Artin's Conjecture
Unconditional Approach and Elliptic Analogue

by

Sourav Sen Gupta

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Mathematics
in
Pure Mathematics

Waterloo, Ontario, Canada, 2008

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

In this thesis, I have explored the different approaches towards proving Artin's 'primitive root' conjecture unconditionally and the elliptic curve analogue of the same. This conjecture was posed by E. Artin in the year 1927, and it still remains an open problem. In 1967, C. Hooley proved the conjecture based on the assumption of the generalized Riemann hypothesis. Thereafter, the mathematicians tried to get rid of the assumption and it seemed quite a daunting task. In 1983, the pioneering attempt was made by R. Gupta and M. Ram Murty, who proved unconditionally that there exists a specific set of 13 distinct numbers such that for at least one of them, the conjecture is true. Along the same line, using sieve theory, D. R. Heath-Brown reduced this set down to 3 distinct primes in the year 1986. This is the best unconditional result we have so far. In the first part of this thesis, we will review the sieve theoretic approach taken by Gupta-Murty and Heath-Brown. The second half of the thesis will deal with the elliptic curve analogue of the Artin's conjecture, which is also known as the Lang-Trotter conjecture. Lang and Trotter proposed the elliptic curve analogue in 1977, including the higher rank version, and also proceeded to set up the mathematical formulation to prove the same. The analogue conjecture was proved by Gupta and Murty in the year 1986, assuming the generalized Riemann hypothesis, for curves with complex multiplication. They also proved the higher rank version of the same. We will discuss their proof in details, involving the sieve theoretic approach in the elliptic curve setup. Finally, I will conclude the thesis with a refinement proposed by Gupta and Murty to find out a finite set of points on the curve such that at least one satisfies the conjecture.

Acknowledgements

First of all, I would like to thank my supervisors, Professor Wentang Kuo and Professor Yu-Ru Liu for their constant support, encouragement and guidance throughout my Masters program. It was my honor to work under their prized supervision. I am thankful to Professor Michael Rubinstein and Professor Kevin Hare, the readers of my thesis, for their invaluable suggestions and corrections.

I would like to thank my parents for their faith in me during my stay abroad. I am also grateful to my house mates, my friends and my colleagues for their encouragement and occasional distractions when I needed those the most. Finally, I will take this opportunity to thank Dr. Sankar Ghosh, my high school teacher and my mentor, whose encouragement has motivated me to pursue a career in mathematics and teaching.

I am not a witness to God
He is just an open conjecture
My faith rests upon my parents
For my past, present and future

I dedicate this thesis to my parents (Maa and Bapi) who are by my side in each and every step of my life. I love you.

Contents

Chapter 1

Introduction

"The deepest interrelationships in analysis are of an arithmetical nature"

- Hermann Minkowski

In the preface to his 'Diophantische Approximationen', Minkowski made this famous remark which has become a proven conviction for all the number theorists around the world. Gauss discovered and described such an amazing interrelationship in his 'Disquisitiones Arithmeticae'. Let us take a look at Gauss's observation.

1.1 Gauss's Observation

Gauss asked the following questions regarding the period length of decimal fractions

- Why does $\frac{1}{17} = 0.0588235294117647058823529411764705...$ have a period of 16?
- Why on the other hand $\frac{1}{37} = 0.027027027...$ has a period length 3?
- Why does the binary fraction expansion of $\frac{1}{99007599}$ has a period length of nearly 50 million?

To answer these questions, Gauss observed the following. Let us assume that p is a prime not equal to 2 or 5 and let

$$\frac{1}{p} = 0.a_1a_2...a_k...$$

be its decimal expansion with period k. Then, we can observe that

$$\frac{1}{p} = \left(\frac{a_1}{10} + \frac{a_2}{10^2} + \cdots + \frac{a_k}{10^k}\right)\left(1 + \frac{1}{10^k} + \frac{1}{10^{2k}} + \cdots\right) = \frac{M}{10^k - 1}$$

for some integer M, and hence $10^k - 1 = Mp$, i.e, $10^k \equiv 1 \pmod{p}$. So, from this argument it is clear that the period of the decimal fraction expansion of $\frac{1}{p}$ depends on the least exponent k such that the above mentioned congruence relation holds true. In other words, the period length is equal to the 'order' of 10 modulo p.

1.1.1 Order Modulo Primes

For a prime p, the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic of order $p-1$. So, if the order of 10 modulo p is the period length k, then we must have $0 < k \leq p-1$. Thus the largest period of the decimal expansion of $\frac{1}{p}$ can occur if and only if 10 has order $p-1$ modulo p, i.e, if 10 be a cyclic generator of the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$. In number theory, we refer to the cyclic generators of this group as the 'Primitive Roots' of the prime p. So, the largest period will occur for 10 being a primitive root of p. More generally, the period of the base a representation of $\frac{1}{p}$ will be the largest, i.e, $p-1$, if and only if a is a primitive root modulo p, i.e, a satisfies the congruence relation $a^k \equiv 1 \pmod{p}$ for the smallest value of $k = p-1$ with $p \nmid a$. For a general integer $n = \prod p_i$ which is a product of distinct primes p_i, if $\gcd(a, n) = 1$ then the period length of $\frac{1}{n}$ expanded in base a will be given by lcm $\{\text{ord } (a) \text{ modulo } p_i\}$ [16].

1.1.2 Primitive Roots of Primes

In the case of a given prime p, the number of its primitive roots is well known to be $\phi(p-1)$, where ϕ is the famous Euler's totient function which counts the number of positive integers less than or equal to a certain number which are coprime to it. Gauss thought of reversing the question. Instead of fixing a prime p and asking the number of its primitive roots, Gauss suggested to fix a random integer, 10 say, and ask how many times it is a primitive root modulo p, where p varies over all the primes. Though Gauss posed this question and also had an intuition that 10 will be a primitive root for infinitely many primes, he did not provide any definite answer or a general conjecture to show how often a number is a primitive root modulo primes. His intuition was formalized in a number theoretic setting in terms of a conjecture by E. Artin in 1927 [2].

1.2 Artin's Conjecture

Conjecture 1.1 (Artin's Conjecture) *For any given integer a, if $a \neq 0, 1, -1$ and if a is not a perfect square, then there exist infinitely many primes p for which a is a primitive root modulo p.*

Moreover, if $N_a(x)$ denotes the number of primes $p \leq x$ for which a is a primitive root, then the stronger version of the conjecture states

Conjecture 1.2 (Artin's Conjecture: Stronger Form) *If the integer $a \neq 0, 1, -1$ and a is not a perfect square, then there exists a positive constant $A(a)$ depending on a such that for $x \to \infty$, $N_a(x) \sim A(a)\frac{x}{\log x}$.*

1.2.1 Artin's Intuition

In the stronger form of the conjecture, the quantity $\frac{x}{\log x}$ is just the density of primes in integers, obtained from the prime number theorem. Regarding the positive constant $A(a)$, Artin's intuition was as follows [2].

The necessary and sufficient condition for a being a primitive root of p is

$$a^{(p-1)/q} \not\equiv 1 \pmod{p}$$

for every prime divisor q of $p-1$. This is because of the fact that if k is the order of a modulo p, then $k|(p-1)$, and if $k \neq (p-1)$, then $k|(p-1)/q$ for some prime divisor q of $p-1$. From a heuristic point of view, a is a primitive root of p if the following two events do not occur for any prime divisor q of $p-1$

$$\begin{aligned} p &\equiv 1 \pmod{q} \\ a^{(p-1)/q} &\equiv 1 \pmod{p} \end{aligned}$$

Let us invert the problem scenario to fix q and find the probability that a prime p satisfies the above two conditions. By Dirichlet's theorem, $q|(p-1)$, i.e, $p \equiv 1 \pmod{q}$ is true for primes p with frequency $\frac{1}{q-1}$. Again, $a^{(p-1)/q} \equiv 1 \pmod{p}$ occurs with a probability of $\frac{1}{q}$. The probability that both these events occur simultaneously is $\frac{1}{q(q-1)}$ as they can be assumed to be independent. The probability that a is a primitive root of p is equal to the probability that the above mentioned two events do not occur for any q. Hence, the constant term $A(a)$ which denotes this probability can heuristically be estimated by

$$\prod_{q \text{ prime}} \left(1 - \frac{1}{q(q-1)}\right)$$

1.3 Approaches to Prove Artin's Conjecture

Since the proposal of the conjecture in 1927, a lot of mathematicians have tried to prove it through different approaches. The first successful approach towards proving the conjecture was by C. Hooley in the year 1967.

1.3.1 Hooley's Conditional Approach

In his paper [11], Hooley proved the Artin's conjecture as well as its stronger asymptotic version for $N_a(x)$ subject to the assumption of the generalized Riemann hypothesis, which is a natural extension of the original Riemann hypothesis to the Dedekind zeta function of a number field. The final implication of Hooley's proof is that if Artin's conjecture is false, then the generalized Riemann hypothesis is false as well.

1.3.2 Gupta and Murty's Unconditional Approach

After Hooley proved the conjecture on a conditional base of Riemann hypothesis, mathematicians started exploring the conjecture without any conditional assumptions. The first successful attempt in this case was pioneered by R. Gupta and M. Ram Murty [7]. In 1983, they proved, without any conditions, that there is a specific set of 13 distinct numbers such that for at least one of these 13 numbers, Artin's conjecture is true. This was the first unconditional proof of the existence of some number for which the conjecture is true.

1.3.3 Heath-Brown's Unconditional Approach

To prove the Artin's conjecture completely and unconditionally, the set of 13 integers had to be reduced down to 1. Gupta, Kumar Murty and Ram Murty proved the conjecture for a set of 7 integers. The largest break through came in 1986 from D.R. Heath-Brown [10]. He used a refined sieve theory result by Fouvry and Iwaniec [6] and Chen's 'Reversal of Roles' technique to reduce this set down to a set of 3 primes. The implication of his result is that the conjecture is unconditionally true for almost all, except at most 2 exceptional, primes.

We will discuss in details the unconditional approaches by Gupta-Murty and Heath-Brown in Chapter 2, where we will notice the extent to which analysis and sieving techniques are used in such a core arithmetical problem.

1.4 Artin's Conjecture: Elliptic Curve Analogue

It is a general trait in number theory to view a specific problem from different analogous standpoints by constructing its analogues in various mathematical frameworks. Similarly, an analogue of Artin's conjecture for elliptic curves was formulated by Lang and Trotter in 1977.

1.4.1 Lang and Trotter

The elliptic curve analogue of the Artin's Conjecture was formulated by Lang and Trotter [15] in 1977. As the original conjecture talks about the density of primes for which a given integer would be a primitive root, the analogue deals with the density of primes for which the reduction of an elliptic curve modulo that prime would have a given rational point as a primitive point. So, we are essentially moving to the frame of elliptic curve groups and points on the curves from the general space of integers and primitive roots. They considered the analogue of a primitive root to be a primitive point which is the generator of the elliptic curve group reduced modulo a prime. With this setup, they proposed the following analogue of Artin's conjecture.

Conjecture 1.3 (Lang and Trotter) *If we consider an elliptic curve $E(\mathbb{Q})$ defined over the rationals and a rational point $a \in E(\mathbb{Q})$ of infinite order, then that point a will be a primitive point of $\overline{E}(\mathbb{F}_p)$, the reduction of E modulo p, for infinitely many primes p, i.e, the point $\overline{a}$, reduction of a modulo p, will generate $\overline{E}(\mathbb{F}_p)$ for infinitely many primes p.*

They also proposed an analogous conjecture for the higher rank elliptic curves and proceeded to set up the mathematical platform to prove these analogues. We will discuss more about their approach in Chapter 3.

1.4.2 Gupta and Murty

The analogous conjecture proposed by Lang and Trotter was extended to form an analogue of the stronger asymptotic version by R. Gupta and M. Ram Murty [8] in 1986. In this paper, they also proved the stronger version of the elliptic curve conjecture with the assumption of generalized Riemann hypothesis and for the primes that split completely in some quadratic extension of $\mathbb{Q}$ where the elliptic curve has complex multiplication over the whole ring of integers of that extension.

Gupta and Murty also proved that the higher rank version of the conjecture proposed by Lang and Trotter is true under the assumption of the generalized Riemann hypothesis for elliptic curves with rank as high as 18 with no complex multiplication or 10 in case of complex multiplication. In the same paper, they refined this result to show that the assumption of GRH can be relaxed to an assumption of α-GRH. We will discuss these results in details in Chapter 3. Besides, they also proposed an unconditional approach in the elliptic curve analogue and obtained a set of exceptional points, same as in the general unconditional approach. We will discuss this refinement in the concluding portion of this thesis.

In this thesis, I will discuss the different approaches tried out so far in the direction of proving Artin's Conjecture. Chapter 2 will deal with the unconditional approaches taken by Gupta-Murty and Heath-Brown, using sieve theory and techniques from analytic number theory. Chapter 3 deals with the elliptic curve analogue of the conjecture in details and I will discuss the approaches taken by Lang-Trotter and Gupta-Murty in proving the analogue. I will conclude the thesis through an overall discussion of the latest progresses in this field of number theory.

Chapter 2

Artin's Conjecture: Unconditional Approach

The first successful attempt towards proving the Artin's conjecture, without any conditional assumption, was by R. Gupta and M. Ram Murty [7], in 1983. They proved the theorem in Section 2.1 which essentially implies that the conjecture is unconditionally true for almost all integers, except at most 12. Thereafter, D.R. Heath-Brown reduced this set down to a set of 2 exceptional primes using refined sieving techniques. We will discuss his approach in Section 2.2.

2.1 Result 1: Gupta and Murty

Gupta and Murty attempted to prove the stronger version of the Artin's conjecture. So, if we define

$$N_a(x) \;=\; \#\{p \leq x \;:\; a \text{ is a primitive root of } p\}$$

then, the following result by Gupta and Murty proposes an asymptotic estimate of $N_a(x)$ without any conditional assumption.

Theorem 2.1 (Gupta and Murty, 1984) *Let q, r and s denote three distinct primes. If we define the following set*

$$S = \left\{qs^2, q^3r^2, q^2r, r^3s^2, r^2s, q^2s^3, qr^3, q^2r^3s, q^3s, qr^2s^3, qrs\right\}$$

then for some $a \in S$, there exists a $\delta > 0$ such that

$$N_a(x) \geq \frac{\delta x}{\log^2 x}$$

Proof. The proof of this theorem relies heavily on the following lemmas. We will first proceed to prove the theorem assuming the results to be true, and then we will subsequently prove the lemmas in the following subsection. For the proof of this theorem and the lemmas in this section, we will write q, r and s to denote three distinct primes.

Lemma 2.1 *There exists a $\delta > 0$ such that*

$$\#\{p \leq x \ : \ \mathbb{F}_p^* = \langle q, r, s \rangle\} \ \geq \ \frac{\delta x}{\log^2 x}$$

Proof. Proved in Section 2.1.1.

Lemma 2.2 *Let us consider the 3-tuple of non-negative integers $u = (u_1, u_2, u_3)$, where we denote $q^{u_1} r^{u_2} s^{u_3}$ by $(q, r, s)^u$. Now, if we have a set S_1 of 3-tuples satisfying*

(i) For any $u \in S_1$, $u \not\equiv (0, 0, 0) \pmod 2$

(ii) For each $u \in S_1$, there is at most one $v \in S_1$ such that $v \neq u$ and $v \equiv u \pmod 2$

(iii) For each 2-dimensional subspace $V \subset \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^3$, any three elements of $S_V = \{u \in S_1 \ : \ u \not\equiv \ v \pmod 2 \ \forall \ v \in V\}$ are linearly independent

and if $\mathbb{F}_p^* = \langle q, r, s \rangle$, then for some $u \in S_1$, $(q, r, s)^u$ is a primitive root modulo p provided that $(p-1)$ has at most 3 odd prime divisors, all sufficiently large.

Proof. Proved in Section 2.1.1.

Now, with respect to the conditions (i) and (ii) in Lemma 2.2, we can construct the following set of thirteen 3-tuples:

$$\begin{aligned} S_1 = \{&(1,0,2),(3,2,0),(2,1,0),(0,3,2),(0,2,1),(2,0,3),\\ &(1,3,0),(3,1,2),(0,1,3),(2,3,1),(3,0,1),(1,2,3),(1,1,1)\} \end{aligned}$$

where the elements of the first 6 pairs of 3-tuples are mutually congruent modulo 2. We just need to verify the validity of condition (iii) to apply the result of Lemma 2.2 to this set S_1. To verify this condition, we need to consider the following two cases

I. Let the three elements $x_1, x_2, x_3 \in S_V$ are incongruent modulo 2. If y_1, y_2, y_3 be the reduction of x_1, x_2, x_3 modulo 2, then we can observe that $a \cdot y_1 \not\equiv 0 \pmod 2$ and $a \cdot y_2 \not\equiv 0 \pmod 2$ implies $a \cdot (y_1 + y_2) \equiv 0 \pmod 2$, for $a = (a_1, a_2, a_3)$ as in the proof of Lemma 2.2. Hence, $y_3 \neq y_1 + y_2$ as $a \cdot y_3 \not\equiv 0 \pmod 2$. So, x_1, x_2, x_3 are linearly independent.

II. Let two elements of the three are congruent, i.e. $x_1 \equiv x_2 \pmod 2$, say. Then the cross product of these two will surely be a multiple of one of the following 6 vectors:

$$(2, -3, -1), (-1, 2, -3), (-3, -1, 2), (-3, 1, 4), (4, -3, 1), (1, 4, -3)$$

In each of these cases, x_1 and x_2 are the only vectors in S_1 which are orthogonal to it. Thus, any three elements of this kind in S_1 will be linearly independent.

Thus, we obtain that the set S_1 as constructed above follows all the conditions of Lemma 2.2. Therefore, if $\mathbb{F}_p^* = \langle q, r, s \rangle$, then for some $u \in S_1$, $(q, r, s)^u$ is a primitive root modulo p, provided that $(p-1)$ has at most 3 odd prime divisors, all sufficiently large. By Lemma 2.1, we also know that there exists a $\delta > 0$ such that $\mathbb{F}_p^* = \langle q, r, s \rangle$ for at least $\frac{\delta x}{\log^2 x}$ primes $p \leq x$. Hence, the theorem follows for the set S which consists of the elements $(q, r, s)^u$ for $u \in S_1$. □

2.1.1 Proof of Lemmas

Proof of Lemma 2.1

Proof of this lemma almost entirely depends on the following result. Actually, the following result constructs the main framework behind proving Theorem 2.1.

Lemma 2.3 *Let us fix a prime q and a constant $0 < \epsilon < \frac{1}{4}$. If $\alpha = \frac{1}{4} + \epsilon$, then there exists a constant $c > 0$ such that*

$$\#\left\{p \leq x \ : \ \left(\frac{q}{p}\right) = -1, \ t \text{ is prime and } t|(p-1) \Rightarrow t = 2 \text{ or } t > x^{\alpha}\right\} \geq \frac{cx}{\log^2 x}$$

Proof. This lemma is the key element in proving Theorem 2.1. The result can be proved for the exponent $\alpha = \frac{1}{4} - \epsilon$ using Theorem 1 of Iwaniec [13] and the Bombieri-Vinogradov theorem. A finite set can be obtained in Theorem 2.1 just by proving Lemma 2.3 with an exponent $\alpha > 0$. The lower bound Selberg sieve can be utilized along with the Bombieri-Vinogradov theorem to prove the same result

for $\alpha = \frac{1}{6} - \epsilon$. Gupta and Murty [7] used a finer result by Iwaniec [12] to get the specific value of $\alpha = \frac{1}{4} + \epsilon$ and to obtain the thirteen element optimal set in this case. The size of this set S in the theorem decreases if Lemma 2.3 is strengthened by increasing the value of α. We will see a nice improvement to this Lemma by Heath-Brown [10] in the next section which allows him to strengthen the theorem by proving it true for a 3-element set. $\square$

Now, let us embark on our path of proving Lemma 2.1. Let us consider the primes $p \leq x$ such that p does not split in $\mathbb{Q}(\sqrt{q})$, i.e. $\left(\frac{q}{p}\right) = -1$, and for t prime, $t|(p-1) \ \Rightarrow t = 2$ or $t > x^{\frac{1}{4}+\epsilon}$. Then, by Lemma 2.3, we obtain that the number of such primes p is at least $\frac{\delta x}{\log^2 x}$. Now, for these primes, let us count the number of occasions where $\mathbb{F}_p^* \neq \langle q, r, s \rangle$. If $\mathbb{F}_p^* \neq \langle q, r, s \rangle$, let us assume that the prime t divides the index of $\langle q, r, s \rangle$ in $\mathbb{F}_p^*$. Then, obviously $t|(p-1)$ and hence either $t = 2$ or $t > x^{\frac{1}{4}+\epsilon}$. But, if $t = 2$, then we obtain

$$2|[\mathbb{F}_p^* : \langle q \rangle] \ \Rightarrow \ \left(\frac{q}{p}\right) = 1 \ \Rightarrow \ p \text{ splits in } \mathbb{Q}(\sqrt{q})$$

which is a contradiction as per the choice of p. Therefore, we can say that

$$t|[\mathbb{F}_p^* : \langle q, r, s \rangle] \ \Rightarrow \ t > x^{\frac{1}{4}+\epsilon} \ \Rightarrow \ |\langle q, r, s \rangle| < x^{\frac{3}{4}-\epsilon}$$

Now, we will require the following result to count the number of such exceptional primes p for which $|\langle q, r, s \rangle| < x^{\frac{3}{4}-\epsilon}$.

