5-2009

On Elliptic Curves, Modular Forms, and the Distribution of Primes

Ethan Smith
Clemson University, ethancsmith@gmail.com

On Elliptic Curves, Modular Forms, and the Distribution of Primes

A Dissertation
Presented to
the Graduate School of
Clemson University

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy
Mathematical Sciences

by
Ethan C. Smith
May 2009

Accepted by:
Dr. Kevin James, Committee Chair
Dr. Neil J. Calkin
Dr. Hiren Maharaj
Dr. Hui Xue

Abstract

In this thesis, we present four problems related to elliptic curves, modular forms, the distribution of primes, or some combination of the three. The first chapter surveys the relevant background material necessary for understanding the remainder of the thesis. The four following chapters present our problems of interest and their solutions. In the final chapter, we present our conclusions as well as a few possible directions for future research.

Hurwitz class numbers are known to have connections to many areas of number theory. In particular, they are intimately connected to the theory of binary quadratic forms, the structure of imaginary quadratic number fields, the theory of elliptic curves, and the theory of modular forms. Hurwitz class number identities of a certain type are studied in Chapter 2. To prove these identities, we demonstrate three different techniques. The first method involves a relation between the Hurwitz class number and elliptic curves, while the second and third methods involve connections to modular forms.

In Chapter 3, we explore the construction of finite field elements of high multiplicative order arising from modular curves. The field elements are constructed recursively using the equations that Elkies discovered to describe explicit modular towers. Using elementary techniques, we prove lower bounds for the orders of these elements.

Prime distribution has been a central theme in number theory for hundreds of years. Mean square error estimates for the Chebotarëv Density Theorem are proved in Chapter 4. These estimates are related to the classical Barban-Davenport-Halberstam Theorem and will prove to be indispensable for our work in Chapter 5, where we take up the study of the Lang-Trotter Conjecture "on average" for elliptic curves defined over number fields.

We begin Chapter 4 by proving upper bounds on the mean square error in Chebotarëv's theorem. It is this upper bound which features as a key ingredient in Chapter 5. As another application of this upper bound, we continue in Chapter 4 to prove an asymptotic formula for the mean square error.

In Chapter 5, we turn to the discussion of the Lang-Trotter Conjecture for number fields "on average." The Lang-Trotter Conjecture is an important conjecture purporting to give information about the arithmetic of elliptic curves, the distribution of primes, and GL_2-representations of the absolute Galois group. In this chapter, we present some results in support of the conjecture. In particular, we show that the conjecture holds in an average sense when one averages over all elliptic curves defined over a given number field.

Dedication

To my dear wife, Andrea

Acknowledgments

I would like to express my sincere gratitude to my advisor, Kevin James, for his support and guidance. I greatly appreciate his advice - mathematical and otherwise. It has been a wonderful experience to work under his direction. I am also very grateful to the other members of my doctoral committee: Neil Calkin, Hiren Maharaj, and Hui Xue. I have also greatly benefitted from the advice of Jim Brown and Robert Osburn. In addition, I am thankful to Ken Ono for his suggestion concerning the application of the Eichler-Selberg Trace Formula in Chapter 2. I am also thankful to Andrew Granville both for his suggestion that I pursue the asymptotic formula for the generalization of the Barban-Davenport-Halberstam Theorem appearing in Chapter 4 as well as for pointing me toward the paper of Hooley that was so helpful in achieving the result. I wish to thank those of my coauthors not already mentioned: Brittany Brown, Jessica Burkhart, Tim Flowers, Shuhong Gao, Justine Hyde-Volpe, Shelly Manber, Jared Ruiz, and Amy Stout. Finally, I wish to thank my wife, Andrea, for reading and editing the contents of this thesis many times and in various forms.

Table of Contents

List of Tables

List of Figures

Chapter 1

Elliptic Curves, Modular Forms, and the Distribution of Primes

In this chapter we give an overview of several topics that will form the background for the remainder of the thesis. These topics include various facts and theorems from algebraic and analytic number theory as well as the theory of elliptic curves and modular forms.

1.1 Classical Distribution of Primes

The analytic number theory facts stated in this section may be found in [IK04]; most of the algebraic number theory facts may be found in [Mar77, Chap. 3] or [Lan94, Chap. I] except for the facts concerning Frobenius substitution in infinite extension. Many, but not all, of those facts may be found in [Mur02] and [DS05, Sect. 9.3].

1.1.1 Factorization of Primes and Frobenius Substitution

Let K be a number field. By a prime of K, we will always mean a prime a ideal $\mathfrak{p}$ of its ring of integers, which we denote by $\mathcal{O}_K$. For each prime $\mathfrak{p}$ of K, there is a unique prime number $p \in \mathbb{Z}$ such that $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$. The quotient $\mathcal{O}_K/\mathfrak{p}$ is then isomorphic to the finite field $\mathbb{F}_{p^m}$ for some $m \in \mathbb{N}$. The *absolute degree* of $\mathfrak{p}$ is defined by $\deg \mathfrak{p} := [\mathcal{O}_K/\mathfrak{p} : \mathbb{F}_p] = m$.

Suppose that L/K is an extension of number fields, and let $\mathcal{O}_L$ stand for the ring of integers of L. The rings $\mathcal{O}_L$ and $\mathcal{O}_K$ are well-known to be Dedekind domains, and hence possess the property of unique factorization of ideals. In particular, given a prime ideal $\mathfrak{p}$ of K, we may write

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g_\mathfrak{p}} \mathfrak{P}_i^{e_{\mathfrak{P}_i|\mathfrak{p}}}, \tag{1.1}$$

where $\mathfrak{P}_i$ is a prime of L for $1 \leq i \leq g_\mathfrak{p}$. For each $1 \leq i \leq g_\mathfrak{p}$, we have $\mathcal{O}_K \cap \mathfrak{P}_i = \mathfrak{p}$. The primes $\mathfrak{P}_i$ are said to *lie above* $\mathfrak{p}$, and we denote this by $\mathfrak{P}_i|\mathfrak{p}$. We also say that $\mathfrak{p}$ *lies below* or *lies in* $\mathfrak{P}$. The exponent $e_{\mathfrak{P}_i|\mathfrak{p}}$ is called the *ramification index* of $\mathfrak{P}_i$ over $\mathfrak{p}$.

If $\mathfrak{P}$ is any prime of L lying above $\mathfrak{p}$, then we have an associated extension of finite fields since $\mathbb{F}_{p^m} \cong \mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{P} \cong \mathbb{F}_{p^{mf}}$. The degree of this extension is called the *inertial degree* of $\mathfrak{P}$ over $\mathfrak{p}$, and we denote it by $f_{\mathfrak{P}|\mathfrak{p}} = f$. The values e and f satisfy the identity

$$\sum_{j=1}^{g_\mathfrak{p}} e_{\mathfrak{P}_i|\mathfrak{p}} f_{\mathfrak{P}_i|\mathfrak{p}} = [L : K], \tag{1.2}$$

and are "multiplicative" in extensions. That is, if L, K, $\mathfrak{P}$, and $\mathfrak{p}$ are as above and if F is an extension of L with a prime $\mathfrak{Q}$ lying above $\mathfrak{P}$, then $f_{\mathfrak{Q}|\mathfrak{p}} = f_{\mathfrak{Q}|\mathfrak{P}} f_{\mathfrak{P}|\mathfrak{p}}$ and $e_{\mathfrak{Q}|\mathfrak{p}} = e_{\mathfrak{Q}|\mathfrak{P}} e_{\mathfrak{P}|\mathfrak{p}}$.

Now, assume that the extension L/K is Galois. In this case,

$$\begin{aligned} e_{\mathfrak{P}_1|\mathfrak{p}} &= e_{\mathfrak{P}_2|\mathfrak{p}} = \cdots = e_{\mathfrak{P}_{g_\mathfrak{p}}|\mathfrak{p}}, \\ f_{\mathfrak{P}_1|\mathfrak{p}} &= f_{\mathfrak{P}_2|\mathfrak{p}} = \cdots = f_{\mathfrak{P}_{g_\mathfrak{p}}|\mathfrak{p}}, \end{aligned}$$

and we denote the common values by $e_\mathfrak{p}$ and $f_\mathfrak{p}$, respectively. Furthermore, we have the identity $e_\mathfrak{p} f_\mathfrak{p} g_\mathfrak{p} = [L : K]$. If $e_\mathfrak{p} = 1$, we say $\mathfrak{p}$ is *unramified* in L, and if $f_\mathfrak{p} = 1$ as well, we say $\mathfrak{p}$ *splits completely* in L. In the case that more than one extension is under consideration, we also write $g_\mathfrak{p}(L)$, $f_\mathfrak{p}(L)$ and $e_\mathfrak{p}(L)$ since the values depend on the extension of K.

In what follows, we continue to assume that L/K is Galois with group G and record several important implications of that assumption. See either [Lan94, pp. 12-18] or [Mar77, pp.98-109] for the facts recorded in the following three theorems.

Theorem 1.1.1. *Let $\mathfrak{p}$ be a prime of K.*

1. *If $\mathfrak{P}$ is a prime of L lying above $\mathfrak{p}$, then for each $\sigma \in G$, $\sigma\mathfrak{P}$ is also a prime of L lying above $\mathfrak{p}$.*
2. *If $\mathfrak{P}$, $\mathfrak{P}'$ are primes of L both lying above $\mathfrak{p}$, then there exists a $\sigma \in G$ such that $\mathfrak{P}' = \sigma\mathfrak{P}$.*

In other words, G acts transitively on the primes lying above $\mathfrak{p}$.

Given a prime $\mathfrak{P}$ of $\mathcal{O}_L$ lying above a prime $\mathfrak{p}$ of $\mathcal{O}_K$, the *decomposition group* and the *inertia group* of $\mathfrak{P}$ are respectively defined by

$$\begin{aligned} D_{\mathfrak{P}} &:= \{\sigma \in G : \sigma\mathfrak{P} = \mathfrak{P}\}, \\ I_{\mathfrak{P}} &:= \{\sigma \in D_{\mathfrak{P}} : \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}}\ \forall \alpha \in \mathcal{O}_L\}. \end{aligned}$$

Theorem 1.1.2. *The sequence*

$$\begin{tikzcd} \mathbf{1} \arrow[r] & I_{\mathfrak{P}} \arrow[r] & D_{\mathfrak{P}} \arrow[r] & \operatorname{Gal}\left(\mathbb{F}_{p^{mf}}/\mathbb{F}_{p^m}\right) \arrow[r] & \mathbf{1} \end{tikzcd}$$

is exact, where $m = \deg \mathfrak{p}$ and $f = f_{\mathfrak{P}|\mathfrak{p}}$.

From the theory of finite fields, $\operatorname{Gal}(\mathbb{F}_{p^{mf}}/\mathbb{F}_{p^m})$ is known to be a cyclic group of order f generated by the *Frobenius automorphism* ($x \mapsto x^{p^m}$). Any representative of the coset of $I_{\mathfrak{P}}$ mapping to this generator is called a *Frobenius substitution* or a *Frobenius element* at $\mathfrak{P}$ and is denoted by $\left(\frac{L/K}{\mathfrak{P}}\right)$. In the case that $\operatorname{Gal}(L/K)$ is Abelian, $\left(\frac{L/K}{\mathfrak{P}}\right)$ is often referred to as the *Artin symbol* and can be viewed as a generalization of the Legendre symbol. If $\mathfrak{P}$ is unramified above $\mathfrak{p}$, then the inertia group $I_{\mathfrak{P}}$ is trivial and hence, the Frobenius substitution is well-defined as the unique element of $\operatorname{Gal}(L/K)$ satisfying

$$\left(\frac{L/K}{\mathfrak{P}}\right)\alpha \equiv \alpha^{\mathrm{N}\mathfrak{p}} \pmod{\mathfrak{P}} \tag{1.3}$$

for all $\alpha \in \mathcal{O}_L$.

Theorem 1.1.3. *If $\sigma \in G$, then*

1. $D_{\sigma\mathfrak{P}} = \sigma D_{\mathfrak{P}} \sigma^{-1}$,

2. $I_{\sigma\mathfrak{P}} = \sigma I_{\mathfrak{P}} \sigma^{-1}$, *and*

3. $\left(\frac{L/K}{\sigma\mathfrak{P}}\right) = \sigma \left(\frac{L/K}{\mathfrak{P}}\right) \sigma^{-1}$.

Remark 1.1.4. If $\mathfrak{p}$ is unramified in L, we also write $\left(\frac{L/K}{\mathfrak{p}}\right)$ to mean the Frobenius element of any prime $\mathfrak{P}$ lying above $\mathfrak{p}$. By (1.1.3) and Theorem 1.1.1, we see that $\left(\frac{L/K}{\mathfrak{p}}\right)$ is defined only up to conjugacy in $\mathrm{Gal}(L/K)$. Thus, by $\left(\frac{L/K}{\mathfrak{p}}\right)$ we will sometimes mean the conjugacy class and sometimes mean any representative of the conjugacy class. Furthermore, $\mathfrak{p}$ splits completely in L if and only if $\left(\frac{L/K}{\mathfrak{p}}\right)$ is the trivial class.

Example 1.1.5. Suppose $K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_q)$, where ζ_q is a primitive q-th root of unity. Then the extension is Galois with group isomorphic $(\mathbb{Z}/q\mathbb{Z})^*$. In fact, if $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$, then $\sigma(\zeta_q) = \zeta_q^a$ for some $1 \le a \le q$ with $(a, q) = 1$. Let p be a rational prime not dividing q. Then one may check that p does not ramify in $\mathbb{Q}(\zeta_q)$ and $p \equiv a \pmod{q}$ with $(a, q) = 1$. Furthermore, $\left(\frac{\mathbb{Q}(\zeta_q)/\mathbb{Q}}{p}\right)$ is the unique $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ such that $\sigma(\zeta_q) = \zeta_q^a$.

Remark 1.1.6. In the case that K is a general number field and $L = K(\zeta_q)$, the same reasoning shows that the Galois group is isomorphic to a subgroup of $(\mathbb{Z}/q\mathbb{Z})^*$. Furthermore, the Frobenius of a prime $\mathfrak{p}$ of K is determined by the value of $\mathrm{N}\mathfrak{p}$ modulo q.

1.1.2 The Density Theorems of Chebotarëv and Dirichlet

The Chebotarëv Density Theorem is one of the most powerful results concerning the distribution of primes. It may be seen as a generalization of both Dirichlet's Theorem on primes in arithmetic progressions as well as a generalization of the lesser known Frobenius Density Theorem. We state Chebotarëv's theorem in terms of *natural density* as in [IK04, p. 143] since this is the form that we will need later.

Theorem 1.1.7 (The Chebotarëv Density Theorem)**.** *Let L/K be a Galois extension of number fields with group G, and let C be any conjugacy class of G. Then*

$$\sum_{\substack{\mathrm{N}\mathfrak{p}\leq x,\\ \left(\frac{L/K}{\mathfrak{p}}\right)=C}} \log \mathrm{N}\mathfrak{p} \sim \frac{|C|}{|G|}x, \tag{1.4}$$

where the sum is over prime ideals $\mathfrak{p}$ of K which do not ramify in L. Equivalently, we have

$$\#\left\{\mathrm{N}\mathfrak{p}\leq x : \left(\frac{L/K}{\mathfrak{p}}\right)=C\right\} \sim \frac{|C|}{|G|}\frac{x}{\log x}. \tag{1.5}$$

Remark 1.1.8. In many texts, the version of Chebotarëv's theorem appearing in (1.4) is often stated with the sum being over all powers of prime ideals of K. The two statements are easily seen to be equivalent since the difference between the two sums is bounded by a constant multiple of $\sqrt{x}$.

The size of the error in this approximation when averaging over cyclotomic extensions of K will be the subject of Chapter 4. In particular, we will show that the error is quite small on average.

As we saw in Example 1.1.5, the Frobenius $\left(\frac{\mathbb{Q}(\zeta_q)/\mathbb{Q}}{p}\right)$ is determined by the value of p modulo q. Thus, Chebotarëv's theorem may be viewed as a generalization of Dirichlet's Theorem on primes in arithmetic progressions, which states that if $(a,q)=1$, then

$$\sum_{\substack{p\leq x,\\ p\equiv a \pmod q}} \log p \sim \frac{x}{\varphi(q)}. \tag{1.6}$$

Here, $\varphi(q) := |(\mathbb{Z}/q\mathbb{Z})^*|$ is Euler's totient function. For more on the relationship with Dirichlet's Theorem as well as the relationship with the Frobenius Density Theorem, see [SL96]. The article also gives several concrete examples and a nice historical account of the life and work of Chebotarëv.

1.1.3 Frobenius Substitution in the Absolute Galois Group

Throughout suppose that K is a fixed number field with algebraic closure $\overline{K} = \overline{\mathbb{Q}}$. The extension $\overline{K}/K$ is, in fact, a Galois extension. The *absolute Galois group* of $\overline{K}/K$ is $\mathrm{Aut}_K(\overline{K})$ and may be constructed as follows. Consider the system of number fields $F \supseteq K$, which are Galois over K. We may partially order the set under containment, and if $F' \supseteq F \supseteq K$, then we have natural restriction maps

$$\mathrm{Gal}(F/K) \twoheadleftarrow \mathrm{Gal}(F'/K).$$

The absolute Galois group of $\overline{K}/K$ is then realized as

$$G_K := \mathrm{Gal}(\overline{K}/K) := \varprojlim_F \mathrm{Gal}(F/K). \tag{1.7}$$

Since the literature is rather lacking, we now discuss the construction of *absolute Frobenius elements* in some detail. Before proceeding, however, we must recall a couple of facts about inverse limits. First, we recall that the inverse limit functor is left exact meaning that if $\{A_n\}, \{B_n\}, \{C_n\}$ are inverse systems with respective inverse limits $\mathscr{A}, \mathscr{B}, \mathscr{C}$ and further the sequence

$$\mathbf{0} \longrightarrow A_n \longrightarrow B_n \longrightarrow C_n \longrightarrow \mathbf{0} \tag{1.8}$$

is exact for all n, then so is the sequence

$$\mathbf{0} \longrightarrow \mathscr{A} \longrightarrow \mathscr{B} \longrightarrow \mathscr{C}.$$

The so-called *Mittag-Leffler Condition* is a sufficient condition for ensuring that the "lifted" sequence is right exact as well. The condition may be stated as follows. For $m \geq n$, let $u_{m,n}$ denote the map $u_{m,n} : A_m \to A_n$. We say that the system $\{A_n\}$ satisfies the Mittag-Leffler Condition if for each n, the decreasing sequence $u_{m,n}(A_m)$ $(m \geq n)$ stabilizes. If the systems

$\{A_n\}, \{B_n\}, \{C_n\}$ satisfy (1.8) and the system $\{A_n\}$ satisfies the Mittag-Leffler condition, then the sequence

$$\mathbf{0} \longrightarrow \mathscr{A} \longrightarrow \mathscr{B} \longrightarrow \mathscr{C} \longrightarrow \mathbf{0}$$

is also exact. See [Lan02, p. 164] for more details.

We now return to our discussion of absolute Frobenius elements. Let $\mathfrak{p}$ be a prime of K. For each finite Galois extension F/K, compatibly choose a prime $\mathfrak{P}_F$ of F lying above $\mathfrak{p}$. By a compatible choice, we mean that if F'/K and F/K are both finite Galois extensions with $F' \supseteq F$, then $\mathfrak{P}_{F'}$ is chosen so that $\mathfrak{P}_{F'}|\mathfrak{P}_F$. By Theorem 1.1.2, for each finite Galois extension F/K and each prime $\mathfrak{P}_F$ of F lying over $\mathfrak{p}$, we have an exact sequence

$$\mathbf{1} \longrightarrow I_{\mathfrak{P}_F} \longrightarrow D_{\mathfrak{P}_F} \longrightarrow \mathrm{Gal}\left(\mathbb{F}_{p^{mf}}/\mathbb{F}_{p^m}\right) \longrightarrow \mathbf{1}, \tag{1.9}$$

where $f = f_{\mathfrak{P}_F|\mathfrak{p}}$ and $m = \deg \mathfrak{p}$. Given our compatible choice of primes lying above $\mathfrak{p}$, we will show in Proposition 1.1.9 below that the system $(I_{\mathfrak{P}_F})$ satisfies the Mittag-Leffler condition. By [Lan02, Prop. 10.3, p. 164], we may lift to the exact sequence

$$\mathbf{1} \longrightarrow \mathcal{I}_{\mathfrak{p}} \longrightarrow \mathcal{D}_{\mathfrak{p}} \longrightarrow G_{\mathbb{F}_{p^m}} \longrightarrow \mathbf{1}, \tag{1.10}$$

where $\mathcal{I}_{\mathfrak{p}} := \varprojlim_{(F,\mathfrak{P}_F)} I_{\mathfrak{P}_F}$, $\mathcal{D}_{\mathfrak{p}} := \varprojlim_{(F,\mathfrak{P}_F)} D_{\mathfrak{P}_F}$, and $G_{\mathbb{F}_{p^m}} := \mathrm{Gal}\left(\overline{\mathbb{F}}_{p^m}/\mathbb{F}_{p^m}\right)$ is the absolute Galois group of $\overline{\mathbb{F}}_{p^m}/\mathbb{F}_{p^m}$. Thus, through inverse limits, we construct an absolute decomposition group and an absolute inertia group above $\mathfrak{p}$. The groups obtained through the limit depend of course on the system of compatible primes lying above $\mathfrak{p}$. However, by Theorems 1.1.1 and 1.1.3, it is possible to show that conjugation by an element of the absolute Galois group G_K produces another absolute decomposition group and absolute inertia group above $\mathfrak{p}$. Moreover, any other compatible choice of primes lying above $\mathfrak{p}$ produces an absolute decomposition group and absolute inertia group above $\mathfrak{p}$ which is conjugate to any given absolute decomposition group and absolute inertia group. Thus, the situation is analogous to the case of finite Galois extensions.

The absolute Galois group $G_{\mathbb{F}_{p^m}}$ is an infinite cyclic group generated by the Frobenius automorphism $(x \mapsto x^{p^m})$. Thus, the exact sequence of (1.10) allows us to define an absolute Frobenius element above $\mathfrak{p}$ to be any element of the coset mapping to the Frobenius map of $G_{\mathbb{F}_{p^m}}$. We denote any such element by $\mathrm{Frob}_{\mathfrak{p}}$.

Proposition 1.1.9. *For any compatible system of primes* $(\mathfrak{P}_F)$ *lying above* $\mathfrak{p}$*, the system* $(I_{\mathfrak{P}_F})$ *satisfies the Mittag-Leffler condition.*

Proof. Let F/K be a finite Galois extension and let $\mathfrak{P} = \mathfrak{P}_F$ be a prime of F lying above $\mathfrak{p}$. Further suppose F'/K is a finite Galois extension with $F' \supseteq F$, and let $\mathfrak{P}' = \mathfrak{P}_{F'}$ be a prime of F' chosen compatibly with $\mathfrak{P}$. That is, $\mathfrak{P}'|\mathfrak{P}$. Let $D_{\mathfrak{P}'|\mathfrak{P}}$ and $I_{\mathfrak{P}'|\mathfrak{P}}$ respectively denote the decomposition group and the inertia group of $\mathfrak{P}'$ in $\mathrm{Gal}(F'/F)$. Then

$$D_{\mathfrak{P}'|\mathfrak{P}} = D_{\mathfrak{P}'} \cap \mathrm{Gal}(F'/F),$$
$$I_{\mathfrak{P}'|\mathfrak{P}} = I_{\mathfrak{P}'} \cap \mathrm{Gal}(F'/F),$$

and the following diagram commutes, where each row is exact by Theorem 1.1.2.

$$\begin{tikzcd}
\mathbf{1} \arrow[r] & I_{\mathfrak{P}'|\mathfrak{P}} \arrow[r] \arrow[d, hook] & D_{\mathfrak{P}'|\mathfrak{P}} \arrow[r, "h'"] \arrow[d, hook] & \mathrm{Gal}\left(\mathbb{F}_{p^{mf'}}/\mathbb{F}_{p^{mf}}\right) \arrow[r] \arrow[d, hook] & \mathbf{1} \\
\mathbf{1} \arrow[r] & I_{\mathfrak{P}'} \arrow[r] \arrow[d, "\mathrm{Res}"] & D_{\mathfrak{P}'} \arrow[r, "h'"] \arrow[d, "\mathrm{Res}"] & \mathrm{Gal}\left(\mathbb{F}_{p^{mf'}}/\mathbb{F}_{p^m}\right) \arrow[r] \arrow[d, two heads, "\mathrm{Res}_{p^m}"] & \mathbf{1} \\
\mathbf{1} \arrow[r] & I_{\mathfrak{P}} \arrow[r] & D_{\mathfrak{P}} \arrow[r, "h"] & \mathrm{Gal}\left(\mathbb{F}_{p^{mf}}/\mathbb{F}_{p^m}\right) \arrow[r] & \mathbf{1}
\end{tikzcd}$$

(1.11)

Here, $f' = f_{\mathfrak{P}'|\mathfrak{p}}$, $f = f_{\mathfrak{P}|\mathfrak{p}}$, and $m = \deg \mathfrak{p}$. The hooked arrows are obvious inclusions, and hence are injective. It is a basic fact of Galois theory in finite fields that Res_{p^m} is surjective. The map $\mathrm{Res} : I_{\mathfrak{P}'} \to I_{\mathfrak{P}}$ is of course induced by the usual restriction $\mathrm{Gal}(F'/K) \twoheadrightarrow \mathrm{Gal}(F/K)$.

