Frobenius Fields of Elliptic Curves

Geeta Johal

A Thesis
in
The Department
of
Mathematics and Statistics

Presented in Partial Fulfillment of the Requirements
for the Degree of Master of Science (Mathematics) at
Concordia University
Montreal, Quebec, Canada

March 2007

Your file Votre référence
ISBN: 978-0-494-28883-2
Our file Notre référence
ISBN: 978-0-494-28883-2

ABSTRACT

Frobenius Fields of Elliptic Curves

Geeta Johal

Let E be an elliptic curve without complex multiplication defined over Q. Let $Q(\sqrt{-D})$ be a fixed imaginary field where $D > 0$ is a nonsquare integer. Let ϕ_p denote the Frobenius endomorphism of E at p. The Frobenius field of ϕ_p is denoted by $Q(\pi_p)$. In this thesis, we find upper bounds for the number of primes p whose Frobenius fields $Q(\pi_p)$ equal a fixed imaginary quadratic field $Q(\sqrt{-D})$.

In *The Square Sieve and the Lang-Trotter Conjecture*, A. Cojocaru, E. Fouvry and M. Murty found upper bounds for this problem by applying the Chebotarev Density Theorem on the torsion fields $Q(E[m])$ associated with E. Based on Serre's theorem, those fields have Galois groups $GL_2(Z/mZ)$.

In this thesis, we improve their result by considering smaller extensions $F_E[m] \subseteq Q(E[m])$ over Q with Galois groups $PGL_2(Z/mZ)$ and by applying an explicit version of the Chebotarev Density Theorem to those fields. More precisely, we show that the bound obtained by A. Cojocaru, E. Fouvry and M. Murty under the Generalized Riemann Hypothesis, can be improved from $O(x^{17/18}\log x)$ to $O(x^{13/14}\log x)$. Under the additional condition of Artin's Holomorphy Conjecture, the bound obtained by A. Cojocaru, E. Fouvry and M. Murty can be improved from $O(x^{13/14}\log x)$ to $O(x^{7/8}\log x)$.

Acknowledgements

I am grateful to my supervisor Professor Chantal David for accepting me as her student and helping me work in this area. Throughout the preparation of this thesis, her continuous guidance, dedication and corrections of my work have made the success of this research possible. I truly appreciate all of the time she sacrificed for me to help me understand the concepts necessary for this work and her incredible patience to work with me.

I wish to express my gratitude to the Department of Mathematics and Statistics for giving me the opportunity to pursue graduate studies and for helping me financially throughout my studies. I am thankful to every Professor in the Department of Mathematics and Statistics who has had a valuable influence on my education. I would like to thank Anne-Marie for always providing me with help and support during my graduate studies.

Contents

Chapter 1

Introduction

Let E be an elliptic curve over $\mathbb{Z}$, i.e the set of solutions to an equation of the form $y^2 = x^3 + ax^2 + bx + c$ where $a, b, c \in \mathbb{Z}$ and the discriminant of E, Δ_E is not equal to zero. For each prime

$$p \nmid (-4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2),$$

we say that p has good reduction and E reduces to an elliptic curve $\overline{E}$ over $\mathbb{F}_p$ where

$$y^2 = x^3 + \overline{a}x^2 + \overline{b}x + \overline{c}$$

for $\overline{a} \equiv a \mod p$, $\overline{b} \equiv b \mod p$ and $\overline{c} \equiv c \mod p$ where $\overline{a}, \overline{b}, \overline{c}$ are the classes of $a, b, c \mod p$ respectively. The Frobenius map

$$\phi_p : (x, y) \mapsto (x^p, y^p)$$

is an endomorphism of E and satisfies the polynomial

$$x^2 - a_p x + p$$

where $a_p = \#E(\mathbb{F}_p) - p - 1$ is an integer and where $\#E(\mathbb{F}_p)$ is to be defined in section 2.8. By Hasse's inequality, we know that $|a_p| \leq 2\sqrt{p}$ which implies that the characteristic polynomial has two distinct roots which are complex conjugates. We denote them as π_p and $\overline{\pi_p}$. Adjoining any of these roots to $\mathbb{Q}$, we get a quadratic imaginary field extension of $\mathbb{Q}$ which we denote by $\mathbb{Q}(\pi_p)$. This is referred to as the Frobenius field at p. We consider the following question: If we fix E over $\mathbb{Q}$ and fix K a quadratic imaginary field, how many primes p of good reduction yield a Frobenius field which is equal to the field K? For D a positive square free integer let

$$P_E(\mathbb{Q}(\sqrt{-D}), x) = \#\{p \leq x : p \text{ has good reduction and } \mathbb{Q}(\pi_p) = \mathbb{Q}(\sqrt{-D})\}.$$

Conjecture 1.0.1 (Lang-Trotter (1976)) *Let E be a non-CM elliptic curve defined over $\mathbb{Q}$. Let K be a fixed imaginary quadratic field. Then there exists a positive constant $C_{E,K}$ such that, as $x \to \infty$,*

$$P_E(K, x) \sim C_{E,K} \frac{x^{1/2}}{\log x}$$

where $C_{E,K}$ depends on the elliptic curve E and the field K.

We consider in this thesis, the problem of finding upper bounds for $P_E(\mathbb{Q}(\sqrt{-D}), x)$ thus, giving partial evidence towards the Lang-Trotter conjecture. Our technique is based on a paper by [CoFoMu] where the authors obtain the following result:

Theorem 1.0.2 ([CoFoMu], Theorem 1.2) *Let E be a non-CM elliptic curve defined over $\mathbb{Q}$ with conductor N. Let $\mathbb{Q}(\sqrt{-D})$ be a fixed imaginary quadratic field. Let $x \geq 3$ be a positive real number.*

(a) If we assume GRH for the Dedekind zeta functions of the division fields of E, then

$$P_E(\mathbb{Q}(\sqrt{-D}), x) \ll_N x^{17/18} \log x$$

(b) If we assume GRH and Artin's Holomorphy Conjecture (denoted AHC) for the L-functions of the irreducible characters of the Galois groups of the division fields of E then

$$P_E(\mathbb{Q}(\sqrt{-D}), x) \ll_N x^{13/14} \log x$$

the symbol $\ll_N$ means that the implicit constant depends on N.

The proof for this theorem in [CoFoMu] relies on the study of the torsion fields $\mathbb{Q}(E[m])$ associated with E (see section 2.5 for the definition of these fields). By a theorem of Serre,

$$\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) \simeq GL_2(\mathbb{Z}/m\mathbb{Z})$$

for almost all integers m. The authors of [CoFoMu] obtain their theorem by applying an explicit version of the Chebotarev Density Theorem to the above mentioned fields. We get an improvement of their result by considering smaller

extensions over $\mathbb{Q}$ with Galois groups $PGL_2(\mathbb{Z}/m\mathbb{Z})$, and applying the Chebotarev Density Theorem to those extensions. More precisely, we obtain the following

Theorem 1.0.3 *Let E be a non-CM elliptic curve defined over $\mathbb{Q}$ with conductor N. Let $\mathbb{Q}(\sqrt{-D})$ be a fixed imaginary quadratic field. Let $x \geq 3$ be a positive real number.*

(a) If we assume GRH for the Dedekind zeta functions of the division fields of E, then

$$P_E(\mathbb{Q}(\sqrt{-D}), x) \ll_N x^{13/14} \log x$$

(b) If we assume GRH and Artin's Holomorphy Conjecture (denoted AHC) for the L-functions of the irreducible characters of the Galois groups of the division fields of E then

$$P_E(\mathbb{Q}(\sqrt{-D}), x) \ll_N x^{7/8} \log x$$

This thesis is divided into four chapters. Following the introduction, Chapter 2 serves as an introduction to elliptic curves and provides the theoretical background needed for the results that we intend to prove.

Chapter 3, discusses the essential tools needed to prove the main theorem such as the Chebotarev density theorem, properties of the matrix group $PGL_2(\mathbb{Z}/p\mathbb{Z})$ and the Square Sieve. In Chapter 4, we prove our main result.

Chapter 2

Elliptic Curves

2.1 Affine Weierstrass form

An elliptic curve E is the union of the set of affine points (x, y) with coordinates in some field K over which the elliptic curve is defined and a point at infinity. The point at infinity however, has coordinates in the projective plane. This will be further discussed in section 2.3. We introduce the three types of equations of E that occur in the affine plane. The generalized Weierstrass equation has the following form:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $a_1, a_2, a_3, a_4, a_5, a_6$ are coefficients in some field K. Let

$$\begin{aligned} b_1 &= a_1^2 + 4a_2 \\ b_2 &= 2a_4 + a_1 a_3 \\ b_3 &= a_3^2 + 4a_6 \\ b_4 &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2. \end{aligned}$$

The discriminant of E, denoted Δ_E, is defined as

$$\Delta_E = -b_1^2 b_4 - 8b_2^3 - 27b_3^2 + 9b_1 b_2 b_3.$$

We consider only nonsingular curves, i.e curves when $\Delta_E \neq 0$. This means that every point on the elliptic curve has a tangent line. If the characteristic of $\overline{K} \neq 2$ we can simplify the above equation by completing the square as follows:

$$\left(y + \frac{a_1 x}{2} + \frac{a_3}{2}\right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right) x^2 + a_4 x + \left(\frac{a_3^2}{4} + a_6\right).$$

The equation can be simplified to

$$E : y_1^2 = x^3 + ax^2 + bx + c$$

where

$$y_1 = y + \frac{a_1 x}{2} + \frac{a_3}{2}$$

and the a, b, c correspond to the coefficients in the above equation. This equation is referred to as the Weierstrass form. If E is in this form then

$$\Delta_E = -4a^3 c + a^2 b^2 + 18abc - 4b^3 - 27c^2.$$

If the characteristic of $\overline{K} \neq 2, 3$ we can get rid of the x^2 term by replacing x by $x = x_1 - a/3$ this yields an equation of the form:

$$\begin{aligned} y_1^2 &= \left(x_1 - \frac{a}{3}\right)^3 + a\left(x_1 - \frac{a}{3}\right)^2 + b\left(x_1 - \frac{a}{3}\right) + c \\ y_1^2 &= x_1^3 + \left(-\frac{a^2}{3} + b\right)x_1 + \left(\frac{2a^3}{27} - \frac{ab}{3} + c\right) \end{aligned}$$

which can be simplified to

$$E : y_1^2 = x_1^3 + Ax_1 + B$$

where A, B correspond to the coefficients of the powers of x_1 given above. This equation is referred to as the Weierstrass normal form. If E has the Weierstrass normal form, then

$$\Delta_E = -16(4A^3 + 27B^2).$$

If the coefficients of E are elements of K, then we say that E is defined over K. In this thesis, we work exclusively with the Weierstrass form.

2.2 Projective Plane

The projective plane is defined over a field K as

$$\mathbb{P}^2 = \{(x, y, z) : x, y, z \in K \text{ not all zero}\}/\sim .$$

This is the equivalence class of triples (x, y, z) with $x, y, z \in K$ which we will denote as $[x, y, z]$. Two triples (x_1, y_1, z_1) and (x_2, y_2, z_2) are in the same equivalence

class if there exists a nonzero element $\lambda \in K$ such that

$$(x_1, y_1, z_1) = (\lambda x_2, \lambda y_2, \lambda z_2).$$

If $z \neq 0$, then $[x, y, z] = [x/z, y/z, 1]$. If $z = 0$, then dividing by z gives us ∞ for the x and y coordinates. Therefore, $[x, y, 0]$ are called points at infinity. There is a map from the two-dimensional affine plane

$$\mathbb{A}^2 = \{(x, y) \in K^2\}$$

to the projective plane

$$\mathbb{A}^2 \hookrightarrow \mathbb{P}^2$$

$$(x, y) \rightarrow [x, y, 1].$$

$\mathbb{P}^2$ is the union of the points in $\mathbb{A}^2$ and the points at infinity. The set of all points at infinity form the line at infinity which we denote by $Z = 0$. Algebraic curves in $\mathbb{A}^2$ are of the form

$$f(x, y) = \sum a_{ij} x^i y^j = 0.$$

In the projective plane we use homogeneous polynomials

$$F(X, Y, Z) = \sum a_{ij} X^i Y^j Z^{d-i-j}$$

where d =degree$(f(x, y))$ to define curves in $\mathbb{P}^2$. We can convert a curve in $\mathbb{A}^2$ to a curve in $\mathbb{P}^2$ by making the substitution $x = X/Z$ and $y = Y/Z$ into $f(x, y) = 0$.

To obtain the original curve in $\mathbb{A}^2$ we can just substitute $Z = 1$ into $F(X, Y, Z)$ this gives $f(x, y)$. In other words,

$$F(X, Y, 1) = f(x, y).$$

We have that

$$F(\lambda X, \lambda Y, \lambda Z) = \lambda^d F(X, Y, Z)$$

therefore, the set of solutions to the homogeneous polynomial in $\mathbb{P}^2$ is well defined.