Lemma 2.4 *Let us consider the following set*

$$G = \left\{ q^a r^b s^c \ : \ a, b, c \in \mathbb{Z} \right\}$$

and let G_p be the reduction of G modulo p for any prime $p > \max(q, r, s)$. Then

$$\#\{p \ : \ |G_p| < y\} \ = \ O(y^{\frac{4}{3}})$$

Proof. To prove this lemma, we first count the 3-tuples $(a, b, c) \in \mathbb{Z}^3$ such that $|a| + |b| + |c| \leq Y$. Now, by lattice point counting arguments within a sphere, we know that in such a case $|G_p| \geq \frac{4}{3}Y^3 + O(Y^2)$. To get the situation of the lemma, i.e, $|G_p| < y$, we choose $Y = y^{\frac{1}{3}}$. Now, if $|G_p| < y$, then there exists at least two distinct 3-tuples (a, b, c) and (e, f, g) such that

$$q^a r^b s^c \equiv q^e r^f s^g \pmod{p}$$

Now, as we do not necessarily know whether $a > e$, $b > f$ or $c > g$, we can conclude at this point that p divides the numerator of $(q^{a-e} r^{b-f} s^{c-g} - 1)$ where

$|a-e|+|b-f|+|c-g| \leq 2Y$. The number of such 3-tuples, by the previous argument, is $\frac{4}{3}(2Y)^3 + O(Y^2)$ and each such 3-tuple gives rise to at most $O(Y)$ number of prime factors in the numerator. So, the number of primes p which satisfy $|G_p| < y$ is $O(Y^4)$, i.e, $O(y^{\frac{4}{3}})$. Hence the result follows. □

Using Lemma 2.4, we get that the number of exceptional primes p for which $|\langle q, r, s\rangle| < x^{\frac{3}{4}-\epsilon}$ is $O(x^{1-\epsilon})$. This is the count of the exceptional primes for which $\mathbb{F}_p^* \neq \langle q, r, s\rangle$, out of the initial set of $\frac{\delta x}{\log^2 x}$ primes. Hence, the result follows. □

Proof of Lemma 2.2

Let us consider g to be a primitive root of p and let us take

$$q \equiv g^{a_1} \pmod{p}, \quad r \equiv g^{a_2} \pmod{p}, \quad s \equiv g^{a_3} \pmod{p}$$

If we write $a = (a_1, a_2, a_3)$, then $a \not\equiv 0 \pmod 2$ as $\gcd(a_1, a_2, a_3, p-1) = 1$. In that case, if V be the subspace of $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^3$ orthogonal to $\langle a\rangle$, then $\dim(V) = 2$. The conditions (i) and (ii) imply that $|S_V| \geq 7$. Now, an element $u \in S_V$ will generate a primitive root $(q, r, s)^u \pmod p$ if and only if $a_1u_1 + a_2u_2 + a_3u_3 = a \cdot u$ is coprime to $(p-1)$. We know that $2 \nmid a \cdot u$ for all $u \in S_V$. Furthermore, if we pick any 3 elements $u, v, w \in S_V$, then for each odd prime $t|(p-1)$, t will divide at most two of the numbers $a \cdot u$, $a \cdot v$, $a \cdot w$. Hence, there exists at least one element $u \in S_V$ for which $\gcd(a \cdot u, p-1) = 1$ and therefore we will obtain at least one primitive root $(q, r, s)^u \pmod p$. □

2.2 Result 2: Heath-Brown

In 1986, D. R. Heath-Brown [10] introduced an improvement of Gupta and Murty's result. He reduced down the critical set S, as defined in Theorem 2.1, to a set of size 3 instead of 13. The result he proved is as follows.

Theorem 2.2 (Heath-Brown, 1986) *Let us define the following set of multiplicatively independent non-zero integers*

$$\tilde{S} = \{q, r, s\}$$

that is if $q^e r^f s^g = 1$ then $e = f = g = 0$ for any $e, f, g \in \mathbb{Z}$. Now, if we suppose that none of $q, r, s, -3qr, -3qs, -3rs, qrs$ is a square, then at least for one $a \in \tilde{S}$, we have

$$N_a(x) \gg \frac{x}{\log^2 x}$$

2.2.1 Proof of Theorem 2.2

The proof of this theorem relies on some crucial results and their improved versions. We will first state the lemmas and prove the theorem based on those, and prove the lemmas thereafter in the following subsection.

Lemmas and their refinements

The improvement proposed by Heath-Brown is primarily based on an strengthened version of the sieve result stated as Lemma 2.3 by Gupta and Murty [7]. Let us define a statement "$n = P_r(\alpha)$" as follows.

Definition 2.1

$$\text{“}n = P_r(\alpha)\text{”} \;\Rightarrow\; \text{“}n \textit{ is a prime}\text{” OR}$$
$$\text{“}n = \prod_{i=1}^{k} p_i \;\; \textit{for } k \leq r \textit{ and } p_i > n^{\alpha} \;\forall\; i = 1, ..., k\text{”}$$

In view of this, Heath-Brown showed the following result.

Lemma 2.5 *Let $K = 2^k$ for $k = 1, 2$ or 3. Also let u and v be coprime integers such that $K|(u-1)$, $16|v$ and $\left(\frac{u-1}{K}, v\right) = 1$. Then there exists an $\alpha \in (\frac{1}{4}, \frac{1}{2}]$, possibly depending on k, u, v such that*

$$\#\left\{p \leq x \;:\; p \equiv u \pmod{v}, \frac{p-1}{K} = P_2(\alpha)\right\} \gg \frac{x}{\log^2 x}$$

where the implied constant may depend on k, u, v and α.

Proof. Proved in Section 2.2.2.

Now let us define another statement "$n = P_r(\alpha, \delta)$" as follows.

Definition 2.2

$$\text{“}n = P_r(\alpha, \delta)\text{”} \;\Rightarrow\; \text{“}n \textit{ is a prime}\text{” OR}$$
$$\text{“}n = \prod_{i=1}^{k} p_i \;\; \textit{for } k \leq r \textit{ and } n^{\alpha} < p_i < n^{\frac{1}{2}-\delta} \;\forall\; i = 1, ..., k\text{”}$$

Based on this definition, Heath-Brown modifies Lemma 2.5 to get a refined sieve result as follows.

Lemma 2.6 *Let us suppose K, k, u, v are defined as in Lemma 2.5. Then there exist $\alpha \in (\frac{1}{4}, \frac{1}{2})$ and $\delta \in (0, \frac{1}{2} - \alpha)$ such that*

$$\#\left\{p \leq x \ : \ p \equiv u \pmod{v}, \frac{p-1}{K} = P_2(\alpha, \delta)\right\} \gg \frac{x}{\log^2 x}$$

Proof. Proved in Section 2.2.2.

Construction of K, u and v

It is evident that if an integer is a quadratic residue modulo p, it cannot be a primitive root. Hence, we want to construct the integers K, u and v as defined in Lemma 2.5 such that q, r and s each are quadratic non-residues of every prime $p \equiv u \pmod{v}$. This choice of K, u, v will depend only on q, r and s. We can first observe the following result.

Claim 2.1 *The following equation has infinitely many solutions in prime p.*

$$\left(\frac{-3}{p}\right) = \left(\frac{q}{p}\right) = \left(\frac{r}{p}\right) = \left(\frac{s}{p}\right) = -1$$

Proof. We know that for a fixed integer n, which is not a perfect square, we will get $\sum_{p \leq x} \left(\frac{n}{p}\right) = o(\pi(x))$ as $x \to \infty$. Now, let us run n over all the 16 numbers $(-3)^e q^f r^g s^h$ with $0 \leq e, f, g, h \leq 1$. In this case, n cannot be a square if $e+f+g+h$ is odd, since q, r, s are multiplicatively independent as per the assumption of the theorem. Hence we get

$$\sum_{p \leq x} \left[1 - \left(\frac{-3}{p}\right)\right]\left[1 - \left(\frac{q}{p}\right)\right]\left[1 - \left(\frac{r}{p}\right)\right]\left[1 - \left(\frac{s}{p}\right)\right] = \sum_n (-1)^{e+f+g+h} \sum_{p \leq x} \left(\frac{n}{p}\right)$$

asymptotically approaching $O(\pi(x))$ as $x \to \infty$. Now, if any one of $\left(\frac{-3}{p}\right), \left(\frac{q}{p}\right), \left(\frac{r}{p}\right)$ or $\left(\frac{s}{p}\right)$ is 1, the term in the summand above will be 0. But as the sum is $O(\pi(x))$,

$$\left(\frac{-3}{p}\right) = \left(\frac{q}{p}\right) = \left(\frac{r}{p}\right) = \left(\frac{s}{p}\right) = -1$$

must have infinitely many solutions in primes p. Hence, the result follows. □

With the above result in mind, let us fix a particular prime p_0 satisfying the equation in Claim 2.1. We see that $p_0 \equiv 5 \pmod{6}$ as -3 is a quadratic non-residue modulo p_0. Now, for each odd prime $l | qrs$, let us take $u_l = p_0$ if $l \nmid (p_0 - 1)$ and $u_l = 4p_0$ if $l | (p_0 - 1)$. We get the following result in such a case.

Claim 2.2 *$l \nmid (u_l - 1)$ in each of the cases discussed above.*

Proof. If $l \nmid (p_0 - 1)$, setting $u_l = p_0$ ensures $l \nmid (u_l - 1)$. In the case where $l|(p_0 - 1)$, since $p_0 \equiv 5 \pmod 6$, we can write $p_0 = 6j + 5$ and $l|(6j + 4) \Rightarrow l|(3j + 2)$, as l is odd. But in such a case, setting $u_l = 4p_0$ gives $u_l - 1 = 24j + 19 = 8(3j + 2) + 3$ and hence $l \nmid (u_l - 1)$. □

Let us also define $u_2 = p_0$ if $16 \nmid (p_0 - 1)$ and $u_2 = p_0 - 8$ if $16|(p_0 - 1)$. Let us set u to be solution of the simultaneous congruence equations $u \equiv u_2 \pmod{16}$ and $u \equiv u_l \pmod l$. Such a solution exists by the Chinese Remainder Theorem. So, we get that if $2^k|(u - 1)$, then k can be either 1,2 or 3 from the u_2 congruence relation. Again if we set $v = 16qrs$, then $l \nmid (u - 1)$ for any odd prime $l|v$, from the u_l congruence conditions. Hence, $\left(\frac{u-1}{K}, v\right) = 1$ if we set $K = 2^k$ to be the highest power of 2 dividing $u - 1$.

Further, if $p \equiv u \pmod v$ then $p \equiv p_0 \pmod 8$ and $p \equiv p_0$ or $4p_0 \pmod l$ for every odd prime $l|v$. Thus $\left(\frac{q}{p}\right) = \left(\frac{q}{p_0}\right) = -1$, and similar for r and s. Now, based on this construction of K, u and v, we will prove the theorem.

Proof of Theorem 2.2

As the construction of K, u and v satisfy the conditions of Lemma 2.6, we can conclude that there exists a constant c such that there are at least $cx/\log^2 x$ primes $p \leq x$ satisfying $p \not\equiv 1 \pmod{16}$, $(p - 1)/K = P_2(\alpha, \delta)$ and $\left(\frac{q}{p}\right) = \left(\frac{r}{p}\right) = \left(\frac{s}{p}\right) = -1$. Now, two cases may arise. Either $(p - 1)/K$ is a prime or it is a product of two primes p_1 and p_2.

Let us consider the first case, where $(p - 1)/K$ is a prime itself. In such a case, an element q can have order K or $p - 1$ in the group $(\mathbb{Z}/p\mathbb{Z})^*$. Again, at least one of q, r and s is not equal to ± 1 as they are multiplicatively independent. Hence, q is a primitive root modulo p if $p > q^K$. Same argument holds for r and s.

Considering the second case, let $(p - 1)/K = p_1 p_2$ with $p^\alpha \leq p_1 \leq p^{1/2-\delta}$ where $\alpha > \frac{1}{4}$ and $\delta > 0$. In this case, an element q may have order K, Kp_1, Kp_2 or $Kp_1p_2 = p - 1$. For large enough $p > q^K$, we can eliminate the first possibility. Let us try to estimate the number of primes $p \leq x$ for which q has order Kp_1.

$$\begin{aligned}\#\left\{p \leq x \ : \ \operatorname{ord}(q) = e \leq x^{\frac{1}{2}-\delta}\right\} &\leq \sum_{e \leq x^{1/2-\delta}} \#\{p|(q^e - 1)\} \\ &\ll \sum_{e \leq x^{1/2-\delta}} \log(q^e - 1) \ll \sum_{e \leq x^{1/2-\delta}} e \ll x^{1-2\delta}\end{aligned}$$

So, for a fixed q, there are $O\left(x^{1-2\delta}\right) = o(x/\log^2 x)$ primes $p \leq x$ for which one or more of q, r or s has order Kp_1.

Now let us consider the case where q, r and s all have order Kp_2. In this case, all the numbers $n = q^e r^f s^g$ with $0 \leq e, f, g \leq 3x^{(1-\alpha)/3}$ satisfy the relation $n^{Kp_2} \equiv 1 \pmod{p}$ so that n takes at most Kp_2 values modulo p. But there are at least $27x^{1-\alpha} \geq 27p^{1-\alpha} \geq 27p_2$ triples (e, f, g). Hence, by the pigeon hole principle, there must be two distinct triples (e_1, f_1, g_1) and (e_2, f_2, g_2) such that

$$q^{e_1} r^{f_1} s^{g_1} \equiv q^{e_2} r^{f_2} s^{g_2} \pmod{p} \Rightarrow q^{e_1 - e_2} r^{f_1 - f_2} s^{g_1 - g2} \equiv 1 \pmod{p}$$

So, p divides the numerator of a number $N = q^e r^f s^g - 1$ where $|e|, |f|, |g| \leq 3x^{(1-\alpha)/3}$ and $(e, f, g) \neq (0, 0, 0)$. The number of such prime factors p of the numerator of N is bounded by $\log |N| \ll \max(|e|, |f|, |g|) \ll x^{(1-\alpha)/3}$. Again, the number of triples (e, f, g) is $O(x^{1-\alpha})$. Hence the total number of possible primes $p \leq x$ for which q, r and s all has order Kp_2 is $O(x^{4(1-\alpha)/3}) = o(x/\log^2 x)$.

The analysis in the above two cases cover all the situations where none of q, r or s is a primitive root of p. The number of such primes $p \leq x$ is $o(x/\log^2 x)$. This proves the theorem. □

2.2.2 Proof of Lemmas

Proof of Lemma 2.5

To prove this Lemma, we will need to use the following result (Lemma 2.7) as a platform. But, let us introduce a new term before that.

Definition 2.3 *Recall that an arithmetic function is any function $f : \mathbb{Z}^+ \to \mathbb{C}$. Let $Q \geq 1$ and let $\lambda(q)$ be an arithmetic function with support $[1, Q]$. Suppose that for any $M, N \geq 1$ with $MN = Q$, we can write λ as a convolution*

$$\lambda(q) = \sum_{\substack{mn=q \\ m \leq M, n \leq N}} \alpha(m)\beta(n)$$

where α and β are arithmetic functions which may depend on M and N respectively, and for which $|\alpha(m)|, |\beta(n)| \leq 1$. Then we can say that λ is "a well factorable function of level Q".

Let us also define $\pi(x; a, b) = \#\{p \leq x \ : \ p \text{ prime}, p \equiv b \pmod{a}\}$. Based on these definitions, we can state the following result.

Lemma 2.7 *Let $(u,v)=1$ and for any q such that $(q,v)=1$, define u^* to be the solution of the congruences $u^* \equiv u \pmod{v}$ and $u^* \equiv 1 \pmod{q}$. Then, for any well factorable function λ of level $x^{\frac{4}{7}-\epsilon}$, we have, for $\epsilon, A > 0$*

$$\sum_{(q,v)=1} \lambda(q) \left(\pi(x; qv, u^*) - \frac{\mathrm{li}(x)}{\phi(qv)} \right) \ll \frac{x}{(\log x)^A}$$

where the implied constant may depend on u, v, ϵ and A.

Proof. If we look at the result closely, we will see that we are counting primes p which satisfy the following condition

$$p \equiv u^* \pmod{qv} \Rightarrow p \equiv 1 \pmod{q} \text{ and } p \equiv u \pmod{v}$$

Counting the primes for the first condition $p \equiv 1 \pmod{q}$ can be performed using the following result by Bombieri, Friedlander and Iwaniec [3].

Proposition 2.1 *Let $a \neq 0$, $\epsilon > 0$ and $Q = x^{\frac{4}{7}-\epsilon}$. For any well factorable function $\lambda(q)$ of level Q and any $A > 0$ we have*

$$\sum_{(q,a)=1} \lambda(q) \left(\psi(x; q, a) - \frac{x}{\phi(q)} \right) \ll \frac{x}{(\log x)^A}$$

where the constant implied depends at most on ϵ, a and A and

$$\psi(x; q, a) = \sum_{\substack{n \leq x \\ n \equiv a \pmod{q}}} \Lambda(n)$$

with Λ being the von Mangoldt function.

Proof. See the proof of Theorem 10 in [3]. □

Based on Proposition 2.1, let us choose the constant a to be 1 and write ψ in terms of π using partial summation as follows [1]

$$\begin{aligned}
\psi(x; q, a) &= \sum_{\substack{n \leq x \\ n \equiv a \pmod{q}}} \Lambda(n) = \sum_{\substack{p^m \leq x \\ p^m \equiv a \pmod{q}}} \log p \\
&= \sum_{\substack{p \leq x \\ p \equiv a \pmod{q}}} \log p + O\left(\frac{x}{(\log x)^B} \right) \text{ for some } B \geq 1 \\
&= \log x \sum_{\substack{p \leq x \\ p \equiv a \pmod{q}}} 1 + O\left(\frac{x}{(\log x)^B} \right) \text{ summing by parts} \\
&= \log x \cdot \pi(x; q, a) + O\left(\frac{x}{(\log x)^B} \right)
\end{aligned}$$

Now, we have to take care that we are counting primes p satisfying the second condition $p \equiv u \pmod{v}$ as well. To count these primes, a simple modification in the proof of Theorem 10 in [3] will be required. The proof of Theorem 10 relies on the Theorems 1, 2 and 5* of [3]. So, to introduce the second condition, we can modify these theorems slightly and complete the proof of Theorem 10 [3] in that line. The sketch of the proof with the modifications is outlined in [10], pp 29-30. $\square$

Now, let us turn our attention to the proof of Lemma 2.5. Define the following two sets

$$\mathcal{A} = \left\{ \frac{p-1}{K} \ : \ p \leq x, \ p \equiv u \pmod{v} \right\}$$

$$\text{and} \quad \mathcal{B} = \{ p \leq x \ : \ p = 1 + Kp_1p_2p_3 \text{ with some } p_i \geq x^{\alpha}, \text{ and } p \equiv u \pmod{v} \}$$

where the different orderings of p_1, p_2 and p_3 are counted distinctly, so that $\mathcal{B}$ is a multiset. Now, if p is chosen such that $\frac{p-1}{K} \in \mathcal{A}$, and if $\frac{p-1}{K}$ has no prime factors less than x^{α}, then either $\frac{p-1}{K} = P_2(\alpha)$ or $\frac{p-1}{K} \in \mathcal{B}$. Considering all the 6 orderings of p_1, p_2 and p_3 in $\mathcal{B}$, we obtain that

$$\begin{aligned} & \# \left\{ p \leq x \ : \ p \equiv u \pmod{v}, \frac{p-1}{K} = P_2(\alpha) \right\} \\ & \geq \ \# \{ a \in \mathcal{A} \ : \ (a, P(x^{\alpha})) = 1 \} \ - \ \frac{1}{6} \# \{ p \in \mathcal{B} \ : \ p \text{ prime} \} \ + \ O\left(x^{1-\alpha}\right) \\ & = \ S(\mathcal{A}, x^{\alpha}) \ - \ \frac{1}{6} S\left(\mathcal{B}, x^{\frac{1}{2}}\right) \ + \ O\left(x^{1-\alpha}\right) \end{aligned}$$

in the usual sieve theory notation [4], where $P(x^{\alpha})$ denotes the product of all the primes below x^{α} and $S(\mathcal{A}, y)$ denotes the set of all elements from $\mathcal{A}$ which have no prime divisors less than y.