Since our choice of $(F', \mathfrak{P}')$ was subject only to the compatibility condition and was arbitrary otherwise, it is sufficient to show that the map $\mathrm{Res} : I_{\mathfrak{P}'} \to I_{\mathfrak{P}}$ is always surjective. Let $\sigma \in I_{\mathfrak{P}} \subseteq \mathrm{Gal}(F/K)$. From basic Galois theory, there exists a $\tau \in \mathrm{Gal}(F'/K)$ such that $\tau|_F = \sigma$. By Theorem 1.1.1, $\tau\mathfrak{P}'$ is a prime of F' lying above $\mathfrak{p}$. Since $\tau|_F = \sigma \in I_{\mathfrak{P}} \subseteq D_{\mathfrak{P}}$, we see that $\tau\mathfrak{P} = \mathfrak{P}$, and hence $\tau\mathfrak{P}'$ lies above $\mathfrak{P}$ as well. By Theorem 1.1.1, there exists $\tau_0 \in \mathrm{Gal}(F'/F)$ so that $\tau_0\tau\mathfrak{P}' = \mathfrak{P}'$. Thus, $\tau_0\tau|_F = \sigma$ and $\tau_0\tau \in D_{\mathfrak{P}'}$. Therefore, we may replace τ by $\tau_0\tau \in D_{\mathfrak{P}'}$. By the commutativity of the above diagram and the exactness of the bottom row, $1 = h(\sigma) = h(\mathrm{Res}(\tau)) = \mathrm{Res}_{p^m}(h'(\tau))$. Thus, $h'(\tau) \in \mathrm{Gal}\left(\mathbb{F}_{p^{mf'}}/\mathbb{F}_{p^{mf}}\right)$ and by the exactness of the top row, there exists $\tau_1 \in D_{\mathfrak{P}'|\mathfrak{P}}$ such that $h'(\tau_1) = h'(\tau)$. Therefore, $\tau_1^{-1}\tau \in I_{\mathfrak{P}'}$ and $\tau_1^{-1}\tau|_F = \sigma$ since $\tau_1^{-1} \in \mathrm{Gal}(F'/F)$. □

1.2 Elliptic Curves

In this section, we review some of the basic definitions and facts concerning elliptic curves. For more details, the reader is referred to [DS05, Kna92, Kob93, Sil86].

1.2.1 Weierstrass Equations

Let K be any field. A *Weierstrass equation* over K is a cubic equation of the form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1.12}$$

where $a_1, a_2, a_3, a_4, a_6 \in K$. It is convenient to define the values

$$\begin{aligned} b_2 &:= a_1^2 + 4a_2, & b_4 &:= a_1a_3 + 2a_4, \\ b_6 &:= a_3^2 + 4a_6, & b_8 &:= a_1^2a_6 - a_1a_3a_4 + a_2a_3^2 + 4a_2a_6 - a_4^2, \\ \Delta &:= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6. \end{aligned} \tag{1.13}$$

The value $\Delta = \Delta(E)$ is called the *discriminant* of the equation E, and the equation is said to be *nonsingular* if $\Delta \neq 0$.

Definition 1.2.1. Let $\overline{K}$ be an algebraic closure of K. If E is a nonsingular Weierstrass equation (1.12), then the set of $(x, y) \in \overline{K} \times \overline{K}$ satisfying (1.12) together with a *point at infinity*, denoted $\mathscr{O}$, is called an **elliptic curve**. The set of K-rational points on E is

$$E(K) := \{(x, y) \in K \times K : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, x\} \cup \{\mathscr{O}\}.$$

Example 1.2.2. Let $K = \mathbb{Q}$ and consider the equation

$$E : y^2 = x^3 + 1. \tag{1.14}$$

The discriminant of the equation is $\Delta = -432$, and hence E defines an elliptic curve.

Given an elliptic curve with Weierstrass equation (1.12), an *admissible change of variables* is an invertible change of variables producing another Weierstrass equation and keeping the point at infinity fixed. The most general admissible change of variables is one of the form

$$x = u^2x' + r, \qquad y = u^3y' + su^2x' + t, \qquad u, r, s, t \in K, u \neq 0. \tag{1.15}$$

Curves with equations related by an admissible change of variables are said to be *isomorphic*. Define the values

$$c_4 := b_2^2 - 24b_4, \qquad c_6 := -b_2^3 + 36b_2b_4 - 216b_6. \tag{1.16}$$

In the case that the characteristic of K is not 2 or 3, we may make the change of variables $(x, y) \mapsto ((x - 3b_2)/36, y/108)$ to equation (1.12) to obtain a Weierstrass equation of the form

$$E : y^2 = x^3 - 27c_4x - 54c_6. \tag{1.17}$$

Calculation of the discriminant yields $\Delta = \frac{c_4^3 - c_6^2}{1728}$. Therefore, in the case that the characteristic of K is not 2 or 3, we can always assume that we have a model for our elliptic curve of the form

$$E_{A,B} : y^2 = x^3 + Ax + B, \qquad A, B \in K. \tag{1.18}$$

The discriminant may be calculated as $\Delta = -16(4A^3 + 27B^2)$.

Remark 1.2.3. The only admissible change of variables preserving this form of equation is

$$x = u^2 x', \qquad y = u^3 y', \qquad u \in K^* \tag{1.19}$$

which has the effect

$$u^4 A' = A, \qquad u^6 B' = B, \qquad u^{12} \Delta' = \Delta. \tag{1.20}$$

1.2.2 The Group Law

We now show how to define an Abelian group operation on $E(K)$ with the point at infinity as the identity element.

Definition 1.2.4 (Group Law)**.** The point at infinity $\mathscr{O}$ is the identity. Given $P = (x_P, y_P) \in E(K)\backslash\{\mathscr{O}\}$, the inverse of P is

$$-P := (x_P, -y_P - a_1 x_P - a_3).$$

Now suppose that $Q = (x_Q, y_Q) \in E(K)\backslash\{\mathscr{O}\}$ and $Q \neq -P$. Define

$$\lambda := \begin{cases} \frac{y_Q - y_P}{x_Q - x_P}, & x_P \neq x_Q, \\ \frac{3x_P^2 + 2a_2 x_P + a_4 - a_1 y_P}{a_1 x_P + a_3 + 2y_P}, & x_P = x_q; \end{cases}$$

$$\mu := \begin{cases} \frac{y_P x_Q - y_Q x_P}{x_Q - x_P}, & x_P \neq x_Q, \\ \frac{-x_P^3 + a_4 x_P + 2a_6 - a_3 y_P}{a_1 x_P + a_3 + 2y_P}, & x_P = x_Q. \end{cases}$$

In addition, define the rational functions

$$r(x_P, y_P, x_Q, y_Q) := \lambda^2 + a_1\lambda - a_2 - x_P - x_Q,$$

$$s(x_P, y_P, x_Q, y_Q) := -(\lambda + a_1) r(x_P, y_P, x_Q, y_Q) - \mu - a_3.$$

If $x_Q = x_P$ and $y_Q = -y_P - a_1 x_P - a_3$, then $P + Q := \mathscr{O}$; otherwise

$$P + Q := (r(x_P, y_P, x_Q, y_Q), s(x_P, y_P, x_Q, y_Q)).$$

It turns out that $P + Q \in E(K)$ and that $E(K)$ is an Abelian group under the operation of $+$. The above definition has a geometric interpretation in terms of chords and tangents. If P and Q are points on the curve, then the line l connecting P and Q must intersect the curve in a third point (counting multiplicities) by Bezout's Theorem [Sil86, p. 55]. If we call this third point R, then $P + Q = -R$. In the case $K = \mathbb{R}$, we can sketch a graph of the curve and depict the addition of two distinct points as in Figure 1.1 on page 13.

Given a point P on E and an integer m, we define multiplication by m to be the result of adding P to itself m times if $m > 0$ and the result of adding $-P$ to itself $-m$ times if $m < 0$. We denote this operation by $[m]P$. In the case $K = \mathbb{R}$, we can depict "doubling" of a point as in Figure 1.2 on page 14.

Definition 1.2.5. The set of m**-torsion points** or m**-division points** of an elliptic curve

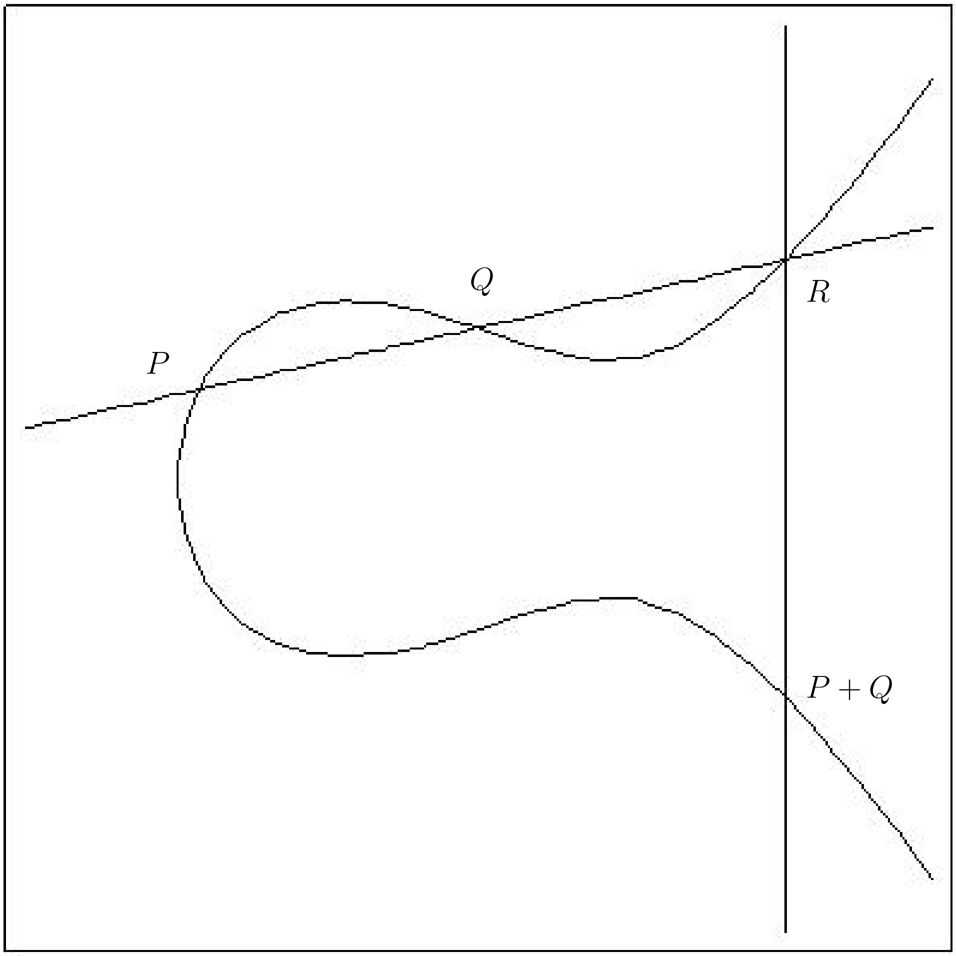

Figure 1.1: Addition of distinct points on an elliptic curve

E is defined to be the set

$$E[m] := \ker[m] = \{P \in E(\overline{K}) : [m]P = \mathscr{O}\}.$$

Remark 1.2.6. Using the group law equations of Definition 1.2.4, for any given $m \in \mathbb{N}$, we can find polynomial equations with coefficients in K for the x and y coordinates of the points in $E[m]\backslash\{\mathscr{O}\}$.

Remark 1.2.7. $E[m]$ is a subgroup of E.

Remark 1.2.8. If we wish to consider only those m-torsion points which are K-rational, we

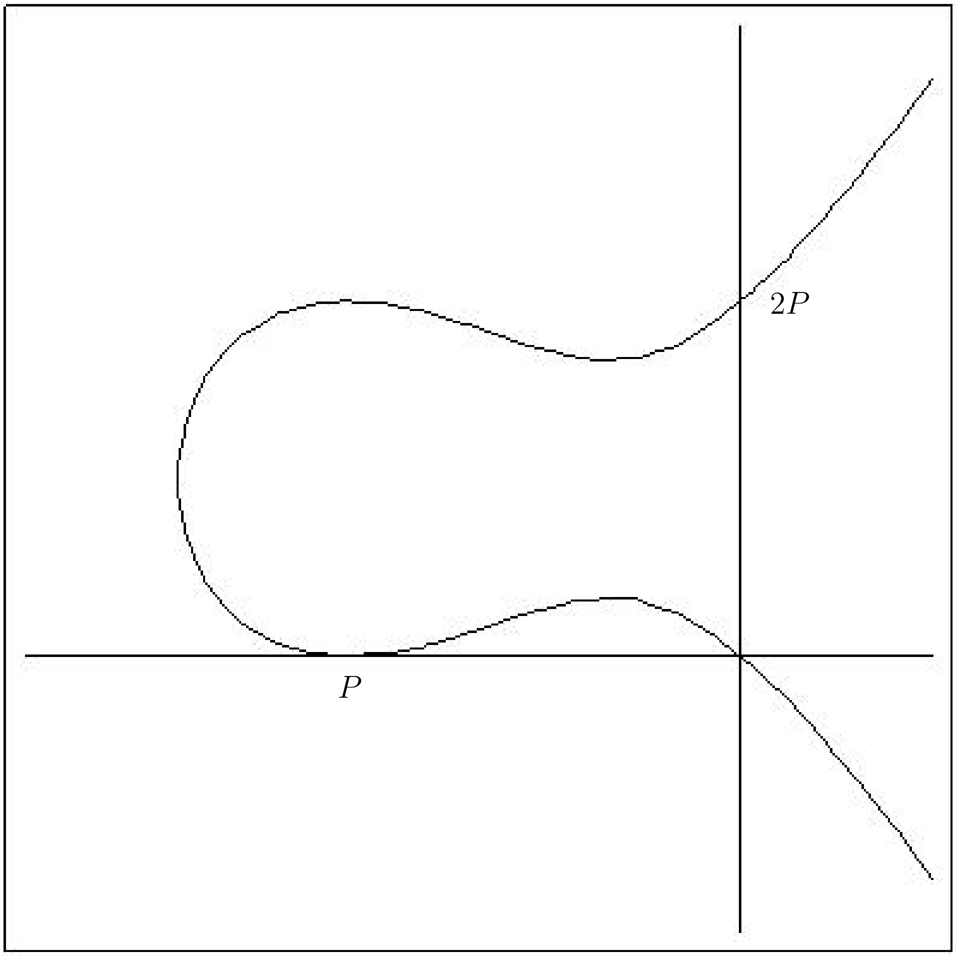

Figure 1.2: Doubling of a point on an elliptic curve

write $E[m](K)$.

Theorem 1.2.9. $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

Definition 1.2.10. Given an elliptic curve E defined over K and an integer m, the **m-division field** of E over K is the field obtained by adjoining to K the x and y coordinates of each point in $E[m]\backslash\{\mathscr{O}\}$. We denote this field by $K(E[m])$.

Remark 1.2.11. Given an elliptic curve E and an integer $m > 0$, it is a simple exercise to write down a recursive formula that produces a polynomial $P_m(x) \in K[x]$ whose roots are precisely the x-coordinates of the points in $E[m]\backslash\{\mathscr{O}\}$. Such a polynomial is called a *division polynomial.* See [Sil86, Exer. 3.7, p. 105] for example. The y-coordinates may then be obtained from the equation for E once the x-coordinates are known.

See [Kob93, Prop. 14, p. 37] for the following fact about the division fields associated to an elliptic curve.

Theorem 1.2.12. *$K(E[m])/K$ is a Galois extension of number fields.*

1.2.3 Elliptic Curves over Finite Fields

If p is a rational prime greater than 3 and f is a positive integer, then any elliptic curve over $\mathbb{F}_{p^f}$ maybe realized as $E_{a,b} : y^2 = x^3 + ax + b$ with $a, b \in \mathbb{F}_{p^f}$. Given a fixed elliptic curve $E_{a,b}$ defined over $\mathbb{F}_{p^f}$, we will often need to count the number of equations of the same form which are isomorphic to $E_{a,b}$. Remark 1.2.3 together with a simple counting argument shows that the number of pairs $(a', b') \in \mathbb{F}_{p^f} \times \mathbb{F}_{p^f}$ with $E_{a',b'} \cong E_{a,b}$ is equal to

$$\begin{cases} \frac{p^f-1}{6}, & a = 0 \text{ and } p^f \equiv 1 \pmod 3 \\ \frac{p^f-1}{4}, & b = 0 \text{ and } p^f \equiv 1 \pmod 4 \\ \frac{p^f-1}{2}, & \text{otherwise.} \end{cases} \tag{1.21}$$

The counting argument relies on the fact $\mathbb{F}_{p^f}$ contains the third roots of unity if and only if $p^f \equiv 1 \pmod 3$ and the fact that $\mathbb{F}_{p^f}$ contains the fourth roots of unity if and only if $p^f \equiv 1 \pmod 4$.

Now suppose that K is a number field. We may always assume that our elliptic curves are given by Weierstrass equations with integral coefficients, that is, coefficients in $\mathcal{O}_K$.

Definition 1.2.13. Let E be an elliptic curve over K and suppose that $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$. A Weierstrass equation for E is said to be **minimal** at $\mathfrak{p}$ if $\text{ord}_{\mathfrak{p}}(\Delta)$ is minimal among all curves isomorphic to E.

Remark 1.2.14. Suppose E is given by $y^2 = x^3 + Ax + B$ and $\mathfrak{p}$ does not contain 6, then we have a simple test for minimality: E is minimal at $\mathfrak{p}$ if and only if $\operatorname{ord}_{\mathfrak{p}}(A) < 4$ and $\operatorname{ord}_{\mathfrak{p}}(B) < 6$. See [Sil86, Remark 1.1, p. 172].

Given an elliptic curve E defined over K, a prime $\mathfrak{p}$, and a minimal Weierstrass equation (1.12) for E at $\mathfrak{p}$, we define the *reduction* of E modulo $\mathfrak{p}$ to be the solution set of

$$E^{\mathfrak{p}} : y^2 + \overline{a_1}xy + \overline{a_3}y = x^3 + \overline{a_2}x^2 + \overline{a_4}x + \overline{a_6} \tag{1.22}$$

over $\mathcal{O}_K/\mathfrak{p}$, where $\overline{a_i}$ denotes the reduction of a_i modulo $\mathfrak{p}$. We of course include the point at infinity in the solution set. If $\mathfrak{p} \nmid \Delta(E)$, then $E^{\mathfrak{p}}$ is nonsingular and hence defines an elliptic curve over the finite field $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_{p^f}$, where $f = f_{\mathfrak{p}|p}$. In this case, we say that E has *good reduction* at $\mathfrak{p}$. Otherwise, we say that E has *bad reduction* at $\mathfrak{p}$.

Throughout this thesis, we will frequently make use of two results about elliptic curves over finite fields. The first is due to Hasse and the second is due to Deuring.

Theorem 1.2.15 (Hasse's bound)**.** *Let E be an elliptic curve defined over $\mathbb{F}_{p^f}$. Then*

$$\left| p^f + 1 - \#E(\mathbb{F}_{p^f}) \right| \leq 2p^{f/2}.$$

Given an elliptic curve E defined over K and a prime $\mathfrak{p}$ lying above the rational prime p, we define

$$a_{\mathfrak{p}}(E) := \mathrm{N}\mathfrak{p} + 1 - \#E^{\mathfrak{p}}(\mathbb{F}_{p^f}), \tag{1.23}$$

where $f = f_{\mathfrak{p}|p} = \deg \mathfrak{p}$. This value is called the *trace of Frobenius* at $\mathfrak{p}$ for reasons we will explain later.

To state Deuring's Theorem, we must first recall some basic facts about binary quadratic forms. For a positive integer D, we denote the set of positive definite binary quadratic forms $Q(x, y) = ax^2 + bxy + cy^2$ of discriminant $-D = b^2 - 4ac$ by $\mathcal{Q}_D$. The set is easily seen to be empty unless $D \equiv 0, 3 \pmod 4$. The group $\Gamma := \mathrm{SL}_2(\mathbb{Z})$ acts on $\mathcal{Q}_D$ via

$$\left(\begin{smallmatrix}\alpha & \beta \\ \gamma & \delta\end{smallmatrix}\right) Q(x,y) := Q(\alpha x+\beta y, \gamma x+\delta y). \tag{1.24}$$

This action induces an equivalence relation on $\mathcal{Q}_D$. If we restrict attention to the forms in $\mathcal{Q}_D/\Gamma$ which are *primitive* (i.e. $(a,b,c)=1$), then we obtain a group called the *form class group* under an operation called *composition*. The number of equivalence classes of primitive forms is called the class number and is denoted by $h(-D)$. The form class group has important implications for class field theory in imaginary quadratic fields. In particular, there is an isomorphism between the form class group of discriminant $-D$ and the ideal class group of the unique imaginary quadratic order of discriminant $-D$. Thus, the class number of the form class group coincides with the *Dirichlet class number*. See [Cox89, Chap. 1] for details.

Definition 1.2.16. The **Kronecker class number** $\tilde{H}(-D)$ is defined by

$$\tilde{H}(-D) = \sum_{\substack{k^2 \mid D \\ \frac{-D}{k^2} \equiv 0,1 \pmod 4}} h\left(\frac{-D}{k^2}\right).$$

The following result, which is typically attributed to Deuring, provides a connection between the Kronecker class number and elliptic curves over finite fields. See [Sch87], [Deu41], or [Len87].

Theorem 1.2.17 (Deuring)**.** *Let p be a prime, f a positive integer, and r an integer. If we let $N_{p^f}(r)$ denote the number of isomorphism classes of elliptic curves over $\mathbb{F}_{p^f}$ with exactly*

p^f+1-r points, then

$$N_{p^f}(r)=\begin{cases}\tilde{H}\left(r^2-4p^f\right), & \textit{if } r^2<4p^f, p\nmid r\\ \tilde{H}(-4p), & \textit{if } r=0, 2\nmid f\\ 1, & \textit{if } r^2=2p^f, p=2, 2\nmid f\\ 1, & \textit{if } r^2=3p^f, p=3, 2\nmid f\\ \frac{1}{12}\left(p+6-4\left(\frac{-3}{p}\right)-3\left(\frac{-4}{p}\right)\right), & \textit{if } r^2=4p^f, 2|f\\ 1-\left(\frac{-3}{p}\right), & \textit{if } r^2=p^f, 2|f\\ 1-\left(\frac{-4}{p}\right), & \textit{if } r=0, 2|f\\ 0, & \textit{otherwise.}\end{cases}$$

Hurwitz defined a quantity related to $\tilde{H}(D)$ called the *Hurwitz class number* .