2.3 Projective Weierstrass Equation

As mentioned in section 2.1, an elliptic curve consists of an affine part and a point at infinity. We are given the following equation:

$$E : y^2 = x^3 + ax^2 + bx + c$$

where E is defined over some field K. To work in the projective plane, we must first make this equation homogeneous by using the substitution $x = X/Z$ and $y = Y/Z$. This yields

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3.$$

We want to find the intersection of this equation with the line at infinity $Z = 0$. Substituting $Z = 0$ into the equation we get $X^3 = 0$. There is a triple root at $X = 0$. The corresponding projective plane coordinates are $[0, Y, 0]$ where Y can

have any value. However, in $\mathbb{P}^2$ this is the same as $[0,1,0]$ this is our point at infinity. It is the only point at infinity which satisfies E. We denote this point as O.

In order to see that O is non-singular, we write the Weierstrass equation in homogeneous form:

$$F(X,Y,Z) = Y^2Z - X^3 - aX^2Z - bXZ^2 - cZ^3 = 0.$$

Using the coordinates of O ($[0,1,0]$ in the projective plane $\mathbb{P}^2$), we can evaluate the derivative of O at these coordinates.

$$\begin{aligned}
\frac{\partial F}{\partial X}[0,1,0] &= (-3X^2 - 2aXZ - bZ^2)[0,1,0] = 0 \\
\frac{\partial F}{\partial Y}[0,1,0] &= (2YZ)[0,1,0] = 0 \\
\frac{\partial F}{\partial Z}[0,1,0] &= (Y^2 - aX^2 - 2bXZ - 3cZ^2)[0,1,0] = 1 \neq 0
\end{aligned}$$

At least one partial derivative of O is nonzero, therefore O is a non-singular point of E. The tangent line at O is given by

$$\left(\frac{\partial F}{\partial X}\right)_{P=[0,1,0]} X + \left(\frac{\partial F}{\partial Y}\right)_{P=[0,1,0]} (Y-1) + \left(\frac{\partial F}{\partial Z}\right)_{P=[0,1,0]} Z = 0$$

which simplifies to

$$Z = 0.$$

Therefore, the tangent line at the point of infinity O is just the line at infinity $Z = 0$ which meets E with multiplicity 3 at O.

2.4 Group Law

Let E be defined over $\mathbb{Q}$. If two rational points P and Q are on E, then we can find a third rational point by the following method: first we draw a line through the two rational points P and Q. Both P and Q are rational so we get a rational line which meets the elliptic curve at one more point. We denote this new point as $P*Q$. By solving the system of equations, we see that the point of intersection $P*Q$ must also be rational. If we start with only one rational point P then we can get another rational point by taking the tangent line at P. The tangent line meets the elliptic curve E twice at P. We denote the other point of intersection as $P*P$.

If we look at all of the rational points on E, we can make this set into a group by defining an identity element and addition as follows: first we take O as our identity element. We count it as a rational point that cannot be seen. We treat the remainder of the points which satisfy E as points in $\mathbb{A}^2$. A vertical line intersecting E will intersect E at two points in $\mathbb{A}^2$ and the point O. To add two points P, Q we draw the line through P and Q and find the third point of intersection $P*Q$. We draw the line through O and $P*Q$ which is just a vertical line through $P*Q$ and take the third point of intersection of the line with E as the point $P+Q$. To find the negative of a point P we draw the line joining P and O and take the third intersection of the line with E as $-P$. If E is in Weierstrass

form

$$E : y^2 = x^3 + ax^2 + bx + c$$

then E is symmetric about the x-axis so $P + Q$ is just $P * Q$ reflected about the x-axis. In Weierstrass form $-P$ is just P reflected about the x-axis. This is obvious from the fact that both (x, y) and $(x, -y)$ satisfy the above equation if one does.

If E is the generalized Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

then

$$-P = (x, -a_1x - a_3 - y).$$

This follows from the fact that if we have a quadratic polynomial the sum of the two roots must equal to the negative coefficient of the linear term. In this case, we know that one of the roots is y. The sum of both roots is

$$-a_1x - a_3$$

so we get

$$-a_1x - a_3 - y$$

as the other root. Therefore, if P is a point (x, y) and we want to find the point which intersects the vertical line through P and O we get

$$-P = (x, -a_1x - a_3 - y).$$

For O the point at infinity, if we take the tangent line at O this gives us the line at infinity. The third point of intersection is O because the line at infinity meets E at O with multiplicity 3. Also, we have $-O = O$. This above construction makes $E(\mathbb{Q})$ into an additive abelian group.

Proposition 2.4.1 ([Si2], Chapter 3, Proposition 2.2) *The addition law has the following properties:*

1. *If a line L intersects E at (not necessarily distinct) points P, Q, R then $(P+Q)+R = O$*
2. $P + O = P \quad \forall P \in E$
3. $P + Q = Q + P \quad \forall P, Q \in E$
4. *let $P \in E$ then there is a point $-P$ so that $P - P = O$*
5. $(P+Q)+R = P+(Q+R)$
6. $E(K) = \{(x,y) \in K^2 | y^2 = x^3 + ax^2 + bx + c\} \cup O$. *$E(K)$ is a subgroup of E.*

We do not state the proof for the above proposition here. It can be found in [Si2] p.55.

Remark 2.4.2 *Part* 1 *says that if P, Q, R lie on the same line then their sum as we define it, is equal to the point at infinity O. Part* 6 *refers to the points in K*

which satisfy E. Given the way that addition is defined it is easy to see that the law is commutative.

2.5 Torsion Points

Let K be a field and let $\overline{K}$ be the algebraic closure of K.

Definition 2.5.1 *A point P on E has finite order if $mP = O$ for some positive integer m. P is said to be a torsion point if it satisfies the above property.*

The set of all torsion points with order dividing m is a subgroup of $E(\overline{K})$. If P and Q have order dividing m then by taking the least common multiple of the orders of P and Q, we can see that their sum and difference also have order dividing m.

Definition 2.5.2 *Let E be an elliptic curve defined over a field K and m a positive integer. The m-torsion subgroup of E is denoted as*

$$E[m](\overline{K}) = \{P \in E(\overline{K}) \mid mP = O\}.$$

The torsion subgroup of E denoted as E_{tors}, is the set of points of finite order where

$$E_{tors} = \bigcup_{m=1}^{\infty} E[m](\overline{K}).$$

So $E_{tors}(K)$ will denote points of finite order in $E(K)$.

For notational convenience, if E is defined over a field K, then $E[m]$ will mean $E[m](\overline{K})$.

Proposition 2.5.3 ([Si1], Chapter 6, Section 2) *If the characteristic of a field K denoted as $char(K)$ is coprime to some positive integer m i.e $(m, char(K)) = 1$, then as an abstract group, $E[m] \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ that is, $E[m]$ is the direct sum of two cyclic groups of order m.*

The above proposition implies that there are m^2 m-torsion points and that the abelian group $E[m]$ can be generated by two points P_1 and P_2 which are a basis of $E[m]$. This means that every element of $E[m]$ can be written as a linear combination of these two points i.e

$$a_1P_1 + a_2P_2$$

where $a_1, a_2 \in \mathbb{Z}/m\mathbb{Z}$. These torsion points can be used to generate field extensions of $\mathbb{Q}$.

Proposition 2.5.4 ([Si1], Chapter 6, Section 2) *Let E be an elliptic curve with coefficients in $\mathbb{Q}$, and let K be a Galois extension of $\mathbb{Q}$.*

1. *$E(K)$ is a subgroup of $E(\mathbb{C})$.*

2. *For $P \in E(K)$ and $\sigma \in Gal(K/\mathbb{Q})$, define $\sigma(P)$ by*

$$\sigma(P) = \begin{cases} (\sigma(x), \sigma(y)) & \text{if } P = (x, y) \\ O & \text{if } P = O. \end{cases}$$

Then $\sigma(P) \in E(K)$.

3. *For all* $P \in E(K)$ *and all* $\sigma, \tau \in Gal(K/\mathbb{Q})$,

$$(\sigma\tau)(P) = \sigma(\tau(P)).$$

Further, the identity element acts trivially $e(P) = P$.

4. *For all* $P, Q \in E(K)$ *and all* $\sigma \in Gal(K/\mathbb{Q})$,

$$\sigma(P+Q) = \sigma(P) + \sigma(Q) \text{ and } \sigma(-P) = -\sigma(P).$$

Hence, $\sigma(nP) = n\sigma(P)$ *for all integers* n.

5. *If* $P \in E(K)$ *has order* n *and if* $\sigma \in Gal(K/\mathbb{Q})$, *then* $\sigma(P)$ *also has order* n.

Proof: 1. If P_1 and P_2 are in $E(K)$, their x and y coordinates are in K, now using the formulas for the addition law $P_1 \pm P_2$ also have coordinates in K. Therefore, $E(K)$ is closed under addition and subtraction, so it is a subgroup of $E(\mathbb{C})$.

2. Let $P = (x, y) \in E(K)$. To show that $\sigma(P)$ is a point of $E(K)$ we use the fact that $\sigma : K \to K$ is a homomorphism which fixes $\mathbb{Q}$. Therefore,

$$\begin{aligned} P \in E(K) &\Rightarrow y^2 - x^3 - ax^2 - bx - c = 0 \\ \sigma(P) &= \sigma(y^2 - x^3 - ax^2 - bx - c) = 0 \\ &= \sigma(y)^2 - \sigma(x)^3 - \sigma(a)\sigma(x)^2 - \sigma(b)\sigma(x) - \sigma(c) = 0 \\ &= \sigma(y)^2 - \sigma(x)^3 - a\sigma(x)^2 - b\sigma(x) - c = 0 \\ &= (\sigma(x), \sigma(y)) \in E(K) \end{aligned}$$

3. If $P = (x, y)$ then

$$\begin{aligned} \sigma\tau(P) &= (\sigma\tau(x), \sigma\tau(y)) \\ &= (\sigma(\tau(x)), \sigma(\tau(y))) \\ &= \sigma(\tau(x), \tau(y)) \\ &= \sigma(\tau(P)) \end{aligned}$$

4. This follows from the fact that the addition law is given by rational functions with coefficients in $\mathbb{Q}$.

5. If $P \in E(K)$ has order n. Then using 4, we get

$$n\sigma(P) = \sigma(nP) = \sigma(O) = O$$

so $\sigma(P)$ has order dividing n. To see that the order is n, we suppose that $m\sigma(P) = O$. However, from 4 this implies that $\sigma(mP) = O$. We take the inverse σ^{-1} of σ on both sides to get

$$O = \sigma^{-1}(O) = \sigma^{-1}(\sigma(mP)) = mP$$

since P has order n this implies that $m \geq n$. Therefore, $\sigma(P)$ has order n. □

Proposition 2.5.5 ([Si1], Chapter 6, Section 2)

Let E be an elliptic curve given by Weierstrass equation

$$E : y^2 = x^3 + ax^2 + bx + c$$

with rational coefficients $a, b, c \in \mathbb{Q}$.

(a) Let $P = (x_1, y_1) \in \mathbb{C}$ be a point of order m. Then x_1 and y_1 are algebraic over $\mathbb{Q}$.

(b) Let

$$\{(x_1, y_1), \ldots, (x_{m^2-1}, y_{m^2-1})\}$$

be the set of points on E of order dividing m. Then

$$\mathbb{Q}(E[m]) = \mathbb{Q}(x_1, y_1, \ldots, x_{m^2-1}, y_{m^2-1})$$

is a finite Galois extension of $\mathbb{Q}$.

Proof: (a) Let $K = \mathbb{Q}(E[m])$. One can show that every field homomorphism $\sigma : K \to \mathbb{C}$ is determined by specifying some permutation of the points $P_1, \ldots, P_m$. This means that there are only finitely many such homomorphisms. If some x_i or y_i were not algebraic over $\mathbb{Q}$, then the field K would have infinite degree over $\mathbb{Q}$, so there would be infinitely many distinct homomorphisms $K \to \mathbb{C}$. Therefore, all of the x_i's and y_i's must be algebraic over $\mathbb{Q}$.

