ON A GENERALISATION OF ARTIN'S CONJECTURE.

J. SIVARAMAN

ABSTRACT. In 2004, Golomb conjectured that the set

$$\{p : [\mathbb{F}_p^* : \langle a \rangle \bmod p] = r\}$$

has a positive density for any squarefree integer a and positive r. This was however shown by Moree to be inconsistent with earlier work of Lenstra and Murata. In 2009, Moree refined Golomb's conjecure by eliminating all the cases where the above set is finite and generalising the conjecture to rational a. In 2008 however, Franc and Ram Murty had already shown that in certain cases Golomb's conjecture hold true under the Generalised Riemann Hypothesis for certain Dedekind zeta functions. In this paper we prove unconditionally that for a positive integer r with $(r, 6) = 1$, there exist infinitely many integers a_r, as suggested by Moree's refined conjecture, for which the set

$$\{p : [\mathbb{F}_p^* : \langle a_r \rangle \bmod p] = r\}$$

is infinite.

1. INTRODUCTION AND STATEMENT OF THE THEOREM

Artin's famous conjecture on primitive roots [1] states that any number which is not -1 or a square is a primitive root for a positive density of primes. A conjecture also exists for the exact value of this density. Artin's conjecture has eluded mathematicians for nearly a century now but this has paved way towards the study of a much larger class of "Artin-type" problems. The most well known paper in this direction was due to Lenstra [11] in 1977, where he reformulated Artin's conjecture into a new framework which included problems arising from global fields, most notably the famous problem on finding Euclidean domains among rings of integers of number fields. We begin by stating Lenstra's conjecture in the number field context.

Conjecture 1. (Lenstra [11]) *Given a Galois extension of number fields $\mathbf{M}/\mathbf{K}$, a subset $C \subset \mathrm{Gal}(\mathbf{M}/\mathbf{K})$ which is a union of conjugacy classes, a finitely generated subgroup $W \subset \mathbf{K}^*$ of rank at least 1 modulo its torsion subgroup and an integer $r > 0$, the set of prime ideals $\mathfrak{p}$ of $\mathcal{O}_{\mathbf{K}}$ which satisfy*

- $(\mathfrak{p}, \mathbf{M}/\mathbf{K}) \subset C$,
- $v_{\mathfrak{p}}(w) = 0$ *for all* $w \in W$,
- *if* $\psi : W \to (\mathcal{O}_{\mathbf{K}}/\mathfrak{p})^*$ *is the natural projection map, then* $[(\mathcal{O}_{\mathbf{K}}/\mathfrak{p})^* : \psi(W)] \mid r$,

has a natural density.

Key words and phrases. Primitive roots, Artin's conjecture.

Here $(\mathfrak{p}, \mathbf{M}/\mathbf{K})$ is used to denote the Artin symbol of $\mathfrak{p}$ in $\mathrm{Gal}(\mathbf{M}/\mathbf{K})$. If one were to only consider the second and third conditions above in the case where $\mathbf{M} = \mathbf{K} = \mathbb{Q}$, then using the lower bound linear sieve and the Bombieri-Vinogradov theorem one can show that

$$|\{p \leqslant x \;:\; \ell \mid [\mathbb{F}_p^* : \psi(W)] \implies \ell \mid 2r \text{ or } \ell > x^\eta\}| \gg \frac{x}{\log^2 x}$$

where we have used ℓ to denote a prime and η is a constant determined by the level of distribution in the Bombieri-Vinogradov theorem. These results were known as early as 1974 as seen in the work of Bombieri on the Selberg sieve [2]. This is also the point where the 1984 paper of Gupta and Ram Murty [5] on Artin's conjecture germinates. The proof proceeds by showing that for $r = 1$ the primes p for which $[\mathbb{F}_p^* : \psi(W)]$ has large prime divisors are negligible for large $|W|$ (in terms of rank). Lenstra's conjecture now demands the addition of a non-abelian splitting condition to this problem. However, this non-abelian splitting condition discreetly presents itself even in seemingly naive generalisations of Artin's conjecture. This generalisation was introduced by Murata [14] in 1991.

Murata [14] considered the problem of counting

$$N_{a,r}(x) := |\{p \leqslant x \;:\; [\mathbb{F}_p^* : \psi(\langle a \rangle)] = r\}|$$

for a squarefree integer a and positive integer r. His main motivation towards considering this problem was a application towards counting Weiferich primes. He showed, under the assumption of the Generalised Riemann Hypothesis for certain Dedekind zeta functions (GRH), that for any squarefree a and positive integer r,

$$N_{a,r}(x) = C_{a,r}\,\mathrm{Li}(x) + \mathrm{O}_{a,r}\left(\frac{x \log\log x}{\log^2 x}\right).$$

However his computations showed that this constant $C_{a,r}$ may sometimes be zero. On the other hand in 2004, over personal communications, Golomb suggested the following conjecture to Ram Murty. He suggested that

Conjecture 2. *For every squarefree integer $a > 1$ and every positive integer r, the set*

$$\{p \;:\; [\mathbb{F}_p^* : \psi(\langle a \rangle)] = r\}$$

is infinite. Moreover the density of such primes is asymptotic to a constant depending only on a and r.

In 2008, Franc and Murty prove an asymptotic for $N_{a,r}(x)$ where a is any positive integer (which is not an ℓ-th power for any prime ℓ) under the Generalised Riemann Hypothesis for Dedekind zeta functions (GRH). They compute an expression for the constant and show that if

- r is odd,
- a is not an ℓ-th power for any prime ℓ,
- $a = b^2 c$ with $b \in \mathbb{Z}_{>0}$, c even and squarefree,

this constant is positive. Thereby proving infinitude of the set $N_{a,r}$ in this case, under the assumption of the GRH. Moree [13] in 2009, gave a modified version of Golomb's conjecture with a exact expression for the constant, incorporating into it the work of Lenstra and Murata. He also generalised the conjecture to the case where a is a rational number. In addition, he gave an exhaustive list of the all the cases in which Golomb's conjecture fails. We will state here one of the cases of Moree's refined conjecture, which we tackle in this article.

Conjecture 3. (Moree, [13]) *Let $a \in \mathbb{Q}\backslash\{-1,0,1\}$ and $r \geqslant 1$ be an arbitrary integer. Let d_a be the discriminant of $\mathbb{Q}(\sqrt{a})$. If $[2, d_a] \nmid r$ then $N_{a,r}$ is infinite.*

In this paper we prove unconditionally that the set $N_{a,r}$ is infinite when r is an positive integer, with $(r, 6) = 1$, for infinitely many positive integers a with $d_a \nmid r$. We note that this is consistent with Moree's refined conjecture.