Definition 1.2.18. The **Hurwitz class number** $H(D)$ is the following weighted count of classes of (not necessarily primitive) binary quadratic forms:

$$H(D):=\sum_{Q\in\mathcal{Q}_D/\Gamma}\frac{2}{|\Gamma_Q|},$$

where Γ_Q denotes the stabilizer of Q in Γ.

Remark 1.2.19. A straightforward calculation yields

$$|\Gamma_Q|=\begin{cases}4, & Q(x,y)=a(x^2+y^2),\\ 6, & Q(x,y)=a(x^2+xy+y^2),\\ 2, & \text{otherwise.}\end{cases}$$

Remark 1.2.20. It is also common to put $H(0):=-1/12$.

We also have an equivalent definition of the Hurwitz class number in terms of Dirichlet class numbers, viz.,

$$H(D) := 2 \sum_{\substack{k^2 \mid D, \\ -D/k^2 \equiv 0,1 \pmod 4}} \frac{h(-D/k^2)}{w(-D/k^2)}, \tag{1.25}$$

where $w(-d)$ denotes the cardinality of the unit group of the imaginary quadratic order of discriminant $-d$. In terms of the Hurwitz class number, we restate Deuring's Theorem as follows.

Corollary 1.2.21. *Let p be a prime, f a positive integer, and r an integer such that $r^2 < 4p^f$. Then the number of isomorphism classes of elliptic curves over $\mathbb{F}_{p^f}$ with exactly $p^f + 1 - r$ points is equal to $H\left(4p^f - r^2\right) + c_{r,p^f}$, where*

$$c_{r,p^f} := \begin{cases} 1/2, & r^2 - 4p^f = -4\alpha^2 \text{ for some } \alpha \in \mathbb{Z}, \\ 2/3, & r^2 - 4p^f = -3\alpha^2 \text{ for some } \alpha \in \mathbb{Z}, \\ 0, & \text{otherwise.} \end{cases}$$

1.2.4 Galois Representations and Elliptic Curves

The details for much of this section in the case that $K = \mathbb{Q}$ are contained in [DS05, Sect. 9.4] and more generally in [Sil86, Sect. III.7]. Let E be an elliptic curve defined over K, and let ℓ be a rational prime. For any $n \in \mathbb{N}$, we have the map

$$E[\ell^{n-1}] \twoheadleftarrow\!\!\xleftarrow{[\ell]} E[\ell^n].$$

Thus, the multiplication by ℓ map on E makes the ℓ-power torsion subgroups of E into an inverse system. The *ℓ-adic Tate module* of E is defined to be the inverse limit:

$$\mathrm{T}_\ell(E) := \varprojlim E[\ell^n]. \tag{1.26}$$

Theorem 1.2.9 may be used to construct an isomorphism $\mathrm{T}_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$, where $\mathbb{Z}_\ell$ denotes the ℓ-adic integers. For each $n \in \mathbb{N}$, the absolute Galois group G_K acts naturally on the points of $E[\ell^n]$ determining an automorphism of the group. This action is compatible with the inverse system of ℓ-power torsion groups, meaning that the diagram

$$\begin{tikzcd}
G_K \arrow[r] \arrow[dr] & \mathrm{Aut}(E[\ell^n]) \cong \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \arrow[d] \\
 & \mathrm{Aut}(E[\ell^{n-1}] \cong \mathrm{GL}_2(\mathbb{Z}/\ell^{n-1}\mathbb{Z}))
\end{tikzcd}$$

commutes for each $n \in \mathbb{N}$. Thus, we obtain an action of G_K on the Tate module, which induces the ℓ-adic representation

$$\rho_{E,\ell} : G_K \longrightarrow \mathrm{Aut}(\mathrm{T}_\ell(E)) \cong \mathrm{GL}_2(\mathbb{Z}_\ell). \tag{1.27}$$

For a general ℓ-adic representation $\rho : G_K \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell)$ and a prime $\mathfrak{p}$ of K, we say that ρ is *unramified* at $\mathfrak{p}$ if $\mathcal{I}_\mathfrak{p} \subseteq \ker \rho$ for every absolute inertia group $\mathcal{I}_\mathfrak{p}$ above $\mathfrak{p}$. Suppose that ρ is unramified at $\mathfrak{p}$. Then the absolute Frobenius elements above $\mathfrak{p}$ are all conjugate to one another. Hence, by elementary considerations from linear algebra, the trace $\mathrm{tr}\rho(\mathrm{Frob}_\mathfrak{p})$ and the determinant $\det \rho(\mathrm{Frob}_\mathfrak{p})$ are well-defined as they do not depend on the choice of $\mathrm{Frob}_\mathfrak{p}$ lying above $\mathfrak{p}$.

The facts contained in the following theorem can be gleaned from [Ser98, Chap. IV, 1.3]. For more explanation in the case $K = \mathbb{Q}$, see also [DS05, Thm. 9.4.1, p. 383].

Theorem 1.2.22. *Let ℓ be a rational prime, and let E be an elliptic curve over K with discriminant $\Delta(E)$. The representation $\rho_{E,\ell}$ is unramified at every prime $\mathfrak{p}$ of K such that $\mathfrak{p} \nmid \ell\Delta(E)$. Furthermore, if* $\mathrm{Frob}_\mathfrak{p}$ *is any absolute Frobenius above $\mathfrak{p}$, then the characteristic equation of $\rho_{E,\ell}(\mathrm{Frob}_p)$ is*

$$x^2 - a_\mathfrak{p}(E)x + \mathrm{N}\mathfrak{p}$$

where $a_{\mathfrak{p}}(E) = \mathrm{N}\mathfrak{p} + 1 - \#E(\mathbb{F}_{p^m})$*,* $m = \deg \mathfrak{p}$*.*

Remark 1.2.23. It is for this reason that the value $a_{\mathfrak{p}}(E)$ defined in Section 1.2.3 is called the trace of Frobenius.

Remark 1.2.24. Note that the coefficients of the characteristic polynomial do not depend on the prime ℓ.

We now combine all the ℓ-adic representations associated to our elliptic curve E to obtain the representation

$$\rho_E : G_K \longrightarrow \prod_{\ell} \mathrm{GL}_2(\mathbb{Z}_\ell),$$

where the product is over all rational primes ℓ. Just as it is natural to study the distribution of primes associated to a fixed conjugacy class in the Galois group of any finite Galois extension of K, it is also natural to study the distribution of primes with a fixed trace of Frobenius under the representation $\rho_{E,\ell}$. Noting that $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \cong \prod_{\ell | m} \mathrm{GL}_2(\mathbb{Z}/\ell^{\mathrm{ord}_\ell(m)}\mathbb{Z})$ by the Chinese Remainder Theorem, we have the following commutative diagram.

$$\begin{tikzcd}
G_K \arrow[r, "\rho_E"] \arrow[d] & \prod_{\ell} \mathrm{GL}_2(\mathbb{Z}_\ell) \arrow[d, "\pi_m"] \\
\mathrm{Gal}(K(E[m])/K) \arrow[r] & \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})
\end{tikzcd} \tag{1.28}$$

Thus, our representation ρ_E of the absolute Galois group G_K induces a representation of $\mathrm{Gal}(K(E[m])/K)$ in $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. Hence, as a corollary of the Chebotarëv Density Theorem (Theorem 1.1.7), we have the following. Given fixed integers a and m, there exists a constant $C_{E,a,m}$ such that

$$\#\{\mathrm{N}\mathfrak{p} \leq x : a_{\mathfrak{p}}(E) \equiv a \pmod{m}\} \sim C_{E,a,m} \frac{x}{\log x}. \tag{1.29}$$

Arguing consistently with the Chebotarëv Density Theorem and the Sato-Tate Conjecture, Lang and Trotter provide heuristics for a refined version of (1.29) in [LT76]. We will not discuss the Sato-Tate Conjecture in detail in this thesis. However, we do note that Richard Taylor has recently announced a proof of the Sato-Tate Conjecture for elliptic curves over totally real number fields which satisfy some very mild conditions [Tay].

Conjecture 1.2.25 (Lang-Trotter Conjecture)**.** *Let E be a fixed elliptic curve defined over $\mathbb{Q}$, and let r be a fixed integer. In the case that $r = 0$, assume further that E does not posses complex multiplication. Define the prime counting function*

$$\pi_E^r(x) := \{p \leq x : a_p(E) = r\}.$$

Then there exists a positive constant $C_{E,r}$ such that

$$\pi_E^r(x) \sim C_{E,r}\frac{\sqrt{x}}{\log x}.$$

Remark 1.2.26. More precisely, Lang and Trotter conjectured that

$$\pi_E^r(x) \sim C_{E,r}\pi_{1/2}(x),$$

where

$$\pi_{1/2}(x) := \int_2^x \frac{dt}{2\sqrt{t}\log t}.$$

However, integration by parts gives

$$\pi_{1/2}(x) = \frac{\sqrt{x}}{\log x} + \int_2^x \frac{dt}{\sqrt{t}(\log t)^2} \sim \frac{\sqrt{x}}{\log x}.$$

In order to precisely state the conjectured form of the constant $C_{E,r}$, we need the following result of Serre, which for elliptic curves defined over $\mathbb{Q}$ defines an integer M_E encoding where the representation ρ_E fails to be surjective. See [Ser72] or [Ser98, Chap. IV, 3.1].

Theorem 1.2.27 (Serre)**.** *For any elliptic curve E defined over K, there exists an integer $M_E \geq 1$ such that*

1. *if $G(M_E)$ denotes the projection of $\rho_E(G_K)$ onto $\prod_{\ell \mid M_E} \mathrm{GL}_2(\mathbb{Z}_\ell)$, then*

$$\rho_E(G_K) = \prod_{\ell \nmid M} \mathrm{GL}_2(\mathbb{Z}_\ell) \times G(M_E).$$

2. *Furthermore,*

$$G(M_E) = \pi_{M_E}^{-1}\left(\tilde{\rho}_{E,M_E}(G_K)\right),$$

where $\tilde{\rho}_{E,m} = \pi_m \circ \rho_E$ and π_m was defined in (1.28)*.*

In terms of the integer M_E, the conjectured form of the constant is

$$\begin{aligned} C_{E,r} &= M_E \frac{\#\left[\tilde{\rho}_{E,M_E}(G_{\mathbb{Q}})\right]_r}{\#\tilde{\rho}_{E,M_E}(G_{\mathbb{Q}})} \prod_{\ell \nmid M_E} \frac{\ell \# \left[\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})\right]_r}{\#\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})} \\ &= M_E \frac{\#\left[\tilde{\rho}_{E,M_E}(G_{\mathbb{Q}})\right]_r}{\#\tilde{\rho}_{E,M_E}(G_{\mathbb{Q}})} \prod_{\substack{\ell \nmid M_E \\ \ell \nmid r}} \frac{\ell(\ell^2 - \ell - 1)}{(\ell+1)(\ell-1)^2} \prod_{\substack{\ell \nmid M_E \\ \ell \mid r}} \frac{\ell^2}{\ell^2 - 1}, \end{aligned} \tag{1.30}$$

where for any ring R and any subgroup H of $\mathrm{GL}_2(R)$, H_r denotes the set of elements of H with trace equal to r. For a general number field K, the heuristics of Lang and Trotter suggest the following conjecture for elliptic curves defined over K.

Conjecture 1.2.28 (Lang-Trotter Conjecture for Number Fields)**.** *Let E be a fixed elliptic curve defined over K, let r be a fixed integer, and let f be a fixed positive integer. Define the prime counting function*

$$\pi_E^{r,f}(x) := \{\mathrm{N}\mathfrak{p} \leq x : \deg \mathfrak{p} = f, a_{\mathfrak{p}}(E) = r\}.$$

Then if $r \neq 0$ or if E does not have complex multiplication, there exists a positive constant $C_{E,r,f}$ such that

$$\pi_E^{r,f}(x) \sim C_{E,r,f} \begin{cases} \frac{\sqrt{x}}{\log x}, & f = 1, \\ \log\log x, & f = 2, \\ 1, & f \geq 3. \end{cases}$$

Chapter 5 will be concerned with showing that this conjecture holds "on average" for the case $f = 1$ under the assumption that $K/\mathbb{Q}$ is Galois.

1.3 Modular Curves and Modular Forms

We now give a quick overview of modular curves and modular forms. For proofs and further detail the reader may consult [Kob93, Miy89, DS05]. For a survey covering many of the ways in which modular forms arise in number theory, see [Ono04] as well.

1.3.1 Definitions and Examples

We begin by recalling the relevant definitions. The **upper half-plane** is defined to be the set of complex numbers with positive imaginary part, and is denoted by $\mathfrak{H}$. The **full modular group** is $\Gamma := \mathrm{SL}_2(\mathbb{Z})$. For a positive integer N, we define the *congruence subgroup* $\Gamma_0(N)$ by $\Gamma_0(N) := \left\{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \pmod N\right\}$.

The full modular group acts on $\mathfrak{H}^* := \mathfrak{H} \cup \mathbb{Q} \cup \{\infty\}$ via Möbius transformations. That is, for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$,

$$z \mapsto \gamma z := \frac{az+b}{cz+d}, \tag{1.31}$$

where we mean that ∞ is mapped to a/c and $-d/c$ is mapped to ∞. The quotient space $\Gamma_0(N)\backslash\mathfrak{H}$ is the set of orbits $\{\Gamma_0(N)z : z \in \mathfrak{H}\}$. A $\Gamma_0(N)$-equivalence class of $\mathbb{Q} \cup \{\infty\}$ is referred to as a **cusp** of $\Gamma_0(N)\backslash\mathfrak{H}$. The extended quotient $\Gamma\backslash\mathfrak{H}^*$ is an example of a **modular curve**, and is denoted by $X_0(N)$.

We are interested in functions which satisfy certain transformation laws under the action of $\Gamma_0(N)$ on $\mathfrak{H}$. Let $f : \mathfrak{H} \to \mathbb{C}$ be holomorphic, and let $k \in \frac{1}{2}\mathbb{Z}$. In the case that k is not integral, we put $z^k := (\sqrt{z})^{2k}$, where $\sqrt{\cdot}$ denotes the principal branch of the square root. We let $\left(\frac{c}{d}\right)$ denote Kronecker's generalization of the Lengendre symbol except that we put $\left(\frac{0}{\pm 1}\right) := 1$. Now, let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. We define the **weight** k **operator** $[\gamma]_k$ by

$$(f[\gamma]_k)(z) = \begin{cases} (cz+d)^{-k} f(\gamma z), & k \in \mathbb{Z}, \\ \left(\frac{c}{d}\right)^{-2k} \left(\frac{-1}{d}\right)^{k} (cz+d)^{-k} f(\gamma z), & k \in \frac{1}{2} + \mathbb{Z}, \end{cases} \tag{1.32}$$

Note that the definition differs depending on whether k is integral or half-integral.

Definition 1.3.1. Let $k \in \frac{1}{2}\mathbb{Z}$, and let χ be a Dirichlet character modulo N, where $4|N$ if k is not integral. A holomorphic function $f : \mathfrak{H} \to \mathbb{C}$ is said to be a **modular form** of weight k and Nebentypus χ for $\Gamma_0(N)$ if

1. $f[\gamma]_k = \chi(d) f$ for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$;

2. $f[\xi]_k$ possesses a Fourier expansion of the form

$$(f[\xi]_k)(z) = \sum_{n=0}^{\infty} a_{\xi,n} q_N^n$$

for all $\xi \in \mathrm{SL}_2(\mathbb{Z})$, where $q_N := e^{\frac{2\pi i z}{N}}$.

If, in addition, $a_{\xi,0} = 0$ for all $\xi \in \mathrm{SL}_2(\mathbb{Z})$, we say that f is a **cusp form**.

Remark 1.3.2. If $s \in \mathbb{Q} \cup \{\infty\}$ represents a cusp of $\Gamma_0(N)\backslash\mathfrak{H}$, then there exists a $\xi \in \mathrm{SL}_2(\mathbb{Z})$ such that $\xi s = \infty$. The Fourier expansion of $f[\xi]_k$ is called the expansion of f at the cusp s. The expansion does not depend on the choice of ξ taking s to ∞.

Remark 1.3.3. In the case that we have a Fourier expansion in q_1, we will write q instead.

Remark 1.3.4. We denote the set of modular forms of weight k and Nebentypus χ for $\Gamma_0(N)$ by $\mathscr{M}_k(N, \chi)$ and the set of cusp forms by $\mathscr{S}_k(N, \chi)$. In the case that $\chi = \chi_0$ is the trivial character modulo N, it is customary to suppress the character.

Example 1.3.5. The classical theta function

$$\theta(z) := \sum_{n \in \mathbb{Z}} q^{n^2} \tag{1.33}$$

is well-known to be a modular form of weight 1/2, level 4, i.e., $\theta(z) \in \mathscr{M}_{1/2}(4)$. See [SS77, p. 32].

Theorem 1.3.6. *$\mathscr{M}_k(N,\chi)$ is a finite dimensional complex vector space and $\mathscr{S}_k(N,\chi)$ is a subspace.*

Remark 1.3.7. It is easy to show that if k is an integer, then $\mathscr{M}_k(N,\chi) = \{0\}$ unless k and χ have the same parity, i.e., $\chi(-1) = (-1)^k$. Similarly, one shows that if k is a half-integer, then χ must be even.

Definition 1.3.8. We define the **Eisenstein subspace** $\mathscr{E}_k(N,\chi)$ to be the complement of the subspace of cusp forms. That is, we write

$$\mathscr{M}_k(N,\chi) = \mathscr{E}_k(N,\chi) \oplus \mathscr{S}_k(N,\chi).$$

An element of the Eisenstein subspace is called an **Eisenstein series**.

1.3.2 Computations with Modular Forms and the Construction of Eisenstein Series

A remarkable fact about modular forms is that one only needs to compute a finite number of Fourier coefficients in order to uniquely determine a form given that one knows its level and weight. The following is implied by [Fre94, Prop. 1.1].

Theorem 1.3.9. *Suppose that $f(z) = \sum_{n\geq 0} a_n q^n, g(z) = \sum_{n\geq 0} b_n q^n \in \mathscr{M}_k(N,\chi)$ Further, suppose that $a_n = b_n$ for $0 \leq n \leq \frac{kN}{12}\prod_{p|N}\left(1+\frac{1}{p}\right)$. Then $f = g$.*

We now show how to construct integer weight Eisenstein series as in [Miy89, pp. 176-177]. Let χ be any Dirichlet character of conductor m. The *generalized Bernoulli numbers* associated to χ are denoted by $B_{n,\chi}$ and defined by the identity

$$\sum_{a=1}^{m} \frac{\chi(a)te^{at}}{e^{mt}-1} = \sum_{n=0}^{\infty} \frac{B_{n,\chi}}{n!}t^n.$$

Throughout this thesis χ_0 will always denote a trivial character unless otherwise noted. Now, let k be an integer, and let χ_1 and χ_2 be Dirichlet characters modulo M_1 and M_2 respectively. Put $\chi = \chi_1\chi_2$ and $M = M_1M_2$. Assume that χ and k have the same parity, i.e, $\chi(-1) = (-1)^k$. In addition, assume that χ_1 and χ_2 satisfy the following:

1. if $k = 2$ and both χ_1 and χ_2 are trivial, then $M_1 = 1$ and M_2 is prime;
2. otherwise, χ_1 and χ_2 are primitive.

Theorem 1.3.10. *Let $E_k(z; \chi_1, \chi_2) := \sum_{n\geq 0} a_n q^n$, where*

$$a_0 = \begin{cases} 0, & k \neq 1, \chi_1 \neq \chi_0 \text{ or } \chi_1 \neq \chi_0, \chi_2 \neq \chi_0, \\ \frac{M-1}{24}, & k = 2, \chi_1 = \chi_2 = \chi_0, \\ -B_{k,\chi}/2k, & \text{otherwise}; \end{cases}$$

$$a_n = \sum_{0<d|n} \chi_1(n/d)\chi_2(d)d^{k-1}$$

for $n \geq 1$. Then $E_k(z; \chi_1, \chi_2) \in \mathscr{E}_k(M, \chi)$.

Example 1.3.11. Let $\left(\frac{\cdot}{3}\right)$ denote the Legendre symbol modulo 3. Then

$$\begin{aligned} E_2\left(z; \left(\frac{\cdot}{3}\right), \left(\frac{\cdot}{3}\right)\right) &= \sum_{n\geq 1}\left(\sum_{d|n}\left(\frac{n}{3}\right)d\right)q^n = \sum_{n\geq 1}\left(\frac{n}{3}\right)\sigma(n)q^n \\ &= q - 3q^2 + 7q^4 - 6q^5 + 8q^7 - 15q^8 + \ldots \end{aligned}$$

is a weight 2 modular form of level 9 and trivial character.

Given a level N, weight k, and character χ, one may construct a basis for $\mathscr{E}_k(N, \chi)$ entirely from the Eisenstein series of Theorem 1.3.10. In particular, we have

$$\mathscr{E}_k(N, \chi) = \langle E_k(lz; \chi_1, \chi_2) : lM_1M_2|N,\ \chi_1\chi_2 = \chi\rangle_{\mathbb{C}}$$

See [Miy89, (4.7.17), p. 179].

One may also consider half-integral weight Eisenstein series as in [Kob93, Chap. IV] or so-called Cohen-Eisenstein series as constructed in [Coh75]. We shall not need these series in this thesis except that we note that Cohen's construction for case of weight 3/2 fails to produce a modular form [Coh75, p. 274]. Rather it produces a very special form, whose Fourier coefficients are Hurwitz class numbers:

$$\mathscr{H}(z) := \sum_{N\geq 0} H(N)q^N + \frac{1}{16\pi\sqrt{y}} \sum_{f=-\infty}^{\infty} \alpha(f^2 y)q^{-f^2}, \tag{1.34}$$

where $y = \Im(z)$ and $\alpha(t) = \int_1^\infty e^{-4\pi u t} u^{-3/2} du$. The same form also appears in the work of Hirzebruch and Zagier in [HZ76], where it is proved that the form still transforms like a a modular form of weight 3/2. In fact, it is an example of a *Maass form.* A stronger version of the following proposition appears without proof in [Coh75, Cor. 3.4]. However, we have only been able to supply proof for the form presented here.

Proposition 1.3.12. *If $-b$ is a quadratic non-residue modulo a, then*

$$\mathscr{H}_1(z; a, b) := \sum_{N\equiv b \pmod a} H(N)q^N \in \mathscr{M}_{3/2}(G_a),$$

where

$$G_a = \left\{ \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \Gamma_0(A) : \alpha^2 \equiv 1 \pmod a \right\},$$

and we take $A = a^2$ if $4|a$ and $A = 4a^2$ otherwise.

1.3.3 Cusp Forms and Elliptic Curves

Thanks to work of Breuil, Conrad, Diamond, Taylor and Wiles [Wil95, TW95, BCDT01], we know that elliptic curves defined over $\mathbb{Q}$ are strongly connected to modular forms through their associated L-series. To fully state the Modularity Theorem, we would need to define the conductor of an elliptic curve. Suffice it to say that the conductor of an elliptic curve E is a certain integral ideal of K (or in the case $K = \mathbb{Q}$, a positive integer) which measures the complexity of the curve. In particular, it encodes information about the places of bad reduction and the type of bad reduction. For a precise definition of the conductor, please see [Sil94, Chap. IV, §10]. Given an elliptic curve E defined over $\mathbb{Q}$, recall the values $a_p(E)$ defined via equation (1.23). In [DS05, Thm. 8.8.1, p. 356], we find the following statement of the Modularity Theorem.