(b) Let $\sigma : K \to \mathbb{C}$ be a field homomorphism. In order to prove that K is Galois over $\mathbb{Q}$, we must show that $\sigma(K) = K$. The map is determined by where it sends the x_i's and the y_i's. Each point P is in $E[m]$ and from the proposition we proved,

$$O = \sigma(O) = \sigma(mP) = m\sigma(P),$$

so $\sigma(P)$ is also in $E[m]$. This means that $\sigma(P)$ is one of the P_j's with $i = j$ being allowed. Therefore, the x and y coordinates of $\sigma(P_i)$ are already in K. In other

words, $\sigma(x_i), \sigma(y_i) \in K$. This is true for each $1 \leq i \leq m$, and so $\sigma(K) \subset K$, which completes the proof that K is a Galois extension of $\mathbb{Q}$. $\square$

2.6 Galois Representations

As proved in proposition 2.5.4 (5), every element σ of $\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$ sends $E[m]$ to itself. It is an isomorphism because each $\sigma \in \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$ has an inverse element σ^{-1} which maps the image $\sigma(P)$ in $E[m]$ back to the original point P in $E[m]$. In other words,

$$\begin{aligned} \sigma : E[m] &\rightarrow E[m] \\ P &\mapsto \sigma(P) \end{aligned}$$

is an element of the group of automorphisms of $E[m]$ denoted as $\mathrm{Aut}(E[m])$. If we fix a basis $\{P_1, P_2\}$ for $E[m]$, then any $P \in E[m]$ writes as

$$P = a_1 P_1 + a_2 P_2$$

where $a_1, a_2 \in \mathbb{Z}/m\mathbb{Z}$. We can rewrite $\sigma(P)$ as

$$\sigma(P) = a_1 \sigma(P_1) + a_2 \sigma(P_2).$$

Any isomorphism σ from $E[m]$ to itself is determined by the values given to the basis elements P_1 and P_2. We can write $\sigma(P_1)$ and $\sigma(P_2)$ as linear combinations of P_1 and P_2 with coefficients in $\mathbb{Z}/m\mathbb{Z}$. If we write

$$\begin{aligned} \sigma(P_1) &= \alpha_\sigma P_1 + \gamma_\sigma P_2 \\ \sigma(P_2) &= \beta_\sigma P_1 + \delta_\sigma P_2 \end{aligned}$$

where $\alpha_\sigma, \beta_\sigma, \gamma_\sigma, \delta_\sigma$ are uniquely determined by σ, then we can write

$$(\sigma(P_1), \sigma(P_2)) = (P_1, P_2) \begin{pmatrix} \alpha_\sigma & \beta_\sigma \\ \gamma_\sigma & \delta_\sigma \end{pmatrix}$$

the matrix belongs to the set of 2×2 matrices with coefficients in $\mathbb{Z}/m\mathbb{Z}$ with determinant $\in (\mathbb{Z}/m\mathbb{Z})^*$ ($GL_2(\mathbb{Z}/m\mathbb{Z})$ matrices). In $\mathrm{Aut}(E[m])$, σ has an inverse therefore the matrix must also be invertible this is why the determinant is invertible. We have the following map:

$$\begin{aligned} \rho_m : \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) &\rightarrow GL_2(\mathbb{Z}/m\mathbb{Z}) \\ \sigma &\mapsto \begin{pmatrix} \alpha_\sigma & \beta_\sigma \\ \gamma_\sigma & \delta_\sigma \end{pmatrix} \end{aligned}$$

ρ_m is a homomorphism which associates each element σ of $\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$ to an isomorphism from $E[m]$ to itself to a matrix in $GL_2(\mathbb{Z}/m\mathbb{Z})$. This map is a one-to-one homomorphism although it is not necessarily onto. However, Serre provides a theorem which describes conditions under which this map is onto.

Theorem 2.6.1 (Serre's Theorem, [Si1], Chapter 6, Section 3) *Let E be an elliptic curve given by a Weierstrass equation with rational coefficients. Assume E does not have complex multiplication. There is an integer $A \geq 1$, depending on the curve E, so that if m is any integer relatively prime to A, then the Galois representation*

$$\rho_m : \mathit{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) \rightarrow GL_2(\mathbb{Z}/m\mathbb{Z})$$

is an isomorphism.

2.7 Galois Representations for $PGL_2(\mathbb{Z}/m\mathbb{Z})$

Let E and A be as in Theorem 2.6.1. For our purpose, we want to consider a subfield of $\mathbb{Q}(E[m])$. Let m be an integer such that $(m, A) = 1$. By Serre's Theorem, $\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$ is isomorphic to $GL_2(\mathbb{Z}/m\mathbb{Z})$. The set of 2×2 scalar matrices in $GL_2(\mathbb{Z}/m\mathbb{Z})$

$$\begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix}, \qquad r \in (\mathbb{Z}/m\mathbb{Z})^*$$

form a subgroup of $GL_2(\mathbb{Z}/m\mathbb{Z})$ denoted as H. This is a normal subgroup of $GL_2(\mathbb{Z}/m\mathbb{Z})$. Let

$$F_E[m] = \mathbb{Q}(E[m])^H$$

be the field corresponding to H under the Galois correspondence, i.e $F_E[m]$ is the fixed field of H. Suppose $(m, A) = 1$. Then, using Theorem 2.6.1 and the Fundamental Theorem of Galois Theory, $F_E[m]/\mathbb{Q}$ is a Galois extension with Galois group

$$\mathrm{Gal}(F_E[m]/\mathbb{Q}) \simeq GL_2(\mathbb{Z}/m\mathbb{Z})/H = PGL_2(\mathbb{Z}/m\mathbb{Z}).$$

This is an essential tool to prove our main theorem and for future reference, we restate it as:

Theorem 2.7.1 *Let E be a (non-CM) elliptic curve given by a Weierstrass equation with rational coefficients. Let A be the constant in Theorem 2.6.1. For any*

m where $(m, A) = 1$ the Galois representation

$$\overline{\rho}_m : \ Gal(F_E[m]/\mathbb{Q}) \to PGL_2(\mathbb{Z}/m\mathbb{Z})$$

is an isomorphism.

2.8 Elliptic Curves over Finite Fields

Let p be an odd prime number. Consider the elliptic curve $y^2 = x^3 + ax^2 + bx + c$ where $a, b, c \in \mathbb{F}_p$ and let Δ_E denote the discriminant of E so $p \nmid \Delta_E$. Then

$$E(\mathbb{F}_p) = \{(x, y) \mid x, y \in \mathbb{F}_p, f(x, y) = 0\}.$$

This group is finite given that there are only a finite number of possibilities for x and y.

In order to estimate the size of $E(\mathbb{F}_p)$ we can use the Legendre symbol for $a \in \mathbb{Z}$.

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a square in } \mathbb{F}_p \\ -1 & \text{if } a \text{ is not a square in } \mathbb{F}_p \\ 0 & \text{if } a = 0 \text{ in } \mathbb{F}_p \end{cases}$$

Theorem 2.8.1 ([Wa], Chapter 4, Section 3) *Let E be an elliptic curve $y^2 = x^3 + ax^2 + bx + c$ over $\mathbb{F}_p$. Then*

$$\#E(\mathbb{F}_p) = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + ax^2 + bx + c}{p}\right)$$

Proof: For $x^3 + ax^2 + bx + c \neq 0$, if $x^3 + ax^2 + bx + c$ is a square in $\mathbb{F}_p$ then y has two corresponding solutions so there are two points. If $x^3 + ax^2 + bx + c$ is not a

square then there will be no solutions. For $x^3+ax^2+bx+c=0$ there will be one solution. We must also add the point at infinity. This gives

$$\#E(\mathbb{F}_p) = \sum_{x\in\mathbb{F}_p}\left(1+\left(\frac{x^3+ax^2+bx+c}{p}\right)\right)+1.$$

If we take the sum of 1 over all of the $x \in \mathbb{F}_p$ then we get:

$$\begin{aligned}\#E(\mathbb{F}_p) &= \sum_{x\in\mathbb{F}_p} 1 + \sum_{x\in\mathbb{F}_p}\left(\frac{x^3+ax^2+bx+c}{p}\right)+1\\ &= p+1+\sum_{x\in\mathbb{F}_p}\left(\frac{x^3+ax^2+bx+c}{p}\right)\end{aligned}$$

The p results from the fact that there are p possible values for x. □

Remark 2.8.2 *We want to estimate the error term which is*

$$\sum_{x\in\mathbb{F}_p}\left(\frac{x^3+ax^2+bx+c}{p}\right).$$

If $f(x)=x^3+ax^2+bx+c$ has distinct roots then the tendency for $f(x)$ to be squares or nonsquares is roughly equal. The following theorem by Hasse-Weil provides a bound for this error term.

Theorem 2.8.3 (Hasse-Weil Theorem, [Si1], Chapter 4, Section 1) *Let E be an elliptic curve defined over the finite field $\mathbb{F}_p$ then the number of points on E with coordinates in $\mathbb{F}_p$ is $p+1+\varepsilon$ where the error term ε satisfies $|\varepsilon| \leq 2\sqrt{p}$.*

Remark 2.8.4 *This means that the number of points in $E(\mathbb{F}_p)$ lies in the following interval:*

$$-2\sqrt{p}+p+1 \leq \#E(\mathbb{F}_p) \leq 2\sqrt{p}+p+1$$

2.9 Conductor of an Elliptic Curve

Let E be an elliptic curve defined over $\mathbb{Q}$. We can multiply the equation of E by the common denominator of its coefficients to obtain an elliptic curve defined over $\mathbb{Z}$ and reduce this curve mod p. Let $\overline{E}$ denote the reduction of E modulo p. The following definitions can be found in [Si2].

Definition 2.9.1 *We classify E according to the properties of $\overline{E}$. There are three possibilities for the reduction of E modulo p:*

(a) E has good reduction over $\mathbb{Q}$ if $\overline{E}$ is nonsingular.

(b) E has multiplicative reduction over $\mathbb{Q}$ if $\overline{E}$ has a node. A node is a singular point with two distinct tangent directions.

(c) E has additive reduction over $\mathbb{Q}$ if $\overline{E}$ has a cusp. A cusp is a singular point with one tangent direction.

In the cases of (b) and (c), E is said to have bad reduction at p. This occurs when $p \mid \Delta_E$.

Definition 2.9.2 *The conductor N of an elliptic curve E is defined as*

$$N = \prod_{p|\Delta_E} p^{e(p)}$$

where for $p \neq 2, 3$*:*

$$e(p) = \begin{cases} 1 & \text{if } E \text{ has multiplicative reduction at } p \\ 2 & \text{if } E \text{ has additive reduction at } p \end{cases}$$

If $p = 2, 3$*, we refer the reader to [Si2] p.361 and for the definition of* $e(p)$*. In any case,* $e(p) \leq 6$*.*

2.10 The Endomorphism Ring

Let $\overline{K}$ denote the algebraic closure of a field K. Given E an elliptic curve defined over K, the endomorphism ring of E is an important invariant of E and is denoted by $\mathrm{End}_{\overline{K}}(E)$. It is the set of algebraic maps Φ which are group homomorphisms from E to itself, i.e

$$\Phi : E \to E.$$

For any field L containing K, we denote by $\mathrm{End}_L(E)$ the set of endomorphisms defined over L. We let $\mathrm{End}(E)$ denote $\mathrm{End}_{\overline{K}}(E)$.

For every integer m in $\mathbb{Z}$, the multiplication map $[m]$ is $\in \mathrm{End}(E)$. If E is defined over K, then the multiplication-by-m map is also defined over K. It is defined as

$$[m]P = P + \ldots + P$$

where the summation is of m P's. For $m < 0$, $[m]P = [-m](-P)$ where the summation is of $|m|$ $(-P)$'s and $[0]$ maps to the point at infinity ($[0]P = O$). If

$m \neq 0$ then the map is non-zero and $\mathbb{Z} \subseteq \text{End}(E)$. The kernel of this map is $E[m]$, the set of m-torsion points on E.

In the case where the characteristic of $K = 0$, the theorem below describes what the endomorphism ring of E will look like.

Theorem 2.10.1 ([Si2], Chapter 6, Theorem 6.1) *If E is defined over a field K, of characteristic 0, then the endomorphism ring of E is isomorphic to $\mathbb{Z}$ ($End(E) \simeq \mathbb{Z}$) or it is an order in a quadratic imaginary field.*

In the latter case, we say that E has complex multiplication (CM). For a proof of the theorem, see [Si2] p.165.

Remark 2.10.2 *If E is a curve with complex multiplication (CM), then for primes of ordinary reduction for E, i.e the primes for which $a_p \neq 0$ where $a_p = \#E(\mathbb{F}_p) - p - 1$ the following holds:*

$$\mathbb{Q}(\pi_p) = End(E) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

This is why our main theorem holds only in the case of elliptic curves without complex multiplication. For non-CM curves, as the prime p varies, we expect to get infinitely many distinct fields $\mathbb{Q}(\pi_p)$.

We now look at the case where E is defined over $\mathbb{F}_p$. We define the Frobenius

map

$$\begin{aligned} \phi_p : E &\rightarrow E^p \\ (x, y) &\mapsto (x^p, y^p) \\ O &\mapsto O \end{aligned}$$

As E is defined over $\mathbb{F}_p$, $E^p = E$ and therefore, $\phi_p \in \mathrm{End}(E)$.