Theorem 4. *Let r be a positive integer with $(r, 6) = 1$. There exist infinitely many explicitly computable finite sets S_r such that $d_a \nmid r$ for all $a \in S_r$ and for at least one $a \in S_r$*

$$|\{p \leqslant x : [\mathbb{F}_p^* : \langle a \rangle \bmod p] = r\}| \gg \frac{x}{\log^2 x}.$$

In Section 2, we state some preliminaries required for the proof of Theorem 4. In Section 3, we state and prove some requisite algebraic and sieve theoretic lemmas and in Section 4 we give the proof of Theorem 4.

2. Preliminaries

In this section we introduce some of the preliminaries required for the proofs of our theorems. We begin with some notations. Consider a Galois extension of $\mathbb{Q}$ given by a number field $\mathbf{K}$ and denote the Galois group by G. Given a prime $p \in \mathbb{Z}_{>0}$ which is unramified in $\mathbf{K}$, we use $(p, \mathbf{K}/\mathbb{Q})$ to denote the Artin symbol of $p\mathbb{Z}$. It is known that the Artin symbol is a conjugacy class in G. Let us denote an arbitrary conjugacy class in G by C. We now define by

$$\pi(x) := |\{p \leqslant x\}| \qquad \text{and} \qquad \pi_C(x) := |\{p \leqslant x : (p, \mathbf{K}/\mathbb{Q}) = C\}|.$$

In addition, given two positive integers a, q with $(a, q) = 1$, we use

$$\pi_C(x, q, a) := |\{p \leqslant x : p \equiv a \bmod q, (p, \mathbf{K}/\mathbb{Q}) = C\}|.$$

By the Chebotarev density theorem we know that

$$\pi_C(x, q, a) \sim \delta(C, q, a)\pi(x)$$

for some positive density $\delta(C, q, a)$. If the cyclotomic field $\mathbb{Q}(\zeta_q)$ and $\mathbf{K}$ are linearly disjoint over $\mathbb{Q}$ then

$$\delta(C, q, a) = \frac{|C|}{|G|} \cdot \frac{1}{\phi(q)}$$

where ϕ denotes the Euler totient function. The Bombieri-Vinogradov variant due to Kumar Murty and Ram Murty is a statement about the average deviation of $\pi_C(x, q, a)$ from $\delta(C, q, a)\pi(x)$. More precisely, it states the following.

Theorem 5 (Kumar Murty and Ram Murty [3])**.** *For any $A > 0$ and $\epsilon > 0$ small, we have*

$$\sideset{}{'}\sum_{q \leqslant x^{\alpha-\epsilon}} \max_{(a,q)=1} \max_{y \leqslant x} |\pi_C(y, q, a) - \delta(C, q, a)\pi(y)| \ll \frac{x}{\log^A x}$$

where the $'$ indicates that the sum is over $\mathbf{K}$ with $\mathbf{K} \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}$. Here, α is a constant that depends on C, G and satisfies

$$\alpha \geqslant \min\left(\frac{2}{|G|}, \frac{1}{2}\right).$$

We will now briefly discuss some notations required for the statement of the linear sieve which we will use to find the lower bounds. Let $\mathcal{A}$ be a set of integers, $\mathcal{P}$ be a set of primes and $z \geqslant 2$ be a real number. We define

$$S(\mathcal{A}; \mathcal{P}, z) := \left|\{n \in \mathcal{A} \ : \ (n, P(z)) = 1\}\right| \text{ where } P(z) = \prod_{\substack{p \leqslant z \\ p \in \mathcal{P}}} p.$$

For q square free we define

$$\mathcal{A}_q := \{a \in \mathcal{A} : a \equiv 0 \bmod q\}$$

and choose a function ω_0 such that $\frac{\omega_0(p)}{p}X$ will give an estimate of $|\mathcal{A}_p|$ for p prime where X denotes the size of the set $\mathcal{A}$. For any prime p we define another function ω as

$$\omega(p) = \begin{cases} \omega_0(p) & \text{if } \ p \in \mathcal{P} \\ 0 & \text{if } \ p \notin \mathcal{P}. \end{cases}$$

We set $\omega(1) = 1$. For any square free number q, $\omega(q) = \Pi_{p|q}\omega(p)$. Further, for any square free number q define

$$R_q := |\mathcal{A}_q| - \frac{\omega(q)}{q}X.$$

The linear sieve will be applicable if the sets $\mathcal{A}$ and $\mathcal{P}$ follow the conditions given below:

(1) there exists a constant $A_1 \geqslant 1$ such that

$$0 \leqslant \frac{\omega(p)}{p} \leqslant 1 - \frac{1}{A_1}$$

for every prime $p \in \mathcal{P}$.

(2) there exist constants $L \geqslant 1$ and $A_2 \geqslant 1$ independent of z and w such that if $2 \leqslant w \leqslant z$, then

$$-L \leqslant \sum_{w \leqslant p < z} \frac{\omega(p)\log p}{p} - \log\frac{z}{w} \leqslant A_2.$$

(3) there exists an β with $0 < \beta < 1$ such that

$$\sum_{\substack{q \leqslant \frac{X^\beta}{(\log X)^{A_3}}, \\ p|q \implies p \in \mathcal{P}}} \mu^2(q) 3^{\nu(q)} |R_q| \leqslant A_4 \frac{X}{\log^2 X}$$

for some constants $A_3 \geqslant 1$, $A_4 \geqslant 1$.

Theorem 6 (Halberstam and Richert [6]). *If $\mathcal{A}$ and $\mathcal{P}$ satisfy the above three conditions and if $z \leqslant X$, then*

$$S(\mathcal{A}; \mathcal{P}, z) \geqslant X \prod_{\substack{p \leqslant z \\ p \in \mathcal{P}}} \left(1 - \frac{\omega(p)}{p}\right) \left\{ f\left(\beta \frac{\log X}{\log z}\right) - \frac{B}{(\log X)^{\frac{1}{14}}} \right\}$$

where B is an absolute constant and for $2 \leqslant u \leqslant 4$, $f(u) := \frac{2e^\gamma \log(u-1)}{u}$. Here γ is Euler-Mascheroni constant.