Theorem 1.3.13 (Modularity Theorem)**.** *Let E be an elliptic curve over $\mathbb{Q}$ with conductor N_E. Then there exists some newform $f(z) = \sum_{n\geq 1} a_n(f)q^n \in \mathscr{S}_2(N_E)$, such that $a_p(f) = a_p(E)$ for all primes p.*

Example 1.3.14. Consider the elliptic curve $E : y^2 = x^3 + 1$. The series

$$f_E(z) := \sum_{n\geq 1} a_n(E)q^n = q - 4q^7 + 2q^{13} + 8q^{19} - 5q^{25} - 4q^{31} + \dots \tag{1.35}$$

is a cusp form of weight 2, level 36, and trivial character. This curve is rather unusual in that we can write down a reasonably simply formula for the coefficients. As a consequence of [IR90, Thm. 4, p. 305], for a prime p, we have

$$a_p(E) = \begin{cases} 0, & p = 2, 3, \text{ or } p \equiv 2 \pmod 3, \\ 2\Re\left(\left(\frac{2}{\pi}\right)_3 \pi\right), & p \equiv 1 \pmod 3, \end{cases} \tag{1.36}$$

where $\left(\frac{\cdot}{\pi}\right)_3$ is the third power residue symbol, π is either *primary* prime factor of p in the principal ideal domain $\mathbb{Z}[\zeta_3]$ and ζ_3 is a primitive third root of unity. A prime element $\pi = a + b\zeta_3$ of $\mathbb{Z}[\zeta_3]$ is said to be primary if $\pi \equiv 2 \pmod{3\mathbb{Z}[\zeta_3]}$. See [IR90, p. 113].

1.3.4 Hecke Operators and the Eichler-Selberg Trace Formula

Hecke operators are linear transformations acting on spaces of modular forms. The definition differs slightly between the integer and half-integer weight case. In this thesis, we will only need the definition for the integer weight case. Other natural definitions for Hecke operators exists aside from the one we present here. See [Kob93, Chap. 3] for example.

Definition 1.3.15. Let k and N be positive integers, and let χ be a Dirichlet character modulo N. Let $f(z) = \sum_{n\geq 0} a_n q^n \in \mathscr{M}_k(\Gamma_0(N), \chi)$. For each rational prime p, the action of the p-th Hecke operator, $T_{p,k,\chi}$, on $f(z)$ is defined by

$$f(z)|T_{p,k,\chi} := \sum_{n\geq 0}(a_{pn} + \chi(p)p^{k-1}a_{n/p})q^n,$$

where we apply the convention that $a_{n/p} = 0$ if $p \nmid n$. For a general positive integer m, the action of the m-th Hecke operator is defined by

$$f(z)|T_{m,k,\chi} := \sum_{n\geq 0}\left(\sum_{d|(m,n)} \chi(d)d^{k-1}a_{mn/d^2}\right) q^n.$$

Remark 1.3.16. In the case that χ is trivial, we suppress the character on the Hecke operator and simply write $T_{m,k}$.

Remark 1.3.17. If $f(z)$ is a cusp form, then it turns out that $f(z)|T_{m,k,\chi}$ is as well.

The Eichler-Selberg Trace Formula gives the value of the trace of the n-th Hecke operator acting on the space $\mathscr{S}_k(N, \chi)$. We give Hijikata's statement as found in [HPS89, pp. 12-13].

Theorem 1.3.18 (Eichler-Selberg Trace Formula)**.** *Let k be an integer greater than or equal to 2. Let ψ be a character modulo N, and assume that $(-1)^k\psi(-1) = 1$. Decompose ψ as $\psi = \prod_{\ell|N}\psi_\ell$, where for each prime ℓ dividing N, ψ_ℓ is a character modulo ℓ^{ν_ℓ} and $\nu_\ell = \mathrm{ord}_\ell(N)$. Then for $(n, N) = 1$, the trace of $T_{n,k,\psi}$ acting on $\mathscr{S}_k(N, \psi)$ is given by*

$$\mathrm{tr}_{N,\psi}T_{n,k,\psi} = \delta(\psi)\deg T_{n,k,\psi} + \delta(\sqrt{n})\left[\frac{k-1}{12}N\prod_{\ell|N}\left(1+\frac{1}{\ell}\right) - \frac{\sqrt{n}}{2}\prod_{\ell|N}\mathrm{par}(\ell)\right]$$
$$- \sum_s a(s)\sum_f b(s,f)\prod_{\ell|N}c_\psi(s,f,\ell),$$

where

$$\delta(\psi) := \begin{cases} 1, & k = 2, \psi = \chi_0 \\ 0, & \textit{otherwise}; \end{cases}$$

$$\delta(\sqrt{n}) := \begin{cases} n^{k/2-1}\psi(\sqrt{n}), & \textit{if } n \textit{ is a perfect square,} \\ 0, & \textit{otherwise}; \end{cases}$$

$$\mathrm{par}(\ell) := \begin{cases} 2\ell^{\nu_\ell - e_\ell}, & e_\ell \geq \rho_\ell + 1 \\ \ell^{\rho_\ell} + \ell^{\rho_\ell - 1}, & e_\ell \leq \rho_\ell \textit{ and } \nu_\ell \textit{ is even,} \\ 2\ell^{\rho_\ell}, & e_\ell \leq \rho_\ell \textit{ and } \nu_\ell \textit{ is odd.} \end{cases}$$

Here for a fixed $\ell | N$, $\rho_\ell = \left\lfloor \frac{\nu_\ell}{2} \right\rfloor$ *and* $e_\ell = e(\psi_\ell)$ *is the exponential conductor of* ψ_ℓ. *The meaning of* $s, a(s), b(s,f)$, *and* $c_\psi(s,f,\ell)$ *are given as follows.*

The index s *runs over all integers in the three following sets:*

$$\begin{aligned} H &:= \{s : s^2 - 4n = t^2\}, \\ E_1 &:= \{s : s^2 - 4n = t^2 m, m \textit{ squarefree and } 0 > m \equiv 1 \pmod 4\}, \\ E_2 &:= \{s : s^2 - 4n = t^2 4m, m \textit{ squarefree and } 0 > m \equiv 2, 3 \pmod 4\}. \end{aligned}$$

Let $\Phi_s(X) := X^2 - sX + n$ *with roots* x *and* y *in* $\mathbb{C}$. *Put*

$$a(s) := \begin{cases} \min\{|x|, |y|\}^{k-1} |x-y|^{-1} \mathrm{sgn}(x)^k, & s \in H, \\ \frac{x^{k-1} - y^{k-1}}{2(x-y)}, & s \in E_1 \cup E_2. \end{cases}$$

For each fixed s, *let* f *run over the positive divisors of* t, *and let*

$$b(s,f) := \begin{cases} \frac{1}{2}\varphi((s^2-4n)^{1/2}/f), & s \in H, \\ 2\frac{h((s^2-4n)^{1/2}/f^2)}{w((s^2-4n)/f^2)}, & s \in E_1 \cup E_2, \end{cases}$$

where φ is Euler's totient function and $h(d)$ is the class number of the order of $\mathbb{Q}(\sqrt{d})$ of discriminant d and $w(d)$ is the cardinality of its unit group.

For a pair (s,f) fixed and a prime divisor ℓ of N, let $b_\ell = \operatorname{ord}_\ell(f)$, and put $\tilde{A} := \{x \in \mathbb{Z} : \Phi_s(x) \equiv 0 \pmod{\ell^{\nu_\ell+2b_e}}, 2x \equiv s \pmod{\ell_\ell^b}\}$ and $\tilde{B} := \{x \in \tilde{A} : \Phi_s(x) \equiv 0 \pmod{\ell^{\nu_\ell+2b_\ell+1}}\}$. Let $A(s,f,\ell)$ (resp. $B(s,f,\ell)$ be a complete set of representatives for $\tilde{A}$ (resp. $\tilde{B}$) modulo $\ell^{\nu_\ell+b_\ell}$, and let $B'(s,f,\ell) := \{s - z : z \in B(s,f,\ell)\}$. Then

$$c_\psi(s,f,\ell) := \begin{cases} \displaystyle\sum_{x\in A(s,f,\ell)} \psi_\ell(x), & (s^2-4n)/f^2 \not\equiv 0 \pmod{\ell}, \\ \displaystyle\sum_{x\in A(s,f,\ell)} \psi_\ell(x) + \sum_{y\in B'(s,f,\ell)} \psi_\ell(y), & (s^2-4n)/f^2 \equiv 0 \pmod{\ell}. \end{cases}$$

In Chapter 2, we will show how the trace formula may be used to derive Hurwitz class number identities.

1.4 Organization of the Thesis

The remainder of the thesis is organized as follows. In Chapter 2, we prove identities of a certain type for the Hurwitz class number. In Chapter 3, we construct elements of finite fields of high multiplicative order using explicit equations for modular curves. In Chapter 4, we prove an upper bound and an asymptotic formula for the mean square error in the Chebotarëv Density Theorem when averaging over cyclotomic extensions of a fixed number field. In Chapter 5, we prove that the Lang-Trotter Conjecture for elliptic curves defined over Galois number fields holds "on average." Finally, in Chapter 6, we discuss directions for future work.

Chapter 2

Elliptic Curves, Modular Forms, and Sums of Hurwitz Class Numbers

This chapter concerns the proof of several identities for the Hurwitz class number. The results presented here originally appeared as [BCF^{+}08].

2.1 Statement of Theorems

We begin by restating the definition of the Hurwitz class number in a slightly different form. The reader will note that the following entirely agrees with Definition 1.2.18.

Definition 2.1.1. For an integer $N \geq 0$, the Hurwitz class number $H(N)$ is defined as follows. $H(0) = -1/12$. If $N \equiv 1$ or $2 \pmod 4$, then $H(N) = 0$. Otherwise, $H(N)$ is the number of classes of not necessarily primitive positive definite quadratic forms of discriminant $-N$, except that those classes which have a representative which is a multiple of the form x^2+y^2 should be counted with weight $1/2$ and those which have a representative which is a multiple of the form $x^2 + xy + y^2$ should be counted with weight $1/3$.

Several nice identities are known for sums of Hurwitz class numbers. For example, it is known that if p is a prime, then

$$\sum_{|r|<2\sqrt{p}} H(4p-r^2) = 2p, \tag{2.1}$$

where the sum is over integers r (both positive, negative, and zero). See for example [Cox89, p. 322] or [Eic55, p. 154].

In this paper, we investigate the behavior of this sum with additional condition $r \equiv c \pmod{m}$. In particular, if we split the sum according to the parity of r, then we have the following.

Theorem 2.1.2. *If p is an odd prime, then*

$$\sum_{\substack{|r|<2\sqrt{p}, \\ r\equiv c \pmod 2}} H(4p-r^2) = \begin{cases} \frac{4p-2}{3}, & \text{if } c=0, \\ \frac{2p+2}{3}, & \text{if } c=1. \end{cases}$$

Once we have the above result, we use the ideas contained within its proof to quickly prove the next.

Theorem 2.1.3. *If p is an odd prime,*

$$\sum_{\substack{|r|<2\sqrt{p}, \\ r\equiv c \pmod 4}} H(4p-r^2) = \begin{cases} \frac{p+1}{3}, & c \equiv \pm 1 \pmod 4, \\ \frac{5p-7}{6}, & c \equiv p+1 \pmod 4, \\ \frac{p+1}{2}, & c \equiv p-1 \pmod 4. \end{cases}$$

We also fully characterize the case $m=3$ by proving the following formulae.

Theorem 2.1.4. *If p is prime, then*

$$\sum_{\substack{|r|<2\sqrt{p},\\ r\equiv c \pmod 3}} H(4p-r^2) = \begin{cases} \frac{p+1}{2}, & \textit{if } c\equiv 0 \pmod 3,\ p\equiv 1 \pmod 3,\\ p-1, & \textit{if } c\equiv 0 \pmod 3,\ p\equiv 2 \pmod 3,\\ \frac{3p-1}{4}, & \textit{if } c\equiv \pm 1 \pmod 3,\ p\equiv 1 \pmod 3,\\ \frac{p+1}{2}, & \textit{if } c\equiv \pm 1 \pmod 3,\ p\equiv 2 \pmod 3. \end{cases}$$

We also have a partial characterization for the sum split according to the value of r modulo 5.

Theorem 2.1.5. *If p is prime, then*

$$\sum_{\substack{|r|<2\sqrt{p},\\ r\equiv c \pmod 5}} H(4p-r^2) = \begin{cases} \frac{p-1}{2}, & \textit{if } c\equiv \pm(p+1) \pmod 5,\ p\equiv \pm 2 \pmod 5,\\ \frac{p-3}{2}, & \textit{if } c\equiv 0 \pmod 5,\ p\equiv 4 \pmod 5. \end{cases}$$

All of the above theorems may be proven by exploiting the relationship between Hurwitz class numbers and elliptic curves over finite fields. In Section 2.2, we will state this relationship and show how it is used to prove Theorem 2.1.2. We will then briefly sketch how to use the same method for the proof of Theorem 2.1.3 as well as several cases of Theorem 2.1.7 below.

In Section 2.3, we will use a result about the modularity of certain "partial" generating functions for the Hurwitz class number to prove Theorem 2.1.4. The interesting thing about this method is that it leads to a far more general result than what is obtainable by the method of Section 2.2. Out of this result, it is possible to extract a version of Theorem 2.1.4 for p not necessarily prime as well as the following.

Theorem 2.1.6. *If $(n,6)=1$ and there exists a prime $p\equiv 2 \pmod 3$ such that $ord_p(n)\equiv 1 \pmod 2$, then*

$$\sum_{\substack{|r|<\sqrt{n},\\ r\equiv c_n \pmod 3}} H(n-r^2) = \frac{\sigma(n)}{12},$$

where we take $c_n = 0$ if $n \equiv 1 \pmod 3$, and $c_n = 1$ or 2 if $n \equiv 2 \pmod 3$.

A third method of proof will be discussed in Section 2.4, which uses the Eichler-Selberg Trace Formula. See Theorem 1.3.18 of Chapter 1. This method will allow us to prove the cases of the following result that remain unproven at the end of Section 2.2.

Theorem 2.1.7. *If p is prime, then*

$$\sum_{\substack{|r|<2\sqrt{p},\\ r\equiv c \pmod 7}} H(4p-r^2) = \begin{cases} \frac{p+1}{3}, & c \equiv 0 \pmod 7,\ p \equiv 3,5 \pmod 7, \\ \frac{p-5}{3}, & c \equiv 0 \pmod 7,\ p \equiv 6 \pmod 7, \\ \frac{p-2}{3}, & c \equiv \pm(p+1) \pmod 7,\ p \equiv 2,3,4,5 \pmod 7, \\ \frac{p+1}{3}, & c \equiv \pm 2 \pmod 7,\ p \equiv 6 \pmod 7. \end{cases}$$

Finally, in Section 2.5, we list several conjectures, which are strongly supported by computational evidence. We also give a few partial results and discuss strategies for future work.

2.2 Elliptic Curves and Hurwitz Class Numbers

The proofs we give in this section are combinatorial in nature and depend on the corollary of Deuring's Theorem on page 19. For convenience, we restate the corollary for the case of elliptic curves over prime finite fields.

Corollary 2.2.1. *For $|r| < 2\sqrt{p}$, the number of isomorphism classes of elliptic curves over $\mathbb{F}_p$ with exactly $p+1-r$ points is given by $H(4p-r^2) + c_{r,p}$, where*

$$c_{r,p} = \begin{cases} 1/2, & \textit{if } \ r^2-4p = -4\alpha^2 \textit{ for some } \alpha \in \mathbb{Z}, \\ 2/3, & \textit{if } \ r^2-4p = -3\alpha^2 \textit{ for some } \alpha \in \mathbb{Z}, \\ 0, & \textit{otherwise.} \end{cases} \tag{2.2}$$

Thus, the number of isomorphism classes of elliptic curves $E/\mathbb{F}_p$ such that $m|\#E(\mathbb{F}_p)$ is equal to

$$\sum_{\substack{|r|<2\sqrt{p} \\ r\equiv p+1 \pmod{m}}} \left(H(4p-r^2)+c_{r,p}\right). \tag{2.3}$$

This is the main fact that we will exploit in this section. Another useful fact that we will exploit throughout the paper is the symmetry of our sums. In particular,

$$\sum_{\substack{|r|<2\sqrt{p} \\ r\equiv c \pmod{m}}} H(4p-r^2) = \sum_{\substack{|r|<2\sqrt{p} \\ r\equiv -c \pmod{m}}} H(4p-r^2). \tag{2.4}$$

Proof of Theorem 2.1.2. For $p=3$, the identities may be checked by direct calculation. For the remainder of the proof, we will assume p is prime and strictly greater than 3.

Let $N_{2,p}$ denote the number of isomorphism classes of elliptic curves over $\mathbb{F}_p$ possessing 2-torsion, and recall that E has 2-torsion if and only if $2|(p+1-r)$. Thus,

$$N_{2,p} = \sum_{\substack{|r|<2\sqrt{p} \\ r\equiv p+1 \pmod{2}}} \left(H(4p-r^2)+c_{r,p}\right). \tag{2.5}$$

We will proceed by computing $N_{2,p}$, the number of isomorphism classes of elliptic curves possessing 2-torsion over $\mathbb{F}_p$. Then, we will compute the correction term, $\sum c_{r,p}$. In light of (2.1) and (2.5), Theorem 2.1.2 will follow.

We first recall the relevant background concerning elliptic curves with 2-torsion over $\mathbb{F}_p$. The reader is referred to [Kna92] or [Sil86] for more details. If E is an elliptic curve with 2-torsion then, we can move a point of order 2 to the origin in order to obtain a model for E of the form

$$E_{b,c}: y^2 = x^3+bx^2+cx. \tag{2.6}$$

The discriminant of such a curve is given by

$$\Delta = 16c^2(b^2-4c). \tag{2.7}$$

We will omit from consideration those pairs (b, c) for which the resulting curve has zero discriminant since these curves are singular.

Following [Sil86, pp. 46-48], we take $c_4 = 16(b^2 - 3c)$ and $c_6 = 32b(9c - 2b^2)$. Then since $\mathrm{char}(\mathbb{F}_p) \neq 2, 3$, $E_{b,c}$ is isomorphic to the curve

$$E' : y^2 = x^3 - 27c_4x - 54c_6. \tag{2.8}$$

The curves in this form that are isomorphic to (2.8) are

$$y^2 = x^3 - 27u^4c_4x - 54u^6c_6,\ u \neq 0. \tag{2.9}$$

Thus, given any elliptic curve, the number of $(A, B) \in \mathbb{F}_p^2$ for which the given curve is isomorphic to $E : y^2 = x^3 + Ax + B$ is

$$\begin{cases} \frac{p-1}{6}, & \text{if } A = 0 \text{ and } p \equiv 1 \pmod 3, \\ \frac{p-1}{4}, & \text{if } B = 0 \text{ and } p \equiv 1 \pmod 4, \\ \frac{p-1}{2}, & \text{otherwise.} \end{cases}$$

We are interested in how many curves $E_{b,c}$ give the same c_4 and c_6 coefficients. Given an elliptic curve $E : y^2 = x^3 + Ax + B$ with 2-torsion over $\mathbb{F}_p$, each choice of an order 2 point to be moved to the origin yields a different model $E_{b,c}$. Thus, the number of $E_{b,c}$ which have the same c_4 and c_6 coefficients is equal to the number of order 2 points possessed by the curves. This is either 1 or 3 depending on whether the curves have full or cyclic 2-torsion.

Thus, the number of (b, c) for which $E_{b,c}$ is isomorphic to a given curve is

$$\begin{cases} \frac{p-1}{6}, & c_4 = 0,\ p \equiv 1 \pmod 3 \text{ and 2-torsion is cyclic,} \\ \frac{p-1}{4}, & c_6 = 0,\ p \equiv 1 \pmod 4 \text{ and 2-torsion is cyclic,} \\ \frac{p-1}{2}, & \text{otherwise with cyclic 2-torsion,} \\ \frac{p-1}{2}, & c_4 = 0,\ p \equiv 1 \pmod 3 \text{ and 2-torsion is full,} \\ \frac{3(p-1)}{4}, & c_6 = 0,\ p \equiv 1 \pmod 4 \text{ and 2-torsion is full,} \\ \frac{3(p-1)}{2}, & \text{otherwise with full 2-torsion.} \end{cases} \tag{2.10}$$

The proof of Theorem 2.1.2 will follow immediately from the following two propositions.

Proposition 2.2.2. *If $p > 3$ is prime, then the number of isomorphism classes of elliptic curves possessing 2-torsion over $\mathbb{F}_p$ is given by*

$$N_{2,p} = \begin{cases} \frac{4p+8}{3}, & \text{if } p \equiv 1 \pmod{12}, \\ \frac{4p+4}{3}, & \text{if } p \equiv 5 \pmod{12}, \\ \frac{4p+2}{3}, & \text{if } p \equiv 7 \pmod{12}, \\ \frac{4p-2}{3}, & \text{if } p \equiv 11 \pmod{12}. \end{cases}$$

Proof. In view of (2.10), we want to count the number of curves $E_{b,c}$ that fall into each of six categories. Let A_1 denote the number of curves with cyclic 2-torsion and $c_4 = 0$, A_2 denote the number of curves with cyclic 2-torsion and $c_6 = 0$, A_3 denote the number of curves with cyclic 2-torsion and $c_4c_6 \neq 0$, A_4 denote the number of curves with full 2-torsion and $c_4 = 0$, A_5 denote the number of curves with full 2-torsion and $c_6 = 0$ and A_6 denote the number of curves with $c_4c_6 \neq 0$. Then $N_{2,p}$ can be computed by determining A_i for $i = 1, \ldots, 6$ and applying (2.10).

Now, an elliptic curve $E_{b,c}$ has full 2-torsion if and only if $b^2 - 4c$ is a square modulo

p. Thus, the number of curves possessing full 2-torsion over $\mathbb{F}_p$ is given by

$$\sum_{\substack{b=0,\\ b^2\neq 4c}}^{p-1} \sum_{c=1}^{p-1} \frac{1}{2}\left[\left(\frac{b^2-4c}{p}\right)+1\right] = \frac{(p-1)(p-2)}{2}, \tag{2.11}$$

and the number of curves possessing cyclic 2-torsion over $\mathbb{F}_p$ is given by

$$\sum_{\substack{b=0,\\ b^2\neq 4c}}^{p-1} \sum_{c=1}^{p-1} -\frac{1}{2}\left[\left(\frac{b^2-4c}{p}\right)-1\right] = \frac{p(p-1)}{2}. \tag{2.12}$$

Note that if $c_4 = 0$, then $b^2 \equiv 3c \pmod{p}$ and hence $\left(\frac{c}{p}\right) = \left(\frac{3}{p}\right)$. Thus, there are $p-1$ nonsingular curves (2.6) that give $c_4 = 0$. If a nonsingular curve $E_{b,c}$ possesses full 2-torsion and $c_4 = 0$, then $1 = \left(\frac{b^2-4c}{p}\right) = \left(\frac{-c}{p}\right) = \left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$. Thus, when $p \equiv 1 \pmod{3}$, all $p-1$ nonsingular curves $E_{b,c}$ with $c_4 = 0$ will have full 2-torsion, and when $p \equiv 2 \pmod{3}$, all will have cyclic 2-torsion. Thus,

$$\begin{aligned} A_1 &= \begin{cases} 0, & p \equiv 1 \pmod{3}, \\ p-1, & p \equiv 2 \pmod{3}, \end{cases} \\ A_4 &= \begin{cases} p-1, & p \equiv 1 \pmod{3}, \\ 0, & p \equiv 2 \pmod{3}. \end{cases} \end{aligned}$$

Similar computations lead to

$$\begin{aligned} A_2 &= \frac{p-1}{2}, \\ A_5 &= \frac{3(p-1)}{2}. \end{aligned}$$

Finally, using (2.11) and (2.12), we see that

$$\begin{aligned} A_3 &= \begin{cases} \frac{(p-1)^2}{2}, & p \equiv 1 \pmod 3, \\ \frac{(p-3)(p-1)}{2}, & p \equiv 2 \pmod 3, \end{cases} \\ A_6 &= \begin{cases} \frac{(p-1)(p-7)}{2}, & p \equiv 1 \pmod 3, \\ \frac{(p-1)(p-5)}{2}, & p \equiv 2 \pmod 3. \end{cases} \end{aligned}$$

Combining these with (2.10), the result follows. □

We now compute the correction term in (2.5).