Proposition 2.10.3 ([Wa], Chapter 3, Proposition 4.7) *Let E be defined over $\mathbb{F}_p$. Then*

$$\#Ker(\phi_p - 1) = \#E(\mathbb{F}_p) = deg(\phi_p - 1)$$

where the degree of the endomorphism is the degree of the associated function field (see [Wa] p.46 for a precise definition).

Recall that if φ is an endomorphism of E, then we obtain a 2×2 matrix with entries in $\mathbb{Z}/m\mathbb{Z}$ which describe the action of φ on a basis $\{P_1, P_2\}$ of $E[m]$.

Proposition 2.10.4 ([Wa], Chapter 3, Proposition 3.15) *Let φ be an endomorphism of an elliptic curve E defined over a field K. Let m be a positive integer not divisible by the characteristic of K. Then* $\det((\varphi)_m) \equiv deg(\varphi) \mod m$. *Where $(\varphi)_m$ denotes the 2×2 matrix which describes the action of φ on $E[m]$.*

Let $p \nmid m$. We now look at the action of ϕ_p denoted as $(\phi_p)_m$, on $E[m](\overline{\mathbb{F}_p})$,

the set of m-torsion points of E over the algebraic closure of $\mathbb{F}_p$. As $(p, m) = 1$,

$$\mathrm{Aut}(E[m])(\mathbb{F}_p) \simeq GL_2(\mathbb{Z}/m\mathbb{Z}).$$

If we fix a basis for the m-torsion points, $\phi_p \in \mathrm{Aut}(E[m])$ can be seen as a 2×2 matrix in $GL_2(\mathbb{Z}/m\mathbb{Z})$.

Theorem 2.10.5 ([Wa], Chapter 4, Theorem 4.10) *Let P_1 and P_2 denote a fixed basis for $E[m]$ and let $p \nmid m$. Let $(\phi_p)_m$ denote the 2×2 matrix in $GL_2(\mathbb{Z}/m\mathbb{Z})$ which corresponds to the action of ϕ_p on the basis elements P_1 and P_2. Then*

$$\begin{aligned} tr(\phi_p)_m &\equiv a_p \mod m \\ \det(\phi_p)_m &\equiv p \mod m \end{aligned}$$

where $a_p = p + 1 - \#E(\mathbb{F}_p)$.

Proof: Let $m \geq 1$ where $(m, p) = 1$. Then ϕ_p induces a matrix $(\phi_p)_m$ that describes the action ϕ_p on $E[m]$. Let

$$(\phi_p)_m = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Using proposition 2.10.3 and proposition 2.10.4 we have

$$\begin{aligned}
\#\mathrm{Ker}(\phi_p - 1) &= deg(\phi_p - 1) \\
&\equiv \det\left((\phi_p)_m - I\right) \mod m \\
&\equiv \det\begin{pmatrix} a-1 & b \\ c & d-1 \end{pmatrix} \mod m \\
&\equiv ad - d - a + 1 - bc \mod m \\
&\equiv (ad - bc) - (a + d) + 1 \mod m
\end{aligned}$$

by proposition 2.10.4, $ad - bc = \det(\phi_p)_m \equiv deg(\phi_p) = p \mod m$ and

$$a_p = p + 1 - \#E(\mathbb{F}_p) = p + 1 - deg(\phi_p - 1).$$

By proposition 2.10.3,

$$a_p = p + 1 - \#\mathrm{Ker}(\phi_p - 1)$$

which implies

$$\#\mathrm{Ker}(\phi_p - 1) = p + 1 - a_p \equiv p + 1 - (a + d) \mod m$$

thus $a_p \equiv (a + d) \mod m = \mathrm{tr}((\phi_p)_m)$. □

Theorem 2.10.6 ([Wa], Chapter 4, Theorem 4.10) *Let E be defined over $\mathbb{F}_p$ and let ϕ_p denote the Frobenius endomorphism of E. Then ϕ_p satisfies the polynomial in $End(E)$*

$$x^2 - a_p x + p = 0$$

where $a_p = p + 1 - \#E(\mathbb{F}_p)$.

Proof: If $\phi_p^2 - a_p\phi_p + p$ is not the 0 endomorphism then its kernel is finite. Using theorem 2.10.5, we know that for $(p, m) = 1$, the trace and determinant of $(\phi_p)_m$ is a_p and p. By the Cayley-Hamilton theorem, this implies that $(\phi_p)_m^2 - a_p(\phi_p)_m + pI \equiv 0 \pmod{m}$. Here, I denotes the 2×2 identity matrix. The characteristic polynomial of $(\phi_p)_m$ is therefore, $x^2 - a_p x + p$. Since there are infinitely many choices for m, the kernel of $\phi_p^2 - a_p\phi_p + p$ is infinite and so the endomorphism is equal to 0. □

Corollary 2.10.7 *The Frobenius field $\mathbb{Q}(\pi_p)$ is a quadratic imaginary field.*

Proof: Now according to the (Hasse-Weil) theorem we know that

$$-2\sqrt{p} \leq \#E(\mathbb{F}_p) - p - 1 \leq 2\sqrt{p}$$

or equivalently,

$$-2\sqrt{p} \leq a_p \leq 2\sqrt{p}$$

For $x^2 - a_p x + p$ this implies that the discriminant $\sqrt{a_p^2 - 4p} < 0$. The two roots of the characteristic equation, are therefore, complex conjugates $\pi_p, \overline{\pi_p}$. The field extension $\mathbb{Q}(\pi_p)$ of $\mathbb{Q}$ that we get by adjoining one of these roots is a quadratic imaginary field. □

Theorem 2.10.8 *If E is an elliptic curve defined over $\mathbb{F}_p$, then $End(E)$ is either an order in a quadratic imaginary field or an order in a quaternion algebra.*

For proof, see [Si2] p.137.

Chapter 3

Preliminaries for Main Proof

3.1 The Chebotarev Density Theorem

The Chebotarev Density Theorem is an important tool for proving our results. However, before stating the theorem, we recall certain facts about Galois extensions. In what follows, L/K is a finite number field extension, O_K is the ring of algebraic integers in K, O_L is the ring of algebraic integers in L, $\mathfrak{p}$ is a prime ideal in K and $Q_1, \ldots, Q_r$ are the prime ideals in L which lie above $\mathfrak{p}$. In other words, these prime ideals occur in the factorization of $\mathfrak{p}O_L$ in O_L.

Definition 3.1.1 *Let L/K be a field extension not necessarily Galois. Let $\mathfrak{p}$ be a prime in K. Then,*

$$\mathfrak{p}O_L = {Q_1}^{e_1} \ldots {Q_r}^{e_r}$$

is the unique factorization of $\mathfrak{p}$ in terms of primes in L. The e_i are referred to as the ramification indices. If any of the $e_i \geq 2$ we say that $\mathfrak{p}$ ramifies in L.

Theorem 3.1.2 ([Ma], p.70) *Let L/K be a Galois extension and let $\mathfrak{p}$ be a prime of O_K. Let $Q_1, \ldots, Q_r$ be the primes of L lying over $\mathfrak{p}$. Then $Gal(L/K)$ acts transitively on this set of primes. That is, for any $1 \leq i, j \leq r$, there exists $\sigma \in Gal(L/K)$ such that $\sigma(Q_i) = Q_j$.*

Frobenius conjectured that there is an association between an element of the Galois group Gal(L/K) and each unramified prime $\mathfrak{p}$ in O_K. This association can be made using the Frobenius substitution at $\mathfrak{p}$. Chebotarev proved the theorem which would relate the density of unramified primes to the density of their corresponding elements in the Galois group. Before describing the Frobenius substitution at $\mathfrak{p}$, we need the following definitions.

Definition 3.1.3 *Let Q be a prime ideal in L. The decomposition group D_Q is the subgroup of $Gal(L/K)$ consisting of the $\sigma \in Gal(L/K)$ such that $\sigma(Q) = Q$.*

Definition 3.1.4 *The inertia group I_Q is the subgroup of $Gal(L/K)$ consisting of the $\sigma \in Gal(L/K)$ such that $\sigma(x) \equiv x \mod Q$ for all $x \in O_L$. We have that $I_Q \leq D_Q$.*

The following map is surjective see [Ma] p.99.

$$\begin{aligned} \psi : D_Q &\rightarrow \mathrm{Gal}\left(\frac{O_L}{Q}/\frac{O_K}{\mathfrak{p}}\right) \\ \sigma &\mapsto (x \mod Q \mapsto \sigma(x) \mod Q) \end{aligned}$$

The kernel of this map consists of all of the elements of D_Q which map to the identity automorphism in

$$\mathrm{Gal}\left(\frac{O_L}{Q}/\frac{O_K}{\mathfrak{p}}\right).$$

The kernel is clearly just the inertia group I_Q. Therefore, we have a short exact sequence

$$1 \to I_Q \to D_Q \to \mathrm{Gal}\left(\frac{O_L}{Q}/\frac{O_K}{\mathfrak{p}}\right) \to 1$$

where the map from I_Q to D_Q is injective because all the elements in I_Q are in D_Q and the map ψ is surjective. So we have that,

$$\frac{D_Q}{I_Q} \cong \mathrm{Gal}\left(\frac{O_L}{Q}/\frac{O_K}{\mathfrak{p}}\right).$$

Both O_L/Q and $O_K/\mathfrak{p}$ are finite fields of characteristic p where p is a prime number in $\mathbb{Z}$. Their Galois group is cyclic and generated by the Frobenius automorphism $\pi_{\mathfrak{p}}$ of $O_K/\mathfrak{p}$. Where

$$\pi_{\mathfrak{p}} : x \mapsto x^{\#O_K/\mathfrak{p}}.$$

In other words,

$$\mathrm{Gal}\left(\frac{O_L}{Q}/\frac{O_K}{\mathfrak{p}}\right) = < \pi_{\mathfrak{p}} > .$$

Let σ_Q be the element of D_Q which maps to the generator $\pi_{\mathfrak{p}}$ of the Galois group. This element is called the Frobenius element at Q and it is only defined modulo I_Q.

When $\mathfrak{p}$ is unramified, we have that $I_Q = 1$ where 1 is the identity automorphism and $\sigma(Q)$ is well defined. See [Ma] p.100.

For $\mathfrak{p}$ unramified, the Artin symbol at $\mathfrak{p}$ denoted as $\sigma_\mathfrak{p}$ is the conjugacy class of all of the Frobenius elements of primes lying above $\mathfrak{p}$. Or equivalently,

$$\sigma_\mathfrak{p} = \{\sigma \in D_Q \ : Q \mid \mathfrak{p}\}.$$

Theorem 3.1.5 (Chebotarev Density Theorem (CDT)) *Let $K \subset L$ be Galois, and let $C \subset G = Gal(L/K)$ be a conjugacy class. Then*

$$\Pi_C(L/K) = \{\mathfrak{p} : \ \mathfrak{p} \text{ a prime of } K, \mathfrak{p} \text{ unramified in } L, \sigma_\mathfrak{p} \in C\}$$

has density $\#C/\#G$.

For our purpose, we will be working with field extensions of $\mathbb{Q}$ so the primes of concern to us are precisely the prime numbers p in $O_\mathbb{Q} = \mathbb{Z}$. Let $L/\mathbb{Q}$ be a finite Galois extension with group G. Let $n_L = [L : \mathbb{Q}]$ and d_L denote the discriminant. For each conjugacy class C of G we define

$$\Pi_C(x, L/\mathbb{Q}) := \#\{p \leq x : \ p \text{ unramified in } L/\mathbb{Q}, \ \sigma_p \subseteq C\}$$

The Chebotarev Density Theorem asserts that as $x \to \infty$,

$$\Pi_C(x, L/\mathbb{Q}) \sim \frac{\#C}{\#G} Li(x)$$

where

$$Li(x) = \int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x}$$

as $x \rightarrow \infty$.

J. Lagarias and A.Odlyzko (1976) were the first to derive explicit error terms for this theorem. Two versions the CDT were proved one was unconditional and the other relied on the assumption of the Generalized Riemann Hypothesis. Each result expressed the error term as a function of $x, \#C, \#G, n_L = [L : \mathbb{Q}]$ and d_L. See [LaOd]. The error terms were further refined by J.-P. Serre and improved by K. Murty, R. Murty and N. Saradha. We list the two main theorems we will use in the proof of our main results. The first theorem is a refinement due to Serre of the version given in [LaOd].

Theorem 3.1.6 ([Se], p.133) *Assuming GRH for the Dedekind zeta function of L, we have that, for all $x \geq 3$,*

$$\Pi_C(x, L/\mathbb{Q}) = \frac{\#C}{\#G} Lix + O\left((\#C)x^{1/2}\left(\frac{log|d_L|}{n_L} + logx\right)\right)$$

The implied O-constant is absolute.