We now state a useful result from [15] due to Ram Murty (see also Gupta and Ram Murty [5]).

Lemma 7. (Gupta and Ram Murty [5], Ram Murty [15]) *Suppose that $\{p_1, \ldots, p_t\}$ is a set of t distinct rational primes. Let $\Gamma = \{p_1^{a_1} \cdots p_t^{a_t} : a_i \in \mathbb{N}\}$ and $\Gamma_p = \{a \bmod p : a \in \Gamma\}$. Then*

$$|\{p : p \textit{ is prime and } |\Gamma_p| \leqslant y\}| \ll y^{\frac{t+1}{t}}.$$

We conclude this section with a theorem due to Leopoldt on the genus number of a number field. For definition and results on genus number, see [9].

Theorem 8. (Leopoldt [12], Pg 52 [9]) *For an abelian number field $\mathbf{K}$ the genus number $g_{\mathbf{K}}$ is given by*

$$g_{\mathbf{K}} = \frac{\prod_p e(p)}{[\mathbf{K} : \mathbb{Q}]}$$

where the product runs over rational primes p and $e(p)$ is the ramification index of p with respect to the field $\mathbf{K}$.

Remark 9. *Note that any unramified extension of $\mathbf{K}$, which is abelian over $\mathbb{Q}$, must have degree dividing $g_{\mathbf{K}}$.*

3. REQUISITE LEMMAS

From the work of Gupta and Murty [5] as well as Heath-Brown [7], we may assume $r > 1$. For the constant α as stated in Theorem 5 and real constants $\epsilon, \epsilon_1 > 0$ with $\epsilon_1 < \frac{1}{2}$, we let

$$t = \left[\frac{2}{(\alpha - \epsilon)(1 - \epsilon_1)} \right].$$

Given a positive integer r with $(r, 6) = 1$, we choose t distinct odd primes $\{p_1, \ldots p_t\}$ with the following properties:

(1) $p_i(p_i - 1)$ co-prime to r for $1 \leqslant i \leqslant t$ and
(2) $p_1 \equiv 5 \bmod 12$.

Such a choice exists because for every prime $\ell \mid r$ with $\ell > 3$ there exists a residue class $a \bmod \ell$ such that for $p_i \equiv a \bmod \ell$,

$$\ell \nmid p_i(p_i - 1).$$

Let us use $\operatorname{rad}(r)$ to denote the radical of r. By the Chinese remainder theorem, there exists a residue class $b \bmod \operatorname{rad}(r)$ such that primes $p_i \equiv b \bmod \operatorname{rad}(r)$ satisfy

$$(r, p_i(p_i - 1)) = 1.$$

Therefore for each p_i we have infinitely many choices. Further denote by

$$W := \langle p_1, \ldots p_t \rangle$$

the monoid generated by the t primes and W_p the monoid read modulo a prime $p \in \mathbb{Z}$. Let $\mathbf{L}_r$ denote the number field $\mathbb{Q}(\zeta_r, p_1^{1/r}, \ldots, p_t^{1/r})$.

Lemma 10. *With at most finitely many exceptions, if a prime $p \in \mathbb{Z}_{>0}$ splits completely in $\mathbf{L}_r$ then $r \mid [\mathbb{F}_p^* : W_p]$. In particular for every $a \in W$, we have $r \mid [\mathbb{F}_p^* : \langle a \rangle \bmod p]$.*

Proof. If p splits in L_r, it splits in $\mathbb{Q}(\zeta_r, p_i^{1/r})$ for $1 \leqslant i \leqslant t$. This in turn implies that p splits in $\mathbb{Q}(\zeta_r)$ and $\mathbb{Q}(p_i^{1/r})$. By the Dedekind Kummer theorem, with at most finitely many exceptions for p, we have that the polynomial $X^r - p_i$ splits completely into linear factors modulo $p\mathbb{Z}$. Therefore p_i has an r-th root modulo $p\mathbb{Z}$ for all i. Hence a has an r-th root modulo $p\mathbb{Z}$ for all $a \in W$. This implies that

$$a^{\frac{p-1}{r}} \equiv 1 \bmod p\mathbb{Z} \qquad \text{for all } a \in W.$$

This immediately gives us the second part of the claim. For the first part, we observe that since $\mathbb{F}_p^*$ is cyclic, there is a unique group in $\mathbb{F}_p^*$ of order $\frac{p-1}{r}$. This implies that W_p is contained in this unique subgroup. This gives us

$$|W_p| \mid \frac{p-1}{r} \implies r \mid [\mathbb{F}_p^* : W_p].$$

□

We now prove a lemma that will facilitate appropriate use of the linear disjointness condition in Theorem 5. Let $v = 16 \prod_{i=1}^t p_i \cdot \prod_{\ell \mid r} \ell^{k_\ell + 1}$ where k_ℓ is an integer satisfying

$$\ell^{k_\ell} \mid\mid r \text{ for all } \ell \mid r.$$

Further let $\mathbf{F}_r = \mathbf{L}_r \mathbb{Q}(\zeta_v)$. We can now state the following lemma.

Lemma 11. *For all squarefree q with $(q, 2 \operatorname{rad}(r) \prod_{i=1}^t p_i) = 1$, we have $F_r \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}$.*

Proof. Let us compute the radical of d_{L_r}, the discriminant of the field L_r. Consider $\mathbb{Q}(p_1^{1/r})$. We know that the ideal $(d_{\mathbb{Q}(p_1^{1/r})})$ contains the discriminant of all the bases of $\mathbb{Q}(p_1^{1/r})$ over $\mathbb{Q}$, contained in $\mathcal{O}_{\mathbb{Q}(p_1^{1/r})}$. This includes the discriminant of the basis $\{1, p_1^{1/r}, p_1^{2/r}, \ldots p_1^{(r-1)/r}\}$. Therefore we know that

$$d_{\mathbb{Q}(p_1^{1/r})} \mid d(1, p_1^{1/r}, p_1^{2/r}, \ldots p_1^{(r-1)/r}) = \prod_{i<j} (\sigma_i p_1^{1/r} - \sigma_j p_1^{1/r})^2.$$