Proposition 2.2.3. *The value of the correction term is given by*

$$\sum_{\substack{|r|<2\sqrt{p}, \\ r \equiv 0 \pmod 2}} c_{r,p} = \begin{cases} 10/3, & p \equiv 1 \pmod{12}, \\ 2, & p \equiv 5 \pmod{12}, \\ 4/3, & p \equiv 7 \pmod{12}, \\ 0, & p \equiv 11 \pmod{12}. \end{cases}$$

Proof. By (2.2), we see that each form proportional to $x^2 + xy + y^2$ contributes 2/3 to the sum while each form proportional to $x^2 + y^2$ contributes 1/2.

Forms proportional to $x^2 + xy + y^2$ arise for those $r \equiv 0 \pmod 2$ for which there exists $\alpha \in \mathbb{Z}\backslash\{0\}$ such that $r^2 - 4p = -3\alpha^2$. Thus, $p = \left(\frac{r+\alpha i\sqrt{3}}{2}\right)\left(\frac{r-\alpha i\sqrt{3}}{2}\right)$. Recall that p factors in $\mathbb{Z}\left[\frac{1+i\sqrt{3}}{2}\right]$ if and only if $p \equiv 1 \pmod 3$. For each such p, there are 6 solutions to the above, but only 2 with r even. Thus, for $p \equiv 1 \pmod 3$, we must add 4/3 to the correction term, and for $p \equiv 2 \pmod 3$, we add 0 to the correction term.

Forms proportional to $x^2 + y^2$ arise for those $r \equiv 0 \pmod 2$ for which there exists $\alpha \in \mathbb{Z}\backslash\{0\}$ such that $r^2 - 4p = -4\alpha^2$. Thus, $p = \frac{r^2+4\alpha^2}{4} = \left(\frac{r}{2} + \alpha i\right)\left(\frac{r}{2} - \alpha i\right)$. Recall that p factors in $\mathbb{Z}[i]$ if and only if $p \equiv 1 \pmod 4$. Given a prime $p \equiv 1 \pmod 4$, there are 4 choices for $r/2$ and hence 4 choices for r. So, we have 4 forms and need to add 2 to the correction term. When $p \equiv 3 \pmod 4$ we add 0 to the correction term. □

Combining the results in Propositions 2.2.2 and 2.2.3, we have

$$\sum_{\substack{|r|<2\sqrt{p} \\ r\equiv 0 \pmod 2}} H(4p-r^2) = N_{2,p} - \sum_{\substack{|r|<2\sqrt{p} \\ r\equiv 0 \pmod 2}} c_{r,p} = \frac{4p-2}{3}.$$

Theorem 2.1.2 now follows from (2.1). □

We now give a sketch of the proof of Theorem 2.1.3. The proof uses some of computations from the proof of Theorem 2.1.2.

Proof Sketch of Theorem 2.1.3. For $c \equiv \pm 1 \pmod 4$, the identities

$$\sum_{\substack{|r|<2\sqrt{p} \\ r\equiv c \pmod 2}} H(4p-r^2) = \frac{p+1}{3}$$

follow directly from Theorem 2.1.2 and (2.4).

By (2.3),

$$\sum_{\substack{|r|<2\sqrt{p} \\ r\equiv p+1 \pmod 4}} \big(H(4p-r^2) + c_{r,p}\big)$$

is equal to the number of isomorphism classes of elliptic curves over $E/\mathbb{F}_p$ with $4|\#E(\mathbb{F}_p)$. This is equal to the number of classes of curves having full 2-torsion plus the number of classes having cyclic 4-torsion over $\mathbb{F}_p$.

As with the Proof of Theorem 2.1.2, the identities may be checked directly for $p = 3$. So, we will assume that $p > 3$. From the proof of Proposition 2.2.2, we see that the number of isomorphism classes of curves having full 2-torsion over $\mathbb{F}_p$ is given by

$$\begin{cases} \frac{p+5}{3}, & p \equiv 1 \pmod{12}, \\ \frac{p+1}{3}, & p \equiv 5 \pmod{12}, \\ \frac{p+2}{3}, & p \equiv 7 \pmod{12}, \\ \frac{p-2}{3}, & p \equiv 11 \pmod{12}. \end{cases}$$

Following [Kna92, pp. 145-147], we see that given any curve with 4-torsion over $\mathbb{F}_p$, we can move the point of order 4 to the origin and place the resulting curve into Tate normal form to find a model for the curve of the form

$$E_b : y^2 + xy - by = x^3 - bx^2, \tag{2.13}$$

which has discriminant $\Delta_b = b^4(1 + 16b)$. Let $P = (0, 0)$ denote the point of order 4 on E_b. Thus, as b runs over all of $\mathbb{F}_p$, we see every class of elliptic curve possessing 4-torsion over $\mathbb{F}_p$. As before, we will omit $b = 0, 16^{-1}$ from consideration since these give singular curves.

Given a curve of the form (2.13), we note that both $P = (0, 0)$ and $-P$ have order 4. We see that moving $-P$ to origin and placing the resulting curve in Tate normal form gives us exactly the same normal form as before. Thus, there is exactly one way to represent each cyclic 4-torsion curve in the form (2.13).

We are only interested in counting the classes which have cyclic 4-torsion and not full 2-torsion (since these have already been counted above). Thus, given a curve (2.13), we move $2P$ to the origin and place the resulting curve in the form (2.6). Thus, we see that the curve has full 2-torsion if and only if $\left(\frac{16b+1}{p}\right) = 1$. Hence, we conclude that there are $(p - 1)/2$ isomorphism classes of curves possessing cyclic 4-torsion but not possessing full 2-torsion over $\mathbb{F}_p$.

Finally, in a manner similar to the proof of Proposition 2.2.3, we check that

$$\sum_{\substack{|r|<2\sqrt{p}, \\ r\equiv p+1 \pmod 4}} c_{r,p} = \begin{cases} 7/3, & p \equiv 1 \pmod{12}, \\ 1, & p \equiv 5 \pmod{12}, \\ 4/3, & p \equiv 7 \pmod{12}, \\ 0, & p \equiv 11 \pmod{12}. \end{cases}$$

Combining all the pieces, the result follows. □

For the remainder of this section, we will need the following result, which allows us to avoid the problem of detecting full m-torsion by only considering primes $p \not\equiv 1 \pmod m$.

Proposition 2.2.4. *If E is an elliptic curve possessing full m-torsion over $\mathbb{F}_p$, then $p \equiv 1 \pmod m$.*

Proof. Let G be the Galois group of $\mathbb{F}_p(E[m])/\mathbb{F}_p$. Then $G = \langle \phi \rangle$, where

$$\phi : \mathbb{F}_p(E[m]) \to \mathbb{F}_p(E[m])$$

is the Frobenius automorphism. We have the representation

$$\rho_m : G \hookrightarrow \mathrm{Aut}(E[m]) \cong \mathrm{Aut}\left(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}\right) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

See [Sil86, p. 89-90].

Now, suppose that E has full m-torsion. Then $\mathbb{F}_p(E[m])/\mathbb{F}_p$ is a trivial extension. Whence, G is trivial and $\rho_m(\phi) = I \in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. Therefore, applying [Sil86, Prop. 2.3, p. 134], we have $p \equiv \det(\rho_m(\phi)) \equiv 1 \pmod m$. □

We omit the proof of Theorem 2.1.5 since it is similar to, but less involved than the following cases of Theorem 2.1.7.

Proof Sketch of Theorem 2.1.7 (Cases: $p \not\equiv 0, 1 \pmod 7; c \equiv \pm(p+1) \pmod 7$). If $p = 3$, the identities may be checked directly. We will assume that $p \neq 3, 7$ and prime. Since we also assume that $p \not\equiv 1 \pmod 7$, we know that no curve may have full 7-torsion over $\mathbb{F}_p$. Thus, if P is a point of order 7, $E[7](\mathbb{F}_p) = \langle P \rangle \cong \mathbb{Z}/7\mathbb{Z}$.

Now, suppose that E possesses 7-torsion, and let P be a point of order 7. In a manner similar to [Kna92, pp. 145-147], we see that we can move P to the origin and put the resulting equation into Tate normal form to obtain a model for E of the form

$$E_s : y^2 + (1 - s^2 + s)xy - (s^3 - s^2)y = x^3 - (s^3 - s^2)x^2, \tag{2.14}$$

which has discriminant $\Delta_s = s^7(s-1)^7(s^3 - 8s^2 + 5s + 1)$.

First, we examine the discriminant. We note that $s = 0, 1$ both result in singular curves and so we omit these values from consideration. The cubic $s^3 - 8s^2 + 5s + 1$ has discriminant 7^4 and hence has Galois group isomorphic to $\mathbb{Z}/3\mathbb{Z}$ (See [Hun74, Cor. 4.7, p. 271]). Thus, the splitting field for the cubic is a degree 3 extension over $\mathbb{Q}$; and we see that the cubic will either be irreducible or split completely over $\mathbb{F}_p$. One can then check that the cubic splits over the cyclotomic field $\mathbb{Q}(\zeta_7)$, where ζ_7 is a primitive 7th root of unity. The field $\mathbb{Q}(\zeta_7)$ has a unique subfield which is cubic over $\mathbb{Q}$, namely $\mathbb{Q}(\zeta_7 + \zeta_7^6)$. Thus, $\mathbb{Q}(\zeta_7 + \zeta_7^6)$ is the splitting field for the cubic $s^3 - 8s^2 + 5s + 1$. By examining the way that rational primes split in $\mathbb{Q}(\zeta_7)$, one can deduce that rational primes are inert in $\mathbb{Q}(\zeta_7 + \zeta_7^6)$ unless $p \equiv \pm 1 \pmod 7$, in which case they split completely. Thus, we see that the cubic $s^3 - 8s^2 + 5s + 1$ has exactly 3 roots over $\mathbb{F}_p$ if $p \equiv \pm 1 \pmod 7$ and is irreducible otherwise. Hence, as s ranges over all of $\mathbb{F}_p$, we see $p - 5$ nonsingular curves (2.14) if $p \equiv \pm 1 \pmod 7$ and $p - 2$ nonsingular curves (2.14) otherwise.

Second, we check that the mapping $s \mapsto (1 - s^2 + s, -(s^3 - s^2))$ is a one to one mapping of $\mathbb{F}_p \backslash \{0, 1\}$ into $\mathbb{F}_p^2$. Hence, as s ranges over all of $\mathbb{F}_p \backslash \{0, 1\}$, we see $p - 2$ distinct equations of the form (2.14).

Next, we check that if we choose to move $-P$ to the origin instead of P, we will obtain exactly the same Tate normal form for E. Moving $2P$ or $3P$ to the origin each result in different normal forms unless $s = 0, 1$ or is a nontrivial cube root of -1, in which case both give exactly the same normal form as moving P to the origin. Note that by the above argument, moving $-2P$ to the origin will give the same normal form as $2P$ and moving $-3P$ to the origin will give the same normal form as $3P$. Now, $s = 0, 1$ both give singular curves; and nontrivial cube roots of -1 exists in $\mathbb{F}_p$ if and only if $p \equiv 1 \pmod 3$, in which case there are exactly 2. Thus, the number of isomorphism classes of curves possessing 7-torsion over $\mathbb{F}_p$ is given by

$$\begin{cases} \frac{p+2}{3}, & p \not\equiv \pm 1 \pmod 7,\ p \equiv 1 \pmod 3, \\ \frac{p-1}{3}, & p \equiv 6 \pmod 7,\ p \equiv 1 \pmod 3, \\ \frac{p-2}{3}, & p \not\equiv \pm 1 \pmod 7,\ p \equiv 2 \pmod 3, \\ \frac{p-5}{3}, & p \equiv 6 \pmod 7,\ p \equiv 2 \pmod 3. \end{cases}$$

Finally, we check that, for $p \not\equiv 1 \pmod 7$,

$$\sum_{\substack{|r|<2\sqrt{p}, \\ r \equiv p+1 \pmod 7}} c_{r,p} = \begin{cases} 4/3, & p \equiv 1 \pmod 3, \\ 0, & \text{otherwise}. \end{cases}$$

The result now follows for $c \equiv \pm(p+1) \pmod 7$ by (2.3) and (2.4). □

The remaining cases of Theorem 2.1.7 will be treated in Section 2.4.

2.3 Modular Forms and Hurwitz Class Numbers

Recall Proposition 1.3.12, which shows how Hurwitz class numbers appear as the Fourier coefficients of certain modular forms of weight 3/2. In particular, if $-b$ is a quadratic non-residue modulo a, then

$$\mathscr{H}_1(z; a, b) := \sum_{N \equiv b \pmod a} H(N) q^N \in \mathscr{M}_{3/2}(G_a),$$

where

$$G_a = \left\{ \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix} \right) \in \Gamma_0(A) : \alpha^2 \equiv 1 \pmod{a} \right\},$$

and we take $A = a^2$ if $4|a$ and $A = 4a^2$ otherwise. We now turn to the proof of Theorem 2.1.4. It will be important that in the case $a = 3$ that the group $G_a = \Gamma_0(36)$.

Proof of Theorem 2.1.4. Recall that the classical theta series $\theta(z) := \sum_{s=-\infty}^{\infty} q^{s^2} \in \mathscr{M}_{1/2}(4)$. Applying Theorem 1.3.12, we see that $\mathscr{H}_1(z;3,1) = \displaystyle\sum_{N \equiv 1 \pmod{3}} H(N)q^N \in \mathscr{M}_{3/2}(36)$. Note that in this case, $G_3 = \Gamma_0(36)$. Thus, we can check that product $\mathscr{H}_1(z;3,1)\theta(z) \in \mathscr{M}_2(36)$. Observe that the coefficients of the product bear a striking resemblance to the sums of interest. Indeed,

$$\begin{aligned}
\mathscr{H}_1(z;3,1)\theta(z) &= \sum_{s=-\infty}^{\infty} \sum_{N\equiv 1 \pmod{3}} H(N)q^{N+s^2} \\
&= \sum_{n\equiv 1 \pmod{3}} \left(\sum_{\substack{|s|<\sqrt{n}, \\ s\equiv 0 \pmod{3}}} H(n-s^2) \right) q^n \\
&\quad + \sum_{n\equiv 2 \pmod{3}} \left(\sum_{\substack{|s|<\sqrt{n}, \\ s\equiv \pm 1 \pmod{3}}} H(n-s^2) \right) q^n.
\end{aligned}$$

We will prove Theorem 2.1.4 by expressing $\mathscr{H}_1(z;3,1)\theta(z)$ as a linear combination of basis forms with "nice" Fourier coefficients. Note that Theorem 1.3.9 says that we will only need to consider the first 13 coefficients in order to do this.

Let χ_0 denote the principal character of conductor 1, and let $\chi_{0,2}$ and $\chi_{0,3}$ denote the trivial characters modulo 2 and 3 respectively. Finally let $\left(\frac{\cdot}{3}\right)$ denote the Legendre symbol modulo 3. Then one can show that the Eisenstein subspace $\mathscr{E}_2(36)$ has dimension

11 over $\mathbb{C}$ and is spanned by

$$\left\{\begin{array}{lll} E_2(z;\chi_0,\chi_{0,2}), & E_2(z;\chi_0,\chi_{0,3}), & E_2(z;\left(\frac{\cdot}{3}\right),\left(\frac{\cdot}{3}\right)), \\ E_2(2z;\chi_0,\chi_{0,2}), & E_2(3z;\chi_0,\chi_{0,2}), & E_2(9z;\chi_0,\chi_{0,2}), \\ E_2(6z;\chi_0,\chi_{0,2}), & E_2(18z;\chi_0,\chi_{0,2}), & E_2(3z;\chi_0,\chi_{0,3}), \\ E_2(2z;\left(\frac{\cdot}{3}\right),\left(\frac{\cdot}{3}\right)), & E_2(4z;\left(\frac{\cdot}{3}\right),\left(\frac{\cdot}{3}\right)) & \end{array}\right\}.$$

The cusp space $\mathscr{S}_2(36)$ is 1 dimensional and is spanned by the cusp form associated to the elliptic curve

$$E: y^2 = x^3 + 1,$$

which is the inverse Mellin transform of the L-series

$$\begin{aligned} L(E,s) &= \prod_{p\nmid 36}(1-a(p)p^{-s}+p^{1-2s})^{-1} = \sum_{(n,6)=1}\frac{a(n)}{n^s} \\ &= \sum_{(n,6)=1}\prod_{p|n}\left[\sum_{\left\lceil\frac{\mathrm{ord}_p(n)}{2}\right\rceil\le k\le \mathrm{ord}_p(n)}\binom{k}{\mathrm{ord}_p(n)-k}a(p)^{2k-\mathrm{ord}_p(n)}(-p)^{\mathrm{ord}_p(n)-k}\right]\frac{1}{n^s}, \end{aligned}$$

where $a(p) := a_p(E) = p+1-\#E(\mathbb{F}_p)$, and we take $a(p)^0 = 1$ even if $a_p(E) = 0$. We will denote this cusp form by $f_E(z)$. See Example 1.3.14 for a description of the coefficients.

One can verify computationally that

$$\begin{aligned} \mathscr{H}_1(z;3,1)\theta(z) &= \frac{-1}{16}E_2(z;\chi_0,\chi_{0,2}) + \frac{3}{16}E_2(z;\chi_0,\chi_{0,3}) + \frac{-1}{24}E_2(z;\left(\frac{\cdot}{3}\right),\left(\frac{\cdot}{3}\right)) \\ &+ \frac{-1}{2}E_2(2z;\chi_0,\chi_{0,2}) + \frac{1}{4}E_2(3z;\chi_0,\chi_{0,2}) + \frac{-3}{16}E_2(9z;\chi_0,\chi_{0,2}) \\ &+ 2E_2(6z;\chi_0,\chi_{0,2}) + \frac{-3}{2}E_2(18z;\chi_0,\chi_{0,2}) + \frac{-3}{16}E_2(3z;\chi_0,\chi_{0,3}) \\ &+ \frac{-1}{8}E_2(2z;\left(\frac{\cdot}{3}\right),\left(\frac{\cdot}{3}\right)) + \frac{-1}{3}E_2(4z;\left(\frac{\cdot}{3}\right),\left(\frac{\cdot}{3}\right)) + \frac{-1}{12}f_E(z). \end{aligned}$$

Let $\sigma(n) := \sigma_1(n) = \sum_{d|n} d$, and define the arithmetic functions

$$\begin{aligned}
\mu_1(n) &:= \sum_{\substack{d|n,\\ d\not\equiv 0 \pmod 2}} d,\\
\mu_2(n) &:= \sum_{\substack{d|n,\\ d\not\equiv 0 \pmod 3}} d,\\
\mu_3(n) &:= \left(\frac{n}{3}\right)\sigma(n).
\end{aligned}$$

Extend these to $\mathbb{Q}$ by setting $\mu_i(r) = 0$ for $r \in \mathbb{Q}\backslash\mathbb{Z}$ $(i = 1, 2, 3)$. Comparing n-th coefficients, we have the following proposition.

Proposition 2.3.1.

$$\begin{aligned}
\sum_{|s|<\sqrt{n}}{}^{*} H(n-s^2) = &- \frac{1}{16}\mu_1(n) + \frac{3}{16}\mu_2(n) - \frac{1}{24}\mu_3(n) - \frac{1}{2}\mu_1(n/2)\\
&+ \frac{1}{4}\mu_1(n/3) - \frac{3}{16}\mu_1(n/9) + 2\mu_1(n/6) - \frac{3}{2}\mu_1(n/18)\\
&- \frac{3}{16}\mu_2(n/3) - \frac{1}{8}\mu_3(n/2) - \frac{1}{3}\mu_3(n/4) - \frac{1}{12}a(n),
\end{aligned}$$

*where the * denotes the fact that if* $n \equiv 1 \pmod 3$, *we take the sum over all* $s \equiv 0 \pmod 3$*; if* $n \equiv 2 \pmod 3$, *we take the sum over all* $s \equiv \pm 1 \pmod 3$.

Using (2.4) and the fact that $a(n) = 0$ if $(n, 6) > 1$, we are able to extract the identities

$$\sum_{\substack{|r|<2\sqrt{p},\\ r\equiv c \pmod 3}} H(4p - r^2) = \begin{cases} \frac{p+1}{2}, & \text{if } p \equiv 1 \pmod 3,\ c = 0,\\ \frac{p+1}{2}, & \text{if } p \equiv 2 \pmod 3,\ c = 1 \text{ or } 2.\end{cases}$$

So, using (2.1), we are able to obtain Theorem 2.1.4 as a corollary. □

At this point, we also note that there is a more general identity than (2.1), which is due to Hurwitz. See [Coh96, p. 236]. In particular, if we let $\lambda(n) := \frac{1}{2}\sum_{d|n}\min(d, n/d)$, then

$$\sum_{|r|<2\sqrt{N}} H(4N-r^2) = 2\sigma(N) - 2\lambda(N).$$

So, this identity together with Proposition 2.3.1 makes it possible to generalize Theorem 2.1.4 for p not necessarily prime.

In addition, if we study the cusp form in our basis carefully, we can extract other nice formulae as well. For example, we can use the fact that $a(p) = 0$ if $p \equiv 2 \pmod 3$ to obtain Theorem 2.1.6. See Example 1.3.14 on page 29.

2.4 The Eichler-Selberg Trace Formula and Hurwitz Class Numbers

Recall that the Eichler-Selberg Trace Formula (Theorem 1.3.18) gives the value of the trace of the n-th Hecke operator acting on $\mathscr{S}_k(N,\psi)$. If we specialize to the case that $n = p$ is prime and assume that the weight $k = 2$ and the character ψ is trivial, then the formula simplifies to the following.

Theorem 2.4.1. *Let p be a prime. The trace of the p-th Hecke operator acting on $\mathscr{S}_2(N)$ is given by*

$$\begin{aligned}\mathrm{tr}_{2,N}(T_p) = p+1 \quad &- \sum_{s\in H}\frac{1}{p-1}\sum_{f|t}\frac{1}{2}\varphi((s^2-4p)^{1/2}/f)\prod_{l|N}c(s,f,l)\\ &- \sum_{s\in E_1\cup E_2}\sum_{f|t}\frac{h((s^2-4p)/f^2)}{w((s^2-4p)/f^2)}\prod_{l|N}c(s,f,l),\end{aligned}$$

where $H = \{s : s^2-4p = t^2\}$, $E_1 = \{s : s^2-4p = t^2m,\ 0 > m \equiv 1 \pmod 4\}$, and $E_2 = \{s : s^2-4p = t^24m,\ 0 > m \equiv 2, 3 \pmod 4\}$.

As before, φ is the Euler φ-function. For $d < 0$, $h(d)$ is the class number of the order of $\mathbb{Q}(\sqrt{d})$ of discriminant d, and $w(d)$ is the cardinality of its unit group. For a prime $l|N$, $c(s,f,l)$ essentially counts the number of solutions to a certain system of congruences.

See Theorem 1.3.18 for more details.

From equation (1.25), if $s \in E_1 \cup E_2$, then

$$H(4p - s^2) = 2 \sum_{f|t} \frac{h((s^2 - 4p)/f^2)}{w((s^2 - 4p)/f^2)}.$$

So, if it is possible to control the $c(s, f, l)$ – in particular, if it is possible to make them constant with respect to f, then there is hope that Hurwitz class number relations may be extracted from the trace formula. Indeed, if p is quadratic nonresidue modulo l for all primes l dividing N, then the computation of $c(s, f, l)$ is quite simple and does not depend on f. For example, if we apply the trace formula to T_p acting on $\mathscr{S}_2(7) = \{0\}$ for $p \equiv 3, 5, 6 \pmod 7$, we have

$$c(s, f, l) = \begin{cases} 2, & p \equiv 3 \pmod 7,\ s \equiv 0, \pm 3, \\ 2, & p \equiv 5 \pmod 7,\ s \equiv 0, \pm 1, \\ 2, & p \equiv 6 \pmod 7,\ s \equiv 0, \pm 2, \\ 0, & \text{otherwise.} \end{cases}$$

The resulting Hurwitz class number relation is the following.