We use the same notation introduced in [CoFoMu] and let $P(L/\mathbb{Q})$ denote the set of rational primes p which ramify in $L/\mathbb{Q}$ and define the product,

$$M(L/\mathbb{Q}) := (\#G) \prod_{p \in P(L/\mathbb{Q})} p.$$

Theorem 3.1.7 ([MuMuSa], p.253-281) *Assuming GRH and AHC for the Artin L-functions attached to the irreducible characters of G, we have that, for all $x \geq 3$,*

$$\Pi_C(x, L/\mathbb{Q}) = \frac{\#C}{\#G} Lix + O((\#C)^{1/2} x^{1/2} log(M(L/\mathbb{Q})x))$$

This theorem is due to K. Murty, R. Murty and N. Saradha (see [MuMuSa]).

3.2 Properties of the Torsion Fields $\mathbb{Q}(E[m])/\mathbb{Q}$

Theorem 3.2.1 *Let $\mathbb{Q}(E[m])$ be the Galois extension of $\mathbb{Q}$. Then the following hold:*

1. *The ramified primes of $\mathbb{Q}(E[m])/\mathbb{Q}$ are the divisors of mN or $m\Delta_E$. Where N is the conductor of E and Δ_E is the discriminant of E.*

2. *Let n_m and d_m denote the degree and discriminant of the finite Galois extension $\mathbb{Q}(E[m])/\mathbb{Q}$. We have the following bounds:*

$$\frac{\log |d_m|}{n_m} \ll \log mN$$

and

$$\log(M(\mathbb{Q}(E[m])/\mathbb{Q})x) \ll \log mN.$$

Proof: For the proof of part 1 of the theorem see [Si2] p.179. The bounds obtained in part 2 can be found in [CoFoMu]. The calculations for these bounds are based on a lemma proved by Serre in [Se] p.130. We will make use of these results in the proof of the main theorem.

Theorem 3.2.2 *Let E be an elliptic curve over $\mathbb{Q}$, and m an integer. Let p be a prime not dividing $m\Delta_E$. Then, the Galois representation*

$$\rho_m : \ Gal(\mathbb{Q}(E[m])/\mathbb{Q}) \to GL_2(\mathbb{Z}/m\mathbb{Z})$$

sends the Artin symbol σ_p to a conjugacy class of matrices such that

$$tr(\rho_m(\sigma_p)) \equiv a_p \mod m$$

$$\det(\rho_m(\sigma_p)) \equiv p \mod m$$

where $a_p = p + 1 - \#\overline{E}(\mathbb{F}_p)$.

Proof: This follows from the definition of the Artin symbol and from Theorem 2.10.5. □

3.3 Matrices in $PGL_2(\mathbb{Z}/p\mathbb{Z})$

Definition 3.3.1 *For any commutative ring R, the general linear group denoted as $GL_2(R)$ is the set of invertible 2×2 matrices with coefficients in R. In other words,*

$$GL_2(R) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in R \text{ and } ad - bc \in R^* \right\}$$

Definition 3.3.2 *The projective linear group, $PGL_2(R)$ is defined as the quotient $GL_2(R)/R^*$ where* $R^* = \left\{ \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} \mid r \in R^* \right\}$

Let p be an odd prime. The matrices in $PGL_2(\mathbb{Z}/p\mathbb{Z})$ are the equivalence classes of invertible 2×2 matrices A, B with entries in $\mathbb{Z}/p\mathbb{Z}$ where $A \sim B$ if A is a nonzero scalar multiple of B mod p. Let us denote the classes of $PGL_2(\mathbb{Z}/p\mathbb{Z})$ as

$$\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} \right].$$

If $a = 0$ then $b \neq 0$ and we can choose the matrix with $b = 1$ as the representative matrix of each class. If a is any nonzero scalar mod p then we can choose the matrix with $a = 1$ because the matrices in each class are equivalent if they can be obtained from one another by multiplication by a nonzero scalar. Each equivalence class in $PGL_2(\mathbb{Z}/p\mathbb{Z})$ has a representative of the form:

$$\left[\begin{pmatrix} 0 & 1 \\ c & d \end{pmatrix}\right] \text{ or } \left[\begin{pmatrix} 1 & b \\ c & d \end{pmatrix}\right].$$

Furthermore, none of these representatives are equivalent.

Lemma 3.3.3 $\#PGL_2(\mathbb{Z}/p\mathbb{Z}) = p(p-1) + p^2(p-1) = p^3 - p$

Proof: We want to determine the number of representatives with $a = 0$ in $PGL_2(\mathbb{Z}/p\mathbb{Z})$. This matrix is in $PGL_2(\mathbb{Z}/p\mathbb{Z})$ if its determinant $-c \neq 0$. There are $p-1$ possibilities for c and p possibilities for d. In total there are $p(p-1)$ classes of this type in $PGL_2(\mathbb{Z}/p\mathbb{Z})$.

To determine the number of matrices of the form $a = 1$ in $PGL_2(\mathbb{Z}/p\mathbb{Z})$ we count the values of b, c, d for which the determinant $d - bc \neq 0$. There are $p \times p$ ways of choosing b and c. When choosing d we have to make sure that the determinant is not zero. Therefore, there are only $p-1$ ways of choosing d for each choice of b and c. In total there are $p^2(p-1)$ classes of this type. So

$$\#PGL_2(\mathbb{Z}/p\mathbb{Z}) = p(p-1) + p^2(p-1) = p^3 - p. \quad \square$$

Lemma 3.3.4 $\#PGL_2(\mathbb{Z}/pq\mathbb{Z}) = (p^3 - p)(q^3 - q)$

Proof: Since

$$PGL_2(\mathbb{Z}/pq\mathbb{Z}) \simeq PGL_2(\mathbb{Z}/p\mathbb{Z}) \times PGL_2(\mathbb{Z}/q\mathbb{Z})$$

follows from the Chinese Remainder theorem, using lemma 3.3.3 we get

$$\begin{aligned} \#PGL_2(\mathbb{Z}/pq\mathbb{Z}) &= \#PGL_2(\mathbb{Z}/p\mathbb{Z}) \times \#PGL_2(\mathbb{Z}/q\mathbb{Z}) \\ &= (p^3 - p)(q^3 - q). \quad \square \end{aligned}$$

We remark that the determinant and trace are not well defined in $PGL_2(\mathbb{Z}/p\mathbb{Z})$: if we multiply a given matrix A by a scalar k then $\mathrm{tr}(kA) = k\mathrm{tr}(A)$ and determinant $\det(kA) = k^2 \det(A)$.

Lemma 3.3.5 *The Legendre symbol,*

$$\left(\frac{4det(A) - tr^2(A)}{p}\right)$$

is well defined for classes A in $PGL_2(\mathbb{Z}/p\mathbb{Z})$

Proof: Let $A \sim B$ in $PGL_2(\mathbb{Z}/p\mathbb{Z})$, then $B = kA$ for some $k \in (\mathbb{Z}/p\mathbb{Z})^*$. Using the Legendre symbol we get:

$$\begin{aligned} \left(\frac{4\det(B) - \mathrm{tr}^2(B)}{p}\right) &= \left(\frac{4\det(kA) - \mathrm{tr}^2(kA)}{p}\right) \\ &= \left(\frac{4k^2\det(A) - k^2\mathrm{tr}^2(A)}{p}\right) \\ &= \left(\frac{k^2}{p}\right)\left(\frac{4\det(A) - \mathrm{tr}^2(A)}{p}\right) \\ &= \left(\frac{4\det(A) - \mathrm{tr}^2(A)}{p}\right) \end{aligned}$$

note since $k \neq 0$, k^2 is a square mod p so the Legendre symbol $\left(\frac{k^2}{p}\right)$ is equal to 1. Therefore, it is well defined. □

Lemma 3.3.6

$$\#\left\{g \in PGL_2(\mathbb{Z}/p\mathbb{Z}) \,\middle|\, \left(\frac{4\det(g) - tr(g)^2}{p}\right) = 0\right\} = p^2$$

Proof: We want to calculate the number of matrices g in $PGL_2(\mathbb{Z}/p\mathbb{Z})$ which have

$$\left(\frac{4\det(g) - \mathrm{tr}(g)^2}{p}\right) = 0.$$

We break this into two cases:

1. Suppose $a = 0$. We want to count the representatives

$$\left[\begin{pmatrix} 0 & 1 \\ c & d \end{pmatrix}\right] \text{ with } \left(\frac{-4c - d^2}{p}\right) = 0.$$

This occurs when $-4c = d^2$. If we vary c, $-4c$ goes through all of the values $1, \ldots, p-1$ (because $c \neq 0$). Half of these ($(p-1)/2$ values) are squares. For each of these squares d has two possible values. In total there are $(p-1)$ matrices with this property.

2. Suppose that $a \neq 0$. We want to count the representatives

$$\left[\begin{pmatrix} 1 & b \\ c & d \end{pmatrix}\right] \text{ with } \left(\frac{4(d - bc) - (1+d)^2}{p}\right) = 0.$$

This occurs when $-4bc = (1-d)^2$.

(a) If $b = 0$: c has p possible values, d has 1 value and so there are p matrices.

(b) If $c = 0$ and $b \neq 0$: d has 1 value and b has $(p-1)$ values so there are $(p-1)$ matrices.

(c) If $b \neq 0$ and $c \neq 0$: then b has $p-1$ values. If we fix b then as c varies, $-4bc$ will go through all of the values $1, \ldots, p-1$ half of which are squares so there are $(p-1)/2$ choices for c. Each square yields two values of d. There are $2(p-1)((p-1)/2) = (p-1)^2$ possibilities. However, we must avoid the case when the determinant is zero i.e $d = bc$. This occurs when $-4d = (1-d)^2$ or $d = -1$. For every fixed $c \neq 0$, we can find a b which gives $d = -1$. There are $p-1$ matrices of this type.

Therefore,

$$\begin{aligned} \#\left\{ g \in PGL_2(\mathbb{Z}/p\mathbb{Z}) \,\middle|\, \left(\frac{4\det(g) - \mathrm{tr}(g)^2}{p}\right) = 0 \right\} &= (p-1) + p + (p-1) \\ &\quad + (p-1)^2 - (p-1) \\ &= p^2. \quad \square \end{aligned}$$

Lemma 3.3.7

$$\#\left\{ g \in PGL_2(\mathbb{Z}/p\mathbb{Z}) \,\middle|\, \left(\frac{-4\det(g) - tr(g)^2}{p}\right) = 1 \right\} = \frac{(p^3-p)}{2} + O(p^2)$$

Lemma 3.3.8

$$\#\left\{g \in PGL_2(\mathbb{Z}/p\mathbb{Z}) \left| \left(\frac{-4\det(g) - tr(g)^2}{p}\right) = -1\right.\right\} = \frac{(p^3-p)}{2} + O(p^2)$$

Proof: To calculate the number of matrices in $PGL_2(\mathbb{Z}/p\mathbb{Z})$ whose Legendre symbol is 1 or -1, the proof is identical in both cases. For p an odd prime, every reduced modulo p system has $(p-1)/2$ squares and $(p-1)/2$ nonsquares modulo p (see [Ap] p.179). We provide the calculations for the case where the Legendre symbol is 1. The proof for when the Legendre symbol is -1 is the same. We begin by analyzing the two general cases:

1. Suppose $a = 0$. We want to calculate the number of representatives

$$\left[\begin{pmatrix} 0 & 1 \\ c & d \end{pmatrix}\right] \text{ with } \left(\frac{-4c-d^2}{p}\right) = 1$$

this occurs when $-4c - d^2$ is a square mod p (-1 when $-4c - d^2$ is a nonsquare mod p). If we fix d and vary c, at most there will be $(p-1)/2$ squares (nonsquares) for $-4c-d^2$. For each fixed value of d, there can be at most $(p-1)/2$ solutions for c which yield a square for the value of $-4c-d^2$. In total there are $p(p-1)/2$ possibilities. However, we must discount the possibilities where $c = 0$ otherwise the determinant will be zero. This occurs when $-4(0)-d^2 = -d^2$ is a square (nonsquare). There can be at most $(p-1)$ values of d will yield a square (nonsquare) so we get $p(p-1)/2 + O(p)$.

2. Suppose that $a \neq 0$. We want to count the number of representatives

$$\left[\begin{pmatrix} 1 & b \\ c & d \end{pmatrix}\right] \text{ with } \left(\frac{4(d-bc)-(1+d)^2}{p}\right) = 1$$

this occurs when $-(d-1)^2-4bc$ is a square mod p (-1 when $-(d-1)^2-4bc$ is a nonsquare mod p). If we fix d and b and vary c, there are at most $(p-1)/2$ squares for every value of d and b so c can have at most $(p-1)/2$ solutions which yield a square for the value of $-(d-1)^2-4bc$. In total, there $p^2(p-1)/2$ such matrices. However, we must avoid the case when $d = bc$ i.e when the determinant is zero. This occurs when $-(d+1)^2$ is a square (nonsquare). There are at most $(p-1)$ values of d which satisfy this condition. Now for every fixed value of c, we can find a b which gives us $bc = d$. In total there are $p^2(p-1)/2+O(p^2)$ possibilities. We have an error term of p^2 matrices.