Here, the σ_i are embeddings of the number field $\mathbb{Q}(p_1^{1/r})$ into $\mathbb{C}$ and the product varies over these embeddings in some fixed order given by the indices i and j. The number of tuples of embeddings (σ_i, σ_j) with $i < j$ is $r(r-1)/2$ and we have

$$\sigma_i p_1^{1/r} = \zeta_r^{a_i} p_1^{1/r}.$$

Without loss of generality let $a_i = i$. Since $r \geqslant 5$, we have $p_1 \mid \prod_{i<j}(\sigma_i p_1^{1/r} - \sigma_j p_1^{1/r})^2$. Now consider

$$\prod_{i<j} (\zeta_r^i - \zeta_r^j)^2.$$

This is the discriminant of $X^r - 1$ and therefore

$$\mathrm{rad}\left(d_{\mathbb{Q}(p_1^{1/r})}\right) \mid \mathrm{rad}(r) p_1.$$

It is known that if $\mathbf{K}$ is the compositum of $\mathbf{K}_1$ and $\mathbf{K}_2$,

$$d_{\mathbf{K}} \mid d_{\mathbf{K}_1}^{[\mathbf{K}:\mathbf{K}_1]} d_{\mathbf{K}_2}^{[\mathbf{K}:\mathbf{K}_2]}.$$

It now follows that

$$\mathrm{rad}(d_{\mathbf{L}_r}) \mid \mathrm{rad}(r) \prod_{i=1}^{t} p_i.$$

It follows from the same fact that $d_{\mathbf{F}_r}$ is coprime to q. If $\mathbf{F}_r \cap \mathbb{Q}(\zeta_q) = \mathbf{K}_1$, then $d_{\mathbf{K}_1} \mid (d_{\mathbf{F}_r}, d_{\mathbb{Q}(\zeta_q)})$. Therefore $\mathbf{F}_r$ is disjoint from $\mathbb{Q}(\zeta_q)$. □

We will also require the following lemma.

Lemma 12. *Let $v = 16 \prod_{i=1}^{t} p_i \cdot \prod_{\ell \mid r} \ell^{k_\ell + 1}$ where $\ell^{k_\ell} \mid\mid r$ for all $\ell \mid r$. Then $\mathbb{Q}(\zeta_v) \cap \mathbf{L}_r = \mathbb{Q}(\zeta_r)$.*

Proof. It is obvious that $\mathbb{Q}(\zeta_r) \subset \mathbb{Q}(\zeta_v) \cap \mathbf{L}_r$. Let $\mathbb{Q}(\zeta_v) \cap \mathbf{L}_r = \mathbf{K}_1$. Consider the extension $\mathbf{K}_1/\mathbb{Q}(\zeta_r)$. We have three possibilities

(1) $\mathbf{K}_1/\mathbb{Q}(\zeta_r)$ is non-trivial and ramified,
(2) $\mathbf{K}_1/\mathbb{Q}(\zeta_r)$ is non-trivial and unramified or
(3) $\mathbf{K}_1/\mathbb{Q}(\zeta_r)$ is trivial.

If $\mathbf{K}_1/\mathbb{Q}(\zeta_r)$ is non-trivial and ramified, it must be ramified at one of primes above $2, p_i$ or some prime ℓ which divides r. From the proof of the previous lemma we have

$$\mathrm{rad}(d_{\mathbf{L}_r}) \mid \mathrm{rad}(r)\prod_{i=1}^{t} p_i.$$

and therefore the prime above 2 does not ramify in $\mathbf{K}_1/\mathbb{Q}(\zeta_r)$. Now suppose that the prime above p_i were to ramify in $\mathbf{K}_1/\mathbb{Q}(\zeta_r)$ for some $1 \leqslant i \leqslant t$. Let its ramification index in $\mathbf{K}_1/\mathbb{Q}(\zeta_r)$ be e. Then e must divide the gcd of the ramification indices of p_i in the extension $\mathbf{L}_r/\mathbb{Q}$ and the extension $\mathbb{Q}(\zeta_v)/\mathbb{Q}$. We now claim that $e \mid (r, p_i - 1)$. We first note that $\left(d_{\mathbb{Q}(\zeta_{v/p_i})}, p_i\right) = 1$. Therefore the ramification index in $\mathbb{Q}(\zeta_v)/\mathbb{Q}$ is $p_i - 1$. To compute the ramification index in $\mathbf{L}_r/\mathbb{Q}$, we note that:

(1) The prime p_i is totally ramified in $\mathbb{Q}(p_i^{1/r})$.
(2) The discriminant

$$\left(d_{\mathbf{L}'_r}, p_i\right) = 1 \text{ where } \mathbf{L}'_r = \mathbb{Q}(\zeta_r, p_1^{1/r}, \ldots, \widehat{p_i^{1/r}}, \ldots p_t^{1/r}).$$

Here the hat is used to indicate that the corresponding term has been removed. This follows from the computation of the radical of $d_{\mathbf{L}'_r}$. This computation is similar to that of $d_{\mathbf{L}_r}$ as demonstrated in the previous lemma.

Therefore the ramification index of p_i in $d_{\mathbf{L'}_r}$ is r. The fact that $1 \neq e \mid (r, p_i - 1)$ contradicts our choice of the p_i. Finally let us suppose that prime above some $\ell \mid r$ ramifies in $\mathbf{K}_1/\mathbb{Q}(\zeta_r)$. Since ℓ is totally ramified in $\mathbb{Q}(\zeta_{\ell^{k_\ell+1}})$ and

$$\left(d_{\mathbb{Q}(\zeta_{v/\ell^{k_\ell+1}})}, \ell\right) = 1,$$

the ramification index of ℓ in $\mathbf{K}_1/\mathbb{Q}$ must be $\ell^{k_\ell}(\ell-1)$. This implies that $\ell \mid [\mathbf{K}_1 : \mathbb{Q}(\zeta_r)]$. Note that $\mathbb{Q}(\zeta_v)/\mathbb{Q}(\zeta_r)$ has degree $8\prod_{i=1}^{t}(p_i - 1)\prod_{\ell \mid r}\ell$. This implies that $\mathbb{Q}(\zeta_v)/\mathbb{Q}(\zeta_r)$ has exactly one subextension of degree ℓ for every $\ell \mid r$. Therefore $\mathbf{K}_1 \supset \mathbb{Q}(\zeta_{r\ell})$ and it follows that $\zeta_{r\ell} \in \mathbf{K}_1$. The extension $\mathbb{Q}(p_1^{1/r})$ is totally ramified at p_1, so

$$\mathbb{Q}(p_1^{1/r}) \cap \mathbb{Q}(\zeta_r) = \mathbb{Q} \text{ and } \mathbb{Q}(p_1^{1/r}) \cap \mathbb{Q}(\zeta_{r\ell}) = \mathbb{Q}.$$