Proposition 2.4.2.

$$\sum_{|s| < 2\sqrt{p}}{}^{*} H(4p - s^2) = p - 1,$$

*where the * denotes the fact that if $p \equiv 3 \pmod 7$, the sum is over all $s \equiv 0, \pm 3 \pmod 7$; if $p \equiv 5 \pmod 7$, the sum is over all $s \equiv 0, \pm 1 \pmod 7$; and if $p \equiv 6 \pmod 7$, the sum is over all $s \equiv 0, \pm 2 \pmod 7$.*

Combining the above proposition with the cases of Theorem 2.1.7 that were proven in Section 2.2, we are able to obtain the remaining formulae in the theorem.

2.5 Conjectures

For all primes p sufficiently large, we conjecture formulae for

$$\sum_{\substack{|r|<2\sqrt{p},\\ r\equiv c \pmod{m}}} H(4p-r^2)$$

in the cases $m = 5, 7$. These values have been checked for primes $p < 1,000,000$. Where an entry is bold and marked by asterisks, the formula is proved in this thesis; where an entry is blank, we were not able to recognize any simple pattern from the computations.

We note that for $m = 5$ and 7, neither the curve counting method of Section 2.2 alone nor the basis of modular forms approach of Section 2.3 alone will be sufficient for a complete characterization of these sums. Rather a combination of the two methods should work.

Conjecture 2.5.1. *The table below gives the value of the sum* $\sum_{\substack{|r|<2\sqrt{p},\\ r\equiv c \ (\mathrm{mod}\ 5)}} H(4p-r^2)$.

	$c = 0$	$c = \pm 1$	$c = \pm 2$
$p \equiv 1 \pmod 5$	$\frac{(p+1)}{2}$	$\frac{(p+1)}{3}$	$\frac{(5p-7)}{12}$
$p \equiv 2 \pmod 5$	$\frac{(p+1)}{3}$	$\frac{(p+1)}{3}$	$*\boldsymbol{\frac{(p-1)}{2}}*$
$p \equiv 3 \pmod 5$	$\frac{(p+1)}{3}$	$*\boldsymbol{\frac{(p-1)}{2}}*$	$\frac{(p+1)}{3}$
$p \equiv 4 \pmod 5$	$*\boldsymbol{\frac{(p-3)}{2}}*$	$\frac{(5p+5)}{12}$	$\frac{(p+1)}{3}$

Table 2.1: Conjecture 2.5.1: $m = 5$

Conjecture 2.5.2. *The table below gives the value of the sum* $\sum_{\substack{|r|<2\sqrt{p},\\ r\equiv c \ (\mathrm{mod}\ 7)}} H(4p-r^2)$.

	$c = 0$	$c = \pm 1$	$c = \pm 2$	$c = \pm 3$
$p \equiv 1 \pmod 7$		$\frac{(p+1)}{3}$		
$p \equiv 2 \pmod 7$				$*\boldsymbol{\frac{(p-2)}{3}}*$
$p \equiv 3 \pmod 7$	$*\boldsymbol{\frac{(p+1)}{3}}*$	$\frac{(p+1)}{4}$	$\frac{(p+1)}{4}$	$*\boldsymbol{\frac{(p-2)}{3}}*$
$p \equiv 4 \pmod 7$			$*\boldsymbol{\frac{(p-2)}{3}}*$	
$p \equiv 5 \pmod 7$	$*\boldsymbol{\frac{(p+1)}{3}}*$	$*\boldsymbol{\frac{(p-2)}{3}}*$	$\frac{(p+1)}{4}$	$\frac{(p+1)}{4}$
$p \equiv 6 \pmod 7$	$*\boldsymbol{\frac{(p-5)}{3}}*$	$\frac{(p+1)}{4}$	$*\boldsymbol{\frac{(p+1)}{3}}*$	$\frac{(p+1)}{4}$

Table 2.2: Conjecture 2.5.2: $m = 7$

For making further progress on these conjectures, it appears that the method of Section 2.3 will be most fruitful. The difficulty in using this method is that, in each case, the group G_m (defined in Theorem 1.3.12) is strictly contained in $\Gamma_0(4m^2)$. So, we will need a much larger basis of modular forms. Certainly a basis for $\mathscr{M}_2(\Gamma_1(4m^2))$ would be sufficient. However, to completely fill in the table, another method will be needed. Perhaps an adaptation of the curve counting method of Section 2.2 for $p \equiv 1 \pmod m$ would be best. The main obstacle to overcome is that one must deal with the presence of full m-torsion curves when $p \equiv 1 \pmod m$.

In general, for a prime m, we note that the curve counting method will give proofs for $c \equiv \pm(p+1) \pmod m$. We also note that, for primes $m \equiv 1 \pmod 4$, the basis of forms method will give proofs for the cases when $4p - c^2$ is not a square; and for primes $m \equiv 3 \pmod 4$, the basis of forms method will give proofs for the cases when $4p - c^2$ is a square. Thus, for a prime m, we will obtain half the cases from the basis of forms approach and we will obtain $2(m-1)+1$ more from the curve counting approach assuming that the case $p \equiv 1 \pmod m$ can be adequately handled. So, at least for primes greater than 7, a third method will be necessary to fully characterize how the sum splits.

Chapter 3

Finite Field Elements of High Order Arising from Modular Curves

In this chapter, we take up the problem of finding elements of the finite fields of large multiplicative order. The method for constructing our elements is based on equations for modular curves. See §1.3. The results contained in this chapter appear in [BCG$^+$09].

Finding large order elements of finite fields has long been a problem of interest, particularly to cryptographers. Given a finite field $\mathbb{F}_q$, Gao [Gao99] gives an algorithm for constructing elements of $\mathbb{F}_{q^n}$ of order greater than

$$n^{\frac{\log_q n}{4\log_q(2\log_q n)}-\frac{1}{2}}.$$

The advantage of the algorithm is that it makes no restriction on q and it allows one to produce a provably high order element in any desired extension of $\mathbb{F}_q$ provided that one can find a polynomial in $\mathbb{F}_q[x]$ with certain desirable properties. Gao conjectures that for any $n > 1$, there exists a polynomial of degree at most $2\log_q n$ satisfying the conditions of his theorem. Conflitti has made some improvement to Gao's construction in [Con01]. However, the aforementioned conjecture remains unproven. Another result concerning the q "shifts" of an element of a general extension of $\mathbb{F}_q$ appears in [GS01, Cor. 4.4].

For special finite fields, it is possible to construct elements which can be proved to have much higher orders. For example, in Theorems 3.1.1 and 3.1.2 of this paper we construct elements of higher order in extensions of $\mathbb{F}_q$ of the form $\mathbb{F}_{q^{2^n}}$ and $\mathbb{F}_{q^{3^n}}$. See [GV95, GvzGP98, GS95b] on orders of Gauss periods and [Che05, Che07] on Kummer extensions. It has been pointed out to us that the method of [Che05, Che07] is able to produce higher order elements in the same extensions as our method. However, our method of construction is new, and we hope that it will prove to be a fruitful technique.

In [Vol07], Voloch shows that under certain conditions, one of the coordinates of a point on a plane curve must have high order. The bounds we obtain through our methods have order of magnitude similar to those predicted in the main theorem of [Vol07]. In a special case however, Voloch is able to achieve bounds which are much better. See section 5 of [Vol07]. Unfortunately, Voloch does not fully state this theorem and only alludes to how one may adapt the proof of his main theorem for this special case. The bounds given in [Vol07] are not as explicit as the ones given in this paper. Moreover, Voloch gives no explicit examples of his theorems. In Section 3.5 of this paper, we apply Voloch's technique to obtain a more explicit version of the special case of his main theorem. We then construct a sequence of elements for which his bounds apply and compare with our methods.

In this paper, we consider elements in finite field towers recursively generated according to the equations for explicit modular towers [Elk98]. We give two explicit constructions: one for odd characteristic and one for characteristic not equal to 3. In the first case, we explicitly construct elements of $\mathbb{F}_{q^{2^n}}$ whose orders are bounded below by $2^{\frac{1}{2}n^2+\frac{3}{2}n+\mathrm{ord}_2(q-1)-1}$. In the second, we obtain elements of $\mathbb{F}_{q^{3^n}}$ whose orders are bounded below by $3^{\frac{1}{2}n^2+\frac{3}{2}n+\mathrm{ord}_3(q-1)}$. Throughout we use the convention that exponentiation is right-associative, i.e., $a^{b^c} := a^{(b^c)}$.

3.1 Constructions Arising from Modular Towers

In [Elk98], Elkies gives a recursive formula for the defining equations of the modular curve $X_0(\ell^n)$ by identifying $X_0(\ell^n)$ within the product $\big(X_0(\ell^2)\big)^{n-1}$ for $n > 1$. For several cases, he even writes explicit equations. For example, in the case $\ell = 2$, the recursion is governed by the rule

$$(x_j^2 - 1)\left(\left(\frac{x_{j+1}+3}{x_{j+1}-1}\right)^2 - 1\right) = 1 \text{ for } j = 1, 2, \ldots, n-2. \tag{3.1}$$

Elkies also notices that under a suitable change of variables and a reduction modulo 3, the equation becomes

$$y_{j+1}^2 = y_j - y_j^2,$$

which was used by Garcia and Stichtenoth [GS96] to recursively construct an asymptotically optimal function field tower. In fact, Elkies notes that many recursively constructed optimal towers may now be seen as arising from these modular curve constructions and speculates that perhaps all such towers are modular in this sense.

In this paper, we use Elkies' formulas to generate high order elements in towers of finite fields. For example, the following construction will yield high order elements in odd characteristic. The equation (3.1) may be manipulated to the form $f(X, Y) = 0$, where

$$f(X, Y) := Y^2 + (6 - 8X^2)Y + (9 - 8X^2), \tag{3.2}$$

and we have made the substitution $X = x_j$ and $Y = x_{j+1}$. Now, choose $q = p^m$ to be an odd prime power such that $\mathbb{F}_q$ contains the fourth roots of unity (i.e. $q \equiv 1 \pmod 4$). Choose $\alpha_0 \in \mathbb{F}_q$ such that $\alpha_0^2 - 1$ is not a square in $\mathbb{F}_q$. In Lemma 3.2.6 (see Section 3.2), we will show that such an α_0 always exists. Finally, define α_n by $f(\alpha_{n-1}, \alpha_n) = 0$ for $n \geq 1$. This construction yields the following result; where, as usual, for a prime ℓ, $\operatorname{ord}_\ell(a)$ denotes the highest power of ℓ dividing a.

Theorem 3.1.1. *Let $\delta_n := \alpha_n^2 - 1$. Then δ_n has degree 2^n over $\mathbb{F}_q$, and the order of δ_n in*

$\mathbb{F}_{q^{2^n}}$ *is greater than* $2^{\frac{1}{2}n^2+\frac{3}{2}n+\mathrm{ord}_2(q-1)}$ *unless* $q \equiv 2 \pmod 3$ *and* $\alpha_0 = \pm\left(\frac{p-1}{2}\right)$*, in which case the order of* δ_n *is greater than* $2^{\frac{1}{2}n^2+\frac{3}{2}n+\mathrm{ord}_2(q-1)-1}$.

To accommodate even characteristic, we have also considered Elkies' formula for $X_0(3^n)$. We will prefer to work with the equation in the polynomial form $g(X,Y) = 0$, where

$$g(X,Y) := Y^3 + (6-9X^3)Y^2 + (12-9X^3)Y + (8-9X^3). \tag{3.3}$$

For this construction, choose q to be a prime power congruent to 1 modulo 3 but not equal to 4. The condition $q \equiv 1 \pmod 3$ assures the presence of the third roots of unity in $\mathbb{F}_q$. Choose $\beta_0 \in \mathbb{F}_q$ such that $\beta_0^3 - 1$ is not a cube in $\mathbb{F}_q$. In Lemma 3.2.7 (see Section 3.2), we show that such a β_0 always exists except when $q = 4$. Finally, define β_n by $g(\beta_{n-1}, \beta_n) = 0$ for $n \geq 1$. For this construction, we have the following result.

Theorem 3.1.2. *Let* $\gamma_n := \beta_n^3 - 1$*. Then* γ_n *has degree* 3^n *over* $\mathbb{F}_q$*, and the order of* γ_n *in* $\mathbb{F}_{q^{3^n}}$ *is greater than* $3^{\frac{1}{2}n^2+\frac{3}{2}n+\mathrm{ord}_3(q-1)}$.

There are two interesting things about the above constructions. The first is that, computationally, the elements δ_n and γ_n appear to have much higher order than our bounds suggest. See Section 3.6 for examples. The second interesting thing is that, as with the case of the optimal function field tower constructions of Garcia and Stichtenoth [GS95a, GS96] arising from these modular curve recipes, our proofs do not at all exploit this modularity. Perhaps the key to achieving better bounds lies in this relationship.

The paper is organized as follows. In Section 3.2, we will state and prove some elementary number theory facts that will be of use to us. In Section 3.3, we consider the first construction; and in Section 3.4, we consider the second. Finally, in Section 3.6, we give a few examples of each of the main theorems.

3.2 Number Theoretic Facts

Recall the following well known fact for detecting perfect n-th powers in finite fields. See [IR90, p. 81] for example.

Fact 3.2.1. *If $q \equiv 1 \pmod{n}$, then $x \in \mathbb{F}_q^*$ is a perfect n-th power if and only if $x^{(q-1)/n} = 1$.*

Also recall the following facts, which can be easily proved.

Fact 3.2.2. *Let $x \in \mathbb{F}_q^*$ of multiplicative order d. For $m, n \in \mathbb{N}$, if $x^n \neq 1$ and $x^{nm} = 1$, then $\gcd(d, m) > 1$.*

Fact 3.2.3. *Let $x \in \mathbb{F}_q^*$ of multiplicative order d. If ℓ is a prime, $m = \operatorname{ord}_\ell(n)$, and x^n is a nontrivial ℓ-th root of unity, then ℓ^{m+1} divides d.*

The following lemmas are useful for bounding the orders of the elements appearing in Theorems 3.1.1 and 3.1.2.

Lemma 3.2.4. *Let $\ell, b \in \mathbb{N}$ such that $b \equiv 1 \pmod{\ell}$, and let $M, N \in \mathbb{N}$ with $M < N$. Then*

$$\gcd\left(\sum_{j=1}^{\ell} b^{\ell^M(\ell-j)}, \sum_{j=1}^{\ell} b^{\ell^N(\ell-j)}\right) = \ell;$$

and hence $\frac{1}{\ell}\sum_{j=1}^{\ell} b^{\ell^M(\ell-j)}$ and $\frac{1}{\ell}\sum_{j=1}^{\ell} b^{\ell^N(\ell-j)}$ are coprime.

Proof. The following computation follows from Euclid's algorithm:

$$\gcd\left(\sum_{j=1}^{\ell} b^{\ell^N(\ell-j)}, b^{\ell^N} - 1\right) = \gcd\left(\ell, b^{\ell^N} - 1\right) = \ell. \tag{3.4}$$

Since $M < N$, repeatedly using the difference of ℓ-th powers formula shows that $\sum_{j=1}^{\ell} b^{\ell^M(\ell-j)}$ divides $b^{\ell^N} - 1$. Also, since $b \equiv 1 \pmod{\ell}$, it is clear that ℓ divides both $\sum_{j=1}^{\ell} b^{\ell^M(\ell-j)}$ and $\sum_{j=1}^{\ell} b^{\ell^N(\ell-j)}$. Therefore,

$$\gcd\left(\sum_{j=1}^{\ell} b^{\ell^M(\ell-j)}, \sum_{j=1}^{\ell} b^{\ell^N(\ell-j)}\right) = \ell.$$

□

Lemma 3.2.5. *Let $\ell, b, N \in \mathbb{N}$ with ℓ prime and $b \equiv 1 \pmod{\ell}$. If p is a prime dividing $\frac{1}{\ell}\sum_{j=1}^{\ell} b^{\ell^N(\ell-j)}$, then $p > \ell^{N+1}$.*

Proof. Since $\ell \geq 2$ and $b \equiv 1 \pmod{\ell}$, ℓ^2 divides $(b^{\ell^N} - 1)$. Hence, $p \neq \ell$ for otherwise, we have a contradiction with (3.4). Thus, p dividing $\frac{1}{\ell}\sum_{j=1}^{\ell} b^{\ell^N(\ell-j)}$ implies that $\sum_{j=1}^{\ell} b^{\ell^N(\ell-j)} \equiv 0 \pmod{p}$. So, b^{ℓ^N} is a nontrivial ℓ-th root of unity modulo p. Therefore, by Fact 3.2.3, ℓ^{N+1} divides $p-1$, and hence $p > \ell^{N+1}$. □

The following two lemmas essentially give the necessary and sufficient conditions for completing the first step in the construction of our towers, i.e., under certain restrictions on q, they demonstrate the existence of α_0 and β_0 each having its desired property. The proofs involve counting $\mathbb{F}_q$ solutions to equations via character sums. We refer the reader to [IR90, Chap. 8] for more on this technique. As in [IR90], for characters ψ and λ on $\mathbb{F}_q$, we denote the Jacobi sum of ψ and λ by $J(\psi, \lambda) := \sum_{a+b=1} \psi(a)\lambda(b)$.

Lemma 3.2.6. *Let q be a prime power. Then there exists $\alpha_0 \in \mathbb{F}_q$ such that $\delta_0 = \alpha_0^2 - 1$ is not a square in $\mathbb{F}_q$ if and only if q is odd.*

Proof. First, note that if q is even, then every element of $\mathbb{F}_q$ is a square. So, we assume that q is odd. We desire $\alpha_0 \in \mathbb{F}_q^*$ such that $\alpha_0^2 - 1$ is not a square. Our method for proving that such an α_0 exists involves counting solutions to the equation $x^2 - y^2 = 1$. Let τ be the unique character of exact order 2 on $\mathbb{F}_q$. Then

$$\begin{aligned}
\#\{(x,y) \in \mathbb{F}_q^2 : x^2 - y^2 = 1\} &= \sum_{\substack{a,b\in\mathbb{F}_q,\\ a+b=1}} \left(\sum_{j=0}^{1} \tau^j(a)\right)\left(\sum_{j=0}^{1} \tau^j(-b)\right) \\
&= \sum_{i=0}^{1}\sum_{j=0}^{1} \tau^j(-1) J(\tau^i, \tau^j) \\
&= q + \tau(-1)J(\tau,\tau) = q - 1.
\end{aligned}$$

On the other hand, if $\alpha_0^2 - 1$ is a square for all choices of α_0, then $\alpha_0^2 - 1 = y^2$ has a solution for all $\alpha_0 \in \mathbb{F}_q$. In this case, we have

$$\begin{aligned}
\#\{(x,y) \in \mathbb{F}_q^2 : x^2 - y^2 = 1\} &= \sum_{\alpha_0 \in \mathbb{F}_q} \#\{y \in \mathbb{F}_q : y^2 = \alpha_0^2 - 1\} \\
&= \sum_{\alpha_0^2 = 1} 1 + \sum_{\alpha_0^2 \neq 1} 2 = 2 + 2(q-2) = 2q - 2.
\end{aligned}$$

Thus, the assumption that $\alpha_0^2 - 1$ is always a square leads to the conclusion $q - 1 = 2q - 2$, which implies $q = 1$, a contradiction. □

Lemma 3.2.7. *Let q be a prime power. Then there exists $\beta_0 \in \mathbb{F}_q$ such that $\gamma_0 = \beta_0^3 - 1$ is not a cube in $\mathbb{F}_q$ if and only if $q \equiv 1 \pmod 3$ and $q \neq 4$.*

Proof. First, note that if $q \not\equiv 1 \pmod 3$, then every element of $\mathbb{F}_q$ is a cube. So, we will assume that $q \equiv 1 \pmod 3$. As mentioned earlier, this means that $\mathbb{F}_q$ contains a primitive third root of unity. We now count $\mathbb{F}_q$ solutions to the equation $x^3 - y^3 = 1$. Let χ be any character of order 3 on $\mathbb{F}_q$.

$$\begin{aligned}
\#\{(x,y) \in \mathbb{F}_q^2 : x^3 - y^3 = 1\} &= \sum_{\substack{a,b \in \mathbb{F}_q, \\ a+b=1}} \left(\sum_{j=0}^{2} \chi^j(a) \right) \left(\sum_{j=0}^{2} \chi^j(-b) \right) \\
&= \sum_{i=0}^{2} \sum_{j=0}^{2} \chi^j(-1) J(\chi^i, \chi^j) \\
&= q - 2\chi(-1) + J(\chi, \chi) + J(\chi^2, \chi^2) \\
&= q - 2 + 2\mathrm{Re} J(\chi, \chi).
\end{aligned}$$

On the other hand, if we assume that $\beta_0^3 - 1$ is a cube for all choices of $\beta_0 \in \mathbb{F}_q$, then

$$\begin{aligned}
\#\{(x,y) \in \mathbb{F}_q^2 : x^3 - y^3 = 1\} &= \sum_{\beta_0 \in \mathbb{F}_q} \#\{y \in \mathbb{F}_q : \beta_0^3 - y^3 = 1\} \\
&= \sum_{\beta_0^3 = 1} 1 + \sum_{\beta_0^3 \neq 1} 3 = 3 + 3(q-3) = 3q - 6.
\end{aligned}$$

Thus, the assumption that $\beta_0^3 - 1$ is always a cube leads to the conclusion that $|2q-4| = |(3q-6)-(q-2)| = |2\mathrm{Re}J(\chi,\chi)| \leq 2\sqrt{q}$, which implies $|q-2| \leq \sqrt{q}$. This implies that $(q-1)(q-4) \leq 0$. The only $q \equiv 1 \pmod 3$ satisfying this inequality is $q = 4$. □

3.3 The Quadratic Tower for Odd Characteristic

In this section, we consider the first tower, which is recursively constructed using (3.2). Throughout this section we will assume that p is an odd prime and that $q = p^m \equiv 1 \pmod 4$. In particular, if $p \equiv 3 \pmod 4$, then $2|m$. As discussed in the introduction, this condition ensures the existence of a primitive fourth root of unity. This will be seen to be a necessary ingredient in the construction of our tower. We also fix α_0 such that $\delta_0 = \alpha_0^2 - 1$ is not a square in $\mathbb{F}_q$. Recall that that Lemma 3.2.6 ensures the existence of such an α_0.

Before moving forward, we need to establish the relationship between δ_n and δ_{n-1}. From (3.2) and the definition of δ_n (see Theorem 3.1.1), we deduce that δ_{n-1} and δ_n are related by $F(\delta_{n-1}, \delta_n) = 0$ $(n \geq 1)$, where

$$F(X,Y) := Y^2 - (48X + 64X^2)Y - 64X. \tag{3.5}$$

We also fix the following more compact notation for the norm. We take

$$\begin{aligned} \mathrm{N}_{n,j} : \mathbb{F}_{q^{2^n}} &\to \mathbb{F}_{q^{2^{n-j}}}, \\ \alpha &\mapsto \alpha^{\prod_{k=1}^{j}(q^{2^{n-k}}+1)}. \end{aligned}$$

For the purpose of making the proof easier to digest, we break Theorem 3.1.1 into a pair of propositions.

Proposition 3.3.1. *The elements α_n and δ_n have degree 2 over $\mathbb{F}_{q^{2^{n-1}}}$ for $n \geq 1$.*

Proof. First note that the discriminant of $f(\alpha_{n-1}, Y)$ is $\delta_{n-1} = \alpha_{n-1}^2 - 1$ for all $n \geq 1$. We will proceed by induction on n. Recall that α_0 was chosen so that δ_0, the discriminant of

$f(\alpha_0, Y)$, is not a square in $\mathbb{F}_q$. Thus, α_1 satisfies an irreducible polynomial of degree 2 over $\mathbb{F}_q$, i.e., α_1 has degree 2 over $\mathbb{F}_q$. We may take $\{1, \alpha_1\}$ as a basis for $\mathbb{F}_q(\alpha_1)$ over $\mathbb{F}_q$. Writing δ_1 in terms of the basis, we have $\delta_1 = \alpha_1^2 - 1 = (8\alpha_0^2 - 6)\alpha_1 + (8\alpha_0^2 - 10)$. So, $\delta_1 \in \mathbb{F}_q$ if and only if $8\alpha_0^2 - 6 = 0$. If $8\alpha_0^2 - 6 = 0$, then $\delta_0 = \alpha_0^2 - 1 = -4^{-1}$, which is a square in $\mathbb{F}_q$ since $\mathbb{F}_q$ contains the fourth roots of unity. This is contrary to our choice of α_0. Thus, δ_1 has degree 2 over $\mathbb{F}_q$ as well.

