai, *Preprint.*
[22] S. S. Pillai, On the divisors of $a^n + 1$, *J. Indian Math. Soc.* (N. S), **6** (1942), 120-121.
[23] K. Prachar, Primzahlverteilung, Springer, New York, 1957.
[24] S. Sen Gupta, Artin's conjecture; Unconditional approach and elliptic analogue, Master's thesis, Waterloo, Ontario, Canada, 2008.
[25] M. Szalay, On the distribution of the primitive roots mod p (in Hungarian), *Mat. Lapok*, **21** (1970), 357-362.
[26] M. Szalay, On the distribution of the primitive roots of a prime, *J. Number Theory*, **7** (1975), 183-188.
[27] R. Thangadurai, A remark on a paper "Primitive roots satisfying a coprime condition", *Preprint*, (2010).
[28] E. Vegh, Primitive roots modulo a prime as consecutive terms of an arithmetic progression, *J. Reine Angew. Math.*, **235** (1969), 185-188.
[29] E. Vegh, Primitive roots modulo a prime as consecutive terms of an arithmetic progression - II, *J. Reine Angew. Math.*, **244** (1970), 108-111.
[30] E. Vegh, A note on the distribution of the primitive roots of a prime, *J. Number Theory*, **3** (1971), 13-18.
[31] E. Vegh, Primitive roots modulo a prime as consecutive terms of an arithmetic progression - III, *J. Reine Angew. Math.*, **256** (1972), 130-137.
[32] S. Wright, Patterns of quadratic residues and nonresidues for infinitely many primes, J. Number Theory, 123 (2007) 120-132.
[33] S. Wright, A combinatorial problem related to quadratic non-residue modulo p, *To appear* Ars Combinatorica.

Florian Luca, Mathematical Institute, UNAM, Ap. Postal, 61-3 (Xangari), CP 58089, Morelia, Michoacán, Mexico
E-mail address: fluca@matmor.unam.mx

Department of Mathematics, Harish-Chandra Research Institute, Chhatnag Road, Jhunsi, Allahabad 211019 INDIA
E-mail address: thanga@hri.res.in