By the same argument

$$\mathbb{Q}(p_2^{1/r}) \cap \mathbb{Q}(p_1^{1/r}, \zeta_r) = \mathbb{Q} \text{ and } \mathbb{Q}(p_2^{1/r}) \cap \mathbb{Q}(p_1^{1/r}, \zeta_{r\ell}) = \mathbb{Q}.$$

Therefore inductively, we get

$$[L_r : \mathbb{Q}] = r^t \cdot \phi(r) \text{ and } [\mathbb{Q}(p_1^{1/r}, \cdots, p_t^{1/r}, \zeta_{r\ell}) : \mathbb{Q}] = r^t \cdot \ell \cdot \phi(r).$$

Therefore $\zeta_{r\ell} \notin \mathbf{K}_1$ and this implies that $\mathbf{K}_1/\mathbb{Q}(\zeta_r)$ is either trivial or non-trivial and unramified. By Theorem 8,

$$\mathrm{rad}([\mathbf{K}_1 : \mathbb{Q}(\zeta_r)]) \mid \phi(r).$$

But as seen above $[\mathbf{L}_r : \mathbb{Q}(\zeta_r)]$ is a power of r. However we know that $\mathrm{rad}((r, \phi(r))) \mid \prod_{\ell | r} \ell$. This implies that

$$\mathrm{rad}([\mathbf{K}_1 : \mathbb{Q}(\zeta_r)]) \mid \prod_{\ell | r} \ell.$$

By degree considerations on $\mathbb{Q}(\zeta_v)$ and $\mathbb{Q}(\zeta_r)$ we have

$$[\mathbf{K}_1 : \mathbb{Q}(\zeta_r)] \mid \prod_{\ell | r} \ell.$$

Again, there is only one subextension of degree ℓ in $\mathbb{Q}(\zeta_v)/\mathbb{Q}(\zeta_r)$, it follows that

$$\mathbf{K}_1 \subseteq \mathbb{Q}(\zeta_{\prod_{\ell^{k_\ell} || r} \ell^{k_\ell + 1}}).$$

Therefore we have that $\mathbf{K}_1$ is a cyclotomic extension containing $\mathbb{Q}(\zeta_r)$ in $\mathbb{Q}(\zeta_v)$ which cannot be unramified if non-trivial. This proves the lemma. □

Before we proceed to the sieve theoretic lemmas, we introduce some more notation. By the Chinese remainder theorem, there exists an integer u_1 such that

$$u_1 \equiv 1 + \ell^{k_\ell} \bmod \ell^{k_\ell + 1} \text{ where } \ell^{k_\ell} \mid\mid r \text{ for all primes } \ell \mid r.$$

Theorem 13. *Fix u_2 such that $(u_2, 16 \prod_{i=1}^t p_i) = 1$, $8 | u_2 - 1$ and $(\frac{u_2 - 1}{8}, 16 \prod_{i=1}^t p_i) = 1$. Let u be an integer congruent to*

$$u_2 \bmod 16 \prod_{i=1}^t p_i \qquad \text{and} \qquad 1 + \ell^{k_\ell} \bmod \ell^{k_\ell + 1} \text{ where } \ell^{k_\ell} \mid\mid r \text{ for all primes } \ell \mid r.$$

Let v be $16 \prod_{i=1}^t p_i \cdot \prod_{\ell^{k_\ell} || r} \ell^{k_\ell + 1}$ where ℓ is used to denote primes. Finally, let $S(x, \epsilon, \epsilon_1)$ denote the set of all primes $p \leqslant x$ such that

(1) $p \equiv u \bmod v$,
(2) p splits completely in L_r,
(3) any prime $\ell | (p - 1)$ satisfies $\ell > x^{\frac{(\alpha - \epsilon)(1 - \epsilon_1)}{2}}$ or $\ell \mid 2r$.

Then, we have

$$S(x, \epsilon, \epsilon_1) \gg \frac{\mathrm{Li}(x)}{\log x}.$$

Proof. Let $\mathbf{M}_r$ be the compositum of $\mathbf{L}_r$ and $\mathbb{Q}(\zeta_v)$ and let us denote the Galois group of $\mathbf{M}_r/\mathbb{Q}$ by H. This is a Galois extension of $\mathbb{Q}$. There exists a conjugacy class C in H such that C restricted to the Galois group of $\mathbf{L}_r/\mathbb{Q}$ is trivial and C restricted to $\mathbb{Q}(\zeta_v)$ corresponds to $u \bmod v$. This follows from the definition of v and Lemma 12. Let

$$\mathcal{A} := \{p - 1 : \ p \text{ prime}, \ p \leqslant x, \ (p, \mathbf{M}_r/\mathbb{Q}) = C\} \qquad \text{and} \qquad \mathcal{P} := \{p : p \text{ prime}, \ (p, v) = 1\}.$$

Now for any square free integer q such that $(q, v) = 1$

$$\mathcal{A}_q := \{a \in \mathcal{A} : q | a\} \qquad \text{and} \qquad |\mathcal{A}_q| = |\{p \leqslant x : \ p \text{ prime}, \ p \equiv 1 \bmod q, \ (p, \mathbf{M}_r/\mathbb{Q}) = C\}|.$$

By Lemma 11 and the definition of $\mathcal{P}$, we know that $\mathbf{M}_r$ is disjoint from $\mathbb{Q}(\zeta_q)$. Therefore $|\mathcal{A}_q| = \pi_C(x,q,1)$. We know that

$$|\mathcal{A}_q| = \frac{|C|\mathrm{Li}(x)}{|G|\phi(q)} + R_q = X\frac{\omega(q)}{q} + R_q$$

where $X = \frac{|C|\mathrm{Li}(x)}{|G|}$ and

$$R_q = \pi_C(x,q,1) - \frac{|C|\mathrm{Li}(x)}{|G|\phi(q)}.$$

For any square free integer q, let

$$\omega(q) = \begin{cases} \frac{q}{\phi(q)} & \text{if } q \text{ is supported on the primes in } \mathcal{P} \\ 0 & \text{otherwise.} \end{cases}$$

On considering only the primes $(p,v)=1$ it follows that

$$\frac{\omega(p)}{p} \leqslant \frac{1}{2}.$$

Further

$$\sum_{w\leqslant p<z} \frac{\log p}{\phi(p)} = \sum_{w\leqslant p<z} \frac{\log p}{p-1} = \sum_{w\leqslant p<z} \frac{\log p}{p} + \mathrm{O}(1) = \log\frac{z}{w} + \mathrm{O}(1).$$