Now, suppose that α_k and δ_k both have degree 2 over $\mathbb{F}_{q^{2^{k-1}}}$ for $1 \leq k \leq n$. Then $f(\alpha_{n-1}, Y)$ is the minimum polynomial of α_n over $\mathbb{F}_{q^{2^{n-1}}}$; and hence, the discriminant is not a square in $\mathbb{F}_{q^{2^{n-1}}}$. In particular,

$$\delta_{n-1}^{(q^{2^{n-1}}-1)/2} = -1. \tag{3.6}$$

Observe that $F(\delta_{n-1}, Y)$ is the minimum polynomial of δ_n over $\mathbb{F}_{q^{2^{n-1}}}$. To prove that the degree of α_{n+1} over $\mathbb{F}_{q^{2^n}}$ is 2, we show that $f(\alpha_n, Y)$ is irreducible over $\mathbb{F}_{q^{2^n}}$. Now,

$$\begin{aligned} \delta_n^{(q^{2^n}-1)/2} &= \left(\delta_n^{(q^{2^{n-1}}+1)}\right)^{(q^{2^{n-1}}-1)/2} = (\mathrm{N}_{n,1}(\delta_n))^{(q^{2^{n-1}}-1)/2} \\ &= (-64\delta_{n-1})^{(q^{2^{n-1}}-1)/2} = -1. \end{aligned}$$

Here we have used (3.6) and the fact that -64 is a square in $\mathbb{F}_{q^{2^{n-1}}}$ since $\mathbb{F}_q$ contains the fourth roots of unity. Thus, δ_n is not a square, and hence $f(\alpha_n, Y)$ is irreducible. So, the set $\{1, \alpha_{n+1}\}$ forms a basis for $\mathbb{F}_{q^{2^{n+1}}}$ over $\mathbb{F}_{q^{2^n}}$. Now, we write δ_{n+1} in terms of the basis, and apply the same argument as for δ_1 to demonstrate that the degree of δ_{n+1} over $\mathbb{F}_{q^{2^n}}$ is 2 as well. This completes the induction and the proof. □

An easy induction proof, exploiting the fact that $F(\delta_{k-1}, Y)$ is the minimum polynomial of δ_k over $\mathbb{F}_{q^{2^{k-1}}}$ for $1 \leq k \leq n$, shows that

$$\mathrm{N}_{n,j}(\delta_n) = (-64)^{(2^j-1)}\delta_{n-j} \tag{3.7}$$

for $1 \leq j \leq n$. This fact will be useful in the proof of the proposition below.

Proposition 3.3.2. *The order of δ_n in $\mathbb{F}_{q^{2^n}}$ is greater than $2^{\frac{1}{2}n^2+\frac{3}{2}n+\mathrm{ord}_2(q-1)}$ unless $q \equiv 2 \pmod 3$ and $\alpha_0 = \pm\left(\frac{p-1}{2}\right)$, in which case the order of δ_n is greater than $2^{\frac{1}{2}n^2+\frac{3}{2}n+\mathrm{ord}_2(q-1)-1}$.*

Proof. We first compute the power of 2 dividing the order of δ_n. Recall from the proof of Proposition 3.3.1 that $\delta_n^{(q^{2^n}-1)/2} \neq 1$; but of course, $\delta_n^{(q^{2^n}-1)} = 1$ since $\delta_n \in \mathbb{F}_{q^{2^n}}$. Since $q \equiv 1 \pmod 4$, $\mathrm{ord}_2(q^{2^j}+1) = 1$ for each $j \geq 1$. Repeatedly using the difference of squares formula, we have

$$\begin{aligned}\mathrm{ord}_2\left(\frac{q^{2^n}-1}{2}\right) &= \mathrm{ord}_2(q-1) - 1 + \sum_{j=0}^{n-1} \mathrm{ord}_2(q^{2^j}+1) \\ &= n - 1 + \mathrm{ord}_2(q-1).\end{aligned}$$

Thus, $2^{n+\mathrm{ord}_2(q-1)}$ divides the order of δ_n by Fact 3.2.3.

Now we look for odd primes dividing the order. By Fact 3.2.2, the order of δ_n has a common factor with $(q^{2^{n-j}}+1)/2$ for each j such that the $\frac{(q^{2^n}-1)}{(q^{2^{n-j}}+1)/2}$ power of δ_n is not equal to 1. By (3.7), we have that the $\frac{(q^{2^n}-1)}{(q^{2^{n-j}}+1)/2}$ power of δ_n is equal to

$$(\mathrm{N}_{n,j-1}(\delta_n))^{2(q^{2^{n-j}}-1)} = ((-64)^{(2^{(j-1)}-1)}\delta_{n-j+1})^{2(q^{2^{n-j}}-1)} = (\delta_{n-j+1})^{2(q^{2^{n-j}}-1)} \neq 1$$

provided that $\delta_{n-j+1}^2 \notin \mathbb{F}_{q^{2^{n-j}}}$. From (3.5), we know that we may write δ_{n-j+1}^2 as

$$\delta_{n-j+1}^2 = (48\delta_{n-j} + 64\delta_{n-j}^2)\delta_{n-j+1} + 64\delta_{n-j}.$$

Thus, $\delta_{n-j+1}^2 \in \mathbb{F}_{q^{n-j}}$ if and only if δ_{n-j} satisfies the equation $48\delta_{n-j} + 64\delta_{n-j}^2 = 0$. If this were the case, then $\delta_{n-j} = 0$ or $\delta_{n-j} = -3^{-1}4$. By Proposition 3.3.1, this implies that $n = j$. However, $\delta_0 = 0$ contradicts the choice of α_0; and $\delta_0 = -4^{-1}3$ contradicts the choice of α_0 unless -3 is not a perfect square, that is, unless $q \equiv 2 \pmod 3$. If $q \equiv 2 \pmod 3$, then the only choices of α_0 that give $\delta_0 = -4^{-1}3$ are $\alpha_0 = \pm\left(\frac{p-1}{2}\right)$. Thus, the order of δ_n has a common factor with $(q^{2^{n-j}}+1)/2$ for each $1 \leq j \leq n$ unless $q \equiv 2 \pmod 3$, $\alpha_0 = \pm\left(\frac{p-1}{2}\right)$, and $j = n$. Each of these factors must be odd since $\mathrm{ord}_2(q^{2^{n-j}} + 1) = 1$ as noted above. By Lemma 3.2.4 with $\ell = 2$ and $b = q$, we see that these factors must be pairwise coprime as well. Hence, we get either n or $n-1$ distinct odd prime factors dividing the order of δ_n depending on the case. By Lemma 3.2.5, each such prime factor must bounded below by 2^{n-j+1}. Therefore, the order of δ_n is bounded below by

$$2^{n+\mathrm{ord}_2(q-1)} \prod_{j=1}^{n} 2^{n-j+1} \quad = \quad 2^{n+\mathrm{ord}_2(q-1)+n(n+1)/2} = 2^{\frac{n^2+3n}{2}+\mathrm{ord}_2(q-1)}$$

unless $q \equiv 2 \pmod 3$ and $\alpha_0 = \pm\left(\frac{p-1}{2}\right)$, in which case the order is bounded below by $2^{\frac{1}{2}n^2+\frac{3}{2}n+\mathrm{ord}_2(q-1)-1}$. □

Theorem 3.1.1 follows by combining the two propositions. The authors would like to point out that it is possible to achieve a slightly better lower bound for the order of δ_n by the following method. First, choose a square root of δ_{n-1}, say $\sqrt{\delta_{n-1}} \in \mathbb{F}_{q^{2^n}}$. Then use the method above to prove a lower bound for the order of $\sqrt{\delta_{n-1}}$. Finally, deduce a bound for the order of δ_n. The improvement, however, only affects the coefficient of n in the exponent. Since computationally our bounds do not appear to be that close to the truth, we have decided to work directly with δ_n instead.

3.4 The Cubic Tower for Characteristic Not 3

In this section, we consider the second tower, which is recursively constructed using (3.3). Recall that, for this tower, we assume that $q \equiv 1 \pmod 3$ and $q \neq 4$. This means that $\mathbb{F}_q$ will contain the third roots of unity, and hence the third roots of -1 as well. We also fix a β_0 such that $\gamma_0 = \beta_0^3 - 1$ is not a cube in $\mathbb{F}_q$. Recall that Lemma 3.2.7 ensures the existence of such a β_0.

Before we begin the proof of Theorem 3.1.2, we need to establish the relationship between γ_{n-1} and γ_n. The relationship is given by $G(\gamma_{n-1}, \gamma_n) = 0$ for $n \geq 1$, where

$$G(X, Y) := Y^3 - (270X + 972X^2 + 729X^3)Y^2 - (972X + 729X^2)Y - 729X. \tag{3.8}$$

This follows from (3.3) and the definition of γ_n. We also fix the following notation for the norm.

$$\begin{array}{rcl} \mathrm{N}_{n,j} : \mathbb{F}_{q^{3^n}} & \longrightarrow & \mathbb{F}_{q^{3^{n-j}}}, \\ \beta & \longmapsto & \beta^{\prod_{k=1}^{j}\left(\left(q^{3^{n-k}}\right)^2 + q^{3^{n-k}} + 1\right)}. \end{array}$$

As in section 3.3, we break the result into two smaller propositions.

Proposition 3.4.1. *The elements β_n and γ_n both have degree 3 over $\mathbb{F}_{q^{3^{n-1}}}$ for $n \geq 1$.*

Proof. By carefully examining the cubic formula applied to the polynomial, one observes that $g(\beta_{n-1}, Y)$ is irreducible if and only if $\gamma_{n-1} = \beta_{n-1}^3 - 1$ is not a cube in $\mathbb{F}_{q^{3^{n-1}}}$. Thus, β_n will have degree 3 over $\mathbb{F}_{q^{3^{n-1}}}$ if and only if γ_{n-1} is not a cube in $\mathbb{F}_{q^{3^{n-1}}}$ for all $n \geq 1$. As with the proof of Proposition 3.3.1, we proceed by induction on n. Recall that β_0 was chosen so that γ_0 is not a cube in $\mathbb{F}_q$. Thus, β_1 has degree 3 over $\mathbb{F}_q$. So, we may take $\{1, \beta_1, \beta_1^2\}$ as a basis for $\mathbb{F}_{q^3}$ over $\mathbb{F}_q$. Writing γ_1 in terms of the basis, we have

$$\gamma_1 = \beta_1^3 - 1 = (9\beta_0^3 - 6)\beta_1^2 + (9\beta_0^3 - 12)\beta_1 + (9\beta_0^3 - 9).$$

So, $\gamma_1 \in \mathbb{F}_q$ if and only if $9\beta_0^3 - 6 = 0$ and $9\beta_0^3 - 12 = 0$. This leads to the conclusion that $\gamma_0 = -3^{-1}$ and $\gamma_0 = 3^{-1}$, which implies that $2 = 0$, i.e., the characteristic is 2. In this case, we are led to the conclusion that $\gamma_0 = 1$, which is a cube. This of course is contrary to our choice of γ_0. Therefore, $\gamma_1 \notin \mathbb{F}_q$, i.e., the degree of γ_1 over $\mathbb{F}_q$ is 3. This completes the trivial case.

Now, let ω be a primitive cube root of unity in $\mathbb{F}_q$ and suppose that β_k and γ_k both have degree 3 over $\mathbb{F}_{q^{3^{k-1}}}$ for $1 \leq k \leq n$. Then $g(\beta_{n-1}, Y)$ is the minimum polynomial of

β_n over $\mathbb{F}_{q^{3^{n-1}}}$; and hence γ_{n-1} is not a cube in $\mathbb{F}_{q^{3^{n-1}}}$. In particular,

$$\gamma_{n-1}^{(q^{3^{n-1}}-1)/3} = \omega.$$

Observe that $G(\gamma_{n-1}, Y)$ is the minimum polynomial of γ_n over $\mathbb{F}_{q^{3^{n-1}}}$. Thus,

$$\begin{aligned}\gamma_n^{(q^{3^n}-1)/3} &= \left(\gamma_n^{\left(\left(q^{3^{n-1}}\right)^2+q^{3^{n-1}}+1\right)}\right)^{(q^{3^{n-1}}-1)/3} = (\mathrm{N}_{n,1}(\gamma_n))^{(q^{3^{n-1}}-1)/3}\\ &= (-729\gamma_{n-1})^{(q^{3^{n-1}}-1)/3} = \omega;\end{aligned}$$

i.e., β_{n+1} has degree 3 over $\mathbb{F}_{q^{3^n}}$. To prove that γ_{n+1} also has degree 3 over $\mathbb{F}_{q^{3^n}}$, write γ_{n+1} in terms of the $\mathbb{F}_{q^{3^n}}$-basis $\{1, \beta_{n+1}, \beta_{n+1}^2\}$, and proceed as we did for γ_1. □

An easy induction proof using the fact that $G(\gamma_{k-1}, Y)$ is the minimum polynomial of γ_k over $\mathbb{F}_{q^{3^{k-1}}}$ for $1 \le k \le n$, shows that

$$\mathrm{N}_{n,j}(\gamma_n) = (-729)^{(3^j-1)}\gamma_{n-j}$$

for $1 \le j \le n$.

Proposition 3.4.2. *The order of γ_n in $\mathbb{F}_{q^{3^n}}$ is greater than $3^{\frac{1}{2}n^2+\frac{3}{2}n+\mathrm{ord}_3(q-1)}$.*

Proof. We first compute the power of 3 dividing the order of γ_n. Recall from the proof of Proposition 3.4.1 that $\gamma_n^{(q^{3^n}-1)/3} \neq 1$. However, $\gamma_n^{(q^{3^n}-1)} = 1$ since $\gamma_n \in \mathbb{F}_{q^{3^n}}$. Since $q \equiv 1 \pmod 3$, $\mathrm{ord}_3((q^{3^j})^2 + q^{3^j} + 1) = 1$ for each $j \ge 1$. Repeatedly using the difference of cubes formula, we have

$$\begin{aligned}\mathrm{ord}_3\left(\frac{q^{3^n}-1}{3}\right) &= \mathrm{ord}_3(q-1) - 1 + \sum_{j=0}^{n-1}\mathrm{ord}_3\left(\left(q^{3^j}\right)^2 + q^{3^j} + 1\right)\\ &= n - 1 + \mathrm{ord}_3(q-1).\end{aligned}$$

Thus, $3^{n+\mathrm{ord}_3(q-1)}$ divides the order of γ by Fact 3.2.3.

Now, we look for primes dividing the order that are not equal to 3. In particular, we will show that the order of γ_n has a common factor with $((q^{3^{n-j}})^2 + q^{3^{n-j}} + 1)/3$ for each $1 \leq j \leq n$. This factor must not be a multiple of 3 since $\mathrm{ord}_3((q^{3^{n-j}})^2 + q^{3^{n-j}} + 1) = 1$ as noted above. By Lemma 3.2.4, with $\ell = 3$ and $b = q$, we see that these factors must be pairwise coprime as well. Hence, we get n distinct prime factors dividing the order of γ_n, none of which are equal to 3. By Lemma 3.2.5, each of these primes must be bounded below by 3^{n-j+1}. Hence, if we can show that the order of γ_n has a common factor with $((q^{3^{n-j}})^2 + q^{3^{n-j}} + 1)/3$ for $1 \leq j \leq n$, then we have that the order of γ_n is bounded below by

$$3^{n+\mathrm{ord}_3(q-1)} \prod_{j=1}^{n} 3^{n-j+1} \quad = \quad 3^{n+\mathrm{ord}_3(q-1)+n(n+1)/2} = 3^{\frac{n^2+3n}{2}+\mathrm{ord}_3(q-1)}.$$

By Fact 3.2.2, the proof will be complete when we show that the $\frac{q^{3^n}-1}{((q^{3^{n-j}})^2+q^{3^{n-j}}+1)/3}$ power of δ_n is not equal to 1 for $1 \leq j \leq n$. Now, δ_n raised to the $\frac{q^{3^n}-1}{((q^{3^{n-j}})^2+q^{3^{n-j}}+1)/3}$ power is equal to

$$(\mathrm{N}_{n,j-1}(\gamma_n))^{3(q^{3^{n-j}}-1)} = ((-729)^{(3^{(j-1)}-1)}\gamma_{n-j+1})^{3(q^{3^{n-j}}-1)} \neq 1$$

provided $\gamma_{n-j+1}^3 \notin \mathbb{F}_{q^{3^{n-j}}}$. From (3.8), we know that we may write γ_{n-j+1}^3 as

$$\gamma_{n-j+1}^3 = (270\gamma_{n-j} + 972\gamma_{n-j}^2 + 729\gamma_{n-j}^3)\gamma_{n-j+1}^2 + (972\gamma_{n-j} + 729\gamma_{n-j}^2)\gamma_{n-j+1} + 729\gamma_{n-j}.$$

Thus, $\gamma_{n-j+1}^3 \in \mathbb{F}_{q^{3^{n-j}}}$ if only if γ_{n-j} satisfies the system

$$\begin{aligned} 270\gamma_{n-j} + 972\gamma_{n-j}^2 + 729\gamma_{n-j}^3 &= 0, \\ 972\gamma_{n-j} + 729\gamma_{n-j}^2 &= 0. \end{aligned}$$

Suppose that γ_{n-j} does satisfy the above system. If the characteristic is 2, the first equation implies that $\gamma_{n-j} = 0$, which is a contradiction. Suppose then that the characteristic is not

2. Solving the system, we have $-3^{-2}(6+\sqrt{6}) = \gamma_{n-j} = -3^{-1}4$, where $\sqrt{6}$ may be any square root of 6. This leads to the conclusion that $30 = 0$. Hence, the characteristic must be 5. By Proposition 3.4.1, we see that $j = n$ since $\gamma_{n-j} = -3^{-1}4 \in \mathbb{F}_q$. However, this means that $\gamma_0 = 2$, which is in contradiction with the choice of β_0 since 2 is a perfect cube in this case. □

3.5 Comparison with a Recent Result of Voloch

The following is an improvement of a result of Voloch [Vol07, Sect. 5]. The proof is similar to the proof of the main theorem in [Vol07], but more elementary in the sense that we avoid working with algebraic function fields.

Theorem 3.5.1. *Let q be a prime power, and let $0 < \epsilon, \eta < 1$. For d sufficiently large, if $a \in \overline{\mathbb{F}}_q$ has order r and degree d over $\mathbb{F}_q$ with $r < d^{2-2\epsilon}$, then $a-1$ has order at least $\exp((1-\eta)\frac{2\epsilon}{3}d^{\epsilon/3}\log d)$. The degree d need only be large enough for the inequalities of* (3.9) *and* (3.10) *to hold, which depends only on the choices of ϵ and η.*

Proof. Let $0 < \epsilon < 1$ be given, and put $N := \lceil d^{1-\epsilon} \rceil$. Note that $(r, q) = 1$ since r divides one less than a power of q and q is a prime power. Also, note that the elements a^{q^i}, $0 \le i \le d-1$, are distinct. It follows that the multiplicative order of q modulo r is exactly d. For each coset Γ of $\langle q \rangle$ in $(\mathbb{Z}/r\mathbb{Z})^*$, we define $J_\Gamma := \{n \le N : n \mod r \in \Gamma\}$. Note that there are $[(\mathbb{Z}/r\mathbb{Z})^* : \langle q \rangle] = \phi(r)/d$ cosets of $\langle q \rangle$ in $(\mathbb{Z}/r\mathbb{Z})^*$. Now

$$\sum_{\Gamma} |J_\Gamma| = \#\{1 \le n \le N : \gcd(n, r) = 1\} = \frac{N\phi(r)}{r} + O(r^{\epsilon/10}),$$

where the sum is over all cosets of Γ in $(\mathbb{Z}/r\mathbb{Z})^*$. Thus, there exists a coset $\Gamma = \gamma\langle q \rangle$ such that $|J_\Gamma|$ is at least the average. That is, $|J_\Gamma| \ge \frac{Nd}{r} + O(dr^{\epsilon/10}/\phi(r))$. Thus, there exists a positive constant c_ϵ so that $|J_\Gamma| \ge \frac{Nd}{r} - c_\epsilon \frac{dr^{\epsilon/10}}{\phi(r)} \ge d^\epsilon - c_\epsilon d^{\frac{\epsilon-\epsilon^2}{5}}$ since $d \le \phi(r)$.

Since γ is coprime to r, write $\alpha\gamma + \beta r = 1$ and take $c = a^\alpha$. Then $a = c^\gamma$, and c has order r and degree at least d. Let $b := a - 1$. For each $n \in J_\Gamma$, there exists j_n such that

$n \equiv \gamma q^{j_n} \pmod{r}$. Whence $c^n = c^{\gamma q^{j_n}} = a^{q^{j_n}}$, and so $b^{q^{j_n}} = a^{q^{j_n}} - 1 = c^n - 1$.

Now, for every $I \subset J_\Gamma$ we write $b_I := \prod_{n \in I}(c^n - 1) = \prod_{n_j \in I} b^{q^{n_j}}$ which is a power of b. Put $T = \left[d^{\epsilon/3}\right]$, and observe that for d sufficiently large

$$NT = \left\lceil d^{1-\epsilon} \right\rceil \left[d^{\epsilon/3}\right] < d. \tag{3.9}$$

We claim that for all distinct $I, I' \subset J_\Gamma$ with $|I| = |I'| = T$ we have that $b_I \neq b_{I'}$. Suppose that $b_I = b_{I'}$, and consider the non-zero polynomial

$$p(t) = \prod_{n \in I}(t^n - 1) - \prod_{n \in I'}(t^n - 1).$$

Observe that $p(c) = b_I - b_{I'} = 0$, and so $\deg p(t) \geq \deg_{\mathbb{F}_q} c \geq d$. On the other hand, we have that $\deg p(t) \leq NT < d$, a contradiction. Thus $b_I \neq b_{I'}$ as claimed.

It follows that there are at least $\binom{|J_\Gamma|}{T}$ distinct powers of b. Choose $0 < \eta < 1$. Then, for d sufficiently large,

$$\begin{aligned}\binom{|J_\Gamma|}{T} &\geq \left(\frac{|J_\Gamma|}{d^{\epsilon/3}} - 1\right)^{d^{\epsilon/3}} \geq \left(d^{2\epsilon/3} - c_\epsilon d^{-\frac{\epsilon(2+3\epsilon)}{15}} - 1\right)^{d^{\epsilon/3}} \\ &\geq \exp\left((1-\eta)\frac{2\epsilon}{3} d^{\epsilon/3} \log d\right),\end{aligned} \tag{3.10}$$

as required. □

In order to compare this result to Theorem 3.1.1, one may choose $a = a_n$ to be a primitive 2^n-th root of unity in $\overline{\mathbb{F}}_q$. The degree of a over $\mathbb{F}_q$ will be $2^{n - \mathrm{ord}_2(q-1)}$. Then, for n sufficiently large, the conditions of the above theorem will be satisfied. Similarly, one may choose a to be a primitive 3^n-th root of unity in $\overline{\mathbb{F}}_q$ to compare with Theorem 3.1.2.

Because of the requirement that a must have low order relative to its degree, there are many fields in which Theorem 3.5.1 will not apply. Furthermore, one may check that even though the bound of Theorem 3.5.1 will eventually dominate the bounds of Theorems 3.1.1 and 3.1.2, there will always be a range (in terms of n) in which the bounds of Theorems 3.1.1

and 3.1.2 will be larger. For example, suppose we apply Theorem 3.5.1 to the case mentioned above, and we maximize the bound of Theorem 3.5.1 by setting $\epsilon = 1$ and $\eta = 0$. Further, suppose we minimize the bound of Theorem 3.1.1 by say assuming that $\operatorname{ord}_2(q-1) = 1$. Note that this will also serve to maximize the bound of Theorem 3.5.1. Under these assumptions, we may check that the bound of Theorem 3.1.1 will dominate for $n \leq 11$. However, we note that Theorem 3.5.1 does not actually apply if we choose $\epsilon = 1$ and $\eta = 0$; and the range of n for which Theorem 3.1.1 will dominate will be larger for any appropriate choice of ϵ and η.