Therefore,

$$\begin{aligned} \#\left\{g \in PGL_2(\mathbb{Z}/p\mathbb{Z}) \,\middle|\, \left(\frac{-4\det(g)-\mathrm{tr}(g)^2}{p}\right) = 1\right\} &= \frac{p(p-1)}{2} + O(p) \\ &\quad + p^2\frac{(p-1)}{2} + O(p^2) \\ &= \frac{(p^3-p)}{2} + O(p^2). \quad \square \end{aligned}$$

3.4 The Square Sieve

The Square Sieve will play an important part in our proof of the main theorem. We state it here without providing the proof. The proof can be found in [CoFoMu].

Theorem 3.4.1 (The Square Sieve) *Let A be a finite set of not necessarily distinct, nonzero integers, and let P be a set of (distinct) odd primes. Set*

$$S(A) := \#\{\mu \in A |\ \mu \text{ is a square}\}$$

Then

$$S(A) \leq \frac{\#A}{\#P} + \max_{\substack{l,q \in P \\ l \neq q}} \left| \sum_{\mu \in A} \left(\frac{\mu}{lq} \right) \right| + \frac{2}{\#P} \sum_{\mu \in A} \sum_{\substack{l \in P \\ (\mu,l) \neq 1}} 1 + \frac{1}{(\#P)^2} \sum_{\mu \in A} \left(\sum_{\substack{l \in P \\ (\mu,l) \neq 1}} 1 \right)^2,$$

where $(\frac{\cdot}{lq})$ denotes the Jacobi symbol , (μ, l) denotes the greatest common divisor of μ and l, and max denotes the maximum element of the above set of numbers.

Chapter 4

Proof of Main Theorem

4.1 Overview of Main Theorem

Fix E an elliptic curve over $\mathbb{Q}$, and let $K = \mathbb{Q}(\sqrt{-D})$ be a fixed quadratic imaginary extension where $D > 0$ is a fixed square free integer. Let

$$P_E(\mathbb{Q}(\sqrt{-D}), x) = \#\{p \leq x | \; p \nmid \Delta_E, \mathbb{Q}(\pi_p) = \mathbb{Q}(\sqrt{-D})\}.$$

We prove in this chapter the main theorem.

Theorem 1.0.3 *Let E be a non-CM elliptic curve defined over $\mathbb{Q}$ with conductor N. Let $\mathbb{Q}(\sqrt{-D})$ be a fixed imaginary quadratic field. Let $x \geq 3$ be a positive real number.*

(a) if we assume GRH for the Dedekind zeta functions of the division fields of E, then

$$P_E(\mathbb{Q}(\sqrt{-D}), x) \ll_N x^{13/14} \log x$$

(b) if we assume GRH and Artin's Holomorphy Conjecture (denoted AHC) for

the L-functions of the irreducible characters of the Galois groups of the division fields of E then

$$P_E(\mathbb{Q}(\sqrt{-D}), x) \ll_N x^{7/8} \log x$$

Throughout the proof, p, q, l will denote odd rational primes, x and z will denote positive real numbers. Given an elliptic curve E defined over $\mathbb{Q}$ and of discriminant Δ_E, the prime p we use will not divide Δ_E. For $|f(x)| = Mg(x)$ we write $f(x) \ll g(x)$ or $f(x) = O(g(x))$ to indicate that the constant M is absolute. We also use the notaton $\asymp$ which implies that $f(x) \ll g(x) \ll f(x)$.

4.2 Proof of Theorem 1.0.3 part (a)

Proof: To prove part (a) of the theorem, we use same procedure and notation introduced in [CoFoMu]. The first half of the calculations can be found in [CoFoMu]. However, for completeness we include them here. We want to find an upper bound for the number of primes $p \leq x$, $p \nmid \Delta_E$, for which $\mathbb{Q}(\pi_p) = \mathbb{Q}(\sqrt{-D})$, this occurs when the discriminant of $x^2 - a_p x + p$ is negative. Which implies $\sqrt{a_p^2 - 4p} = \sqrt{-D}m$ or equivalently,

$$4p - a_p^2 = Dm^2$$

for some nonzero integer m. Multiplying both sides of the equation by D we get that

$$D(4p - a_p^2) = D^2 m^2.$$

To use the Square Sieve, we start by defining A and P as follows:

$$A := \{D(4p - a_p^2) \mid p \leq x\}$$

$$P := \{q \text{ a prime} \mid z < q \leq 2z\}$$

where

$$z = z(x) > aN(\log\log N)^{1/2}$$

is a positive real number depending on x to be chosen later, a denotes a positive absolute constant also to be specified later. For a nonzero integer μ let

$$v_z(\mu) := \#\{l \in P \text{ such that } l|\mu\}.$$

We are finding an upper bound for the number of squares in the set A. From the equation for the Square Sieve and the inequality $v_z(\mu) \ll \log\mu$, we obtain

$$\begin{aligned} S(A) = \#\{\mu \in A \mid \mu \text{ is a square}\} \quad &\leq \quad \frac{\#A}{\#P} + \max_{\substack{l,q \in P \\ l \neq q}} \left| \sum_{\mu \in A} \left(\frac{\mu}{lq}\right) \right| \\ &\quad + O\left(\frac{1}{\#P} \sum_{\mu \in A} \log\mu + \frac{1}{(\#P)^2} \sum_{\mu \in A} (\log\mu)^2 \right) \end{aligned}$$

Using the fact that $\#A \ll \frac{x}{\log x}$, $\#P \asymp \frac{z}{\log z}$, we obtain the following:

$$\begin{aligned}\frac{1}{\#P}\sum_{\mu\in A}\log\mu &\ll \frac{\log z}{z}\left(\sum_{p\le x}\log\left(D(4p-{a_p}^2)\right)\right)\\ &\ll \frac{\log z}{z}\left(\Pi(x)\log D+\sum_{p\le x}\log 4p\right)\\ &\ll \frac{\log z}{z}\left(\frac{x\log D}{\log x}+x\right).\end{aligned}$$

The Prime Number Theorem provides us with the approximation

$$\sum_{p\le x}1=\Pi(x)\sim\frac{x}{\log x}.$$

$$\begin{aligned}\sum_{\mu\in A}(\log\mu)^2 &\ll \sum_{p\le x}(\log D)^2+2(\log D)\sum_{p\le x}\log\left(4p-{a_p}^2\right)\\ &\quad+\sum_{p\le x}(\log(4p-{a_p}^2))^2\end{aligned}$$

$$\frac{1}{(\#P)^2}\sum_{\mu\in A}(\log\mu)^2 \ll \frac{(\log z)^2}{z^2}\left(\frac{x(\log D)^2}{\log x}+x\log D+x\log x\right)$$

Substituting these results into the equation for $S(A)$ we get,

$$\begin{aligned}S(A) &\ll \frac{x\log z}{z\log x}+\max_{\substack{l,q\in P\\ l\neq q}}\left|\sum_{\mu\in A}\left(\frac{\mu}{lq}\right)\right|+\frac{x\log z}{z\log x}\log D+\frac{x\log z}{z}\\ &\quad+\frac{x(\log z)^2}{z^2\log x}(\log D)^2+\frac{x(\log z)^2}{z^2}\log D+\frac{x(\log x)(\log z)^2}{z^2}\end{aligned}$$

To find an upper bound for $S(A)$ we need to find an upper bound for

$$\max_{\substack{l,q\in P\\ l\neq q}}\left|\sum_{\mu\in A}\left(\frac{\mu}{lq}\right)\right|$$

The essential difference in our calculations with those found in [CoFoMu] occurs here. To get an improvement of [CoFoMu], we now use the representation $\overline{\rho_m}$ of Theorem 2.7.1. Since we are dealing with matrices in $PGL_2(\mathbb{Z}/lq\mathbb{Z})$, we cannot count matrices according to the values of their traces and determinants as done in [CoFoMu] because both the trace and determinant are no longer invariant in $PGL_2(\mathbb{Z}/lq\mathbb{Z})$: two matrices which are in the same conjugacy class in $PGL_2(\mathbb{Z}/lq\mathbb{Z})$ can have different traces and determinants. We use the Legendre symbol

$$\left(\frac{4\det(A) - \mathrm{tr}^2(A)}{lq}\right)$$

which is well defined for $A \in PGL_2(\mathbb{Z}/lq\mathbb{Z})$ to separate the primes into four specific sums s_1, s_2, s_3, s_4 and then use the CDT to compute the number of unramified primes whose Artin symbol at p belongs to one of the four corresponding classes $C_1(lq), C_2(lq), C_3(lq), C_4(lq)$ of $\mathrm{Gal}(F_E[lq]/\mathbb{Q})$. Let $l, q \in P$ where $l \neq q$ be fixed. We rewrite the sum as

$$\begin{aligned}
\sum_{\mu \in A}\left(\frac{\mu}{lq}\right) &= \sum_{\substack{p \leq x \\ p \nmid lqN}}\left(\frac{D(4p - {a_p}^2)}{lq}\right) + O(\log N) \\
&= \left(\frac{D}{lq}\right)\sum_{\substack{p \leq x \\ p \nmid lqN}}\left(\frac{4p - {a_p}^2}{l}\right)\left(\frac{4p - {a_p}^2}{q}\right) + O(\log N) \\
&= \left(\frac{D}{lq}\right)(s_1 + s_2 + s_3 + s_4) + O(\log N)
\end{aligned}$$

where s_1, s_2, s_3, s_4 are defined to be:

$$s_1 = \sum_{\substack{p\le x, p\nmid lqN \\ \left(\frac{4p-a_p^2}{l}\right)=\left(\frac{4p-a_p^2}{q}\right)=1}} \left(\frac{4p-a_p^2}{l}\right)\left(\frac{4p-a_p^2}{q}\right) = \sum_{\substack{p\le x, p\nmid lqN \\ \left(\frac{4p-a_p^2}{l}\right)=\left(\frac{4p-a_p^2}{q}\right)=1}} 1$$
$$= \#\left\{p \le x, p \nmid lqN \,\middle|\, \left(\frac{4p-a_p^2}{l}\right) = \left(\frac{4p-a_p^2}{q}\right) = 1\right\}$$

$$s_2 = \sum_{\substack{p\le x, p\nmid lqN \\ \left(\frac{4p-a_p^2}{l}\right)=\left(\frac{4p-a_p^2}{q}\right)=-1}} \left(\frac{4p-a_p^2}{l}\right)\left(\frac{4p-a_p^2}{q}\right) = \sum_{\substack{p\le x, p\nmid lqN \\ \left(\frac{4p-a_p^2}{l}\right)=\left(\frac{4p-a_p^2}{q}\right)=-1}} 1$$
$$= \#\left\{p \le x, p \nmid lqN \,\middle|\, \left(\frac{4p-a_p^2}{l}\right) = \left(\frac{4p-a_p^2}{q}\right) = -1\right\}$$

$$s_3 = \sum_{\substack{p\le x, p\nmid lqN \\ \left(\frac{4p-a_p^2}{l}\right)=1, \left(\frac{4p-a_p^2}{q}\right)=-1}} \left(\frac{4p-a_p^2}{l}\right)\left(\frac{4p-a_p^2}{q}\right) = \sum_{\substack{p\le x, p\nmid lqN \\ \left(\frac{4p-a_p^2}{l}\right)=1, \left(\frac{4p-a_p^2}{q}\right)=-1}} -1$$
$$= -\#\left\{p \le x, p \nmid lqN \,\middle|\, \left(\frac{4p-a_p^2}{l}\right) = 1, \left(\frac{4p-a_p^2}{q}\right) = -1\right\}$$

$$s_4 = \sum_{\substack{p\le x, p\nmid lqN \\ \left(\frac{4p-a_p^2}{l}\right)=-1, \left(\frac{4p-a_p^2}{q}\right)=1}} \left(\frac{4p-a_p^2}{l}\right)\left(\frac{4p-a_p^2}{q}\right) = \sum_{\substack{p\le x, p\nmid lqN \\ \left(\frac{4p-a_p^2}{l}\right)=-1, \left(\frac{4p-a_p^2}{q}\right)=1}} -1$$
$$= -\#\left\{p \le x, p \nmid lqN \,\middle|\, \left(\frac{4p-a_p^2}{l}\right) = -1, \left(\frac{4p-a_p^2}{q}\right) = 1\right\}.$$

Note that we do not define the sums for which one of the Legendre symbols is equal to zero. This is because the sum for which this occurs will be equal to zero. Hence, our calculations will not be affected by them.