Therefore conditions (1) and (2) of Theorem 6 are easily seen to be satisfied. To check condition (3), we consider the sum

$$\sum_{\substack{q\leqslant x^{\alpha-\epsilon}\\ p|q \implies p\in\mathcal{P}}} \mu^2(q)3^{\nu(q)}|R_q|.$$

By the Cauchy-Schwarz inequality,

$$\sum_{\substack{q\leqslant x^{\alpha-\epsilon}\\ p|q \implies p\in\mathcal{P}}} \mu^2(q)3^{\nu(q)}|R_q| \ll \left(\sum_{\substack{q\leqslant x^{\alpha-\epsilon}\\ p|q \implies p\in\mathcal{P}}} \mu^2(q)9^{\nu(q)}|R_q|\right)^{\frac{1}{2}} \left(\sum_{\substack{q\leqslant x^{\alpha-\epsilon}\\ p|q \implies p\in\mathcal{P}}} |R_q|\right)^{\frac{1}{2}}.$$

We know that since

$$\pi_C(x,q,1) \leqslant |\{p\leqslant x : p\equiv 1 \bmod q\}| \leqslant |\{n\leqslant x : n\equiv 1 \bmod q\}| \ll \frac{x}{q} \ll \frac{x}{\phi(q)}$$

we get

$$\frac{1}{x}\left(\sum_{\substack{q\leqslant x^{\alpha-\epsilon}\\ p|q \implies p\in\mathcal{P}}} \mu^2(q)9^{\nu(q)}|R_q|\right) \ll \sum_{q\leqslant x^{\alpha-\epsilon}} \frac{\mu^2(q)9^{\nu(q)}}{\phi(q)} \leqslant \prod_{p\leqslant x^{\alpha-\epsilon}} \left(1+\frac{1}{p-1}\right)^9 \ll \log^9 x.$$

Here the last inequality follows from Mertens' theorem. From the above, Theorem 5 and the prime number theorem, we now have for any $A > 0$

$$\sum_{\substack{q \leqslant x^{\alpha-\epsilon} \\ p \mid q \implies p \in \mathcal{P}}} \mu^2(q) 3^{\nu(q)} |R_q| \ll \frac{x}{\log^A x}.$$

By Theorem 6 we have

$$S(\mathcal{A}; \mathcal{P}, z) \quad \geqslant \quad \frac{|C| \operatorname{Li}(x)}{|G|} \prod_{\substack{p \leqslant z \\ p \in \mathcal{P}}} \left(1 - \frac{\omega(p)}{p}\right) \left\{ f\left((\alpha - \epsilon)\frac{\log X}{\log z}\right) - \frac{B}{(\log X)^{\frac{1}{14}}} \right\}.$$

For an $0 < \epsilon_1 < \frac{1}{2}$, we put $z = x^{\frac{(\alpha-\epsilon)(1-\epsilon_1)}{2}}$, we note that for sufficiently large x

$$(\alpha - \epsilon)\frac{\log X}{\log z} \leqslant 2 \cdot \frac{\log 3x - \log\log x}{(1 - \epsilon_1)\log x} \leqslant \frac{2}{(1 - \epsilon_1)} < 4.$$

Similarly for x sufficiently large

$$(\alpha - \epsilon)\frac{\log X}{\log z} \geqslant 2 \cdot \frac{\log x - \log\log x - \log |G|}{(1 - \epsilon_1)\log x} > 2.$$

Therefore

$$S(\mathcal{A}; \mathcal{P}, x^{\frac{(\alpha-\epsilon)(1-\epsilon_1)}{2}}) \gg \frac{\operatorname{Li}(x)}{\log x}.$$

Since $(u_2 - 1, \prod_{i=1}^{t} p_i) = 1$, we have

$$S(x, \epsilon, \epsilon_1) \gg \frac{x}{\log^2 x}.$$

□

Let p be a prime which does not belong to $\{p_1, \ldots p_t\}$. Then let $\mathbb{F}_p$ denote the finite field of order p and W_p be the image of W in $\mathbb{F}_p^*$. Further, we set $u_2 = 3$ for the rest of the article.

Lemma 14. *For $S(x, \epsilon, \epsilon_1)$ as defined in Theorem 13, we now define*

$$T_1(x) = \{p \leqslant x \ : \ p \in S(x, \epsilon, \epsilon_1), \ \ell \mid [\mathbb{F}_p^* : W_p] \implies \ell \mid r\}.$$

Here we use ℓ to denote a prime. Then we have

$$|T_1(x)| \gg \frac{\operatorname{Li}(x)}{\log x}.$$

Proof. Since 3 is a quadratic non-residue modulo p_1 ($p_1 \equiv 5 \bmod 12$), it follows that $p \in S(x, \epsilon, \epsilon_1)$ is a quadratic non-residue modulo p_1. But since $p_1 \equiv 1 \bmod 4$ it follows by the law of quadratic reciprocity that p_1 is a quadratic non-residue modulo p. This implies that

$$2 \nmid [\mathbb{F}_p^* : W_p].$$

Now by Lemma 7, we get that

$$|\{p \leqslant x \ : \ p \in S(x, \epsilon, \epsilon_1), |W_p| < x^{1 - \frac{(\alpha-\epsilon)(1-\epsilon_1)}{2}}\}| \ll x^{\left(1 - \frac{(\alpha-\epsilon)(1-\epsilon_1)}{2}\right)\left(1 + \frac{1}{t}\right)} = o\left(\frac{x}{\log^2 x}\right).$$

□

4. Proof of Theorem 4

In this section we give the proof of our main theorem. We first recall some notation from the previous section. As seen earlier in the proof, we chose a set of t primes $\{p_1, p_2, \ldots, p_t\}$ with $p_1 \equiv 5 \bmod 12$. We then defined W to be the monoid generated by this set of primes. For any prime $p \notin U = \{p_1, \ldots p_t\}$, we used W_p to denote the image of W in $\mathbb{F}_p^*$. We then defined the set

$$\begin{aligned} S(x, \epsilon, \epsilon_1) \quad = \quad & \{p \leqslant x \ : \ p \equiv u \bmod v, \ p \notin U, \ p \text{ splits in } L_r \\ & \text{and any prime } \ell \mid p-1 \implies \ell \mid 2r \text{ or } \ell > x^{\frac{(\alpha-\epsilon)(1-\epsilon_1)}{2}}\}. \end{aligned}$$

Here, α is as defined in Theorem 5. Further $\epsilon > 0$ and $\epsilon_1 > 0$ are real numbers such that $2\epsilon_1 < 1$. Finally, we defined

$$T_1(x) = \{p \leqslant x \ : \ p \in S(x, \epsilon, \epsilon_1), \ \ell \mid [\mathbb{F}_p^* : W_p] \implies \ell \mid r\}.$$

Under this notation, we now have the following theorem.