Let us start off by estimating $S(\mathcal{A}, x^{\alpha})$. If $(q, v) = 1$, then in the notation of Lemma 2.7, we can write

$$\# \{ a \in \mathcal{A} \ : \ q | a \} \ = \ \pi(x; qv, u^*) \ = \ \frac{\text{li} x}{\phi(qv)} \ + \ r(q)$$

say, where $r(q)$ denotes the remainder term in the sieving process. Note that we have $u \equiv 1 \pmod{K}$, $v \equiv 0 \pmod{K}$ and $(q, v) = 1$. Thus, if $p \equiv u \pmod{v}$ then $p \equiv 1 \pmod{Kq} \ \Leftrightarrow \ p \equiv 1 \pmod{q}$. Now, we can estimate $S(\mathcal{A}, x^{\alpha})$ using the linear sieve with Iwaniec's bilinear form of the remainder term (Theorem 4, [12]). If f be the usual lower bound function of the linear sieve and if we choose $\mu \in [2\alpha, 1]$, then for any $\epsilon > 0$, there exist x_0 and N, depending on ϵ, v and μ such that

$$S(\mathcal{A}, x^{\alpha}) \ \geq \ \frac{\text{li} x}{\phi(v)} \prod_{p \leq x^{\alpha}} \left(1 - \frac{\omega(p)}{p}\right) \left(f\left(\frac{\mu}{\alpha}\right) - \epsilon \right) \ - \ R_0 \ - \ \sum_{n=1}^{N} R_n$$

for $x \geq x_0$, where $\omega(p) = \frac{p}{\phi(p)}$ and the remainder terms are

$$R_0 = \sum_{q<x^{\frac{1}{4}},(q,v)=1} |r(q)| \quad \text{and} \quad R_n = \sum_{(q,v)=1} \lambda_n(q) r(q)$$

for some well factorable function λ_n of level x^μ. Here, we can easily restrict our attention to the primes $p \nmid v$ since the elements of $\mathcal{A}$ are inherently coprime to v because of the condition $\left(\frac{u-1}{K}, v\right) = 1$. Also, we have $r(q) = O\left(\frac{x}{\log^A x}\right)$ from Lemma 2.7 and hence by Bombieri's theorem [4], we obtain $R_0 = O\left(\frac{x}{\log^3 x}\right)$. Lemma 2.7 also gives us $R_n = O\left(\frac{x}{\log^3 x}\right)$ if we choose $\mu < \frac{4}{7}$. Hence, it follows that, for x large enough

$$S\left(\mathcal{A}, x^\alpha\right) \;\geq\; \frac{\mathrm{li} x}{\phi(v)} \prod_{\substack{p \leq x^\alpha \\ p \nmid v}} \left(1 - \frac{1}{p-1}\right) \left(f\left(\frac{4}{7\alpha}\right) - 2\epsilon\right)$$

Let us now turn our attention to $S\left(\mathcal{B}, x^{\frac{1}{2}}\right)$. We observe that for $(q, v) = 1$,

$$\#\{b \in \mathcal{B} \;:\; q|b\} \;=\; \#\left\{p_1 p_2 p_3 \leq \frac{x-1}{K} \;:\; p_i \geq x^\alpha, p_1 p_2 p_3 \equiv l \pmod{\frac{qv}{K}}\right\}$$

where l is a common solution to the congruences $Kl+1 \equiv u \pmod{v}$ and $Kl+1 \equiv 0 \pmod{q}$. Let us define the following terms

$$\begin{aligned} \pi(X; a, d, l) \;&=\; \#\left\{p \leq \frac{X}{a} \;:\; ap \equiv l \pmod{d}\right\} \\ g(a) \;&=\; \#\left\{p_2 p_3 = a \;:\; p_2, p_3 \geq x^\alpha\right\} \\ \text{and} \quad Y \;&=\; \frac{1}{\phi(v/K)} \sum_{a \leq \frac{y}{x^\alpha}} g(a) \left(\pi\left(\frac{y}{a}\right) - \pi\left(x^\alpha\right)\right) \end{aligned}$$

where $y = \frac{x-1}{K}$. Then, for $(q, v) = 1$, we have

$$\begin{aligned} \#\{b \in \mathcal{B} \;:\; q|b\} \;&=\; \sum_{a \leq \frac{y}{x^\alpha}} g(a) \left(\pi\left(y; a, \frac{qv}{K}, l\right) - \pi\left(ax^\alpha; a, \frac{qv}{K}, l\right)\right) \\ &=\; Y \frac{\omega(q)}{q} + r_q \end{aligned}$$

where $\omega(q) = \frac{q}{\phi(q)}$ as before and the remainder is

$$r_q = \sum_{a \leq \frac{y}{x^\alpha}} g(a) \left[\left(\pi\left(y; a, \frac{qv}{K}, l\right) - \frac{\pi(y/a)}{\phi(qv/K)}\right) - \left(\pi\left(ax^\alpha; a, \frac{qv}{K}, l\right) - \frac{\pi(x^\alpha)}{\phi(qv/K)}\right)\right]$$

We can now use the upper bound linear sieve [13] to show that for positive constants ϵ and A, there exists an $x_0(\epsilon, A)$ for which

$$S\left(\mathcal{B}, x^{\frac{1}{2}}\right) \ \leq \ Y \prod_{\substack{p \leq x^{\frac{1}{2}} \\ p \nmid v}} \left(1 - \frac{\omega(p)}{p}\right) (F(1) + \epsilon) \ + \ R$$

for $x \geq x_0$, with F being the usual upper bound function for which $F(1) = 2e^{\gamma}$ where γ is the Euler's constant. Note that we are again taking the estimate over the primes $p \nmid v$ because the condition $(u, v) = 1$ implies $(b, v) = 1$ for all $b \in \mathcal{B}$. The remainder term R is given by

$$R \ = \sum_{\substack{q \leq x^{\frac{1}{2}} (\log x)^{-A} \\ (q,v)=1}} |r_q|$$

To estimate this remainder term, let us first try estimating the error r_q by

$$r_q^{'} = \sum_{\substack{a \leq \frac{y}{x^{\alpha}} \\ (a, \frac{qv}{K})=1}} g(a) \left[\left(\pi\left(y; a, \frac{qv}{K}, l\right) - \frac{\pi(y/a)}{\phi(qv/K)} \right) - \left(\pi\left(ax^{\alpha}; a, \frac{qv}{K}, l\right) - \frac{\pi(x^{\alpha})}{\phi(qv/K)} \right) \right]$$

Since we have $(qv/K, l) = 1$, it implies $\pi\left(y; a, \frac{qv}{K}, l\right) = \pi\left(ax^{\alpha}; a, \frac{qv}{K}, l\right) = 0$ for $(a, qv/K) \neq 1$. Furthermore, $\frac{\pi(y/a)}{\phi(qv/K)} \ll \frac{x \log x}{aq}$ and $\frac{\pi(x^{\alpha})}{\phi(qv/K)} \ll \frac{x \log x}{aq}$. Thus

$$\begin{aligned} r_q - r_q^{'} \ &\ll \sum_{\substack{a \leq x^{1-\alpha} \\ (a, qv/K) \neq 1}} g(a) \frac{x \log x}{aq} \\ &\ll \frac{x \log x}{q} \sum_{\substack{p_2 | qv/K \\ p_2 \geq x^{\alpha}}} \frac{1}{p_2} \left(\sum_{x^{\alpha} \leq p_3 \leq x^{1-\alpha}/p_2} \frac{1}{p_3} \right) \\ &\ll \frac{x \log x}{q} x^{-\alpha} \log x \ = \ \frac{x^{1-\alpha} \log^2 x}{q} \end{aligned}$$

So, if we replace r_q by $r_q^{'}$ to write

$$R^{'} \ = \sum_{\substack{q \leq x^{\frac{1}{2}} (\log x)^{-A} \\ (q,v)=1}} \left| r_q^{'} \right|$$

then $R = R^{'} + O\left(x^{1-\alpha} \log^3 x\right)$. Using Theorem 3 by Pan [17], we can now bound $R^{'}$ by $O\left(\frac{x}{\log^3 x}\right)$ by taking sufficiently large value of A. We are now left with estimating Y to calculate an upper bound for $S\left(\mathcal{B}, x^{\frac{1}{2}}\right)$. In Y, the term involving $\pi(x^{\alpha})$

contributes $O\left(\frac{x}{\log^2 x}\right)$. Using prime number theorem on $\pi(y/a)$ and summation by parts thereafter, we obtain

$$\begin{aligned} Y &\sim \frac{x/K}{\log x} \cdot \frac{1}{\phi(v/K)} \iint_{\substack{\theta,\psi \geq \alpha \\ \theta+\psi \leq 1-\alpha}} \frac{1}{1-\theta-\psi} \frac{d\theta}{\theta} \frac{d\psi}{\psi} \\ &= \frac{x}{\phi(v) \log x} \int_{\alpha}^{1-2\alpha} \log\left(\frac{1-\alpha-\theta}{\alpha}\right) \frac{d\theta}{\theta(1-\theta)} \end{aligned}$$

Again, the product term in $S\left(\mathcal{B}, x^{\frac{1}{2}}\right)$ can be estimated as

$$\begin{aligned} \prod_{\substack{p \leq X \\ p \nmid v}} \left(1 - \frac{\omega(p)}{p}\right) &= \prod_{\substack{p \leq X \\ p \nmid v}} \left(1 - \frac{1}{p-1}\right) \\ &\sim 2 \prod_{2 < p \leq X} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{\substack{p \mid v \\ 2 < p \leq X}} \left(\frac{p-1}{p-2}\right) \prod_{p \leq X} \left(1 - \frac{1}{p}\right) \\ &\sim \frac{2e^{-\gamma}}{\log X} \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{\substack{p \mid v \\ p>2}} \left(\frac{p-1}{p-2}\right) \end{aligned}$$

Combining the estimates of $S(\mathcal{A}, x^{\alpha})$ and $S\left(\mathcal{B}, x^{\frac{1}{2}}\right)$, we obtain

$$\begin{aligned} &\# \left\{ p \leq x \,:\, p \equiv u \pmod{v}, \frac{p-1}{K} = P_2(\alpha) \right\} \\ &\geq (1+o(1)) \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{\substack{p \mid v \\ p>2}} \left(\frac{p-1}{p-2}\right) \\ &\times \frac{x}{\phi(v) \log^2 x} \left(\frac{2e^{-\gamma}}{\alpha} f\left(\frac{4}{7\alpha}\right) - \frac{1}{6} \cdot 2e^{-\gamma} \cdot 4IF(1) \right) \end{aligned}$$

where f and F denote the usual bound functions of a linear sieve and I denotes the integral

$$I = \int_{\alpha}^{1-2\alpha} \log\left(\frac{1-\alpha-\theta}{\alpha}\right) \frac{d\theta}{\theta(1-\theta)}$$

If $2 \leq t \leq 4$ then $f(t) = 2e^{\gamma} t^{-1} \log(t-1)$. Hence for $\frac{1}{7} \leq \alpha \leq \frac{2}{7}$, we have

$$\frac{2e^{-\gamma}}{\alpha} f\left(\frac{4}{7\alpha}\right) - \frac{1}{6} \cdot 2e^{-\gamma} \cdot 4IF(1) = 7 \log\left(\frac{4}{7\alpha} - 1\right) - \frac{8}{3} I$$

which is continuous in α. So, it is sufficient to prove that this term is positive when $\alpha = \frac{1}{4}$. For $\alpha = \frac{1}{4}$, we have

$$\begin{aligned} 7 \log\left(\frac{16}{7} - 1\right) - \frac{8}{3} \int_{\frac{1}{4}}^{\frac{1}{2}} \frac{\log(3-4\theta)}{\theta(1-\theta)} d\theta &\geq 7 \log \frac{9}{7} \int_{\frac{1}{4}}^{\frac{1}{2}} \frac{2-4\theta}{\theta(1-\theta)} d\theta \\ &= 7 \log \frac{9}{7} - \frac{8}{3} \log \frac{16}{9} \geq 0.225 > 0 \end{aligned}$$

Hence, for some $\alpha \in \left(\frac{1}{4}, \frac{1}{2}\right]$, we will have

$$\#\left\{p \leq x \ : \ p \equiv u \pmod{v}, \frac{p-1}{K} = P_2(\alpha)\right\} \ \gg \ \frac{x}{\log^2 x}$$

□

Proof of Lemma 2.6

The base for this lemma is Lemma 2.5 and we will improve upon that to prove this result. Now, in Lemma 2.6, we are supposed to count

$$\begin{aligned}
&\#\left\{p \leq x \ : \ p \equiv u \pmod{v}, \left(\frac{p-1}{K}\right)^{\frac{1}{2}-\delta} \geq p_1 \geq \left(\frac{p-1}{K}\right)^{\alpha}\right\} \\
&= \ \#\left\{p \leq x \ : \ p \equiv u \pmod{v}, p_1, p_2 \geq \left(\frac{p-1}{K}\right)^{\alpha}\right\} \\
&\quad - \ 2 \cdot \#\left\{p \leq x \ : \ p = 1 + Kp_1p_2, \ p_1 \geq \left(\frac{p-1}{K}\right)^{\frac{1}{2}-\delta}, \ p_1 \leq \left(\frac{p-1}{K}\right)^{\alpha}\right\}
\end{aligned}$$

as we should count for both p_1 and p_2 in the second term. Let us assume that the implied constant in Lemma 2.5 is c where $c > 0$. Lemma 2.5 tells us that in the given situation, there exists an $\alpha \in (\frac{1}{4}, \frac{1}{2}]$ such that

$$\#\left\{p \leq x \ : \ p \equiv u \pmod{v}, p_1, p_2 \geq \left(\frac{p-1}{K}\right)^{\alpha}\right\} \ = \ \frac{cx}{\log^2 x} + o\left(\frac{x}{\log^2 x}\right)$$

where $p = 1 + Kp_1p_2$. Hence, we have the following

$$\begin{aligned}
&\#\left\{p \leq x \ : \ p \equiv u \pmod{v}, \left(\frac{p-1}{K}\right)^{\frac{1}{2}-\delta} \geq p_1 \geq \left(\frac{p-1}{K}\right)^{\alpha}\right\} \\
&= \ \frac{cx}{\log^2 x} \ + \ o\left(\frac{x}{\log^2 x}\right) \\
&\quad - \ 2 \cdot \#\left\{p \leq x \ : \ p = 1 + Kp_1p_2, \ p_1 \geq \left(\frac{p-1}{K}\right)^{\frac{1}{2}-\delta}, p_1 \leq \left(\frac{p-1}{K}\right)^{\alpha}\right\} \\
&= \ \frac{cx}{\log^2 x} \ + \ o\left(\frac{x}{\log^2 x}\right) \\
&\quad - \ 2 \cdot \#\left\{\frac{x}{\log^2 x} \leq p \leq x \ : \ p = 1 + Kp_1p_2, \ p_1 \geq p^{\frac{1}{2}-\delta}, p_1 \leq p^{\alpha}\right\}
\end{aligned}$$

as the number of primes below $\frac{x}{\log^2 x}$ is $o\left(\frac{x}{\log^2 x}\right)$. Again, for $\frac{x}{\log^2 x} \leq p \leq x$, we have

$$\begin{aligned}
&p_1 \leq p^{\alpha} \ \Rightarrow \ p_1 \leq p^{\frac{1}{2}} \leq x^{\frac{1}{2}} \\
\text{and} \quad &p_1 \geq p^{\frac{1}{2}-\delta} \ \Rightarrow \ p_1 \geq \left(\frac{x}{\log^2 x}\right)^{\frac{1}{2}-\delta} = x^{\frac{1}{2}-\delta}(\log x)^{1-2\delta} \geq x^{\frac{1}{2}-2\delta}
\end{aligned}$$

as long as x is large enough such that $\log x \leq x^{\frac{\delta}{2\delta-1}}$. Hence, we obtain

$$\begin{aligned}
&\#\left\{p \leq x \ : \ p \equiv u \pmod{v}, \left(\frac{p-1}{K}\right)^{\frac{1}{2}-\delta} \geq p_1 \geq \left(\frac{p-1}{K}\right)^{\alpha}\right\} \\
&= \frac{cx}{\log^2 x} + o\left(\frac{x}{\log^2 x}\right) \\
&\quad - 2 \cdot \#\left\{\frac{x}{\log^2 x} \leq p \leq x \ : \ p = 1 + Kp_1p_2, \ p_1 \geq p^{\frac{1}{2}-\delta}, p_1 \leq p^{\alpha}\right\} \\
&= \frac{cx}{\log^2 x} + o\left(\frac{x}{\log^2 x}\right) \\
&\quad - 2 \cdot \#\left\{p \leq x \ : \ p = 1 + Kp_1p_2, \ x^{\frac{1}{2}-2\delta} \leq p_1 \leq x^{\frac{1}{2}}\right\}
\end{aligned}$$

and it suffices to prove that

$$\#\left\{p \leq x \ : \ p = 1 + Kp_1p_2, \ x^{\frac{1}{2}-2\delta} \leq p_1 \leq x^{\frac{1}{2}}\right\} \leq \frac{cx}{2\log^2 x}$$

Now, Theorem 3.12 in [9] states

Proposition 2.2 *Let a, b, k, l be integers satisfying $ab \neq 0$, $(a, b) = 1$, $2|ab$ and $(k, l) = 1$ for $1 \leq k \leq \log^A x$. Then as $x \to \infty$, we have, uniformly in a, b, k, l, that*

$$\#\left\{p \leq x \ : \ p \equiv l \pmod{k}, ap + b = p'\right\} \ \ll \ \frac{x}{\log^2 x} \prod_{\substack{p|kab \\ p \neq 2}} \frac{p-1}{p-2}$$

Proof. Please refer to the proof of Theorem 3.12 in [9]. □

Let us take $p = p_2$, $a = Kp_1$, $b = 1$, $p' = p$ in the proposition and ignore the congruence criterion to obtain

$$\#\left\{p_2 \leq X \ : \ Kp_1p_2 + 1 = p\right\} \ \ll \ \frac{X}{\log^2 X}\left(\frac{p_1-1}{p_1-2}\right)$$

Now, if we take $X = \frac{x-1}{Kp_1}$ so as to count all primes $p \leq x$, we get

$$\#\left\{p_2 \leq \frac{x-1}{Kp_1} \ : \ Kp_1p_2 + 1 = p\right\} \ \ll \ \frac{x}{p_1 \log^2 x}$$

Summing this quantity over all p_1 in the range $x^{\frac{1}{2}-2\delta} \leq p_1 \leq x^{\frac{1}{2}}$, we obtain

$$\#\left\{p \leq x \ : \ p = 1 + Kp_1p_2, \ x^{\frac{1}{2}-2\delta} \leq p_1 \leq x^{\frac{1}{2}}\right\} \ \ll \ \frac{x}{\log^2 x} \sum_{x^{\frac{1}{2}-2\delta} \leq p_1 \leq x^{\frac{1}{2}}} \frac{1}{p_1}$$

Again, we observe that

$$\begin{aligned}\sum_{x^{\frac{1}{2}-2\delta}\leq p_1\leq x^{\frac{1}{2}}}\frac{1}{p_1} &\ll \ln\ln\left(x^{\frac{1}{2}}\right)-\ln\ln\left(x^{\frac{1}{2}-2\delta}\right)\\ &= \ln\frac{1}{2}+\ln\ln x-\ln\left(\frac{1}{2}-2\delta\right)-\ln\ln x\\ &= -\ln(1-4\delta) \;=\; O(\delta)\end{aligned}$$

and hence the result follows if the constant δ is chosen to be sufficiently small. □

2.2.3 Corollaries

Corollary 2.1 *Let q, r, s be three non-zero integers which are multiplicatively independent. Suppose that none of $q, r, s, -3qr, -3rs, -3sq$ or qrs is a square. Then*

$$\#\{p \leq x \;:\; \textit{at least one of } q, r \textit{ or } s \textit{ is a primitive root modulo } p\} \gg \frac{x}{\log^2 x}$$

Proof. This comes directly from the statement of Theorem 2.2 for three multiplicatively independent integers. □

Corollary 2.2 *There are at most two positive primes for which Artin's conjecture does not hold.*

Proof. As any three positive primes are always multiplicatively independent, we can take any arbitrary set of three primes and Theorem 2.2 says that Artin's conjecture will be true for at least one of them. Hence, there can only be at most two positive primes for which it fails. □

Corollary 2.3 *There are at most three square free integers greater than 1 for which Artin's conjecture does not hold.*

Proof. Let us consider the converse and assume that Artin's conjecture fails for four distinct square-free integers q, r, s, t, all of which are greater than 1. In the subset $\{q, r, s\}$, Corollary 2.1 holds unless q, r, s are multiplicatively dependent. Now, q, r, s can be multiplicatively dependent only if $q = rs$ or $r = sq$ or $s = qr$. Hence, we must have qrs to be a square. Following a similar argument for the subset $\{q, r, t\}$, we get that qrt has to be a square as well. So, $qrs.qrt = (qr)^2st$ has to be a square, whence st is a square. But as both s and t are square free, we must have $s = t$ for st being a square. This contradicts our assumption of four distinct integers failing Artin's conjecture, and the result follows. □

Corollary 2.4 *Let $S \subset \mathbb{Z}$ be the set of integers for which Artin's conjecture does not hold and also suppose that S does not contain any squares. Then*

$$\#\{n \in S \ : \ |n| \leq x\} \ll \log^2 x$$

Proof. Let us consider $S \subset \mathbb{Z}$ to be a set of integers k for which Artin's conjecture fails and S does not contain any squares. There may be two cases depending on the interdependencies of the elements of S.

Case 1: If no three elements of S are multiplicatively independent, then we can consider S to be contained in a set $\{\pm k_1^a k_2^b \ : \ a, b \geq 0\}$, with $k_1, k_2 \neq 0, \pm 1$. In this case, we quite easily obtain

$$\#\{n \in S \ : \ |n| \leq x\} \ \leq \ \#\{a, b \geq 0 \ : \ |k_1^a k_2^b| \leq x\} \ \ll \ \log^2 x$$

Case 2: If there exists three multiplicatively independent elements $k_1, k_2, k_3 \in S$, at least one of $-3k_1k_2, -3k_2k_3, -3k_3k_1$ is not a square. Without loss of generality, let us assume that $-3k_1k_2$ is not a square. Let us denote the set S_0 to be the subset of S containing all the elements multiplicatively dependent on k_1 and k_2, i.e, S_0 is of the form $\{\pm k_1^a k_2^b \ : \ a, b \geq 0\}$. Then, if $k \in S - S_0$, then for the set of integers $\{k, k_1, k_2\}$, Corollary 2.1 holds unless one of $-3kk_1, -3kk_2$ or kk_1k_2 is a square. As no element in S satisfies Artin's conjecture, we may write $S - S_0 = S_1 \cup S_2 \cup S_3$, where for each S_i, there exists some l_i such that kl_i is a square whenever $k \in S_i$. As k is not a square, l_i cannot be a square either. Finally, let us concentrate on each S_i individually. If S_i contains three multiplicatively independent elements m_1, m_2, m_3, then by Corollary 2.1, we must have at least one of $-3m_1m_2, -3m_2m_3, -3m_3m_1$ or $m_1m_2m_3$ to be a square. But this poses a contradiction as neither of m_1, m_2, m_3, l_i is a square and m_1l_i, m_2l_i, m_3l_i are all squares as per our choice of S_i. Hence, each of the sets S_i can be represented in the form $\{\pm m_1^a m_2^b \ : \ a, b \geq 0\}$ and consequently

$$\begin{aligned}
\#\{n \in S \ : \ |n| \leq x\} \ &= \ \#\{n \in S_0 \cup S_1 \cup S_2 \cup S_3 \ : \ |n| \leq x\} \\
&\leq \ \sum_{i=0}^{3} \#\{n \in S_i \ : \ |n| \leq x\} \\
&= \ \sum_{i=0}^{3} \#\{a, b \geq 0 \ : \ |k_1^a k_2^b| \leq x\} \ \ll \ \log^2 x
\end{aligned}$$

As we have considered all the possible configurations of S, the result follows for any such set of integers. $\square$

This concludes our discussion of the unconditional approaches towards proving the Artin's conjecture. The result by D.R. Heath-Brown using the refined sieve results is the best we have so far in this field. The conjecture will be proven unconditionally if we can reduce the set defined by Heath-Brown to a single integer which is not a square, 0 or ± 1. In the next chapter, we will discuss the elliptic curve analogue of Artin's conjecture and its proof by Gupta and Murty.

Chapter 3

Artin's Conjecture: Elliptic Curve Analogue

The elliptic curve analogue of the Artin's Conjecture was formulated by Lang and Trotter [15] in 1977. As the original conjecture talks about the density of primes for which a given integer would be a primitive root, the analogue deals with the density of primes for which the reduction of an elliptic curve modulo that prime would have a given rational point as a primitive point. Let us first introduce some new terms.