Using Theorem 3.2.1(1), the rational primes in $F_E[lq]/\mathbb{Q}$ which do not ramify are precisely those primes p such that $(p, lqN) = 1$. Using the properties for the Artin symbol at p stated in Theorem 3.2.2 for $m = lq$, s_1 can be rewritten in terms of ρ_l and ρ_q as the number of primes $p \leq x$, $p \nmid lqN$ where

$$\left(\frac{4\det(\rho_l(\sigma_p)) - (\mathrm{tr}(\rho_l(\sigma_p)))^2}{l}\right) = \left(\frac{4\det(\rho_q(\sigma_p)) - (\mathrm{tr}(\rho_q(\sigma_p)))^2}{q}\right) = 1.$$

Then s_1 can be evaluated by applying the CDT to the Galois extension $F_E[lq]/\mathbb{Q}$. For $m = lq$ where $(A, lq) = 1$, we can use Theorem 2.7.1 and the Chinese Remainder Theorem to get

$$\mathrm{Gal}(F_E[lq]/\mathbb{Q}) \simeq PGL_2(\mathbb{Z}/lq\mathbb{Z}) \simeq PGL_2(\mathbb{Z}/l\mathbb{Z}) \times PGL_2(\mathbb{Z}/q\mathbb{Z}).$$

Let

$$C_1(lq) \leq \mathrm{Gal}(F_E[lq]/\mathbb{Q}).$$

For notational convenience, let $P_{lq} = PGL_2(\mathbb{Z}/l\mathbb{Z}) \times PGL_2(\mathbb{Z}/q\mathbb{Z})$.

$$C_1(lq) = \left\{ g \in P_{lq} \,\middle|\, \left(\frac{4\det g - (\mathrm{tr}g)^2}{l}\right) = \left(\frac{4\det g - (\mathrm{tr}g)^2}{q}\right) = 1 \right\}.$$

Then

$$s_1 = \#\{p \leq x, p \nmid lqN \mid \overline{\rho}_{lq}(\sigma_p) \subseteq C_1(lq)\}.$$

Using the explicit CDT, Theorem 3.1.6 and the bound in Theorem 3.2.1(2) for the parameter

$$\frac{\log |d_{lq}|}{n_{lq}}$$

$$s_1 = \frac{\#C_1(lq)}{\#PGL_2(\mathbb{Z}/lq\mathbb{Z})} Lix + O((\#C_1(lq))x^{\frac{1}{2}} \log(lqNx)).$$

Lemma 4.2.1 $\#C_1(lq) = (l^3 - l)(q^3 - q)/4 + O(l^3q^2 + l^2q^3)$

Proof: Using the results found in section 3.3, we can substitute the values found in lemma 3.3.4 and lemma 3.3.7 for the number of matrices whose Legendre symbol is 1. Using the fact that

$$PGL_2(\mathbb{Z}/lq\mathbb{Z}) \simeq PGL_2(\mathbb{Z}/l\mathbb{Z}) \times PGL_2(\mathbb{Z}/q\mathbb{Z}),$$

we can calculate $\#C_1(lq)$.

$$\begin{aligned}
\#C_1(lq) &= \left((l^3 - l)/2 + O(l^2)\right)\left((q^3 - q)/2 + O(q^2)\right) \\
&= (l^3 - l)(q^3 - q)/4 + O(q^2)(l^3 - l)/2 \\
&\quad + O(l^2)(q^3 - q)/4 + O(l^2)O(q^2) \\
&= (l^3 - l)(q^3 - q)/4 + O(l^3q^2 + l^2q^3) \quad \square
\end{aligned}$$

Using lemma 4.2.1 we have

$$\begin{aligned}
s_1 &= \frac{(l^3 - l)(q^3 - q)/4 + O(l^3q^2 + l^2q^3)}{(l^3 - l)(q^3 - q)} Lix + O(l^3q^3x^{\frac{1}{2}} \log(lqNx)) \\
&= \frac{(l^3 - l)(q^3 - q)}{4(l^3 - l)(q^3 - q)} Lix + O\left(\frac{l^3q^2 + l^2q^3}{(l^3 - l)(q^3 - q)}\right) Lix + O(l^3q^3x^{\frac{1}{2}} \log(lqNx)) \\
&= \frac{Lix}{4} + O\left(\frac{l^3q^2 + l^2q^3}{l^3q^3}\right) Lix + O(l^3q^3x^{\frac{1}{2}} \log(lqNx)) \\
&= \frac{Lix}{4} + O\left(\left(\frac{1}{q} + \frac{1}{l}\right)\right) Lix + O(l^3q^3x^{\frac{1}{2}} \log(lqNx)).
\end{aligned}$$

To evaluate s_2, s_3, s_4, we proceed in a similar manner as for s_1. Let

$$C_2(lq) = \left\{ g \in P_{lq} \left| \left(\frac{4\det(g) - (\mathrm{tr}(g))^2}{l} \right) = \left(\frac{4\det(g) - (\mathrm{tr}(g))^2}{q} \right) = -1 \right\}.$$

By Theorem 2.7.1, we can restate s_2 as

$$s_2 = \#\{p \leq x, p \nmid lqN \mid \overline{\rho}_{lq}(\sigma_p) \subseteq C_2(lq)\}.$$

Using Theorem 3.1.6 and Theorem 3.2.1(2) for s_2

$$s_2 = \frac{\#C_2(lq)}{\#PGL_2(\mathbb{Z}/lq\mathbb{Z})} Lix + O((\#C_2(lq))x^{\frac{1}{2}} \log(lqNx)).$$

Lemma 4.2.2 $\#C_2(lq) = (l^3 - l)(q^3 - q)/4 + O(l^3q^2 + l^2q^3)$

Proof: Using lemma 3.3.4 and lemma 3.3.8, we can calculate the number of matrices whose Legendre symbol is -1. This gives

$$\begin{aligned} \#C_2(lq) &= ((l^3 - l)/2 + O(l^2))((q^3 - q)/2 + O(q^2)) \\ &= (l^3 - l)(q^3 - q)/4 + O(q^2)(l^3 - l)/2 \\ &\quad + O(l^2)(q^3 - q)/2 + O(l^2)O(q^2) \\ &= (l^3 - l)(q^3 - q)/4 + O(l^3q^2 + l^2q^3). \quad \square \end{aligned}$$

We can calculate s_2 using lemma 4.2.2

$$\begin{aligned} s_2 &= \frac{(l^3 - l)(q^3 - q)/4 + O(l^3q^2 + l^2q^3)}{(l^3 - l)(q^3 - q)} Lix + O(l^3q^3x^{\frac{1}{2}} \log(lqNx)) \\ &= \frac{Lix}{4} + O\left(\left(\frac{1}{q} + \frac{1}{l}\right)\right) Lix + O(l^3q^3x^{\frac{1}{2}} \log(lqNx)). \end{aligned}$$

Let

$$C_3(lq) = \left\{ g \in P_{lq} \,\middle|\, \left(\frac{4\det g - (\mathrm{tr} g)^2}{l}\right) = 1, \left(\frac{4\det g - (\mathrm{tr} g)^2}{q}\right) = -1 \right\}.$$

We rewrite s_3 as

$$s_3 = -\#\{p \leq x, p \nmid lqN \mid \overline{\rho}_{lq}(\sigma_p) \subseteq C_3(lq)\}.$$

To obtain s_3 we use Theorem 3.1.6 and Theorem 3.2.1(2)

$$s_3 = -\frac{\#C_3(lq)}{\#PGL_2(\mathbb{Z}/lq\mathbb{Z})} Lix + O((\#C_3(lq))x^{\frac{1}{2}} \log(lqNx)).$$

Lemma 4.2.3 $\#C_3(lq) = (l^3 - l)(q^3 - q)/4 + O(l^3q^2 + l^2q^3)$

Proof: Using lemma 3.3.4, lemma 3.3.7 and lemma 3.3.8, we have that the number of matrices satisfying the above conditions is

$$\begin{aligned}
\#C_3(lq) &= ((l^3 - l)/2 + O(l^2))((q^3 - q)/2 + O(q^2)) \\
&= (l^3 - l)(q^3 - q)/4 + O(q^2)(l^3 - l)/2 \\
&\quad + O(l^2)(q^3 - q)/2 + O(l^2)O(q^2) \\
&= (l^3 - l)(q^3 - q)/4 + O(l^3q^2 + l^2q^3). \quad \square
\end{aligned}$$

Using lemma 4.2.3 we have

$$\begin{aligned}
s_3 &= -\frac{\#C_3(lq)}{\#PGL_2(\mathbb{Z}/lq\mathbb{Z})} Lix + O((\#C_3(lq))x^{\frac{1}{2}} \log(lqNx)) \\
&= -\frac{(l^3 - l)(q^3 - q)/4 + O(l^3q^2 + l^2q^3)}{(l^3 - l)(q^3 - q)} Lix + O(l^3q^3x^{\frac{1}{2}} \log(lqNx)) \\
&= -\frac{Lix}{4} + O\left(\left(\frac{1}{q} + \frac{1}{l}\right)\right) Lix + O(l^3q^3x^{\frac{1}{2}} \log(lqNx)).
\end{aligned}$$

Let

$$C_4(lq) = \left\{ g \in P_{lq} \middle| \left(\frac{4\det g - (\mathrm{tr} g)^2}{l}\right) = -1, \left(\frac{4\det g - (\mathrm{tr} g)^2}{q}\right) = 1 \right\}.$$

We rewrite s_4 as

$$s_4 = -\#\{p \leq x, p \nmid lqN \mid \overline{\rho}_{lq}(\sigma_p) \subseteq C_4(lq)\}.$$

To calculate s_4 we use Theorem 3.1.6 and Theorem 3.2.1(2):

$$s_4 = -\frac{\#C_4(lq)}{\#PGL_2(\mathbb{Z}/lq\mathbb{Z})} Lix + O((\#C_4(lq))x^{\frac{1}{2}} \log(lqNx)).$$

Lemma 4.2.4 $\#C_4(lq) = (l^3 - l)(q^3 - q)/4 + O(l^3q^2 + l^2q^3)$

Proof: Using lemma 3.3.4, lemma 3.3.7 and lemma 3.3.8, we have that the number of matrices satisfying the above conditions is

$$\begin{aligned}
\#C_4(lq) &= ((l^3 - l)/2 + O(l^2))((q^3 - q)/2 + O(q^2)) \\
&= (l^3 - l)(q^3 - q)/4 + O(q^2)(l^3 - l)/2 \\
&\quad + O(l^2)(q^3 - q)/2 + O(l^2)O(q^2) \\
&= (l^3 - l)(q^3 - q)/4 + O(l^3q^2 + l^2q^3). \quad \square
\end{aligned}$$

Using lemma 4.2.4 we have

$$\begin{aligned}
s_4 &= -\frac{(l^3 - l)(q^3 - q)/4 + O(l^3q^2 + l^2q^3)}{(l^3 - l)(q^3 - q)} Lix + O(l^3q^3x^{\frac{1}{2}} \log(lqNx)) \\
&= -\frac{Lix}{4} + O\left(\left(\frac{1}{q} + \frac{1}{l}\right)\right) Lix + O(l^3q^3x^{\frac{1}{2}} \log(lqNx)).
\end{aligned}$$

Now going back to the original equation, we get

$$\begin{aligned}\sum_{\mu\in A}\left(\frac{\mu}{lq}\right) &= \left(\frac{D}{lq}\right)(s_1+s_2+s_3+s_4)+O(\log N)\\ &= \left(\frac{D}{lq}\right)\left(\frac{1}{4}Lix+\frac{1}{4}Lix-\frac{1}{4}Lix-\frac{1}{4}Lix\right)\\ &\quad +O\left(\left(\frac{1}{q}+\frac{1}{l}\right)Lix\right)+O(l^3q^3x^{\frac{1}{2}}\log(lqNx))\\ &\quad +O(\log N)\\ &= O\left(\left(\frac{1}{q}+\frac{1}{l}\right)Lix\right)+O(l^3q^3x^{\frac{1}{2}}\log(lqNx)).\end{aligned}$$

Since

$$Lix \sim \frac{x}{\log x}$$

the result can be written in terms of z and x. As mentioned earlier, z is a positive real number which depends on x. The primes l, q we are considering are bounded in the interval

$$z < l, q \leq 2z.$$

So we have

$$\frac{1}{2z} \leq \frac{1}{q}, \frac{1}{l} < \frac{1}{z}.$$

Therefore, their sum is also bounded.