Theorem 15. *Let S be a set of $2^{t-2} \times 7$ t-tuples of natural numbers. Further let*

$$\overline{S} = \{(\overline{s_1}, \ldots, \overline{s_t}) \ : \ (s_1, \ldots, s_t) \in S\}$$

where $\overline{s_i}$ denotes $s_i \bmod 2$. Now suppose that S satisfies the following properties:

1. *The element $(0, \ldots, 0) \notin \overline{S}$,*
2. *Consider the natural reduction modulo 2 map*

$$\varphi : S \to \overline{S}.$$

   Then $|\varphi^{-1}(t)| \leqslant 2$ for all $t \in \overline{S}$.

3. *If V is any $t-1$ dimensional subspace of $(\mathbb{Z}/2\mathbb{Z})^t$ and*

$$S_V = \varphi^{-1}(\overline{S} \backslash V),$$

   then any t elements of the set S_V are linearly independent.

Then there exists a tuple $(u_1, \ldots, u_t)$ such that $a = p_1^{u_1} \ldots p_t^{u_t}$ satisfies $[\mathbb{F}_p^* : \langle a \bmod p \rangle] = r$ for all $p \in T_1(x)$ for x sufficiently large.

Before we give the proof of Theorem 15, we record here a result from [10] which shows the existence of the t-tuples required by Theorem 15.

Theorem 16. *Given any $t \geqslant 3$ there exists a set of $2^{t-2} \times 7$, t-tuples with entries in $\mathbb{N}$, satisfying the hypothesis of Theorem 15.*

This is Theorem 10 of [10]. We now proceed to the proof of Theorem 15.

Proof. Let $p_0 \in T_1(x)$. Let g be a generator of $\mathbb{F}_{p_0}^*$. Then for each $i \in \{1, \ldots, t\}$ there exists e_i such that

$$p_i \equiv g^{e_i} \bmod p_0.$$

If $[\mathbb{F}_{p_0}^* : W_{p_0}] = j$ we have $(e_1, \ldots, e_t, p_0 - 1) = j$. To show this, suppose otherwise and let $(e_1, \ldots, e_r, p_0 - 1) = j_1$ and $[\mathbb{F}_{p_0}^* : W_{p_0}] = j$. Since there is a unique subgroup of $\mathbb{F}_{p_0}^*$ of index j given by $\langle g^j \rangle$, we have

$$\langle g^j \rangle = \langle g^{e_1}, \ldots, g^{e_r} \rangle \subset \langle g^{j_1} \rangle.$$

Since $j \equiv hj_1 \bmod (p_0 - 1)$ for some $h \in \mathbb{Z}$, we have $j_1 \mid j$ because j_1 divide $p_0 - 1$ by definition. Conversely since j_1 is the gcd, we have

$$j_1 = \sum_{i=1}^{t} n_i e_i + n_{t+1}(p_0 - 1) \text{ for some } n_i \in \mathbb{Z}.$$

Therefore

$$j_1 \equiv \sum_{i=1}^{r} n_i e_i \bmod (p_0 - 1).$$

However each $e_i \equiv h_i j \bmod (p_0 - 1)$ for some integer h_i. Combining the above

$$j_1 \equiv \sum_{i=1}^{r} n_i h_i j \bmod (p_0 - 1).$$

Since $j \mid p_0 - 1$ we have $j \mid j_1$. By definition of $T_1(x)$, it follows that the index j is odd. This implies that $(e_1, \ldots, e_t) \not\equiv (0, \ldots, 0) \bmod 2$. Let V be the orthogonal complement of the vector space $\{(0, \ldots, 0), (\overline{e_1}, \ldots, \overline{e_t})\}$. Observe that since $t \geqslant 3$

$$|S_V| \geqslant 2^{t-2} \times 7 - 2(2^{t-1} - 1) = 2^{t-2} \times 3 + 2 > 2$$

due to assumption 2 and the fact that V is a $t - 1$ dimensional subspace of $(\mathbb{Z}/2\mathbb{Z})^t$. Further $\overline{p_1^{u_1} \ldots p_t^{u_t}}$ generates a subgroup of index m if and only if $(\sum_1^t u_i e_i, p_0 - 1) = m$.This can be seen from the following argument. Suppose that the index is m and $(\sum_1^t u_i e_i, p_0 - 1) = m_1$. We have

$$\langle g^m \rangle = \langle \overline{p_1^{u_1} \ldots p_t^{u_t}} \rangle \subset \langle g^{m_1} \rangle,$$

so $m_1 \mid m$ since m_1 divides $p_0 - 1$. Conversely there exist integers n_1 and n_2 such that

$$n_1 \sum_1^t u_i e_i + n_2(p_0 - 1) = m_1.$$

Therefore

$$m_1 \equiv n_1 \sum_1^t u_i e_i \bmod (p_0 - 1).$$

However since

$$\langle g^m \rangle = \langle \overline{p_1^{u_1} \ldots p_t^{u_t}} \rangle = \langle g^{\sum_1^r u_i e_i} \rangle$$

we have an integer h_0 such that $\sum_1^r u_i e_i \equiv h_0 m \bmod (p_0 - 1)$. Hence, we have

$$m_1 \equiv n_1 h_0 m \bmod (p_0 - 1).$$

Finally $m \mid p_0 - 1$, so we have $m \mid m_1$. By definition of S_V, we have $2 \nmid \sum_1^t u_i e_i$. Now consider any t elements from S_V as $\{(u_1^{\{i\}}, \ldots, u_t^{\{i\}}) : 1 \leqslant i \leqslant t\}$. Let

$$U_t = \begin{pmatrix} u_1^{\{1\}} & u_2^{\{1\}} & \cdots & u_t^{\{1\}} \\ u_1^{\{2\}} & u_2^{\{2\}} & \cdots & u_t^{\{2\}} \\ \vdots & \vdots & \ddots & \vdots \\ u_1^{\{t\}} & u_2^{\{t\}} & \cdots & u_t^{\{t\}} \end{pmatrix}.$$