Definition 3.1 (Primitive Point) *Given an elliptic curve $E(\mathbb{Q})$ defined over the rationals and a prime p, let the reduction of the elliptic curve modulo p be denoted as $\overline{E}(\mathbb{F}_p)$. Then, a rational point $a \in E(\mathbb{Q})$ is said to be a primitive point of the curve modulo p if $\overline{a}$, the reduction of a modulo p generates $\overline{E}(\mathbb{F}_p)$.*

Based on this definition of a primitive point, the elliptic analogue of Artin's Conjecture is as follows.

Conjecture 3.1 (Lang and Trotter, 1977) *If we consider an elliptic curve $E(\mathbb{Q})$ defined over the rationals and a rational point $a \in E(\mathbb{Q})$ of infinite order, then a will be a primitive point of $\overline{E}(\mathbb{F}_p)$ for infinitely many primes p.*

3.1 Approach 1: Lang and Trotter

In the same paper by Lang and Trotter [15], they took the first approach to prove this analogous conjecture. For a being a primitive point for $\overline{E}(\mathbb{F}_p)$, we mean the

following

$$\langle \overline{a} \rangle = \overline{E}(\mathbb{F}_p) \quad \Leftrightarrow \quad q \nmid [\overline{E}(\mathbb{F}_p) : \langle \overline{a} \rangle] \ \forall \text{ primes } q$$

Let us denote $[\overline{E}(\mathbb{F}_p) : \langle \overline{a} \rangle]$, the index of $\langle \overline{a} \rangle$ in $\overline{E}(\mathbb{F}_p)$, by $i(p)$. Then the criteria of divisibility of $i(p)$ by any prime q is of prime importance for proving the conjecture. Lang and Trotter tried to take a similar approach as Hooley took for proving the classical conjecture in 1967 [11]. They considered the Galois extensions $\mathbb{L}_q = \mathbb{Q}(E[q], q^{-1}a)$ analogous to the splitting fields of $x^q - a = 0$ in Hooley's proof. Here $E[q]$ denotes the q-division points of the elliptic curve $E(\mathbb{Q})$ and $q^{-1}a$ denotes the point $b \in E(\mathbb{C})$ for which $qb = a$.

Now, the Galois group G_q of $\mathbb{L}_q/\mathbb{Q}$ is a semidirect product of subgroups of $GL_2(\mathbb{F}_q)$ and $E[q]$ and is not abelian. Hence, we can always denote the elements $\sigma \in G_q$ as pairs (γ, τ) with $\gamma \in GL_2(\mathbb{F}_q)$ and $\tau \in E[q]$, such that the following relation holds for $u_0 \in q^{-1}a$ and $u \in E[q]$

$$(\gamma, \tau)u = u_0 + \gamma(u - u_0) + \tau$$

Therefore, we have

$$\sigma u = u \quad \Leftrightarrow \quad (\gamma - 1)(u_0 - u) = \tau$$

Lang and Trotter tried to formulate a condition on the Frobenius element $\sigma_p = (\gamma_p, \tau_p) \in G_q$ in order that $q | i(p)$. It is quite obvious that we should choose p so that we have a good reduction of the curve modulo p. This implies that p should be unramified in the ring of integers $\mathcal{O}_{\mathbb{K}}$ and hence we cannot choose $p | q\Delta_E$ when Δ_E is the discriminant of the curve E. Based on these constraints, Lang and Trotter proved the following result.

Lemma 3.1 *The prime q divides the index $i(p)$ if and only if the Frobenius element $\sigma_p \in \overline{S_q}$ where*

$$\overline{S_q} = \{(\gamma_p, \tau_p) \ : \ \textit{(i) } \gamma_p = 1 \textit{ OR}$$
$$\textit{(ii) } \gamma_p \textit{ has eigenvalue 1, } \ker(\gamma_p - 1) \textit{ is cyclic, } \tau_p \in (\gamma_p - 1)E[q]\}$$

Proof. See [15] for the proof.

When Lang and Trotter proceeded to prove the conjecture in light of the condition formulated above, they got that $|\overline{S_q}| \gg q^2$ in the complex multiplication (CM) case and $|\overline{S_q}| \gg q^4$ in the non-CM case. This posed a problem because applying an approach analogous to Hooley's, assuming GRH, produced a very large error term.

3.2 Approach 2: Lang and Trotter

In the same paper, Lang and Trotter also proposed a general form of the conjecture in case of higher rank elliptic curves. In this case, they considered the problem over a free subgroup of the elliptic curve instead of assuming the whole group to be an infinite cyclic one. Their approach was as follows.

Let us suppose that Γ is a free subgroup of rational points of the elliptic curve. In this case, the analogous problem of Artin's conjecture would be to compute the density of the primes p for which the elliptic curve group reduced modulo p is generated by Γ_p, the reduction of the free subgroup modulo p. Lang and Trotter formulated an index divisibility criterion in this case as well. Suppose that $\overline{E}(\mathbb{F}_p)$ and Γ_p be the reductions modulo p of E and Γ respectively. So, the index divisibility criterion in this case will consider the divisibility of the index $i(p) = [\overline{E}(\mathbb{F}_p) : \Gamma_p]$ by primes q.

Now, fix a section $\lambda : \Gamma \to q^{-1}\Gamma$ such that $q(\lambda a) = a$ for all $a \in \Gamma$. Consider the Galois extension $\mathbb{M}_q = \mathbb{Q}(E[q], q^{-1}\Gamma)$ analogous to $\mathbb{L}_q$ in Approach 1. Then the Galois group G_q of $\mathbb{M}_q/\mathbb{Q}$ is a semidirect product of subgroups of $GL_2(\mathbb{F}_q)$ and $E[q]$. Hence, we can always denote the elements $\sigma \in G_q$ as pairs (γ, τ) with $\gamma \in GL_2(\mathbb{F}_q)$ and τ a translation, such that the following relation holds for $u \in q^{-1}\Gamma$

$$(\gamma, \tau)u = \lambda qu + \gamma(u - \lambda qu) + \tau qu$$

Therefore, we have

$$\sigma u = u \quad \Leftrightarrow \quad (\gamma - 1)(u - \lambda qu) = -\tau qu$$

Analogous to Approach 1, Lang and Trotter tried to formulate a condition on the Frobenius element $\sigma_p = (\gamma_p, \tau_p) \in G_q$ such that $q|i(p)$. It is quite obvious that we cannot take $p|q\Delta_E$ when Δ_E is the discriminant of the curve E, as that would give a 'bad' reduction of the curve modulo p. Based on these constraints, Lang and Trotter proved the following result.

Lemma 3.2 *The prime q divides the index $i(p)$ if and only if the Frobenius element $\sigma_p \in S_q$ where*

$$\begin{aligned} S_q = \{(\gamma_p, \tau_p) \ : \ & \textit{(i)} \ \ker(\gamma_p - 1) \textit{ is cyclic and } \tau_p(\Gamma) \subset (\gamma_p - 1)E[q] \textit{ OR} \\ & \textit{(ii)} \ \ker(\gamma_p - 1) = E[q] \textit{ and } \ \operatorname{rank}(\tau_p(\Gamma)) = 0 \textit{ or } 1\} \end{aligned}$$

Proof. See [15] for the proof.

The path to prove this higher rank analogue seemed quite formidable as well. Lang and Trotter encountered problems regarding the estimation of $|S_q|$ and problems with proving the analogue of the Brun-Titchmarsh sieve.

Both the conjecture and the higher rank analogue were finally proved, assuming GRH, by Gupta and Murty in 1986 [8]. They took a different approach in characterizing the divisibility of $i(p)$ to prove the conjecture. We will spend the next few sections analyzing the proofs by Gupta and Murty.

3.3 Result 1: Gupta and Murty

The paper by Gupta and Murty [8] deals with the elliptic curves E which has complex multiplication by the entire ring of integers $\mathcal{O}_{\mathbb{K}}$ of some imaginary quadratic extension $\mathbb{K}$ of $\mathbb{Q}$. Moreover, their method captures only those primes p which split completely in $\mathbb{K}$, which does not pose a problem because there are infinitely many primes satisfying this condition. Based on these criteria, the first result proved by Gupta and Murty is as follows:

Theorem 3.1 (Gupta and Murty, 1986) *Let $E(\mathbb{Q})$ be an elliptic curve defined over the rationals with complex multiplication by $\mathcal{O}_{\mathbb{K}}$ and let a be a rational point of infinite order. If we define*

$$N_a^*(x) = \#\{p \leq x \ : \ p \nmid a, \ p \text{ splits completely in } \mathbb{K}, \ \langle \overline{a} \rangle = \overline{E}(\mathbb{F}_p)\}$$

then under the assumption of generalized Riemann hypothesis, we obtain the following as $x \to \infty$:

$$N_a^*(x) \ = \ C_E(a)\frac{x}{\log x} \ + \ O\left(\frac{x \log\log x}{\log^2 x}\right)$$

3.3.1 Index Divisibility Criteria

Before we start with the formal proof of the theorem, let us discuss the modified index divisibility criteria introduced by Gupta and Murty. As we have seen before,

$$\overline{E}(\mathbb{F}_p) = \langle \overline{a} \rangle \quad \Leftrightarrow \quad i(p) = 1 \quad \Leftrightarrow \quad q \nmid i(p) \ \forall \text{ primes } q$$

So, as we saw before, we take a look at the converse - "What does $q|i(p)$ mean?", and formulate a divisibility criteria for the index. This analysis gives us the following lemma.

Lemma 3.3 *Let $p \nmid q\Delta_E$. Then $q|i(p)$ if and only if either*

(i) $E[q] \subseteq \overline{E}(\mathbb{F}_p)$ *OR*

(ii) The q-primary part of $\overline{E}(\mathbb{F}_p)$ is non-trivial and cyclic and there exists $\overline{b} \in \overline{E}(\mathbb{F}_p)$ such that $q\overline{b} = \overline{a}$

Proof. We know that for the q-division points of the elliptic curve, $E[q] \simeq (\mathbb{Z}/q\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$. So, if $E[q] \subseteq \overline{E}(\mathbb{F}_p)$ holds, then $\overline{E}(\mathbb{F}_p)$ contains both the copies of $(\mathbb{Z}/q\mathbb{Z})$. But, $\langle \overline{a} \rangle$ is cyclic and hence cannot contain more than one copy of $(\mathbb{Z}/q\mathbb{Z})$. Hence, $(\mathbb{Z}/q\mathbb{Z}) \subseteq (\overline{E}(\mathbb{F}_p)/\langle \overline{a} \rangle)$, i.e $q|i(p)$.

If otherwise, $E[q] \nsubseteq \overline{E}(\mathbb{F}_p)$ yet $q|i(p)$, then $\overline{E}(\mathbb{F}_p)$ contains exactly one copy of $(\mathbb{Z}/q\mathbb{Z})$, the q-primary part. So, the q-primary part is non-trivial and cyclic. Again, as $q|i(p)$, we must have some $b \in E$ such that $qb \equiv a \pmod{p}$, i.e $q\overline{b} = \overline{a}$ for $\overline{b} \in \overline{E}(\mathbb{F}_p)$. □

Now, let us analyze the error occurring due to the primes p dividing $q\Delta_E$. The prime divisors of Δ_E introduce an error of $O(1)$. Again, if $p = q$, i.e if $p|i(p)$, then we must have p dividing $|\overline{E}(\mathbb{F}_p)| = p + 1 - a_p$, where $a_p \leq 2\sqrt{p}$, satisfying Hasse's bound [19]. So, if $p|i(p)$, then we must have $a_p \equiv 1 \pmod{p}$ for $p > 5$. By Serre [18], the number of such primes is $o(x/\log x)$. In the specific case of complex multiplication we are considering, this error reduces down to $O(\sqrt{x}/\log x)$, by utilizing some elementary sieve logic. So, we can consider only the primes p such that $p \nmid q\Delta_E$, without exceeding the error bounds.

We will use algebraic number theory to formulate the index divisibility criteria properly. As per our initial assumption, the elliptic curve E has complex multiplication by the entire ring of integers $\mathcal{O}_{\mathbb{K}}$ of some quadratic extension $\mathbb{K}$ of $\mathbb{Q}$. We consider only those primes p which split completely in $\mathbb{K}$.

Let us suppose that $p = \pi_p\overline{\pi_p}$ be the splitting of p in $\mathbb{K}$. Let us define an extension $\mathbb{K}_q$ over $\mathbb{K}$, adjoining the q-division points of E, as $\mathbb{K}_q = \mathbb{K}(E[q])$. Again, given a first degree prime ideal $\mathfrak{q}$ of $\mathcal{O}_{\mathbb{K}}$, let us define an extension as $\mathbb{L}_{\mathfrak{q}} = \mathbb{K}(E[\mathfrak{q}], \mathfrak{q}^{-1}a)$, where $E[\mathfrak{q}]$ denotes the $\mathfrak{q}$-division points of E and $\mathfrak{q}^{-1}a$ denote a point $b \in E$ such that $\alpha b = a$ where $\mathfrak{q} = (\alpha)$. Here, the elliptic curve E is defined over $\mathbb{Q}$ and we take $\mathbb{K}$ to be an imaginary quadratic extension over $\mathbb{Q}$. Now, as E has complex multiplication over the entire ring of integers $\mathcal{O}_{\mathbb{K}}$ of $\mathbb{K}$, we can prove that the extension $\mathbb{K}$ has class number 1. This implies that all the ideals of $\mathcal{O}_{\mathbb{K}}$ are principal. So, we can assume $\mathfrak{q}$ to be principal without any loss of generality. Then, $\mathbb{L}_{\mathfrak{q}}$ is independent of the choice of $\mathfrak{q}^{-1}a$ and is a normal extension of $\mathbb{K}$. Depending on the extensions of

$\mathbb{K}$ defined above, let us translate Lemma 3.3 to these fields to obtain the following result.

Lemma 3.4 *Suppose that p splits in $\mathbb{K}$ as $p = \pi_p\overline{\pi_p}$ and $p \nmid q\Delta_E$. Then*

(i) If q is inert in $\mathbb{K}$, then $q|i(p)$ if and only if p splits completely in $\mathbb{K}_q$.

(ii) If q ramifies or splits in $\mathbb{K}$ as $q = \mathfrak{q}_1\mathfrak{q}_2$, then $q|i(p)$ if and only if (π_p) splits completely in $\mathbb{L}_{\mathfrak{q}_1}$ or $\mathbb{L}_{\mathfrak{q}_2}$ or $\mathbb{K}_q$.

Proof. Before we go into proving this lemma for different cases depending on the behavior of q in $\mathbb{K}$, let us list some useful facts [19]

(a) $|\overline{E}(\mathbb{F}_p)| = p + 1 - a_p = N(\pi_p - 1)$

(b) $\phi\colon P \mapsto \pi_p P$ is a Frobenius endomorphism over $E \pmod{\pi_p}$

Case 1: q is inert in $\mathbb{K}$

$$\begin{aligned} q|i(p) \;\Rightarrow\; q||\overline{E}(\mathbb{F}_p)| \;&\Rightarrow\; N(\pi_p - 1) \equiv 0 \pmod{q} \text{ in } \mathbb{Q} \\ &\Rightarrow\; \pi_p \equiv 1 \pmod{q} \text{ in } \mathbb{K} \\ &\Rightarrow\; \phi \text{ acts trivially on the } q\text{-torsion points of } E \end{aligned}$$

Therefore, by the Ogg-Neron-Shafarevich criterion [19], π_p splits completely in $\mathbb{K}_q = \mathbb{K}(E[q])$, and so does $\overline{\pi_p}$ by a similar argument. Hence, p splits completely in $\mathbb{K}_q$.

Case 2: $q = \mathfrak{q}_1\mathfrak{q}_2$ splits in $\mathbb{K}$

$$\begin{aligned} q|i(p) \;\Rightarrow\; q||\overline{E}(\mathbb{F}_p)| \;&\Rightarrow\; N(\pi_p - 1) \equiv 0 \pmod{q} \text{ in } \mathbb{Q} \\ &\Rightarrow\; \pi_p \equiv 1 \pmod{\mathfrak{q}_1} \text{ in } \mathbb{K} \; AND/OR \\ &\qquad \pi_p \equiv 1 \pmod{\mathfrak{q}_2} \text{ in } \mathbb{K} \\ &\Rightarrow\; \phi \text{ acts trivially on the } \mathfrak{q}_1\text{-torsion points of } E \;\; AND/OR \\ &\qquad \phi \text{ acts trivially on the } \mathfrak{q}_2\text{-torsion points of } E \end{aligned}$$

Therefore, π_p splits completely in $\mathbb{K}_{\mathfrak{q}_1} = \mathbb{K}(E[\mathfrak{q}_1])$ AND/OR in $\mathbb{K}_{\mathfrak{q}_2} = \mathbb{K}(E[\mathfrak{q}_2])$. Again, solvability of $qb \equiv a \pmod{p}$ implies that p has a first degree prime factor in $\mathbb{Q}(q^{-1}a)$. So, in this case, π_p must have a first degree prime factor in $\mathbb{K}(\mathfrak{q}_1^{-1}a)$ and in $\mathbb{K}(\mathfrak{q}_2^{-1}a)$. Hence, π_p splits completely in $\mathbb{L}_{\mathfrak{q}_1}$ AND/OR $\mathbb{L}_{\mathfrak{q}_2}$ as defined before. If both the cases hold, it is equivalent to saying that p splits completely in $\mathbb{K}_q$.

Case 3: $q = \mathfrak{q}^2$ ramifies in $\mathbb{K}$

$$\begin{aligned} q|i(p) \;\Rightarrow\; q||\overline{E}(\mathbb{F}_p)| \;&\Rightarrow\; N(\pi_p - 1) \equiv 0 \pmod{q} \text{ in } \mathbb{Q} \\ &\Rightarrow\; \pi_p \equiv 1 \pmod{\mathfrak{q}^2} \text{ in } \mathbb{K}\ OR \\ &\quad\; \pi_p \equiv 1 \pmod{\mathfrak{q}} \text{ in } \mathbb{K} \\ &\Rightarrow\; \phi \text{ acts trivially on the } \mathfrak{q}^2\text{-torsion points of } E\ \ OR \\ &\quad\; \phi \text{ acts trivially just on the } \mathfrak{q}\text{-torsion points of } E \end{aligned}$$

If the first case holds, then the situation is similar to Case 1 and we can say that p splits completely in $\mathbb{K}_q$. If just the second condition holds, then similar to the argument in Case 2, we obtain that π_p splits completely in $\mathbb{L}_{\mathfrak{q}}$. The result follows.

3.3.2 Proof of the Asymptotic Formula

Let us embark upon the path of proving Theorem 3.1. The first step is to prove the asymptotic formula. Our goal is to find

$$\begin{aligned} N_a^*(x) \;&=\; \#\{p \le x \mid \overline{E}(\mathbb{F}_p) = \langle \overline{a} \rangle\} \\ &=\; \#\{p \le x \mid q \nmid i(p)\ \forall \text{ primes } q\} \end{aligned}$$

Let us define the following

$$\begin{aligned} N(x,y) \;=\; \#\{\pi_p \in \mathbb{K} \mid N(\pi_p) \le x,\ \pi_p \textit{ does not} \text{ split completely in} \\ \mathbb{L}_{\mathfrak{q}} \text{ or } \mathbb{K}_q \text{ for } \textit{any } N(\mathfrak{q}) \le y \text{ or } q \le y\} \end{aligned}$$

Then, as we are counting two prime ideals π_p and $\overline{\pi_p}$ in $\mathbb{K}$ corresponding to each prime p in $\mathbb{Q}$, we have $N_a^*(x) \le \frac{1}{2}N(x,y)$. Again, let us define another term as follows

$$\begin{aligned} M(x,y_1,y_2) \;=\; \#\{p \le x \mid \pi_p \textit{ splits} \text{ completely in } \mathbb{L}_{\mathfrak{q}} \text{ or } \mathbb{K}_q \\ \text{for } \textit{some } y_1 \le N(\mathfrak{q}) \le y_2 \text{ or } y_1 \le q \le y_2\} \end{aligned}$$

Now, we know that for $p \le x$, q is bounded by $|\overline{E}(\mathbb{F}_p)| = p + 1 - a_p$. We can assume without loss of generality that $q \le 2x$. Hence, we get $N_a^*(x) \ge \frac{1}{2}N(x,y) - M(x,y,2x)$. Combining the two bounds for $N_a^*(x)$, we obtain

$$\begin{aligned} \frac{1}{2}N(x,y) \;&\le\; N_a^*(x) \;\le\; \frac{1}{2}N(x,y) - M(x,y,2x) \\ N_a^*(x) \;&=\; \frac{1}{2}N(x,y) + O(M(x,y,2x)) \end{aligned}$$

Analogous to Hooley's approach, we choose specific sub intervals to use specific sieve methods in estimating $M(x, y, 2x)$. We break up the interval $[y, 2x]$ into the subintervals $[y, x^{\frac{1}{2}}/\log^2 x], [x^{\frac{1}{2}}/\log^2 x, x^{\frac{1}{2}}\log^2 x]$ and $[x^{\frac{1}{2}}\log^2 x, 2x]$ with $y = \frac{1}{12}\log x$. Thus, we obtain

$$\begin{aligned} N_a^*(x) &= \frac{1}{2}N\left(x, \frac{1}{12}\log x\right) + O\left(M\left(x, \frac{1}{12}\log x, \frac{x^{\frac{1}{2}}}{\log^2 x}\right)\right) \\ &\quad + O\left(M\left(x, \frac{x^{\frac{1}{2}}}{\log^2 x}, x^{\frac{1}{2}}\log^2 x\right)\right) + O\left(M\left(x, x^{\frac{1}{2}}\log^2 x, 2x\right)\right) \end{aligned}$$

Estimate of $M\left(x, x^{\frac{1}{2}}\log^2 x, 2x\right)$

This estimate is the easiest to compute. If π_p splits completely in $\mathbb{K}_q$, then we must have $q^2|(p+1-a_p)$, i.e $q \leq 2\sqrt{x}$. Now, the range we are considered here is beyond $2\sqrt{x}$ and hence we just need to count the number of π_p splitting completely only in $\mathbb{L}_{\mathfrak{q}}$ with $N(\mathfrak{q})$ in the given range.