$$\frac{1}{z} \leq \frac{1}{q}+\frac{1}{l} < \frac{2}{z}$$

In order to express the term $\log(lqNx)$ in terms of only x and z, we have

$$\log z < \log q, \log l \leq \log 2z$$

and

$$\log(lqNx) = \log(lq) + \log(Nx).$$

Using the fact that

$$\log lq = \log l + \log q,$$

we find the required bound

$$2\log z < \log l + \log q = \log(lq) \leq 2\log 2\log z$$

Substituting these bounds gives the following:

$$\begin{aligned}
\max_{\substack{l,q\in P\\ l\neq q}} \left|\sum_{\mu\in A}\left(\frac{\mu}{lq}\right)\right| &\leq \sum_{\mu\in A}\left(\frac{\mu}{lq}\right) \\
&= O\left(\left(\frac{1}{q}+\frac{1}{l}\right)Lix\right) + O(l^3q^3x^{\frac{1}{2}}\log(lqNx)) \\
&\ll \frac{x}{z\log x} + z^6x^{\frac{1}{2}}\log(zNx)
\end{aligned}$$

We substitute everything back into the equation for $S(A)$.

$$\begin{aligned}
S(A) \ll\ & \frac{x\log z}{z\log x} + \frac{x}{z\log x} + z^6x^{\frac{1}{2}}\log(zNx) + \frac{x\log z}{z\log x}\log D + \frac{x\log z}{z} \\
& + \frac{x(\log z)^2}{z^2\log x}(\log D)^2 + \frac{x(\log z)^2}{z^2}\log D + \frac{x(\log x)(\log z)^2}{z^2}
\end{aligned}$$

The z is a function of x and we want to find the value of z which will yield the best approximation. This occurs when

$$z^6x^{\frac{1}{2}} = \frac{x}{z}.$$

Solving the equation, we choose the following value of z

$$z^7 = x^{\frac{1}{2}}$$

$$z = x^{\frac{1}{14}}.$$

Since $P_E(\mathbb{Q}(\sqrt{-D}), x) = 0$ for square-free $D > 4x$, which allows us to assume $\log D \ll \log x$. Plugging into the initial equation we get

$$\begin{aligned} S(A) &\ll \frac{x \log x^{\frac{1}{14}}}{x^{\frac{1}{14}} \log x} + \frac{x}{x^{\frac{1}{14}} \log x} + x^{\frac{6}{14}} x^{\frac{1}{2}} \log (x^{\frac{1}{14}} N x) + \frac{x \log x^{\frac{1}{14}}}{x^{\frac{1}{14}} \log x} \log x + \frac{x \log x^{\frac{1}{14}}}{x^{\frac{1}{14}}} \\ &\quad + \frac{x (\log x^{\frac{1}{14}})^2}{x^{\frac{2}{14}} \log x} (\log x)^2 + \frac{x (\log x^{\frac{1}{14}})^2}{x^{\frac{2}{14}}} \log x + \frac{x (\log x)(\log x^{\frac{1}{14}})^2}{x^{\frac{2}{14}}} \\ &\ll x^{\frac{13}{14}} + \frac{x^{\frac{13}{14}}}{\log x} + x^{\frac{13}{14}} \log (x^{\frac{15}{14}} N) + x^{\frac{13}{14}} \log x + x^{\frac{13}{14}} \log x \\ &\quad + x^{\frac{12}{14}} (\log x)^3 + x^{\frac{12}{14}} (\log x)^3 + x^{\frac{12}{14}} (\log x)^3 \\ &\ll x^{\frac{13}{14}} \log x. \end{aligned}$$

This gives $P_E(\mathbb{Q}(\sqrt{-D}), x) \leq S(A) \ll_N x^{13/14} \log x$, which completes part (a) of the theorem. □

4.3 Proof of Theorem 1.0.3 part (b)

Proof: If we assume GRH and AHC and use the results found in the proof of the first part of the theorem we can improve the error term for s_1, s_2, s_3, s_4 by using the CDT with explicit error term, Theorem 3.1.7 and Theorem 3.2.1(2).

We obtain

$$\begin{aligned}
s_1 &= \frac{\#C_1(lq)}{\#PGL_2(\mathbb{Z}/lq\mathbb{Z})} Lix + O((\#C_1(lq))^{1/2} x^{1/2} \log(M(L/\mathbb{Q})x)) \\
&= \frac{((l^3-l)/2+O(l^2))((q^3-q)/2+O(q^2))}{(l^3-l)(q^3-q)} Lix + O((l^3q^3)^{\frac{1}{2}} x^{\frac{1}{2}} \log(lqNx)) \\
&= \frac{Lix}{4} + O\left(\left(\frac{1}{q}+\frac{1}{l}\right)\right) Lix + O(l^{\frac{3}{2}} q^{\frac{3}{2}} x^{\frac{1}{2}} \log(lqNx))
\end{aligned}$$

$$\begin{aligned}
s_2 &= \frac{\#C_2(lq)}{\#PGL_2(\mathbb{Z}/lq\mathbb{Z})} Lix + O((\#C_2(lq))^{1/2} x^{1/2} \log(M(L/\mathbb{Q})x)) \\
&= \frac{((l^3-l)/2+O(l^2))((q^3-q)/2+O(q^2))}{(l^3-l)(q^3-q)} Lix + O((l^3q^3)^{\frac{1}{2}} x^{\frac{1}{2}} \log(lqNx)) \\
&= \frac{Lix}{4} + O\left(\left(\frac{1}{q}+\frac{1}{l}\right)\right) Lix + O(l^{\frac{3}{2}} q^{\frac{3}{2}} x^{\frac{1}{2}} \log(lqNx))
\end{aligned}$$

$$\begin{aligned}
s_3 &= -\frac{\#C_3(lq)}{\#PGL_2(\mathbb{Z}/lq\mathbb{Z})} Lix + O((\#C_3(lq))^{1/2} x^{1/2} \log(M(L/\mathbb{Q})x)) \\
&= -\frac{((l^3-l)/2+O(l^2))((q^3-q)/2+O(q^2))}{(l^3-l)(q^3-q)} Lix + O((l^3q^3)^{\frac{1}{2}} x^{\frac{1}{2}} \log(lqNx)) \\
&= -\frac{Lix}{4} + O\left(\left(\frac{1}{q}+\frac{1}{l}\right)\right) Lix + O(l^{\frac{3}{2}} q^{\frac{3}{2}} x^{\frac{1}{2}} \log(lqNx))
\end{aligned}$$

$$\begin{aligned}
s_4 &= -\frac{\#C_4(lq)}{\#PGL_2(\mathbb{Z}/lq\mathbb{Z})} Lix + O((\#C_4(lq))^{1/2} x^{1/2} \log(M(L/\mathbb{Q})x)) \\
&= -\frac{((l^3-l)/2+O(l^2))((q^3-q)/2+O(q^2))}{(l^3-l)(q^3-q)} Lix + O((l^3q^3)^{\frac{1}{2}} x^{\frac{1}{2}} \log(lqNx)) \\
&= -\frac{Lix}{4} + O\left(\left(\frac{1}{q}+\frac{1}{l}\right)\right) Lix + O(l^{\frac{3}{2}} q^{\frac{3}{2}} x^{\frac{1}{2}} \log(lqNx)).
\end{aligned}$$

From part (a), we know that

$$\begin{aligned}\sum_{\mu\in A}\left(\frac{\mu}{lq}\right) &= \left(\frac{D}{lq}\right)(s_1+s_2+s_3+s_4)+O(\log N)\\ &= \left(\frac{D}{lq}\right)\left(\frac{1}{4}Lix+\frac{1}{4}Lix-\frac{1}{4}Lix-\frac{1}{4}Lix\right)\\ &\quad +O\left(\left(\frac{1}{q}+\frac{1}{l}\right)Lix\right)+O(l^{\frac{3}{2}}q^{\frac{3}{2}}x^{\frac{1}{2}}\log(lqNx))\\ &\quad +O(\log N)\\ &= O\left(\left(\frac{1}{q}+\frac{1}{l}\right)Lix\right)+O(l^{\frac{3}{2}}q^{\frac{3}{2}}x^{\frac{1}{2}}\log(lqNx)).\end{aligned}$$

Rewriting everything in terms of x and z,

$$\begin{aligned}\max_{\substack{l,q\in P\\ l\neq q}}\left|\sum_{\mu\in A}\left(\frac{\mu}{lq}\right)\right| &\leq \sum_{\mu\in A}\left(\frac{\mu}{lq}\right)\\ &= O\left(\left(\frac{1}{q}+\frac{1}{l}\right)Lix\right)+O(l^{\frac{3}{2}}q^{\frac{3}{2}}x^{\frac{1}{2}}\log(lqNx))\\ &\ll \frac{x}{z\log x}+z^3x^{\frac{1}{2}}\log(zNx).\end{aligned}$$

Plugging this into the equation for $S(A)$, we get

$$\begin{aligned}S(A) \ll\ & \frac{x\log z}{z\log x}+\frac{x}{z\log x}+z^3x^{\frac{1}{2}}\log(zNx)+\frac{x\log z}{z\log x}\log D+\frac{x\log z}{z}\\ &+\frac{x(\log z)^2}{z^2\log x}(\log D)^2+\frac{x(\log z)^2}{z^2}\log D+\frac{x(\log x)(\log z)^2}{z^2}.\end{aligned}$$

We want to find the value of z which will yield the best approximation. This occurs when

$$z^3x^{\frac{1}{2}}=\frac{x}{z}.$$

Therefore, solving the equation, we choose the following value of z

$$z^4 = x^{\frac{1}{2}}$$

$$z = x^{\frac{1}{8}}.$$

As in part (a), $P_E(\mathbb{Q}(\sqrt{-D}), x) = 0$ for square-free $D > 4x$ which allows us to assume $\log D \ll \log x$. This gives

$$\begin{aligned} S(A) &\ll \frac{x \log x^{\frac{1}{8}}}{x^{\frac{1}{8}} \log x} + \frac{x}{x^{\frac{1}{8}} \log x} + x^{\frac{3}{8}} x^{\frac{1}{2}} \log (x^{\frac{1}{8}} N x) + \frac{x \log x^{\frac{1}{8}}}{x^{\frac{1}{8}} \log x} \log x + \frac{x \log x^{\frac{1}{8}}}{x^{\frac{1}{8}}} \\ &\quad + \frac{x (\log x^{\frac{1}{8}})^2}{x^{\frac{2}{8}} \log x} (\log x)^2 + \frac{x (\log x^{\frac{1}{8}})^2}{x^{\frac{2}{8}}} \log x + \frac{x (\log x)(\log x^{\frac{1}{8}})^2}{x^{\frac{2}{8}}} \\ &\ll x^{\frac{7}{8}} + \frac{x^{\frac{7}{8}}}{\log x} + x^{\frac{7}{8}} \log (x^{\frac{9}{8}} N) + x^{\frac{7}{8}} \log x + x^{\frac{7}{8}} \log x \\ &\quad + x^{\frac{6}{8}} (\log x)^3 + x^{\frac{6}{8}} (\log x)^3 + x^{\frac{6}{8}} (\log x)^3 \\ &\ll x^{\frac{7}{8}} \log x. \end{aligned}$$

This gives $P_E(\mathbb{Q}(\sqrt{-D}), x) \leq S(A) \ll_N x^{7/8} \log x$, which completes part (b) of the theorem. $\square$

Bibliography

[Ap] T. Apostle, *Introduction to analytic number theory*, Springer Verlag, New York, 1976.

[CoFoMu] A. Cojocaru, E. Fouvry and M. Murty, The Square Sieve and the Lang-Trotter Conjecture, *Can. Math. J.* **57** (6) (2005), 1155–1177.

[LaOd] J. Lagarais, A. Odlyzko, Effective versions of the Chebotarev density theorem, in Algebraic Number Fields, A. Fröhlich (ed.) Academic Press, New York, 1977, 409–464.

[LaTr] S. Lang, H. Trotter, Frobenius distributions in GL_2-extensions, Lecture Notes in Mathematics 504, Springer Verlag, 1976.

[Ma] D. Marcus, *Number fields*, Springer Verlag, New York, c1977.

[Mu] M. Murty, *Problems in analytic number theory*, Springer, New York, 2001.

[MuMu] M. Murty, V. Murty, The Chebotarev density theorem and pair correlation of zeros of Artin L-functions, preprint.

[MuMu1] M. Murty, V. Murty, *Non vanishing of L-functions and applications*, Birkhäuser Verlag, Boston, Mass.,c1997.

[MuMuSa] M. Murty, V. Murty, N. Saradha, Modular forms and the Chebotarev density theorem, *Amer. J. Math.* **110**(2) (1998), 253–281

[Se] J-P. Serre, Quelques applications du théorème de densité de Chebotarev, Publ. Math. I. H. E. S., **54** (1981), 123–201.

[Si1] J. Silverman and J. Tate, *Rational points on elliptic curves*, Springer Verlag, New York, c1992.

[Si2] J. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics 106, Springer Verlag, New York, 1986.

[StLe] P. Stevenhagen and H. Lenstra Jr., Chebotarëv and his density theorem, *Math. Intel.* **18** (2) (1996), 26–37 (electronic).

[Wa] L. Washington, *Elliptic curves, Number theory and cryptography*, Chapman Hall/CRC, Boca Raton, c2003.