We have

$$\begin{pmatrix} u_1^{\{1\}} & u_2^{\{1\}} & \cdots & u_t^{\{1\}} \\ u_1^{\{2\}} & u_2^{\{2\}} & \cdots & u_t^{\{2\}} \\ \vdots & \vdots & \ddots & \vdots \\ u_1^{\{t\}} & u_2^{\{t\}} & \cdots & u_t^{\{r\}} \end{pmatrix} . \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_r \end{pmatrix} = \begin{pmatrix} \sum_1^t u_i^{\{1\}} e_i \\ \sum_1^t u_i^{\{2\}} e_i \\ \vdots \\ \sum_1^t u_i^{\{t\}} e_i \end{pmatrix} \tag{1}$$

By assumption we have $\det U_t \neq 0$. Further for x sufficiently large, for $p_0 \in T_1(x)$ we can assume that all odd primes dividing $p_0 - 1$ which are greater than $x^{\frac{(\alpha-\epsilon)(1-\epsilon_1)}{2}}$, are coprime to $\det U_t$. For $p_0 \in T_1(x)$, $p_0 - 1$ has atmost t prime divisors greater than $x^{\frac{(\alpha-\epsilon)(1-\epsilon_1)}{2}}$. Since the index of W_{p_0} is co-prime to all the primes greater than $x^{\frac{(\alpha-\epsilon)(1-\epsilon_1)}{2}}$, the gcd of the e_i's is coprime to all prime divisors of $p_0 - 1$ which are greater than $x^{\frac{(\alpha-\epsilon)(1-\epsilon_1)}{2}}$. Therefore by (1), each prime divisor of $p_0 - 1$ which is greater than $x^{\frac{(\alpha-\epsilon)(1-\epsilon_1)}{2}}$ divides atmost $t - 1$ elements of the form $\sum_1^t u_i e_i$ for any $(u_1, \ldots, u_t) \in S$. So there are

$$2^{t-2} \times 3 + 2 - t(t-1) > 0$$

elements left in S_V. Thus we have elements $(u_1, \ldots, u_t) \in S_V$ such that $a_{p_0} = p_1^{u_1} \ldots p_t^{u_t}$ generates a subgroup of index m where m is divisible only by primes dividing r. However $m \mid p_0 - 1$ where $p_0 \in T_1(x) \subset S(x, \epsilon, \epsilon_1)$. Since p_0 splits in L_r, by Lemma 10 for all but finitely many $p_0 \in T_1(x)$, $r \mid [\mathbb{F}_{p_0}^* : \langle a_{p_0} \rangle \bmod p]$. Finally by the choice of the residue class $u \bmod v$ in the definition of $S(x, \epsilon, \epsilon_1)$, $\ell^{k_\ell + 1} \nmid m$ for all $\ell^{k_\ell} \mid\mid r$. Therefore

$$[\mathbb{F}_{p_0}^* : \langle a_{p_0} \rangle \bmod p] = r.$$

Finally by Pigeon-hole principle, there exists an element $a = p_1^{u_1} \ldots p_t^{u_t} \in W$ with $(u_1, \ldots, u_t) \in S_V$ such that

$$|\{p \leqslant x : [\mathbb{F}_{p_0}^* : \langle a \rangle \bmod p]\}| = r\}| \gg \frac{x}{\log^2 x}.$$

$\square$

Acknowledgments. We would like to thank Professor Purusottam Rath for suggesting the question. We would also like to thank Sanoli Gun and Purusottam Rath for helpful suggestions and encouragement. It is our pleasure to thank the Department of Science and Technology for financial support through the INSPIRE Faculty fellowship and the Indian Statistical Institute, Bangalore for academic support.

References

[1] E. Artin, The Collected Papers of Emil Artin (S. Lang and J. Tate, Eds.), *Reading, Mass.: Addison- Wesley* (1965).

[2] E. Bombieri, *Le grand crible dans la théorie analytique des nombres*, Astérisque, **18** (1974), 112 p.

[3] M. Ram Murty and V. Kumar Murty, *A variant of the Bombieri-Vinogradov theorem*, CMS Conf. Proc. **7**, Amer. Math. Soc., Providence, RI (1987), 243–272.

[4] C. Franc and M. Ram Murty, *On a generalization of Artin's conjecture*, Pure Appl. Math. Q. **4** (2008), 1279–1290.

[5] R. Gupta and M. Ram Murty, *A remark on Artin's conjecture*, Invent. Math. **78** (1984), no. 1, 127–130.

[6] H. Halberstam and H.- E. Richert, Sieve methods, *Academic Press*, New York, (1974).

[7] D. R. Heath-Brown, *Artin's conjecture for primitive roots*, Quart. J. Math. Oxford Ser. (2), **37** (1986), no. 145, 27–38.

[8] C. Hooley, *On Artin's conjecture*, J. reine angew. Math., **226** (1967), 209–220.

[9] M. Ishida, *The genus fields of algebraic number fields*, Lecture notes in Mathematics - 555, Springer-Verlag Berlin Heidelberg (1976).

[10] J. Sivaraman, *Primitive roots for Pjateckiĭ-Šapiro primes*, J. Théor. Nombres Bordeaux **33** (2021), no. 1, 83–94.

[11] H. W. Lenstra Jr., *On Artin's Conjecture and Euclid's Algorithm in Global Fields* Invent. Math. **42** (1977), 201–224.

[12] H. W. Leopoldt, *Zur Geschlechtertheorie in abelschen Zahlkorpern,* Math. Nachr. **9** (1953), 350-362

[13] P. Moree, *On Golomb's near-primitive root conjecture*, MPIM-preprint **106** (2009), pp. 5

[14] L. Murata, *A problem analogous to Artin's conjecture for primitive roots and its applications*, Arch. Math. (Basel) **57** (1991), 555–565.

[15] M. Ram Murty, *Artin's conjecture and elliptic analogues, in Sieve Methods*, Exponential Sums, and their Applications in Number Theory, (eds. G.R.H. Greaves, G. Harman, and M.N. Huxley), Cambridge University Press, (1996), 325-344 .

(J. Sivaraman) Indian Statistical Institute, 8th Mile, Mysore Rd, RVCE Post, Bengaluru, Karnataka 560059.

Email address: jyothsnaa.s@gmail.com