If π_p splits completely in $\mathbb{L}_{\mathfrak{q}}$, then we must have

$$\begin{aligned} \pi_p \mathfrak{q}^{-1}\overline{a} &\equiv \mathfrak{q}^{-1}\overline{a} \pmod{\pi_p} \\ \Rightarrow (\pi_p - 1)\,\mathfrak{q}^{-1}\overline{a} &\equiv 0 \pmod{\pi_p} \\ \Rightarrow \left(\frac{\pi_p - 1}{\beta}\right)\overline{a} &\equiv 0 \pmod{\pi_p} \end{aligned}$$

where β generates $\mathfrak{q}$. Here, $\mathfrak{q}$ is a principal ideal because $\mathbb{K}$ has class number 1 and hence all the ideals of $\mathcal{O}_{\mathbb{K}}$ are principal. Thus, we can write $\mathfrak{q} = (\beta)$ with $\beta \in \mathcal{O}_{\mathbb{K}}$. This implies that $\alpha = \frac{\pi_p - 1}{\beta} \in \mathcal{O}_{\mathbb{K}}$ and we can define a division polynomial for α.

Let us suppose we have E to be an elliptic curve in the Weierstrass normal form with complex multiplication by an order $\mathcal{O}_{\mathbb{K}}$. If $P(x, y)$ is a point on the curve, then the x co-ordinate of αP, for $\alpha \in \mathcal{O}_{\mathbb{K}}$, is given by $(\alpha P)_x = f_\alpha(x)/g_\alpha(x)$ where $f_\alpha(x)$ and $g_\alpha(x)$ are polynomials in x whose degrees depend on α. The roots of $g_\alpha(x)$ are the x-coordinates of the non-zero α division points and hence g_α is called the α division polynomial [19].

So, from the congruence relation above, we obtain $g_\alpha(a) \equiv 0 \pmod{\pi_p}$. Again, we notice that for $N(\mathfrak{q})$ to be in the given range, we should have $N(\alpha) \leq \frac{2x^{1/2}}{\log^2 x}$. Therefore, $M\left(x, x^{\frac{1}{2}}\log^2 x, 2x\right)$ is bounded by the number of prime factors in the numerator of

$$\prod_{x^{\frac{1}{2}}\log^2 x \leq N(\mathfrak{q}) \leq 2x} g_\alpha(a) = \prod_{N(\alpha) \leq 2x^{\frac{1}{2}}\log^2 x} g_\alpha(a) = G_\alpha, \text{ say}$$

The total number of prime factors in the numerator of G_α is bounded by $2\log|G_\alpha|$. Here, we need the following lemma to provide us with an estimate of the coefficients of $g_\alpha(a)$.

Lemma 3.5 *The coefficients of $g_\alpha(x)$ are bounded by $\exp(CN(\alpha)\log N(\alpha))$ for some constant C depending only on the elliptic curve E.*

Proof. Proved in Section 3.3.3.

By Lemma 3.5, we get that $M\left(x, x^{\frac{1}{2}}\log^2 x, 2x\right)$ is bounded by

$$2\log|G_\alpha| \ll \sum_{N(\alpha)\leq \frac{2x^{1/2}}{\log^2 x}} N(\alpha)\log N(\alpha) \ll \frac{x}{\log^3 x}$$

Estimate of $M\left(x, \frac{x^{\frac{1}{2}}}{\log^2 x}, x^{\frac{1}{2}}\log^2 x\right)$

In this estimation, we relax the splitting condition a bit and count all the primes π_p with $N(\pi_p)\leq x$ satisfying either $\pi_p \equiv 1 \pmod{\mathfrak{q}}$ or $\pi_p \equiv 1 \pmod{q}$ for some $\mathfrak{q}$ and q with $\frac{x^{1/2}}{\log^2 x} \leq N(\mathfrak{q}) \leq x^{1/2}\log^2 x$ and $\frac{x^{1/2}}{\log^2 x} \leq q \leq x^{1/2}\log^2 x$.

To count the primes in arithmetic progression in $\mathbb{L}_\mathfrak{q}$, we use the analogue of the Brun-Titchmarsh theorem for number fields. For an ideal $\mathfrak{q}$, the number of primes in arithmetic progression is given by

$$\pi_1(x, \mathbb{L}_\mathfrak{q}) = \#\{\pi_p \mid N(\pi_p)\leq x, \pi_p \equiv 1 \pmod{\mathfrak{q}}\} \ll \frac{x}{\phi(\mathfrak{q})\log(x/N(\mathfrak{q}))}$$

given that $N(\mathfrak{q})\leq x$. Here, in the specified range, we have $N(\mathfrak{q})\leq x^{1/2}\log^2 x$. Hence, we have $\pi_1(x,\mathbb{L}_\mathfrak{q}) \ll \frac{x}{N(\mathfrak{q})\log x}$. Similarly, using the same analogous sieve, we obtain $\pi_1(x,\mathbb{K}_q) \ll \frac{x}{q^2}$ in $\mathbb{K}_q$. Therefore

$$M\left(x, \frac{x^{\frac{1}{2}}}{\log^2 x}, x^{\frac{1}{2}}\log^2 x\right) \ll \frac{x}{\log x} \sum_{\frac{x^{1/2}}{\log^2 x}\leq N(\mathfrak{q})\leq x^{1/2}\log^2 x} \frac{1}{N(\mathfrak{q})} + x \sum_{\frac{x^{1/2}}{\log^2 x}\leq q\leq x^{1/2}\log^2 x} \frac{1}{q^2}$$

Using the appropriate summation formulae and plugging in the bounds for $N(\mathfrak{q})$ and q, we obtain

$$M\left(x, \frac{x^{\frac{1}{2}}}{\log^2 x}, x^{\frac{1}{2}}\log^2 x\right) \ll \frac{x\log\log x}{\log^2 x}$$

We are now left to deal with the estimates of $\frac{1}{2}N(x, \frac{1}{12}\log x)$ and $M\left(x, \frac{1}{12}\log x, \frac{x^{\frac{1}{2}}}{\log^2 x}\right)$. So far, we have obtained the following

$$N_a^*(x) \;=\; \frac{1}{2}N(x, \frac{1}{12}\log x) + O\left(M\left(x, \frac{1}{12}\log x, \frac{x^{\frac{1}{2}}}{\log^2 x}\right)\right) + O\left(\frac{x\log\log x}{\log^2 x}\right)$$

Estimate of $N(x, \frac{1}{12}\log x)$ and $M\left(x, \frac{1}{12}\log x, \frac{x^{\frac{1}{2}}}{\log^2 x}\right)$

Now, to estimate the main two terms, we need to define a new field extension tower as follows. Let $\mathfrak{a}$ be a square free integral ideal in $\mathcal{O}_{\mathbb{K}}$ which is only divisible by prime ideal factors of degree one. Also let s be a square free integer. Define the field extensions

$$\begin{array}{lll} \mathbb{L}_{\mathfrak{a}} & = \prod_{\mathfrak{q}|\mathfrak{a}} \mathbb{L}_{\mathfrak{q}} & = \mathbb{K}(E[\mathfrak{a}], \mathfrak{a}^{-1}a) \\ \mathbb{K}_s & = \prod_{q|s} \mathbb{K}_q & = \mathbb{K}(E[s]) \\ \mathbb{L}_{\mathfrak{a},s} & = \mathbb{L}_{\mathfrak{a}} \cdot \mathbb{K}_s & = \mathbb{K}(E[\mathfrak{a}s], \mathfrak{a}^{-1}a) \end{array}$$

with $[\mathbb{L}_{\mathfrak{a}} : \mathbb{K}] = n(\mathfrak{a})$, $[\mathbb{K}_s : \mathbb{K}] = m(s)$ and $[\mathbb{L}_{\mathfrak{a},s} : \mathbb{K}] = n(\mathfrak{a}, s)$, say. Let the discriminant of $\mathbb{L}_{\mathfrak{a},s}$ over $\mathbb{Q}$ be denoted as $d(\mathfrak{a}, s)$. Also define the following

$$\begin{array}{lll} \pi(x, \mathfrak{a}, s) & = & \#\{\pi_p \in \mathbb{K} \mid N(\pi_p) \leq x, \pi_p \text{ splits completely in } \mathbb{L}_{\mathfrak{a},s}\} \\ \pi(x, \mathfrak{q}) & = & \#\{\pi_p \in \mathbb{K} \mid N(\pi_p) \leq x, \pi_p \text{ splits completely in } \mathbb{L}_{\mathfrak{q}}\} \\ \pi(x, q) & = & \#\{\pi_p \in \mathbb{K} \mid N(\pi_p) \leq x, \pi_p \text{ splits completely in } \mathbb{K}_q\} \end{array}$$

Based on the terms defined above and with the help of an inclusion-exclusion argument, we can write the following

$$N(x, y_1) = \sum_{\substack{N(\mathfrak{q}) \leq y_1 \ \forall \mathfrak{q}|\mathfrak{a} \\ q \leq y_1 \ \forall q|s}} \mu(\mathfrak{a})\mu(s)\pi(x, \mathfrak{a}, s)$$

$$M(x, y_1, y_2) \leq \sum_{y_1 \leq N(\mathfrak{q}) \leq y_2} \pi(x, \mathfrak{q}) + \sum_{y_1 \leq q \leq y_2} \pi(x, q)$$

where the functions $\mu(\mathfrak{a})$ and $\mu(s)$ denote the natural Möbius functions for $\mathcal{O}_{\mathbb{K}}$ and $\mathbb{Z}$ in respective cases. Here, we need to set $y_1 = \frac{1}{12}\log x$ and $y_2 = x^{1/2}/\log^2 x$ and it remains to estimate the function π to obtain the desired estimates of the terms $N(x, y_1)$ and $M(x, y_1, y_2)$.

We can obtain good estimates for the π functions using a theorem by Lagarias and Odlyzko [14], which states

Theorem 3.2 (Lagarias-Odlyzko) *Let $\mathbb{L}/\mathbb{K}$ be a normal extension with degree $[\mathbb{L} : \mathbb{K}] = n$ and discriminant $\text{disc}(\mathbb{L}/\mathbb{Q}) = d$. Let $\pi_C(x, \mathbb{L})$ be the number of first degree prime ideals of $\mathbb{K}$ whose Frobenius automorphism lies in a given conjugacy class C of $\text{Gal}(\mathbb{L}/\mathbb{K})$. If the Dedekind zeta function of $\mathbb{L}$ satisfies the generalized Riemann hypothesis, then*

$$\pi_C(x, \mathbb{L}) = \frac{|C|}{n}\,\text{li}(x) + O\left(|C|x^{\frac{1}{2}}\left(\log x + \frac{\log|d|}{n}\right)\right)$$

In case of the π functions, we are counting the primes splitting completely in the extension, which implies that the Frobenius automorphisms of the primes act trivially and hence the conjugacy class is essentially trivial in this case. If we assume that the Dedekind zeta function of $\mathbb{L}_{\mathfrak{a},s}$ satisfies GRH, we obtain the following

$\mathbb{L}$	$\mathbb{K}$	C	$\pi_C(x,\mathbb{L})$
$\mathbb{L}_{\mathfrak{a},s}$	$\mathbb{K}$	$\{1\}$	$\pi(x,\mathfrak{a},s)=\frac{\mathrm{li}(x)}{n(\mathfrak{a},s)}+O\left(x^{1/2}\left(\log x+\frac{\log\lvert d(\mathfrak{a},s)\rvert}{n(\mathfrak{a},s)}\right)\right)$
$\mathbb{L}_{\mathfrak{q}}$	$\mathbb{K}$	$\{1\}$	$\pi(x,\mathfrak{q})=\frac{\mathrm{li}(x)}{n(\mathfrak{q})}+O\left(x^{1/2}\log x\right)$
$\mathbb{K}_q$	$\mathbb{K}$	$\{1\}$	$\pi(x,q)=\frac{\mathrm{li}(x)}{m(q)}+O\left(x^{1/2}\log x\right)$

Hence, we get the estimate of $N(x,y_1)$ as follows

$$N(x,y_1)=\sum_{\mathfrak{a},s}{}'\frac{\mu(\mathfrak{a})\mu(s)}{n(\mathfrak{a},s)}\ \mathrm{li}(x)\ +\ O\left(x^{1/2}\sum_{\mathfrak{a},s}{}'\left(\log x+\frac{\log\lvert d(\mathfrak{a},s)\rvert}{n(\mathfrak{a},s)}\right)\right)$$

where the dash over the summation denotes that $N(\mathfrak{q})\leq y_1$ for all first degree prime ideals $\mathfrak{q}|\mathfrak{a}$ and $q\leq y_1$ for all primes $q|s$.

Now, we have the following results regarding the estimates of the degree and discriminant of the field extensions

Lemma 3.6

$$\frac{\log\lvert d(\mathfrak{a},s)\rvert}{n(\mathfrak{a},s)}\ll\log N(\mathfrak{a})+\log s$$

Proof. Proved in Section 3.3.3.

Lemma 3.7 *If $\mathfrak{a}$ and s are coprime to $6\Delta_E$, where Δ_E is the discriminant of E, and $(\mathfrak{a},s)$ denote the gcd of $\mathfrak{a}$ and s, then*

$$n(\mathfrak{a},s)=\frac{n(\mathfrak{a})m(s)}{\phi((\mathfrak{a},s))}$$

Proof. Proved in Section 3.3.3.

Again, in the dashed summation, we have at most 2^{3y_1} pairs $(\mathfrak{a},s)$ and for any ideal $\mathfrak{a}$,

$$N(\mathfrak{a})\leq\prod_{N(\mathfrak{q})\leq y_1}N(\mathfrak{q})\quad\Rightarrow\quad\log N(\mathfrak{a})\ll y_1$$

Similarly, we can also obtain $\log s \ll y_1$. With the help of this estimates and Lemma 3.6, we get the error term in $N(x, y_1)$ to be

$$\ll \quad x^{1/2} \sum_{\mathfrak{a},s}{}' (\log x + \log N(\mathfrak{a}) + \log s) \quad \ll \quad x^{1/2} 2^{\frac{1}{4}\log x} \log x \quad \ll \quad x^{1-\epsilon}$$

for any $\epsilon > 0$ for our prior choice of $y_1 = \frac{1}{12}\log x$. Hence, we obtain

$$\begin{aligned} N(x, y_1) &= \sum_{\mathfrak{a},s}{}' \frac{\mu(\mathfrak{a})\mu(s)}{n(\mathfrak{a}, s)} \operatorname{li}(x) \; + \; O\left(x^{1-\epsilon}\right) \\ &= \sum_{\mathfrak{a},s} \frac{\mu(\mathfrak{a})\mu(s)}{n(\mathfrak{a}, s)} \operatorname{li}(x) \; + \; \sum_{\mathfrak{a},s}{}'' \frac{\mu(\mathfrak{a})\mu(s)}{n(\mathfrak{a}, s)} \operatorname{li}(x) \; + \; O\left(x^{1-\epsilon}\right) \end{aligned}$$

where the first summation is over all the square free ideals $\mathfrak{a}$ and all square free numbers s, and the double dash over the second summation indicates that either $N(\mathfrak{a}) \geq y_1$ or $s \geq y_1$.

From Lemma 3.7, we obtain

$$\sum_{\mathfrak{a},s} \frac{\mu(\mathfrak{a})\mu(s)}{n(\mathfrak{a}, s)} \leq \sum_{\mathfrak{a},s} \frac{1}{n(\mathfrak{a}, s)} \ll \sum_{\mathfrak{a},s} \frac{\phi((\mathfrak{a}, s))}{n(\mathfrak{a})m(s)}$$

where the constant implied is due to the divisors of $6\Delta_E$ which contribute to only a finitely many sums if we decompose the original sum according to $(\mathfrak{a}, s, 6\Delta_E)$. As $\phi((\mathfrak{a}, s))$ is a multiplicative function in s for fixed $\mathfrak{a}$, we obtain

$$\begin{aligned} \sum_{\mathfrak{a},s} \frac{\mu(\mathfrak{a})\mu(s)}{n(\mathfrak{a}, s)} &\ll \sum_{\mathfrak{a}} \frac{1}{n(\mathfrak{a})} \prod_{q} \left(1 + \frac{\phi((\mathfrak{a}, q))}{m(q)}\right) \\ &\ll \sum_{\mathfrak{a}} \frac{1}{n(\mathfrak{a})} \prod_{(\mathfrak{a},q)=1} \left(1 + \frac{1}{m(q)}\right) \prod_{(\mathfrak{a},q)\neq 1} \left(1 + \frac{\phi((\mathfrak{a}, q))}{m(q)}\right) \end{aligned}$$

Now, since the first product term is a subsequence of $\prod_q (1 + 1/m(q))$, which converges, we can write

$$\sum_{\mathfrak{a},s} \frac{\mu(\mathfrak{a})\mu(s)}{n(\mathfrak{a}, s)} \ll \sum_{\mathfrak{a}} \frac{1}{n(\mathfrak{a})} \prod_{(\mathfrak{a},q)\neq 1} \left(1 + \frac{\phi((\mathfrak{a}, q))}{m(q)}\right) \ll \sum_{\mathfrak{a}} \frac{2^{w(\mathfrak{a})}}{n(\mathfrak{a})}$$

where $w(\mathfrak{a})$ denotes the number of first degree prime ideal factors of $\mathfrak{a}$. As $2^{w(\mathfrak{a})} = O(N(\mathfrak{a})^{\epsilon})$ and $n(\mathfrak{a}) \geq N(\mathfrak{a})^{3/2}$ for all sufficiently large $N(\mathfrak{a})$, we have the last series to be converging. Hence, we have the unrestricted sum to converge and we can fix

$$\sum_{\mathfrak{a},s} \frac{\mu(\mathfrak{a})\mu(s)}{n(\mathfrak{a}, s)} = \delta$$

The error term comprises of the double dashed summation which contributes the following

$$\sum_{\mathfrak{a},s}{}'' \frac{\mu(\mathfrak{a})\mu(s)}{n(\mathfrak{a},s)} \leq \sum_{\mathfrak{a},s}{}'' \frac{1}{n(\mathfrak{a},s)} \ll \sum_{N(\mathfrak{a})\geq y_1} \frac{1}{n(\mathfrak{a})} + \sum_{s\geq y_1} \frac{1}{m(s)} \ll \frac{\log\log x}{\log x}$$

utilizing some elementary estimates for the ϕ function and putting $y_1 = \frac{1}{12}\log x$. Hence, we obtain

$$\begin{aligned} N(x, \frac{1}{12}\log x) &= \delta \text{ li}(x) + O\left(\frac{\log\log x}{\log x} \text{ li}(x)\right) + O\left(x^{1-\epsilon}\right) \\ &= \delta \text{ li}(x) + O\left(\frac{x\log\log x}{\log^2 x}\right) \end{aligned}$$

Again, from the degree estimates, we also get

$$M(x, y_1, y_2) \ll \sum_{y_1\leq N(\mathfrak{q})\leq y_2} \left(\frac{\text{li}(x)}{n(\mathfrak{q})} + O(x^{1/2}\log x)\right) + \sum_{y_1\leq q\leq y_2} \left(\frac{\text{li}(x)}{m(q)} + O(x^{1/2}\log x)\right)$$

Plugging in the appropriate limits $y_1 = \frac{1}{12}\log x$, $y_2 = x^{1/2}/\log^2 x$ and utilizing the estimates $n(\mathfrak{q}) \gg N(\mathfrak{q})^2$, $m(q) \gg q^2$, we obtain

$$M(x, \frac{1}{12}\log x, \frac{x^{1/2}}{\log^2 x}) \ll \frac{x}{\log^2 x}$$

Combining the estimates of all the terms as derived above, we get

$$N_a^*(x) = \frac{\delta}{2} \text{ li}(x) + O\left(\frac{x\log\log x}{\log^2 x}\right)$$

This proves Theorem 3.1 as δ depends only on the elliptic curve E and a and we can set $C_E(a) = \delta/2$. We will prove the lemmas in the following subsection and the next section will deal with the characterization of the constant δ and analysis of the cases where $C_E(a) > 0$.

3.3.3 Proof of Lemmas

Proof of Lemma 3.5

Let us consider some basic facts about the division polynomial defined earlier. If we have $(\alpha P)_x = f_\alpha(x)/g_\alpha(x)$, then we have $\deg(f_\alpha) = N(\alpha)$ and $\deg(g_\alpha) = N(\alpha) - 1$

where $N(\alpha)$ is the norm of α over $\mathbb{K}$. Again, if we normalize g_α to have leading coefficient α^2, then it will have coefficients in $\mathbb{K}$ and we will have

$$g_\alpha(x) = \alpha^2 \prod_u (x - \wp(u))$$

where the product is over all the non-zero α-division points and $\wp$ is the Weierstrass elliptic function. So, the coefficients of g_α are bounded by

$$N(\alpha) 2^{N(\alpha)} \prod_u \max(1, |\wp(u)|)$$

Now, we use the following result to prove this lemma.

Lemma 3.8 *For any non-zero α-division point u, $\wp(u) \ll N(\alpha)$ and the constant depends only on E.*

Proof. Let us consider the lattice associated to E to be $\Lambda = \omega_0 \mathcal{O}_{\mathbb{K}}$. Then the α-division point u will be $u = \beta\omega_0/\alpha$ for some $\beta \in \mathcal{O}_{\mathbb{K}}$ with $\alpha \nmid \beta$. The distance from u to Λ is given by

$$\min_{\omega \in \Lambda} |u - \omega| = \min_{\gamma \in \mathcal{O}_{\mathbb{K}}} |\omega_0| \left| \frac{\beta}{\alpha} - \gamma \right| = |\omega_0| \min_{\gamma \in \mathcal{O}_{\mathbb{K}}} \sqrt{\frac{N(\beta - \alpha\gamma)}{N(\alpha)}} \geq \frac{|\omega_0|}{\sqrt{N(\alpha)}}$$

Hence, by the definition of the Weierstrass $\wp$ function, we obtain

$$\wp(u) \ll \frac{1}{\left(|\omega_0| / \sqrt{N(\alpha)} \right)^2}$$

and the result follows. □

If we use this result, we obtain that the coefficients of g_α are bounded by $\exp(CN(\alpha) \log N(\alpha))$ where C depends only on the number of α-division points u of the curve E for which $|\wp(u)| > 1$, that is only on E. □

Proof of Lemma 3.6

From a result of Hensel [18], we get that if $\mathbb{L}/\mathbb{Q}$ is a normal extension of degree n and ramified only at the points $p_1, ..., p_m$, then

$$\frac{1}{n} \log |\operatorname{disc}(\mathbb{L}/\mathbb{Q})| \leq \log n + \sum_{j=1}^{m} \log p_j$$

In this case, we clearly have $n = n(\mathfrak{a}, s) \leq n(\mathfrak{a})m(s)$. Again, $m(s) \leq \phi(s\mathcal{O}_{\mathbb{K}})$ and $n(\mathfrak{a}) \leq \phi(\mathfrak{a})N(\mathfrak{a})$ because

$$\mathrm{Gal}(\mathbb{K}(E[\mathfrak{a}])/\mathbb{K}) \subset (\mathcal{O}_{\mathbb{K}}/\mathfrak{a})^* \quad \Rightarrow \quad \mathrm{Gal}(\mathbb{L}_{\mathfrak{a}}/\mathbb{K}) \subset \left\{ \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \in GL_2(\mathcal{O}_{\mathbb{K}}/\mathfrak{a}) \right\}$$

So we obtain $\log n(\mathfrak{a}, s) \ll \log N(\mathfrak{a}) + \log s$ and hence

$$\frac{\log |d(\mathfrak{a}, s)|}{n(\mathfrak{a}, s)} \ll \log N(\mathfrak{a}) + \log s + \sum_{j=1}^{m} \log p_j$$

where the primes p_j run over all the primes which ramify on the extension $\mathbb{L}_{\mathfrak{a}}$. To count these primes, it suffices to count the ones which ramify on the extension $\mathbb{Q}(E[r], r^{-1}a)$ for $r = N(\mathfrak{a})s$, as $\mathbb{L}_{\mathfrak{a}}$ is contained in it. Now, this extension is ramified only at primes which divide r and Δ_E. Hence, we have

$$\frac{\log |d(\mathfrak{a}, s)|}{n(\mathfrak{a}, s)} \ll \log N(\mathfrak{a}) + \log s$$

where the implied constant depends upon E. □

Proof of Lemma 3.7

Let us suppose $\mathfrak{b} = \mathrm{lcm}(\mathfrak{a}, s)$. Then $\mathbb{K}(E[\mathfrak{a}])\mathbb{K}(E[s]) = \mathbb{K}(E[\mathfrak{b}])$. Again it is well known that if a prime $\mathfrak{p}$ does not divide $6\Delta_E$, then $\mathbb{K}(E[\mathfrak{p}])/\mathbb{K}$ is unramified outside $6\mathfrak{p}\Delta_E$ but is totally ramified at $\mathfrak{p}$ and it has Galois group equal to $(\mathcal{O}_{\mathbb{K}}/\mathfrak{p})^*$. Since $(\mathfrak{b}, 6\Delta_E) = 1$, we must have $\mathrm{Gal}(\mathbb{K}(E[\mathfrak{b}])/\mathbb{K}) = (\mathcal{O}_{\mathbb{K}}/\mathfrak{b})^*$. Hence

$$[\mathbb{K}(E[\mathfrak{b}]) : \mathbb{K}] = \phi(\mathfrak{b}) = \frac{[\mathbb{K}(E[\mathfrak{a}]) : \mathbb{K}][\mathbb{K}(E[s]) : \mathbb{K}]}{\phi((\mathfrak{a}, s))}$$

Now, we take the aid of the following result to complete the proof.

Lemma 3.9 *Suppose that $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ are square free, $\mathfrak{a}, \mathfrak{c}$ are products of first degree primes, $(\mathfrak{a}, 6\Delta_E) = 1$, $\mathfrak{a}|\mathfrak{b}$, $\mathfrak{c}|\mathfrak{b}$ and $(N(\mathfrak{a}), N(\mathfrak{c})) = 1$. Then*

$$[\mathbb{K}(E[\mathfrak{b}], \mathfrak{a}^{-1}\mathfrak{c}^{-1}a) : \mathbb{K}(E[\mathfrak{b}], \mathfrak{c}^{-1}a)] = [\mathbb{L}_{\mathfrak{a}} : \mathbb{K}(E[\mathfrak{a}])]$$

Proof. Let us consider the Galois group $\mathrm{Gal}(\mathbb{K}(E[\mathfrak{b}], \mathfrak{a}^{-1}\mathfrak{c}^{-1}a)/\mathbb{K})$. This can be identified with a subgroup G_1 of

$$\left\{ \begin{pmatrix} 1 & \alpha \\ 0 & \beta \end{pmatrix} \ : \ \alpha \in \mathcal{O}_{\mathbb{K}}/\mathfrak{a}\mathfrak{c}, \ \beta \in (\mathcal{O}_{\mathbb{K}}/\mathfrak{b})^* \right\}$$

Again, the Galois group $\mathrm{Gal}(\mathbb{L}_{\mathfrak{a}}/\mathbb{K})$ can be identified with a subgroup G_2 of

$$\left\{ \begin{pmatrix} 1 & \alpha \\ 0 & \beta \end{pmatrix} \ : \ \alpha \in \mathcal{O}_{\mathbb{K}}/\mathfrak{a},\ \beta \in (\mathcal{O}_{\mathbb{K}}/\mathfrak{a})^* \right\}$$

Further, the subfields $\mathbb{K}(E[\mathfrak{b}], \mathfrak{c}^{-1}a)$ and $\mathbb{K}(E[\mathfrak{a}])$ correspond to the subgroups I_1 and I_2 of $\mathcal{O}_{\mathbb{K}}/\mathfrak{a}\mathfrak{c}$ and $\mathcal{O}_{\mathbb{K}}/\mathfrak{a}$ respectively, where

$$I_1 = \left\{ \alpha \ : \ \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \in G_1,\ \alpha \equiv 0 \pmod{\mathfrak{c}} \right\} \qquad I_2 = \left\{ \alpha \ : \ \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \in G_2 \right\}$$

To prove the result, we need to show that $|I_1| = |I_2|$. Now, it will suffice to prove that for each prime $p|N(\mathfrak{a})$, the projections $\phi_1 : I_1 \to \mathcal{O}_{\mathbb{K}}/(\mathfrak{a}, p)$ and $\phi_2 : I_2 \to \mathcal{O}_{\mathbb{K}}/(\mathfrak{a}, p)$ have the same image.

Suppose $p||N(\mathfrak{a})$, such that $(\mathfrak{a}, p) = \mathfrak{p}$ with $N(\mathfrak{p}) = p$. Then $\mathrm{Im}(\phi_1)$ and $\mathrm{Im}(\phi_2)$ can be 0 or $\mathcal{O}_{\mathbb{K}}/\mathfrak{p}$. Now, $\mathrm{Im}(\phi_1) = 0$ if and only if $\mathfrak{p}^{-1}a \in \mathbb{K}(E[\mathfrak{b}], \mathfrak{c}^{-1}a)$ and $\mathrm{Im}(\phi_2) = 0$ if and only if $\mathfrak{p}^{-1}a \in \mathbb{K}(E[\mathfrak{a}])$. This is evident that $\mathfrak{p}^{-1}a \in \mathbb{K}(E[\mathfrak{a}]) \ \Rightarrow \ \mathfrak{p}^{-1}a \in \mathbb{K}(E[\mathfrak{b}], \mathfrak{c}^{-1}a)$ which proves $\mathrm{Im}(\phi_1) = 0 \ \Rightarrow \mathrm{Im}(\phi_2) = 0$. Conversely, if $\mathrm{Im}(\phi_1) = 0$, then the projection $\{\alpha \ : \ \left(\begin{smallmatrix} 1 & \alpha \\ 0 & 1 \end{smallmatrix}\right) \in G_1\} \to \mathcal{O}_{\mathbb{K}}/\mathfrak{p}$ has a trivial image and $\mathfrak{p}^{-1}a \in \mathbb{K}(E[\mathfrak{b}])$. This implies $\mathfrak{p}^{-1}a \in \mathbb{K}(E[\mathfrak{a}])$ since otherwise the non-abelian extension $\mathbb{K}(E[\mathfrak{a}], \mathfrak{p}^{-1}a)$ would be contained in the abelian extension $\mathbb{K}(E[\mathfrak{b}])$, which is impossible. Thus, $\mathrm{Im}(\phi_1) = \mathrm{Im}(\phi_2)$.

Now, let us assume $p^2||N(\mathfrak{a})$ so that $(\mathfrak{a}, p) = \mathfrak{p}_1\mathfrak{p}_2$, say. Since $\mathrm{Gal}(\mathbb{K}(E[\mathfrak{p}])/\mathbb{K}) \simeq (\mathcal{O}_{\mathbb{K}}/p)^*$, we have for any $\delta \in (\mathcal{O}_{\mathbb{K}}/p)^*$, some $\beta \in (\mathcal{O}_{\mathbb{K}}/\mathfrak{a})^*$ and $\gamma \in \mathcal{O}_{\mathbb{K}}/\mathfrak{a}$ with $\beta \equiv \delta \pmod{p}$ and $\left(\begin{smallmatrix} 1 & \gamma \\ 0 & \beta \end{smallmatrix}\right) \in G_2$. Then for any $\alpha \in I_2$,

$$\begin{pmatrix} 1 & \gamma \\ 0 & \beta \end{pmatrix}^{-1} \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \gamma \\ 0 & \beta \end{pmatrix} \ = \ \begin{pmatrix} 1 & \alpha\beta \\ 0 & 1 \end{pmatrix} \ \in \ G_2$$

This shows that $\mathrm{Im}(\phi_2)$ is an ideal in $\mathcal{O}_{\mathbb{K}}/p$. Similarly, $\mathrm{Im}(\phi_1)$ is an ideal. Let us assume $\phi_i^{(j)} : I_i \to \mathcal{O}_{\mathbb{K}}/\mathfrak{p}_j$, so that we can write

$$\mathrm{Im}(\phi_i) \simeq \mathrm{Im}(\phi_i^{(1)}) \times \mathrm{Im}(\phi_i^{(2)})$$

for $i = 1, 2$. With an argument as before we can prove individually that $\mathrm{Im}(\phi_1^{(j)}) = \mathrm{Im}(\phi_2^{(j)})$ for $j = 1, 2$ and hence $\mathrm{Im}(\phi_1) = \mathrm{Im}(\phi_2)$. This proves the result. $\square$

Now, taking $\mathfrak{c} = 1$ in the result above, we obtain

$$
\begin{aligned}
&[\mathbb{K}(E[\mathfrak{b}], \mathfrak{a}^{-1}a) : \mathbb{K}(E[\mathfrak{b}])] = [\mathbb{L}_{\mathfrak{a}} : \mathbb{K}(E[\mathfrak{a}])] \\
\Rightarrow &[\mathbb{K}(E[\mathfrak{b}], \mathfrak{a}^{-1}a) : \mathbb{K}(E[\mathfrak{b}])][\mathbb{K}(E[\mathfrak{b}]) : \mathbb{K}] = \frac{[\mathbb{L}_{\mathfrak{a}} : \mathbb{K}(E[\mathfrak{a}])][\mathbb{K}(E[\mathfrak{a}]) : \mathbb{K}][\mathbb{K}(E[s]) : \mathbb{K}]}{\phi((\mathfrak{a}, s))} \\
\Rightarrow &[\mathbb{L}_{\mathfrak{a},s} : \mathbb{K}] = \frac{[\mathbb{L}_{\mathfrak{a}} : \mathbb{K}][\mathbb{K}_s : \mathbb{K}]}{\phi((\mathfrak{a}, s))} \\
\Rightarrow &n(\mathfrak{a}, s) = \frac{n(\mathfrak{a})m(s)}{\phi((\mathfrak{a}, s))}
\end{aligned}
$$

□

3.4 Result 2: Gupta and Murty

Theorem 3.3 (Gupta and Murty, 1986) *If 2 and 3 are inert in $\mathbb{K}$ or if $\mathbb{K} = \mathbb{Q}(\sqrt{-11})$, then $C_E(a) > 0$. Hence, assuming GRH in these cases, we obtain*

$$N_a^*(x) \gg \frac{x}{\log x}$$

Proof. We have obtained the density δ from the previous section as follows

$$\delta = \sum_{\mathfrak{a},s} \frac{\mu(\mathfrak{a})\mu(s)}{n(\mathfrak{a}, s)}$$

Now, to decompose δ in form of an infinite product, we need the following result

Lemma 3.10 *Let $\mathfrak{a} = \mathfrak{a_1}\mathfrak{b}$, $s = s_1 b$ where $(\mathfrak{a_1}, 6\Delta_E) = (s_1, 6\Delta_E) = 1$ and $\mathfrak{b}, b | 6\Delta_E$. Then $n(\mathfrak{a}, s) = n(\mathfrak{a_1}, s_1)n(\mathfrak{b}, b)$.*

Proof. Proved in Section 3.4.3.

Using Lemma 3.10 and the fact that Möbius function is a multiplicative function over square free $\mathfrak{a}$ and s, we can write

$$\delta = \sum_{\substack{\mathfrak{a_1}, s_1 \\ \mathfrak{b}, b}} \frac{\mu(\mathfrak{a_1})\mu(s_1)}{n(\mathfrak{a_1}, s_1)} \cdot \frac{\mu(\mathfrak{b})\mu(b)}{n(\mathfrak{b}, b)} = \sum_{\mathfrak{b}, b} \frac{\mu(\mathfrak{b})\mu(b)}{n(\mathfrak{b}, b)} \cdot \sum_{\mathfrak{a_1}, s_1} \frac{\mu(\mathfrak{a_1})\mu(s_1)}{n(\mathfrak{a_1}, s_1)} = \delta_0 \cdot \delta_1$$

where

$$\delta_0 = \sum_{\mathfrak{b}, b} \frac{\mu(\mathfrak{b})\mu(b)}{n(\mathfrak{b}, b)} \quad \text{and} \quad \delta_1 = \sum_{\mathfrak{a_1}, s_1} \frac{\mu(\mathfrak{a_1})\mu(s_1)}{n(\mathfrak{a_1}, s_1)}$$

where the above sums run over $\mathfrak{a_1}, s_1$ coprime to $6\Delta_E$ and $\mathfrak{b}, b$ the divisors formed by the first degree prime ideal factors of $(6\Delta_E)$ and prime factors of $6\Delta_E$ respectively. We will analyze the two terms δ_0 and δ_1 individually to prove Theorem 3.3.

3.4.1 Analysis of δ_1

Let us take a look at the second term δ_1 first. As we have $(\mathfrak{a}_1, 6\Delta_E) = (s_1, 6\Delta_E) = 1$, we can utilize Lemma 3.7 to write

$$\delta_1 \;=\; \sum_{\mathfrak{a}_1, s_1} \frac{\mu(\mathfrak{a}_1)\mu(s_1)}{n(\mathfrak{a}_1)m(s_1)}\phi(\mathfrak{a}_1, s_1) \;=\; \sum_{s_1} \frac{\mu(s_1)}{m(s_1)} \prod_{\mathfrak{q}} \left(1 - \frac{\phi(\mathfrak{q}, s_1)}{n(\mathfrak{q})}\right)$$

where the product is over the first degree prime ideals of $\mathcal{O}_{\mathbb{K}}$. As $\mathfrak{q}$ is a prime ideal, $(\mathfrak{q}, s_1) \neq 1$ only when $\mathfrak{q}|s_1$. Again, in that case, $\phi(\mathfrak{q}, s_1)/n(\mathfrak{q}) = \phi(\mathfrak{q})/n(\mathfrak{q}) = 1/N(\mathfrak{q})$. Based on this, we can decompose the infinite product as follows

$$\begin{aligned}
\delta_1 \;&=\; \prod_{\mathfrak{q}} \left(1 - \frac{1}{n(\mathfrak{q})}\right) \cdot \sum_{s_1} \frac{\mu(s_1)}{m(s_1)} \prod_{\mathfrak{q}|s_1} \left(1 - \frac{1}{N(\mathfrak{q})}\right) \left(1 - \frac{1}{n(\mathfrak{q})}\right)^{-1} \\
&=\; \prod_{\substack{q \text{ inert in } \mathbb{K} \\ (q, 6\Delta_E)=1}} \left(1 - \frac{1}{q^2 - 1}\right) \cdot \prod_{\substack{q \text{ splits in } \mathbb{K} \\ (q, 6\Delta_E)=1}} \left(1 - \frac{1}{q^2 - 1}\right) \left(1 - \frac{1}{q - 1}\right) \left(1 + \frac{1}{q}\right) \\
&=\; \prod_{\substack{q \text{ inert in } \mathbb{K} \\ (q, 6\Delta_E)=1}} \left(1 - \frac{1}{q^2 - 1}\right) \cdot \prod_{\substack{q \text{ splits in } \mathbb{K} \\ (q, 6\Delta_E)=1}} \left(1 - \frac{2}{q(q-1)} - \frac{1}{(q-1)^2} + \frac{2}{q(q-1)^2}\right)
\end{aligned}$$

Here, we do not see the prime factors which ramify in $\mathbb{K}$ because of the fact that all those factors divide $6\Delta_E$. Hence, we can conclude that $\delta_1 > 0$. It remains to analyze the cases where $\delta_0 > 0$

3.4.2 Analysis of δ_0

We have obtained, for $\mathfrak{b}$ and b running over the divisors of $6\Delta_E$ formed by first degree prime ideal factors of $(6\Delta_E)$ and prime factors of $6\Delta_E$ respectively,

$$\delta_0 \;=\; \sum_{\mathfrak{b}, b} \frac{\mu(\mathfrak{b})\mu(b)}{n(\mathfrak{b}, b)}$$

Note that δ_0 actually gives the density of prime ideals π_p which do not split in any extension $\mathbb{L}_{\mathfrak{b},b}$. Let us define a new term δ^* which represents the density of prime ideals π_p which do not split completely in any $\mathbb{K}_q$ or $\mathbb{K}(E[\mathfrak{q}])$. Hence, we obtain $\delta_0 \geq \delta^*$. As we are considering only the imaginary quadratic field extensions $\mathbb{K}$ with class number 1, our choices are restricted to $\mathbb{K} = \mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-4})$, $\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-8})$, $\mathbb{Q}(\sqrt{-11})$, $\mathbb{Q}(\sqrt{-19})$, $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$, $\mathbb{Q}(\sqrt{-163})$. Now, we take up different cases to analyze the term δ^* for different $\mathbb{K}$.

Case 1: 2 and 3 are inert in $\mathbb{K}$

If 2 or 3 are inert in $\mathbb{K}$, it means that $\mathbb{K} \neq \mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$. The extension fields obtained by adjoining $E(\mathfrak{q})$ to $\mathbb{K}$ contain the ray class fields. For a given ideal $\mathfrak{a} \in \mathcal{O}_{\mathbb{K}}$, the ray class field $\mathbb{K}(\mathfrak{a})$ has degree $\phi(\mathfrak{a})/w(\mathfrak{a})$ where $w(\mathfrak{a})$ represents the number of inequivalent units modulo $\mathfrak{a}$. Now let us consider the field $\mathbb{T}_{\mathfrak{a}} = \prod_{\mathfrak{p}|\mathfrak{a}} \mathbb{K}(\mathfrak{p})$, where the product is over all the prime ideal divisors $\mathfrak{p}$ of $\mathfrak{a}$. As $\mathfrak{p}$ are distinct prime ideals, we have the fields $\mathbb{K}(\mathfrak{p})$ to be disjoint and hence

$$[\mathbb{T}_{\mathfrak{a}} : \mathbb{K}] \;=\; \prod_{\mathfrak{p}|\mathfrak{a}} [\mathbb{K}(\mathfrak{p}) : \mathbb{K}] \;=\; \prod_{\mathfrak{p}|\mathfrak{a}} \frac{\phi(\mathfrak{p})}{w(\mathfrak{p})}$$

Now, from the definition of δ^*, we obtain

$$\delta^* \;\geq\; \prod_{\mathfrak{p}|6\Delta_E} \left(1 - \frac{w(\mathfrak{p})}{\phi(\mathfrak{p})}\right)$$

From the definition of $w(\mathfrak{p})$, we know that $w(\mathfrak{p}) = 2$ for all $\mathfrak{p} \neq 2$ and $w(\mathfrak{p}) = 1$ for $\mathfrak{p} = 2$. So, $(1 - w(\mathfrak{p}/\phi(\mathfrak{p})) = 0$ only when $\mathfrak{p} = 2$ or 3. In this case, we have 2 and 3 to be inert in $\mathbb{K}$, which means $\mathfrak{p} \neq 2$ or 3, and hence $\delta^* > 0$. So, we have proved that $\delta_0 > 0 \;\Rightarrow\; C_E(a) > 0$ for the cases $\mathbb{K} = \mathbb{Q}(\sqrt{-19}), \mathbb{Q}(\sqrt{-43}), \mathbb{Q}(\sqrt{-67})$ and $\mathbb{Q}(\sqrt{-163})$, where 2 and 3 are inert in $\mathbb{K}$.

Case 2: $\mathbb{K} = \mathbb{Q}(\sqrt{-11})$

This case is a little bit tricky, as 3 splits in $\mathbb{Q}(\sqrt{-11})$. Let us suppose 3 splits as $\mathfrak{p}_1\mathfrak{p}_2$. We will consider the extensions $\mathbb{K}(E[\mathfrak{p}_1])$ and $\mathbb{K}(E[\mathfrak{p}_2])$ instead of the trivial ray class fields in this case. We can write $\mathbb{K}(E[3]) \;=\; \mathbb{K}(E[\mathfrak{p}_1])\mathbb{K}(E[\mathfrak{p}_2])$ where $\mathbb{K}(E[3])$ is disjoint from the fields $\mathbb{K}(\mathfrak{p})$ where $\mathfrak{p} \neq \mathfrak{p}_1$ or $\mathfrak{p}_2$. Hence we have

$$\delta^* \;\geq\; \left(1 - \frac{1}{[\mathbb{K}(E[\mathfrak{p}_1]) : \mathbb{K}]}\right)\left(1 - \frac{1}{[\mathbb{K}(E[\mathfrak{p}_2]) : \mathbb{K}]}\right) \prod_{\substack{\mathfrak{p}|6\Delta_E \\ \mathfrak{p}\neq\mathfrak{p}_1,\mathfrak{p}_2}} \left(1 - \frac{w(\mathfrak{p})}{\phi(\mathfrak{p})}\right)$$

Now, we also know that $\mathbb{K}(E[\mathfrak{p}_1])$ and $\mathbb{K}(E[\mathfrak{p}_2])$ are quadratic extensions of $\mathbb{K}$. Therefore, we can conclude $\delta^* > 0 \;\Rightarrow\; \delta_0 > 0 \;\Rightarrow\; C_E(a) > 0$ in this case as well.

Case 3: $\mathbb{K} = \mathbb{Q}(\sqrt{-7})$

In this case, if E has complex multiplication by the maximal order of $\mathcal{O}_{\mathbb{K}}$, then 2 splits in $\mathbb{K}$. Hence, all the 2-division points are contained in $\mathbb{K}$. Now, if p splits in $\mathbb{K}$, then the 2-division points are contained in $\overline{E}(\mathbb{F}_p)$ as well. Hence, from a similar calculation as before, we see that $\delta_0 = \delta^* = 0$. So, $C_E(a) = 0$ in this case.

Case 4: $\mathbb{K} = \mathbb{Q}(\sqrt{-2})$

For analyzing this case, we will need to utilize the following result.

Lemma 3.11 *Let $\mathbb{K}_i$, $i \in I$, be a finite set of non-trivial disjoint normal extensions of $\mathbb{K}$, and let $\mathbb{L}/\mathbb{K}$ be a normal extension with prime degree. Then*

(i) Either $\mathbb{L} \nsubseteq \prod_{i\in I} \mathbb{K}_i$ or there is a unique minimal subset I_L of I such that $\mathbb{L} \subset \prod_{i\in I_L} \mathbb{K}_i$.

(ii) The density of first degree prime ideals which do not split completely in $\mathbb{L}$ or any $\mathbb{K}_i$ is zero if and only if $\mathbb{L} \subset \prod_{i\in I} \mathbb{K}_i$, $[\mathbb{L} : \mathbb{K}] = 2$, $|I_L|$ is even, and for each $i \in I_L$, $[\mathbb{K}_i : \mathbb{K}] = 2$.

Proof. Proved in Section 3.4.3.

Now in the case $\mathbb{K} = \mathbb{Q}(\sqrt{-2})$, 2 ramifies in $\mathbb{K}$ and 3 splits as $\mathfrak{p}_1\mathfrak{p}_2$, say. Analogous to the case of $\mathbb{K} = \mathbb{Q}(\sqrt{-11})$, here the extensions $\mathbb{K}(E[2]), \mathbb{K}(E[3])$ and $\mathbb{K}(\mathfrak{p})$ for $\mathfrak{p}|6\Delta_E$, $\mathfrak{p} \neq \mathfrak{p}_1, \mathfrak{p}_2, (\sqrt{-2})$ are non-trivial disjoint extension fields of $\mathbb{K}$. Further, only the fields $\mathbb{K}(E[\mathfrak{p}_1]), \mathbb{K}(E[\mathfrak{p}_2])$ and $\mathbb{K}(E[2])$ are quadratic extensions of $\mathbb{K}$.

Let us apply the result of Lemma 3.11 allowing $\mathbb{K}_i$ to range over $\mathbb{K}(E[\mathfrak{p}_1]), \mathbb{K}(E[\mathfrak{p}_2])$, $\mathbb{K}(E[2]), \mathbb{K}(\mathfrak{p})$ and $\mathbb{L} = \mathbb{K}((\sqrt{-2})^{-1}a)$. If $\mathbb{L} = \mathbb{K}$, then there exists some $b \in E(\mathbb{K})$ satisfying $a = \sqrt{-2}b$. This implies $\delta_0 = 0$. Otherwise, if $\mathbb{L}$ is a quadratic extension of $\mathbb{K}$, then $\mathbb{L} \subset \mathbb{K}(E[\mathfrak{p}_1])\mathbb{K}(E[\mathfrak{p}_2])\mathbb{K}(E[2]) \Rightarrow \mathbb{L} = \mathbb{K}(E[2])$ in the case where $\mathfrak{p}_1$ and $\mathfrak{p}_2$ do not ramify in $\mathbb{L}$. In this case, we get $\delta_0 > 0$ from Lemma 3.11. Thus, we obtain $\delta > 0 \Rightarrow C_E(a) > 0$ most of the time in this case.

3.4.3 Proof of Lemmas

Proof of Lemma 3.10

To prove $n(\mathfrak{a}, s) = n(\mathfrak{a}_1, s_1)n(\mathfrak{b}, b)$, it suffices to show that $[\mathbb{L}_{\mathfrak{a},s} : \mathbb{L}_{\mathfrak{b},b}] = [\mathbb{L}_{\mathfrak{a}_1,s_1} : \mathbb{K}]$. We know that if $\mathfrak{p}|\ \mathrm{lcm}(\mathfrak{a}_1, s_1)$, then $\mathbb{K}(E[\mathfrak{p}])$ is an extension of $\mathbb{K}$ in which $\mathfrak{p}$ ramifies completely and the primes not dividing $6\mathfrak{p}\Delta_E$ do not ramify at all. Again, $\mathfrak{p}$ does not ramify in $\mathbb{L}_{\mathfrak{b},b}$. Hence, for $\mathfrak{d} = \ \mathrm{lcm}(\mathfrak{a}, s)$ and $\mathfrak{c} = \ \mathrm{lcm}(\mathfrak{a}_1, s_1)$, we have

$$[\mathbb{K}(E[\mathfrak{d}], \mathfrak{b}^{-1}a) : \mathbb{L}_{\mathfrak{b},b}] = [\mathbb{K}(E[\mathfrak{c}]) : \mathbb{K}]$$

Furthermore, by Lemma 3.9, we have that

$$[\mathbb{L}_{\mathfrak{a}_1} : \mathbb{K}(E[\mathfrak{a}_1])] = [\mathbb{L}_{\mathfrak{a},s} : \mathbb{K}(E[\mathfrak{d}], \mathfrak{b}^{-1}a)] = [\mathbb{L}_{\mathfrak{a}_1,s_1} : \mathbb{K}(E[\mathfrak{c}])]$$

Hence, we can obtain

$$\begin{aligned}[\mathbb{L}_{\mathfrak{a},s} : \mathbb{L}_{\mathfrak{b},b}] &= [\mathbb{L}_{\mathfrak{a},s} : \mathbb{K}(E[\mathfrak{d}], \mathfrak{b}^{-1}a)][\mathbb{K}(E[\mathfrak{d}], \mathfrak{b}^{-1}a) : \mathbb{L}_{\mathfrak{b},b}] \\ &= [\mathbb{L}_{\mathfrak{a}_1,s_1} : \mathbb{K}(E[\mathfrak{c}])][\mathbb{K}(E[\mathfrak{c}]) : \mathbb{K}] \\ &= [\mathbb{L}_{\mathfrak{a}_1,s_1} : \mathbb{K}] \end{aligned}$$

□

Proof of Lemma 3.11

For a subset $J \subset I$, let us define $\mathbb{K}_J = \prod_{i \in J} \mathbb{K}_i$. Now, since the $\mathbb{K}_i$ are disjoint, if $\mathbb{L} \subset \mathbb{K}_{J_1}$ and $\mathbb{L} \subset \mathbb{K}_{J_2}$, we must have $\mathbb{L} \subset \mathbb{K}_{J_1 \cap J_2}$. Thus, if $\mathbb{L} \subset \mathbb{K}_I$, then there exists a minimal subset $I_L \subset I$ such that $\mathbb{L} \subset \mathbb{K}_{I_L}$. Hence, the result in Lemma 3.11 (i) follows.

Let us suppose $\mathbb{L} \not\subset \mathbb{K}_I$. Then as $[\mathbb{L} : \mathbb{K}]$ is prime, $\mathbb{L}$ must be disjoint from all the $\mathbb{K}_i$'s. Hence, we have positive density for the first degree prime ideals not splitting completely in $\mathbb{L}$ or any $\mathbb{K}_i$.

Now, if $\mathbb{L} \subset \mathbb{K}_I$, the density of primes not splitting completely in $\mathbb{L}$ or any $\mathbb{K}_i$ is given by

$$\begin{aligned} &\sum_{J \subset I} \frac{\mu(J)}{[\mathbb{K}_J : \mathbb{K}]} - \frac{1}{[\mathbb{L} : \mathbb{K}]} \sum_{\substack{J \subset I \\ I_L \not\subset J}} \frac{\mu(J)}{\mathbb{K}_J : \mathbb{K}} - \sum_{\substack{J \subset I \\ I_L \subset J}} \frac{\mu(J)}{\mathbb{K}_J : \mathbb{K}} \\ &= \frac{[\mathbb{L} : \mathbb{K}] - 1}{[\mathbb{L} : \mathbb{K}]} \left(\sum_{J \subset I} \frac{\mu(J)}{\mathbb{K}_J : \mathbb{K}} - \sum_{\substack{J \subset I \\ I_L \subset J}} \frac{\mu(J)}{\mathbb{K}_J : \mathbb{K}} \right) \\ &= \frac{[\mathbb{L} : \mathbb{K}] - 1}{[\mathbb{L} : \mathbb{K}]} \left(\prod_{i \in I} \left(1 - \frac{1}{[\mathbb{K}_i : \mathbb{K}]} \right) - \frac{\mu(I_L)}{[\mathbb{K}_{I_L} : \mathbb{K}]} \prod_{i \notin I_L} \left(1 - \frac{1}{[\mathbb{K}_i : \mathbb{K}]} \right) \right) \end{aligned}$$

Hence, the density is zero if and only if we have the following

$$\prod_{i \in I_L} \left(1 - \frac{1}{[\mathbb{K}_i : \mathbb{K}]} \right) = \frac{\mu(I_L)}{[\mathbb{K}_{I_L} : \mathbb{K}]} = \mu(I_L) \prod_{i \in I_L} \frac{1}{[\mathbb{K}_i : \mathbb{K}]}$$

which implies $[\mathbb{K}_i : \mathbb{K}] = 2$ for all $i \in I_L$, $[\mathbb{L} : \mathbb{K}] = 2$ and $\mu(I_L) = 1$. Hence, the claim in Lemma 3.11 (ii) follows. □

3.5 Result 3: Gupta and Murty

In the same paper [8], Gupta and Murty proved the higher rank analogue of the conjecture which was foreseen by Lang and Trotter [15]. They considered a free

subgroup Γ of rational points instead of taking the whole group to be an infinite cyclic one and formulated the conjecture in the lines of Lang and Trotter. Gupta and Murty propose and prove the following theorem about the density of primes p for which the free subgroup Γ will generate the elliptic curve group E under the reduction modulo p, provided the rank of Γ is sufficiently large.

Theorem 3.4 (Gupta and Murty, 1986) *Let $E(\mathbb{Q})$ be an elliptic curve and let Γ be a free subgroup of rational points. If we define*

$$N_\Gamma(x) = \#\{p \leq x \ : \ \Gamma_p = \overline{E}(\mathbb{F}_p)\}$$

where $\overline{E}(\mathbb{F}_p)$ and Γ_p are the images of E and Γ modulo p respectively, under the assumption of generalized Riemann hypothesis, there exists a constant $C_E(\Gamma)$ such that as $x \to \infty$, we obtain:

$$N_\Gamma(x) \ = \ C_E(\Gamma)\frac{x}{\log x} \ + \ o\left(\frac{x}{\log x}\right)$$

and this holds for $\text{rank}(\Gamma) \geq 18$ *in the case where E has no complex multiplication and for* $\text{rank}(\Gamma) \geq 10$ *in the case where E has complex multiplication over the entire ring of integers of some quadratic extension of $\mathbb{Q}$.*

3.5.1 Proof of Theorem 3.4

Let us assume that the points $P_1, P_2, ..., P_r$ are r independent generators of the free subgroup Γ, that is $r =$ $\text{rank}(\Gamma)$. Now, for a prime q, let us consider the extension

$$\mathbb{M}_q = \mathbb{Q}(E[q], q^{-1}P_1, ..., q^{-1}P_r)$$

This extension is a normal extension over $\mathbb{Q}$ and we can easily prove that the Galois group

$$\text{Gal}(\mathbb{M}_q/\mathbb{Q}) \subset GL_2(\mathbb{F}_q) \rtimes E[q]^r$$

So, we may view the elements of the Galois group as pairs $\sigma = (\gamma, \tau)$ where $\gamma \in GL_2(\mathbb{F}_q)$ and $\tau \in E[q]^r$. Hence, we can state the index divisibility criterion to be Lemma 3.2 as formulated by Lang and Trotter.

Now, the primes those divide the discriminant Δ_E and result in a 'bad' reduction introduce an error of $O(1)$ and can be ignored. Again, if $p = q$, then as shown before in Result 1, we obtain $p + 1 - a_p \equiv 0 \pmod{p}$. We know, due to Serre [18], that these primes introduce an error of $o(x/\log x)$. So, within our error bound, we can assume that $p \nmid q\Delta_E$.

It can easily be shown that the number of γ_p such that $\ker(\gamma - 1)$ is cyclic is $q + O(1)$ in the CM case and $q^3 + O(q^2)$ in the non-CM case. Hence the number of elements $\sigma_p \in \text{ Gal}(\mathbb{M}_q/\mathbb{Q})$ satisfying condition (i) of Lemma 3.2 is $q^{r+1} + O(q^r)$ in the CM case and $q^{r+3} + O(q^{r+2})$ in the non-CM case. Again, the number of elements satisfying condition (ii) of Lemma 3.2 is $q^{r+1} + q^r - q$ because for sufficiently large q, the Galois group $\text{ Gal}(\mathbb{M}_q/\mathbb{Q}(E[q]))$ is isomorphic to $E[q]^r$ given by the map

$$(q^{-1}P_1, ..., q^{-1}P_r) \mapsto (q^{-1}P_1 + a_1, ..., q^{-1}P_r + a_r)$$

and clearly $\tau(\Gamma)$ is a subgroup of $E[q]$ generated by $a_1, ..., a_r$.

To prove Theorem 3.4, we need to estimate the following quantity

$$\begin{aligned} N_\Gamma(x) &= \#\{p \leq x \mid \overline{E}(\mathbb{F}_p) = \Gamma_p\} \\ &= \#\{p \leq x \mid q \nmid i(p) \ \forall \text{ primes } q\} \\ &= \#\{p \leq x \mid \sigma_p(\mathbb{M}_q/\mathbb{Q}) \notin S_q \ \forall \text{ primes } q\} \end{aligned}$$

As in the case of Theorem 3.1, let us define the following two terms

$$\begin{aligned} N_\Gamma(x, y) &= \#\{p \leq x \mid \sigma_p(\mathbb{M}_q/\mathbb{Q}) \notin S_q \ \forall \text{ primes } q < y\} \\ M_\Gamma(x, y_1, y_2) &= \#\{p \leq x \mid \sigma_p(\mathbb{M}_q/\mathbb{Q}) \in S_q \text{ for some prime } y_1 < q < y_2\} \end{aligned}$$

Then, similar to the relation formulated in Result 1, we have

$$N_\Gamma(x) = N_\Gamma(x, y_1) + O\left(M_\Gamma(x, y_1, 2x)\right)$$

Estimate of $N_\Gamma(x, y_1)$

Let us consider the extension $\mathbb{M}_s = \prod_{q|s} \mathbb{M}_q$ for a square-free integer s. Then, the sets S_q's for all prime divisors q of s determine a conjugacy class $S_s \subset \text{ Gal}(\mathbb{M}_s/\mathbb{Q})$. Let us define

$$\pi_\Gamma(x, s) = \#\{p \leq x \mid \sigma_p(\mathbb{M}_s/\mathbb{Q}) \in S_s\}$$

Then, by an inclusion-exclusion argument, we obtain

$$N_\Gamma(x, y_1) = \sum_s{}' \mu(s)\pi_\Gamma(x, s)$$

where the dashed summation represents a sum over all s such that $q \leq y_1$ for each prime divisor q of s. To utilize the result of Theorem 3.2 in this case, let us take $C = S_s$, $n = |\text{ Gal}(\mathbb{M}_s/\mathbb{Q})|$, $d = \text{ disc}(\mathbb{M}_s/\mathbb{Q})$. Hence we obtain

$$N_\Gamma(x, y_1) = \sum_s{}' \mu(s)\frac{|S_s|}{n} \text{ li}x + O\left(|S_s|x^{1/2}\sum_s{}'\left(\log x + \frac{\log|d|}{n}\right)\right)$$

Following similar steps as in the proof of Result 1 and fixing $y_1 = \left(\frac{1}{4}\log x\right)^{1/(r+2)}$, we get

$$N_\Gamma(x, y_1) \;=\; \sum_s{}' \mu(s)\delta(s)\ \mathrm{li}x \;+\; O\left(x^{1-\epsilon}\right)$$

where $\delta(s) = |S_s|/n$. Again, as we have $\delta(s) = O(s^{-(r+1)})$, we obtain that if we convert the restricted dashed sum to an unrestricted sum over all s by a procedure similar to Result 1, then $\sum_s \mu(s)\delta(s)$ is absolutely convergent. Hence, we can term it $C_E(\Gamma)$ and we get

$$N_\Gamma(x, y_1) \;=\; C_E(\Gamma)\frac{x}{\log x} \;+\; o\left(\frac{x}{\log x}\right)$$

Estimate of $M_\Gamma(x, y_1, 2x)$

Let us consider the extensions $\mathbb{V}_{q,i} = \mathbb{Q}(E[q], q^{-1}P_i)$ for each of the generators P_i of Γ. Now, if we have $\sigma_p(\mathbb{M}_q/\mathbb{Q}) \in S_q$, then the restriction of σ_p over $\mathbb{V}_{q,i}$ should satisfy the Lang and Trotter criterion mentioned in Lemma 3.1 for all $i = 1, ..., r$. From Approach 1 of Lang and Trotter, we know that the image of S_q restricted to $\mathbb{V}_{q,i}$ would be $O(q^2)$ in the CM case and $O(q^4)$ in the non-CM case. Then, we can utilize Theorem 3.2 once again to obtain

$$M_\Gamma(x, y_1, y_2) \;\leq\; \sum_{y_1<q<y_2} \left(\frac{1}{q^2}\ \mathrm{li}x \;+\; O\left(q^g x^{1/2}\log x\right)\right)$$

where $g = 2$ in the CM case and $g = 4$ in the non-CM case. For our choice of $y_1 = \left(\frac{1}{4}\log x\right)^{1/(r+2)}$, we have the summation of the first term to be $o(x/\log x)$. The error term is $o(y_2^{g+1}x^{1/2})$. So, we choose $y_2^{g+1} = x^{1/2}/\log^2 x$ so that the error term becomes $o(x/\log x)$. With this choice of y_2, we obtain

$$M_\Gamma(x, y_1, 2x) = M_\Gamma(x, y_1, y_2) + M_\Gamma(x, y_2, 2x) = o\left(\frac{x}{\log x}\right) + M_\Gamma(x, y_2, 2x)$$

It remains to deal with the second term $M_\Gamma(x, y_2, 2x)$. Let us break it apart as follows

$$M_\Gamma(x, y_2, 2x) = M_\Gamma(x, y_2, y_3) + M_\Gamma(x, y_3, 2x)$$

Now, for the second term, if $\sigma_p(\mathbb{M}_q/\mathbb{Q}) \in S_q$ for $y_3 < q < 2x$, then $|\Gamma_p| < x/y_3$. Here, we take the help of the following result to choose y_3 as per requirement.

Lemma 3.12 *The number of primes p satisfying $|\Gamma_p| < y$ is $O\left(y^{1+2/r}\right)$.*

Proof. Proved in Section 3.5.2.

Using this result, we obtain that in the range $y_3 < q < 2x$, $M_\Gamma(x, y_3, 2x) = o\left((x/y_3)^{1+2/r}\right)$. Now, if we choose $y_3 = y_2 \log^A x$, then this condition gives us

$$\begin{aligned} M_\Gamma(x, y_3, 2x) &= o\left(\left(x^{1-\frac{1}{2(g+1)}}(\log x)^{-A+\frac{2}{g+1}}\right)^{1+\frac{2}{r}}\right) \\ &= o\left(x^{1-\frac{1}{(g+1)r}+\frac{2}{r}-\frac{1}{2(g+1)}}(\log x)^{\left(-A+\frac{2}{g+1}\right)\left(1+\frac{2}{r}\right)}\right) \end{aligned}$$

So, for sufficiently large A, to obtain $M_\Gamma(x, y_3, 2x) = o(x/\log x)$, we need

$$-\frac{1}{(g+1)r} + \frac{2}{r} - \frac{1}{2(g+1)} \geq 0 \quad \Leftrightarrow \quad r \geq 4g+2$$

We are only left with the term $M_\Gamma(x, y_2, y_3)$. This can be shown to be less than the term $M(x, y_2, y_3)$ as in the proof of Result 1. Further, we can use the Brun-Titchmarsh sieve to prove that $M(x, y_2, y_3) = o(x/\log x)$ for our choice of y_2 and y_3. This proves that

$$M_\Gamma(x, y_1, 2x) = o\left(\frac{x}{\log x}\right) \quad \text{for } r \geq 4g+2$$

As stated earlier, we have $g = 2$ for CM case and $g = 4$ for the non-CM case. Hence, we can conclude that for $r \geq 10$ in the CM case and $r \geq 18$ in the non-CM case

$$N_\Gamma(x) \;=\; C_E(\Gamma)\frac{x}{\log x} \;+\; o\left(\frac{x}{\log x}\right)$$

This completes the proof of Theorem 3.4, where $C_E(\Gamma)$ is a positive constant depending only on the choice of the elliptic curve E and the free subgroup of rational points Γ.

In this context, let us consider the current record for the rank of elliptic curves. Let E be an elliptic curve over $\mathbb{Q}$. By Mordell's theorem, $E(\mathbb{Q})$ is a finitely generated abelian group. This means that $E(\mathbb{Q}) = E(\mathbb{Q})_{tors} \times \mathbb{Z}^r$. By Mazur's theorem [19], we know that $E(\mathbb{Q})_{tors}$ is one of the following 15 groups: $\mathbb{Z}/n\mathbb{Z}$ with $1 \leq n \leq 10$ or $n = 12$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ with $1 \leq m \leq 4$. But, it is not known what specific values of rank r are possible for elliptic curves over $\mathbb{Q}$. The 'folklore' conjecture is that a rank can be arbitrary large. The current record is an example of elliptic curve with $r \geq 28$, found by Elkies in 2006 (the previous record was $r \geq 24$, found by Martin and McMillen in 2000). The highest rank of an elliptic curve which is known exactly is $r = 18$, and it was found by Elkies in 2006. It improves previous records due to Kretschmer ($r = 10$), Schneiders-Zimmer ($r = 11$), Fermigier ($r = 14$), Dujella ($r = 15$) and Elkies ($r = 17$) [5]. Hence, we now have definite curves with sufficiently higher ranks so as to follow Theorem 3.4.

3.5.2 Proof of Lemmas

Proof of Lemma 3.12

As we have already assumed, let $P_1, ..., P_r$ be r independent generators of Γ. We will utilize the concept of canonical height pairing by Néron and Tate [19], which is a positive semidefinite bilinear pairing on $E(\overline{\mathbb{Q}})$ with the property that $\langle P, P\rangle = 0$ if and only if P is a torsion point on the curve. Let us denote the canonical height pairing by $H(P) = \langle P, P\rangle$ and the naive a-height of a point $P = (a, b)$ by $h_a(P) = \log \max(|r|, |s|)$ where $a = r/s$ with r, s coprime. In that case, we have $H(P) = h_a(P) + O(1)$ where the implied constant depends only on E. Let us consider the following set

$$S = \{(n_1, ..., n_r) \in \mathbb{Z}^r : H(n_1P_1 + \cdots + n_rP_r) \leq Cy^{2/r}\}$$

with the constant C satisfying $(C\pi)^{\frac{r}{2}}/\sqrt{R}\Gamma\left(\frac{r}{2}+1\right) > 1$ where $R = \det(\langle P_i, P_j\rangle)$. Now, we will use the following result to prove this lemma.

Lemma 3.13

$$\#\{(n_1, ..., n_r) \in \mathbb{Z}^r : H(n_1P_1+\cdots+n_rP_r) \leq x\} = \frac{(x\pi)^{\frac{r}{2}}}{\sqrt{\det(\langle P_i, P_j\rangle)}\Gamma\left(\frac{r}{2}+1\right)} + O\left(x^{\frac{r-1}{2+\epsilon}}\right)$$

Proof.

$$\begin{aligned}
&\#\left\{(n_1, ..., n_r) \in \mathbb{Z}^r : H(n_1P_1 + \cdots + n_rP_r) \leq x\right\} \\
&= \#\left\{(n_1, ..., n_r) \in \mathbb{Z}^r : \left\langle \sum_{i=1}^{r} n_iP_i, \sum_{i=1}^{r} n_iP_i \right\rangle \leq x\right\} \\
&= \#\left\{(n_1, ..., n_r) \in \mathbb{Z}^r : \sum_{i,j} n_in_j\langle P_i, P_j\rangle \leq x\right\}
\end{aligned}$$

which is equivalent to counting lattice points in the r-dimensional ellipsoid defined by the quadratic form $\sum_{i,j} n_in_j\langle P_i, P_j\rangle \leq x$. The number of lattice points in such an ellipsoid is given by the expression in the lemma [8]. □

Using the result above, we get $|S| > y$. Again, we have $|\Gamma_p| < y$. Hence, by the pigeon hole principle, we must have two distinct r-tuples $(n_1, ..., n_r)$ and $(m_1, ..., m_r)$ such that

$$n_1P_1 + \cdots + n_rP_r \equiv m_1P_1 + \cdots + m_rP_r \pmod{p}$$

So, the denominator of the non-zero point $\sum_{i=1}^{r}(n_i - m_i)P_i = Q$ is divisible by p. The number of such primes is obviously less than $h_a(Q)$. Again, $H(Q) \neq 0$ as Q is not a torsion point for independent $P_1, ..., P_r$. Therefore, $h_a(Q) \ll H(Q) \leq 2Cy^{2/r}$. So, by Lemma 3.13, the number of such points Q is $O(y)$. Now, each of these points Q give rise to at most $O(y^{2/r})$ prime factors. Hence, the total number of primes p satisfying $|\Gamma_p| < y$ is $O(y^{1+2/r})$, as required. □

3.6 Result 4: Gupta and Murty

Continuing the work over the curves with higher ranks, Gupta and Murty noticed that the assumption of generalized Riemann hypothesis can be somewhat relaxed for elliptic curves of higher rank and having complex multiplication. In this case, we will need to assume α-GRH, a weaker version of the original GRH, to obtain an asymptotic formula.

Hypothesis 3.1 (α-GRH) *The α-GRH claims that both the Riemann Zeta function and the Dirichlet L-function have zero free region of $Re(s) > \alpha$ for some $\alpha > \frac{1}{2}$.*

Evidently, it is weaker than GRH which claims a zero free region for $Re(s) > \frac{1}{2}$. Now, let us also assume that the elliptic curve E has CM over the ring of integers of a quadratic extension $\mathbb{K}$ of $\mathbb{Q}$. Then, we may state Result 4 by Gupta and Murty as follows.

Theorem 3.5 (Gupta and Murty, 1986) *Suppose that E is an elliptic curve defined over $\mathbb{Q}$ and has complex multiplication over the entire ring of integers of some quadratic extension $\mathbb{K}$. Let Γ be a free subgroup of rational points with* $\text{rank}(\Gamma) = r$. *Then, if we define:*

$$\tilde{N}_\Gamma(x) = \#\{p \leq x \ : \ \Gamma_p = \overline{E}(\mathbb{F}_p), \ p \text{ splits in } \mathbb{K}\}$$

where $\overline{E}(\mathbb{F}_p)$ and Γ_p are the images of E and Γ modulo p respectively, then under the assumption of $\frac{r}{r+1}$-GRH (special case of α-GRH with $\alpha = \frac{r}{r+1}$), there exists a constant $\tilde{C}_E(\Gamma)$ such that as $x \to \infty$, we obtain

$$\tilde{N}_\Gamma(x) \ = \ \tilde{C}_E(\Gamma)\frac{x}{\log x} \ + \ o\left(\frac{x}{\log x}\right)$$

3.6.1 Proof of Theorem 3.5

Similar to the proof of Result 1 (rank 1 case), let us consider the field extensions $\mathbb{K}_q = \mathbb{K}(E[q])$ and $\mathbb{L}_{\mathfrak{q}} = \mathbb{K}(E[\mathfrak{q}], \mathfrak{q}^{-1}\Gamma)$, where $\mathfrak{q}$ is any first degree prime ideal in the extension $\mathbb{K}$. Analogous to the rank 1 case, we can say that for a prime p which splits as $\pi_p\overline{\pi_p}$ in $\mathbb{K}$, we will have $\overline{E}(\mathbb{F}_p) = \Gamma_p$ if π_p does not split completely in any of $\mathbb{K}_q$ or $\mathbb{L}_{\mathfrak{q}}$.

Let us define the terms $\tilde{N}_\Gamma(x, y_1)$ and $\tilde{M}_\Gamma(x, y_1, y_2)$ analogous to the terms defined in the previous proofs. Obviously, we obtain

$$\tilde{N}_\Gamma(x) \;=\; \tilde{N}_\Gamma(x, y_1) \;+\; O(\tilde{M}_\Gamma(x, y_1, 2x))$$

Estimate of $\tilde{N}_\Gamma(x, y_1)$

Following exactly similar steps as we did in the proof of Result 1 (rank 1 case) and assuming $\left(\frac{r}{r+1}\right)$-GRH for Theorem 3.2, we can prove that

$$\tilde{N}_\Gamma(x, y_1) \;=\; \tilde{C}_E(\Gamma)\frac{x}{\log x} \;+\; o\left(\frac{x}{\log x}\right)$$

if we choose $y_1 = \frac{1}{6(r+1)}\log x$ when $r = \text{ rank}(\Gamma)$. So, it remains to estimate the second term.

Estimate of $\tilde{M}_\Gamma(x, y_1, 2x)$

Let us first break up the range $(y_1, 2x)$ into subdivisions (y_1, y_2), (y_2, y_3) and $(y_3, 2x)$ to get

$$\tilde{M}_\Gamma(x, y_1, 2x) = \tilde{M}_\Gamma(x, y_1, y_2) + \tilde{M}_\Gamma(x, y_2, y_3) + \tilde{M}_\Gamma(x, y_3, 2x)$$

Then, for the first term, assuming the $\frac{r}{r+1}$-GRH once again and following similar steps as in the proof of Result 1 using Theorem 3.2, we obtain

$$\tilde{M}_\Gamma(x, y_1, y_2) = o\left(\frac{x}{\log x}\right)$$

for a suitable choice of $y_2 = x^{1/(r+1)}\log^{-2} x$.

Utilizing the Brun-Titchmarsh theorem for the second term, similar to that in Result 1, we can prove

$$\tilde{M}_\Gamma(x, y_2, y_3) = o\left(\frac{x}{\log x}\right)$$

if we take $y_3 = x^{1/(r+1)} \log^2 x$. It remains to estimate $\tilde{M}_\Gamma(x, y_3, 2x)$.

For this third term, we drop most of the conditions and just count the primes q within the range which divide the index. Now, as per the range constraint, $x^{1/(r+1)} \log^2 x < q, N(\mathfrak{q}) < 2x$. If $q|[\overline{E}(\mathbb{F}_p) : \Gamma_p]$, then two cases may arise:

Case 1: $q|[\overline{E}(\mathbb{F}_p) : \tilde{\Gamma}_p]$ where $\tilde{\Gamma}$ denotes the $\mathcal{O}_\mathbb{K}$-module generated by Γ for E having CM by an order $\mathcal{O}_\mathbb{K}$ in $\mathbb{K}$ and $\tilde{\Gamma}_p$ denotes the reduction of $\tilde{\Gamma}$ modulo π_p. So, we get $|\tilde{\Gamma}_p| < x^{r/(r+1)} \log^{-2} x$. In this case, we use the following result to get the estimate.

Lemma 3.14 *Suppose E has complex multiplication by an order $\mathcal{O}_\mathbb{K}$ in $\mathbb{K}$. Then the number of primes p which split in $\mathbb{K}$ and for which $|\tilde{\Gamma}_p| < y$ is $O(y^{1+1/r})$.*

Proof. Proved in Section 3.6.2.

Hence, the number of primes q in consideration is given by $o(x/\log x)$.

Case 2: $q|[\tilde{\Gamma}_p : \Gamma_p]$ where we use the regular notation. In this case, we use the following result for the estimation.

Lemma 3.15 *Let p split in $\mathbb{K}$ as $\pi_p\overline{\pi_p}$. Then, if $\{1, \omega\}$ be the $\mathbb{Z}$-basis for $\mathcal{O}_\mathbb{K}$, then we can write $\pi_p = c_p + d_p\omega$, say. Now, if q be a prime dividing the index $[\tilde{\Gamma}_p : \Gamma_p]$, then $d_p \equiv 0 \pmod{q}$.*

Proof. Proved in Section 3.6.2.

So, in this case, we get $\pi_p \equiv 1 \pmod{q}$ which in turn means that π_p splits completely in $\mathbb{K}_q$. Following a similar procedure as in the proof of Result 1, the number of such prime ideals in this case is

$$O\left(\sum_{x^{1/(r+1)}<q<2x} \frac{x}{q^2}\right) = O\left(x^{\frac{1}{r+1}}\right) = o\left(\frac{x}{\log x}\right)$$

Therefore we get $\tilde{M}_\Gamma(x, y_1, 2x) = o(x/\log x)$ and this completes the proof of Theorem 3.5 as we obtain

$$\tilde{N}_\Gamma(x) \;=\; \tilde{C}_E(\Gamma)\frac{x}{\log x} \;+\; o\left(\frac{x}{\log x}\right)$$

3.6.2 Proof of Lemmas

Proof of Lemma 3.14

The proof of this lemma is directly in the lines of the proof of Lemma 3.12. We again utilize the concept of canonical height pairing by Néron and Tate. We consider the following set

$$\tilde{S} = \{(\alpha_1, ..., \alpha_r) \in \mathcal{O}_{\mathbb{K}}^r : H(\alpha_1 P_1 + \cdots + \alpha_r P_r) \leq C y^{1/r}\}$$

with the constant C satisfying some similar constraint depending on r and $R = \det(\langle P_i, P_j \rangle)$, as before. Now, we will use the following result instead of Lemma 3.13 to prove this lemma.

Lemma 3.16

$$\#\{(\alpha_1, ..., \alpha_r) \in \mathcal{O}_{\mathbb{K}}^r : H(\alpha_1 P_1 + \cdots + \alpha_r P_r) \leq x\} = O(x^r)$$

Proof. We can assume $\mathbb{K} = \mathbb{Q}(\sqrt{-D})$, with D a square free integer, to be the quadratic extension. To obtain a lower bound for our result, it suffices to count only the α_i's of the form $m_i + n_i\sqrt{-D}$. So, we get

$$\begin{aligned}
&\#\{(\alpha_1, ..., \alpha_r) \in \mathcal{O}_{\mathbb{K}}^r : H(\alpha_1 P_1 + \cdots + \alpha_r P_r) \leq x\} \\
&= \#\left\{(\alpha_1, ..., \alpha_r) \in \mathcal{O}_{\mathbb{K}}^r : \left\langle \sum_{i=1}^r \alpha_i P_i, \sum_{i=1}^r \alpha_i P_i \right\rangle \leq x \right\} \\
&= \#\left\{(\alpha_1, ..., \alpha_r) \in \mathcal{O}_{\mathbb{K}}^r : \sum_{i,j} T(i,j) \leq x \right\}
\end{aligned}$$

where $T(i,j) = m_i m_j \langle P_i, P_j \rangle + 2 m_i n_j \langle P_i, \sqrt{-D} P_j \rangle + n_i n_j \langle \sqrt{-D} P_i, \sqrt{-D} P_j \rangle$. Now, this is equivalent to counting lattice points in the $2r$-dimensional ellipsoid defined by the quadratic form $\sum_{i,j} T(i,j) \leq x$. The number of lattice points in such an ellipsoid is given by the expression $C_R x^r + O(x^{r-1})$ [8], and the result follows. $\square$

Using the result above, we get $|\tilde{S}| > y$. Again, we have $|\tilde{\Gamma}_p| < y$. Hence, by the pigeon hole principle, we must have two distinct r-tuples $(\alpha_1, ..., \alpha_r)$ and $(\beta_1, ..., \beta_r)$ such that

$$\alpha_1 P_1 + \cdots + \alpha_r P_r \equiv \beta_1 P_1 + \cdots + \beta_r P_r \pmod{p}$$

So, the denominator of the non-zero point $\sum_{i=1}^r (\alpha_i - \beta_i) P_i = Q$ is divisible by p. The number of such primes is obviously less than $h_a(Q)$. Again, $H(Q) \neq 0$ as Q is

not a torsion point for independent $P_1, ..., P_r$. Therefore, $h_a(Q) \ll H(Q) \leq 2Cy^{1/r}$. So, by Lemma 3.16, the number of such points Q is $O(y)$. Now, each of these points Q contributes to at most $O(y^{1/r})$ prime factors. Hence, the total number of primes p satisfying $|\tilde{\Gamma}_p| < y$ is $O(y^{1+1/r})$, as required. □

Proof of Lemma 3.15

We have $\tilde{\Gamma}_p = \Gamma_p + \omega\Gamma_p$ for all primes p splitting in $\mathbb{K}$. But we know that π_p, as an automorphism, fixes Γ_p. So, $d_p(\omega\Gamma_p) \subset \Gamma_p$ and hence $[\tilde{\Gamma}_p : \Gamma_p]|d_p$. As $q|[\tilde{\Gamma}_p : \Gamma_p]$, the result follows. □

With the proof of these lemmas, we come to an end of our discussion of the elliptic curve analogue of Artin's conjecture and its proof by Gupta and Murty. No unconditional proof of the analogue has been proposed yet, but Gupta and Murty formulated an unconditional approach to get a finite set of points, one of which will surely satisfy the conjecture. We will outline their idea in the Conclusion chapter.

Chapter 4

Conclusion

So far, we have discussed different unconditional approaches to prove the Artin's conjecture and the proofs of the elliptic curve analogue of the same. Let us try to tie the knots and summarize the discussion.

4.1 Unconditional Approach

The result by D.R. Heath-Brown using the refined sieve results is the best we have so far in this field. The conjecture will be proven unconditionally if we can reduce the set defined by Heath-Brown to a single integer which is not a square, 0 or ± 1. But, the following question remains unanswered till date.

4.1.1 Open Question: Unconditional Proof

Though the conjecture has been proven for almost all integers, it has not been proven completely without the assumption of the generalized Riemann hypothesis. Again, though we know that there are at most 3 exceptional integers for which the conjecture might fail, we cannot explicitly point those three out. Hence, if we go back to Gauss's question: "For how many primes is 10 a primitive root?", we cannot answer this question correctly, as 10 may be one of the 3 exceptional integers. This still poses the unconditional proof of the Artin's conjecture as an intriguing open question in front of the mathematical society.

4.2 Elliptic Curve Analogue

In case of the elliptic curve analogue formulated by Lang and Trotter, we have a more comprehensive answer. We have seen the proof of the conjecture assuming generalized Riemann hypothesis and the proofs of the higher rank versions of the conjecture. Apart from these, Gupta and Murty used refined sieving techniques for the elliptic curves to get a lower bound on $N_\Gamma(x)$, as defined earlier in Chapter 3. I will outline their idea in brief.

4.2.1 Lower Bound for $N_\Gamma(x)$

Suppose we are assuming that the curve has complex multiplication over the ring of integers of some quadratic extension $\mathbb{K}$ of $\mathbb{Q}$. From a refined version of the lower bound sieve proved by Fouvry and Iwaniec [6], we obtain

$$S_\alpha(x) = \#\{p \leq x \ : \ q|(p-1) \ \Rightarrow \ q = 2 \text{ or } q > x^\alpha\} \gg \frac{x}{\log^2 x}$$

for $\alpha = \frac{1}{4} + \epsilon$ when we are counting only the primes which do not split in $\mathbb{Q}\left(\frac{1}{2}\Gamma\right)$ and are inert in $\mathbb{K}$. Now, each prime counted in $S_\alpha(x)$ has the property that if $q|[\overline{E}(\mathbb{F}_p) : \Gamma_p]$, then $q > x^\alpha$ and hence $|\Gamma_p| < x^{1-\alpha}$. By Lemma 3.14, the number of such primes is $\ll \left(x^{1-\alpha}\right)^{1+2/r} = O\left(x^{1-\alpha}\right)$ for $r \geq 6$. Hence, apart from these $O\left(x^{1-\alpha}\right)$ primes, for all the other primes counted in $S_\alpha(x)$, we have $\overline{E}(\mathbb{F}_p) = \Gamma_p$. Therefore, if rank of the curve $r \geq 6$, then

$$N_\Gamma(x) \gg \frac{x}{\log^2 x}$$

4.2.2 Corollary to obtain a Finite Set

From this result, Gupta and Murty proposed a corollary as follows

Corollary 4.1 *There is a finite set S, which can be given explicitly, such that for some $a \in S$, $\overline{E}(\mathbb{F}_p) = \langle \overline{a} \rangle$ for infinitely many primes p, provided that the rank of $E(\mathbb{Q})$ is $r \geq 6$.*

For the outline of the proof of this corollary, please refer to Gupta and Murty's paper [8]. Now, this result gives us an analogue to the finite set approach in the unconditional case. But still the following questions regarding the elliptic curve analogue of Artin's conjecture remain unanswered.

4.2.3 Open Questions: Elliptic Analogue

In case of the elliptic curve analogue of the conjecture, we can state the open problems as follows

- Is the analogous conjecture true unconditionally for all curves?
- Can we formulate the proof without the assumption of complex multiplication of the curve?
- Is the analogue in case of higher rank elliptic curves true without the assumption of GRH?

Though the conjecture still remains to be open from an unconditional point of view and although we might not see a solution to the problem in the near future, it has provided us with an insight of the intertwined fabric of algebraic and analytic number theory with arithmetical problems.

References

[1] Tom M. Apostol. *Introduction to Analytic Number Theory.* Springer-Verlag, 1976. 16

[2] E. Artin. Collected papers. 2, 3

[3] E. Bombieri, J. B. Friedlander, and H. Iwaniec. Primes in arithmetic progressions to large moduli. *Acta. Math.*, 156(1), 1986. 16, 17

[4] A. C. Cojocaru and M. Ram Murty. *An Introduction to Sieve Methods and their Applications.* Cambridge University Press, 2005. 17, 18

[5] A. Dujella. http://web.math.hr/∼duje/tors/rankhist.html. 50

[6] E. Fouvry and H. Iwaniec. Primes in arithmetic progressions. *Acta. Arith.*, 42:197–218, 1983. 4, 58

[7] R. Gupta and M. Ram Murty. A remark on Artin's conjecture. *Inventiones Math.*, 78:127–130, 1984. 4, 7, 10, 12

[8] R. Gupta and M. Ram Murty. Primitive points on elliptic curves. *Compositio Math.*, 58:13–44, 1986. 5, 29, 46, 51, 55, 58

[9] H. Halberstam and H. E. Richert. *Sieve Methods.* Academic Press, London, 1981. 22

[10] D. R. Heath-Brown. Artin's conjecture for primitive roots. *Quart. J. Math. Oxford(2)*, 37:27–38, 1986. 4, 10, 11, 17

[11] C. Hooley. On Artin's conjecture. *J. reine angew. Math*, 225:209–220, 1967. 4, 27

[12] H. Iwaniec. A new form of error term in the linear sieve. *Acta Arith.*, 37:307–320, 1980. 10, 17

[13] H. Iwaniec. Rosser's sieve. *Acta Arith.*, 36:171–202, 1980. 9, 19

[14] J. Lagarias and A. Odlyzko. Effective versions of the Chebotarev density theorem. In A. Frolich, editor, *Algebraic Number Fields*, London and New York, 1977. 1975 Durham Symposium, Academic Press. 35

[15] S. Lang and H. Trotter. Primitive points on elliptic curves. *Bull. Amer. Math. Soc.*, 83:289–292, 1977. 5, 26, 27, 29, 46

[16] M. Ram Murty. Artin's conjecture for primitive roots. *The Mathematical Intelligencer*, 10(4), 1988. 2

[17] C. D. Pan. A new mean value theorem and its applications. *Recent Progress in Analytic Number Theory*, I:275–287, 1981. 19

[18] J. P. Serre. Quelques applications du théorème de densité de Chebotarev. *Publ. Math. I.H.E.S.*, 54:123–201, 1982. 30, 39, 47

[19] J. H. Silverman. *The arithmetic of elliptic curves*. Springer-Verlag, 1986. 30, 31, 33, 50, 51