3.6 Examples of Theorems

In this section we provide the data from the first several iterations for five examples of the main theorems: three for Theorem 3.1.1 and two for Theorem 3.1.2. The tables in this section provide information about the orders of α_n, β_n, δ_n, and γ_n in relation to our bound. We have chosen to take logs of these numbers because of their size. For each example, we note that the actual orders are much higher than our lower bounds. Computations were aided by MAGMA [BCP97].

As our first example of Theorem 3.1.1, we choose $q = 5$ and $\alpha_0 = 2$. See Table 3.1 on page 71. For our second example of Theorem 3.1.1, we choose $q = 9$ and $\alpha_0 = \zeta + 2$, where ζ is a root of $x^2 + 1$. Note that, in this example, δ_n is actually primitive for each of the first eight iterations. See Table 3.2. For our final example of Theorem 3.1.1, we choose $q = 121$ and $\alpha_0 = \eta^8$, where η is a root of $x^2 + 7x + 2$. Here, δ_n is primitive except for $n = 3$ and $n = 7$. See Table 3.3.

We also compute two examples of Theorem 3.1.2. For our first example of Theorem 3.1.2, we choose $q = 7$ and $\beta_0 = 3$. In this example, γ_n appears to alternate between being primitive and not. See Table 3.4 on page 72. For our second example of Theorem 3.1.2, we choose $q = 16$ and $\beta_0 = \xi$, where ξ is a root of $x^4 + x + 1$. Note that here γ_n is primitive for each of the first five iterations. See Table 3.5.

Table 3.1: Theorem 3.1.1: $q = 5$; $\alpha_0 = 2$.

n	$\log_2 \left\lvert \mathbb{F}^*_{5^{2^n}} \right\rvert$	$\log_2 \lvert\langle \alpha_n \rangle\rvert$	$\log_2 \lvert\langle \delta_n \rangle\rvert$	$\log_2 \left(2^{\frac{1}{2}n^2+\frac{3}{2}n+1} \right)$
1	4.59	4.59	3.00	3.00
2	9.28	9.28	7.70	6.00
3	18.6	16.0	17.0	10.0
4	37.1	35.6	31.5	15.0
5	74.2	69.8	68.6	21.0
6	148.	148.	143.	28.0
7	297.	295.	292.	36.0
8	594.	590.	589.	45.0

Table 3.2: Theorem 3.1.1: $q = 9$; $\alpha_0 = \zeta + 2$.

n	$\log_2 \left\lvert \mathbb{F}^*_{9^{2^n}} \right\rvert$	$\log_2 \lvert\langle \alpha_n \rangle\rvert$	$\log_2 \lvert\langle \delta_n \rangle\rvert$	$\log_2 \left(2^{\frac{1}{2}n^2+\frac{3}{2}n+3} \right)$
1	6.32	5.32	6.32	5.00
2	12.7	10.7	12.7	8.00
3	25.4	22.4	25.4	12.0
4	50.8	46.8	50.8	17.0
5	102.	96.5	102.	23.0
6	203.	197.	203.	30.0
7	406.	399.	406.	38.0
8	812.	804.	812.	47.0

Table 3.3: Theorem 3.1.1: $q = 121$; $\alpha_0 = \eta^8$.

n	$\log_2 \left\lvert \mathbb{F}^*_{121^{2^n}} \right\rvert$	$\log_2 \lvert\langle \alpha_n \rangle\rvert$	$\log_2 \lvert\langle \delta_n \rangle\rvert$	$\log_2 \left(2^{\frac{1}{2}n^2+\frac{3}{2}n+3} \right)$
1	13.8	11.8	13.8	5.00
2	27.7	26.7	27.7	8.00
3	55.4	50.8	53.0	12.0
4	111.	109.	111.	17.0
5	222.	216.	222.	23.0
6	443.	440.	443.	30.0
7	886.	874.	883.	38.0

Table 3.4: Theorem 3.1.2: $q = 7$; $\beta_0 = 3$.

n	$\log_2 \left\lvert \mathbb{F}^*_{7^{3^n}} \right\rvert$	$\log_2 \lvert\langle\beta_n\rangle\rvert$	$\log_2 \lvert\langle\gamma_n\rangle\rvert$	$\log_2 \left(3^{\frac{1}{2}n^2+\frac{3}{2}n+1}\right)$
1	8.42	7.41	5.84	4.76
2	25.3	25.3	25.3	9.52
3	75.8	75.8	74.2	15.8
4	228.	228.	228.	23.8
5	682.	681.	681.	33.3

Table 3.5: Theorem 3.1.2: $q = 16$; $\beta_0 = \xi$.

n	$\log_2 \left\lvert \mathbb{F}^*_{16^{3^n}} \right\rvert$	$\log_2 \lvert\langle\beta_n\rangle\rvert$	$\log_2 \lvert\langle\gamma_n\rangle\rvert$	$\log_2 \left(3^{\frac{1}{2}n^2+\frac{3}{2}n+1}\right)$
1	12.0	8.83	12.0	4.76
2	36.0	31.2	36.0	9.52
3	108.	102.	108.	15.8
4	324.	316.	324.	23.8
5	972.	962.	972.	33.3

Chapter 4

The Mean Square Error for the Chebotarëv Density Theorem in Cyclotomic Extensions

With some slight alteration, the results contained within this chapter also appear in [Smib] and [Smia].

4.1 The Barban-Davenport-Halberstam Theorem

The mean square error for Dirichlet's Theorem on primes in arithmetic progressions was first studied by Barban [Bar64] and by Davenport and Halberstam [DH66, DH68]. Bounds such as the following are usually referred to as the Barban-Davenport-Halberstam Theorem, although this particular refinement is attributed to Gallagher. See [Dav80, p. 169].

Theorem 4.1.1. *Let*

$$\psi(x;q,a) := \sum_{\substack{p^m \leq x \\ p^m \equiv a \pmod q}} \log p.$$

Then, for fixed $M > 0$,

$$\sum_{q \le Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left(\psi(x; q, a) - \frac{x}{\varphi(q)} \right)^2 \ll xQ \log x \tag{4.1}$$

if $x(\log x)^{-M} \le Q \le x$.

Here φ is the Euler totient function. In light of the relationship between Dirichlet's Theorem and Chebotarëv's Theorem, the sum on the left of (4.1) may also be viewed as the mean square error in the Chebotarëv Density Theorem when averaging over cyclotomic extensions of $\mathbb{Q}$.

Theorem 4.1.1 was later refined by Montgomery [Mon70] and Hooley [Hoo75] who gave asymptotic formulae for the mean square error sum. See also Theorem 1 of [Cro75]. For recent work in this direction, see [Liu08].

In this chapter, we will concern ourselves with generalizations of the result to the setting of number fields. Number field versions of the result already appear in the literature. For example, Wilson [Wil69] considered mean square error sums for estimating the number of prime ideals falling into a given class of the narrow ideal class group. In [Hin81], Hinz considered mean square error sums for estimating the number of principal prime ideals given by a generator that is congruent to a given algebraic integer modulo an integral ideal and whose conjugates fall into some designated range. Our generalization will be a more straightforward one and will be a key ingredient in the proof of Theorem 5.1.2 in Chapter 5. We will also prove an asymptotic version of the result by an adaption of the methods in [Hoo75].

4.2 A Generalization for Number Fields

Let K be a fixed algebraic number field. Further assume K is normal over $\mathbb{Q}$. We generalize Theorem 4.1.1 by considering the mean square error for the Chebotarëv Density Theorem when averaging over cyclotomic extensions of K. That is, we consider the error in estimating sums of the form

$$\psi_K(x;q,a) := \sum_{\substack{\mathrm{N}\mathfrak{p}^m \le x \\ \mathrm{N}\mathfrak{p}^m \equiv a \pmod q}} \log \mathrm{N}\mathfrak{p},$$

or equivalently, sums of the form

$$\theta_K(x;q,a) := \sum_{\substack{\mathrm{N}\mathfrak{p} \le x \\ \mathrm{N}\mathfrak{p} \equiv a \pmod q}} \log \mathrm{N}\mathfrak{p}.$$

For each $q \in \mathbb{N}$, we put $A_q := K \cap \mathbb{Q}(\zeta_q)$. Then A_q is an Abelian (possibly trivial) extension of $\mathbb{Q}$. Further, we let G_q denote the image of the map

$$\mathrm{Gal}(K(\zeta_q)/K) \hookrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/q\mathbb{Z})^*. \tag{4.2}$$

Whence $G_q \cong \mathrm{Gal}(K(\zeta_q)/K) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_q)/A_q)$.

$$\begin{tikzcd}
 & K(\zeta_q) \arrow[dl, dash] \arrow[dr, dash, "G_q"] & \\
\mathbb{Q}(\zeta_q) \arrow[dr, dash, "G_q"] \arrow[ddr, dash, "(\mathbb{Z}/q\mathbb{Z})^*"'] & & K \arrow[dl, dash] \\
 & A_q \arrow[d, dash] & \\
 & \mathbb{Q} &
\end{tikzcd} \tag{4.3}$$

We make the definition $\varphi_K(q) := |G_q|$. By the Chebotarëv Density Theorem, for each $a \in G_q$,

$$\theta_K(x;q,a) \sim \frac{x}{\varphi_K(q)}. \tag{4.4}$$

In fact, we have the following corollary of Goldstein's generalization of the Siegel-Walfisz

Theorem [Gol70]. For any $M > 0$,

$$\theta_K(x; q, a) = \frac{x}{\varphi_K(q)} + O\left(\frac{x}{(\log x)^M}\right) \tag{4.5}$$

provided that $q \leq (\log x)^M$. For example, see Lemma 4.2.7 below, and follow the standard proof of the classical Siegel-Walfisz Theorem for example.

Theorem 4.2.1. *For any fixed $M > 0$,*

$$\sum_{q \leq Q} \sum_{a \in G_q} \left(\theta_K(x; q, a) - \frac{x}{\varphi_K(q)}\right)^2 \ll xQ \log x$$

if $x(\log x)^{-M} \leq Q \leq x$.

Remark 4.2.2. In [Smib], Theorem 4.2.1 is presented with $\theta_K(x; q, a)$ replaced by $\psi_K(x; q, a)$. The theorem also holds for

$$\theta_{K,1}(x; q, a) := \sum_{\substack{\mathrm{N}\mathfrak{p} \leq x \\ \deg \mathfrak{p} = 1 \\ \mathrm{N}\mathfrak{p} \equiv a \pmod q}} \log \mathrm{N}\mathfrak{p} \tag{4.6}$$

as well, which is the version we will apply in Chapter 5.

Remark 4.2.3. The method of proof is essentially an adaptation of the proof of Theorem 4.1.1 given in [Dav80, pp. 169-171], the main idea being an application of the large sieve.

Remark 4.2.4. As another application of Theorem 4.2.1, we prove asymptotic formulae for the mean square error in Section 4.3. See Theorem 4.3.1 on page 83.

4.2.1 Application of the Large Sieve and Other Preliminary Estimates

Let $\mathcal{X}(q)$ denote the character group modulo q, let $\mathcal{X}^*(q)$ denote the characters which are primitive modulo q, and let $G_q^\perp$ denote the subgroup of characters that are trivial on G_q. Then the character group $\widehat{G_q}$ is isomorphic to $\mathcal{X}(q)/G_q^\perp$, and the number of such characters is $\varphi_K(q) = |G_q| = \varphi(q)/|G_q^\perp|$. As usual, we denote the trivial character of the group $\mathcal{X}(q)$ by χ_0.

For any Hecke character ξ on the ideals of $\mathcal{O}_K$, we define

$$\begin{aligned}\theta_K(x,\xi) &:= \sum_{\mathrm{N}\mathfrak{p}\le x} \xi(\mathfrak{p}) \log \mathrm{N}\mathfrak{p},\\ \psi_K(x,\xi) &:= \sum_{\mathrm{N}\mathfrak{p}^m\le x} \xi(\mathfrak{p}) \log \mathrm{N}\mathfrak{p};\end{aligned}$$

and for any Dirichlet character $\chi \in \mathcal{X}(q)$, we also define

$$\theta'_K(x,\chi\circ \mathrm{N}) := \begin{cases} \theta_K(x,\chi\circ\mathrm{N}), & \chi \not\equiv \chi_0 \pmod{G_q^\perp},\\ \theta_K(x,\chi\circ\mathrm{N}) - x, & \chi \equiv \chi_0 \pmod{G_q^\perp}.\end{cases}$$

$$\psi'_K(x,\chi\circ \mathrm{N}) := \begin{cases} \psi_K(x,\chi\circ\mathrm{N}), & \chi \not\equiv \chi_0 \pmod{G_q^\perp},\\ \psi_K(x,\chi\circ\mathrm{N}) - x, & \chi \equiv \chi_0 \pmod{G_q^\perp}.\end{cases}$$

Lemma 4.2.5.

$$\sum_{q\le Q} \frac{q}{\varphi(q)} \sum_{\chi\in\mathcal{X}^*(q)} |\theta_K(x,\chi\circ\mathrm{N})|^2 \ll (x+Q^2)x\log x.$$

Proof. First, note that

$$\theta_K(x,\chi\circ\mathrm{N}) = \sum_{\mathrm{N}\mathfrak{p}\le x} \chi(\mathrm{N}\mathfrak{p})\log \mathrm{N}\mathfrak{p} = \sum_{p^{f_p}\le x} \chi(p^{f_p}) f_p g_p \log p.$$

We apply the large sieve [Dav80, Thm. 4, p. 160] to see that

$$\begin{aligned}\sum_{q\le Q} \frac{q}{\varphi(q)} \sum_{\chi\in\mathcal{X}^*(q)} |\theta_K(x,\chi\circ\mathrm{N})|^2 &\ll (x+Q^2)\sum_{p^{f_p}\le x} (f_p g_p \log p)^2\\ &= (x+Q^2) g_p \sum_{p^{f_p}\le x} g_p \left(\log p^{f_p}\right)^2\\ &\ll (x+Q^2)\sum_{\mathrm{N}\mathfrak{p}\le x} (\log \mathrm{N}\mathfrak{p})^2\\ &\ll (x+Q^2)x\log x.\end{aligned}$$

□

Lemma 4.2.6. *If ξ_1 and ξ_2 are Hecke characters modulo $\mathfrak{q}_1$ and $\mathfrak{q}_2$ respectively, and if ξ_1 induces ξ_2, then*

$$\theta_K(x,\xi_2) = \theta_K(x,\xi_1) + O\left(\log q\right),$$

where $(q) = \mathfrak{q}_2 \cap \mathbb{Z}$.

Proof.

$$|\theta_K(x,\xi_1) - \theta_K(x,\xi_2)| = \left| \sum_{\substack{\mathrm{N}\mathfrak{p}\leq x \\ \mathfrak{p}|\mathfrak{q}_2}} \xi_1(\mathfrak{p}) \log \mathrm{N}\mathfrak{p} \right| \leq \sum_{\substack{p^{f_p}\leq x \\ p|q}} f_p g_p \log p \ll \log q.$$

□

Lemma 4.2.7. *For any fixed $M > 0$, if χ is a character modulo $q \leq (\log x)^M$, then there exists a positive constant $C = C_M$ (depending on M) such that*

$$\theta'_K(x, \chi\circ \mathrm{N}) \ll x \exp\left\{-C\sqrt{\log x}\right\}.$$

Proof. As a Hecke character on the ideals of $\mathcal{O}_K$, $\chi \circ \mathrm{N}$ may not be primitive modulo $q\mathcal{O}_K$. Let $\xi = \xi_\chi$ be the primitive Hecke character which induces $\chi\circ\mathrm{N}$, and let $\mathfrak{f}_\chi$ be its conductor. Write $s = \sigma + it$. By [IK04, Thm. 5.35, p. 129], there exists an effective constant $c_0 > 0$ such that the Hecke L-function $L(s,\xi) := \sum_{\mathrm{N}\mathfrak{a}\leq x} \xi(\mathfrak{a})(\mathrm{N}\mathfrak{a})^{-s}$ has at most one zero in the region

$$\sigma > 1 - \frac{c_0}{[K:\mathbb{Q}] \log\left(|\Delta_K| \mathrm{N}\mathfrak{f}(|t|+3)\right)}, \tag{4.7}$$

where Δ_K denotes the discriminant of the number field. Further, if such a zero exists, it is real and simple. In the case that such a zero exists, we call it an "exceptional zero" and denote it by β_ξ. Thus, by [IK04, Thm. 5.13, p. 111], there exists $c_1 > 0$ such that

$$\psi_K(x,\xi) = \delta_\xi x - \frac{x^{\beta_\xi}}{\beta_\xi} + O\left(x \exp\left\{ \frac{-c_1 \log x}{\sqrt{\log x} + \log \mathrm{N}\mathfrak{f}_\chi} \right\} (\log(x\mathrm{N}\mathfrak{f}_\chi))^4 \right),$$

where

$$\delta_\xi = \begin{cases} 1, & \xi \text{ trivial}, \\ 0, & \text{otherwise}, \end{cases}$$

and the term x^{β_ξ}/β_ξ is omitted if the L-function $L(s,\xi)$ has no exceptional zero in the region (4.7). Now, since $\mathfrak{f}_\chi | q\mathcal{O}_K$ and $q \le (\log x)^M$, we have the following bound on the error term:

$$x \exp\left\{ \frac{-c_1 \log x}{\sqrt{\log x} + \log \mathrm{N}\mathfrak{f}_\chi} \right\} (\log(x\mathrm{N}\mathfrak{f}_\chi))^4 \ll x \exp\left\{ -c_2 \sqrt{\log x} \right\}$$

for some positive constant c_2.

By [Gol70, Thm. 3.3.2], we see that for every $\epsilon > 0$, there exists a constant $c_\epsilon > 0$ such that if β_ξ is an exceptional zero for $L(s,\xi)$, then

$$\beta_\xi < 1 - \frac{c_\epsilon}{(\mathrm{N}\mathfrak{f}_\chi)^\epsilon} \le 1 - \frac{c_\epsilon}{q^{[K:\mathbb{Q}]\epsilon}}.$$

Thus,

$$x^{\beta_\xi} < x \exp\left\{ -c_\epsilon (\log x) q^{-[K:\mathbb{Q}]\epsilon} \right\} < x \exp\left\{ -c_\epsilon (\log x)^{1/2} \right\}$$

upon choosing ϵ so that $[K:\mathbb{Q}]\epsilon = (2M)^{-1}$. Whence, for $q \le (\log x)^M$, there exists $C > 0$ such that

$$\psi_K(x,\xi) = \delta_\xi x + O\left(x \exp\left\{ -C\sqrt{\log x} \right\} \right).$$

Since

$$\theta_K(x,\xi) = \psi_K(x,\xi) + O(\sqrt{x}),$$

we also have

$$\theta_K(x,\xi) = \delta_\xi x + O\left(x \exp\left\{ -C\sqrt{\log x} \right\} \right).$$

Therefore, by Lemma 4.2.6,

$$\theta'_K(x, \chi \circ \mathrm{N}) \ll x \exp\left\{-C\sqrt{\log x}\right\}$$

for $q \leq (\log x)^M$. □

4.2.2 Proof of the Mean Square Error Bound

We now present the proof of the mean square error bound of Theorem 4.2.1.

Proof of Theorem 4.2.1. For each $a \in G_q$, we denote the error term by

$$E_K(x; q, a) := \theta_K(x; q, a) - \frac{x}{\varphi_K(q)}, \tag{4.8}$$

and note that

$$E_K(x; q, a) = \frac{1}{\varphi_K(q)} \sum_{\chi \in \widehat{G_q}} \bar{\chi}(a)\theta'_K(x, \chi \circ \mathrm{N}).$$

Now we form the square of the Euclidean norm and sum over all $a \in G_q$ to see

$$\begin{aligned}
\sum_{a \in G_q} |E_K(x; q, a)|^2 &= \frac{1}{\varphi_K(q)^2} \sum_{a \in G_q} \left| \sum_{\chi \in \widehat{G_q}} \bar{\chi}(a)\theta'_K(x, \chi \circ \mathrm{N}) \right|^2 \\
&= \frac{1}{\varphi_K(q)^2} \sum_{a \in G_q} \sum_{\chi_1 \in \widehat{G_q}} \sum_{\chi_2 \in \widehat{G_q}} \bar{\chi}_1(a)\chi_2(a)\theta'_K(x, \chi_1 \circ \mathrm{N})\overline{\theta'_K(x, \chi_2 \circ \mathrm{N})} \\
&= \frac{1}{\varphi_K(q)} \sum_{\chi \in \widehat{G_q}} \left|\theta'_K(x, \chi \circ \mathrm{N})\right|^2 \\
&= \frac{1}{\varphi(q)} \sum_{\chi \in \mathcal{X}(q)} \left|\theta'_K(x, \chi \circ \mathrm{N})\right|^2.
\end{aligned} \tag{4.9}$$

For each $\chi \in \mathcal{X}(q)$, we let χ_* denote the primitive character which induces χ. By Lemma 4.2.6, we have $\theta'_K(x, \chi \circ \mathrm{N}) = \theta'_K(x, \chi_* \circ \mathrm{N}) + O(\log q)$. Hence, summing over $q \leq Q$ and exchanging each character for its primitive version, we have

$$\begin{aligned}\sum_{q\le Q}\sum_{a\in G_q} E_K(x;q,a)^2 &\ll \sum_{q\le Q}(\log q)^2 + \sum_{q\le Q}\frac{1}{\varphi(q)}\sum_{\chi\in\mathcal{X}(q)}|\theta_K'(x,\chi_*\circ\mathrm{N})|^2\\ &\ll Q(\log Q)^2 + \sum_{q\le Q}\frac{1}{\varphi(q)}\sum_{\chi\in\mathcal{X}(q)}|\theta_K'(x,\chi_*\circ\mathrm{N})|^2.\end{aligned}$$

The first term on the right is clearly smaller than $xQ\log x$, so we concentrate on the second. Now,

$$\begin{aligned}\sum_{q\le Q}\frac{1}{\varphi(q)}\sum_{\chi\in\mathcal{X}(q)}|\theta_K'(x,\chi_*\circ\mathrm{N})|^2 &= \sum_{q\le Q}\sum_{\chi\in\mathcal{X}^*(q)}|\theta_K'(x,\chi\circ\mathrm{N})|^2\sum_{k\le Q/q}\frac{1}{\varphi(kq)}\\ &\ll \sum_{q\le Q}\frac{1}{\varphi(q)}\left(\log\frac{2Q}{q}\right)\sum_{\chi\in\mathcal{X}^*(q)}|\theta_K'(x,\chi\circ\mathrm{N})|^2\end{aligned}\tag{4.10}$$

since $\sum_{k\le Q/q}1/\varphi(kq)\ll\varphi(q)^{-1}\log(2Q/q)$. See [Dav80, p. 170]. The proof will be complete once we show that (4.10) is smaller than $xQ\log x$ for Q in the specified range.

As with the proof of Theorem 4.1.1 in [Dav80, pp. 169-171], we consider large and small q separately. We start with the large values. Since $\theta_K'(x,\chi\circ\mathrm{N})\ll\theta_K(x,\chi\circ\mathrm{N})$, by Lemma 4.2.5, we have

$$\sum_{U<q\le 2U}\frac{U}{\varphi(q)}\sum_{\chi\in\mathcal{X}^*(q)}|\theta_K'(x,\chi\circ\mathrm{N})|^2 \quad\ll\quad (x+U^2)x\log x,$$

which implies

$$\sum_{U\le q\le 2U}\frac{1}{\varphi(q)}\left(\log\frac{2Q}{q}\right)\sum_{\chi\in\mathcal{X}^*(q)}|\theta_K'(x,\chi\circ\mathrm{N})|^2\ll(xU^{-1}+U)x\log x\left(\log\frac{2Q}{U}\right)$$

for $1 \leq 2U \leq Q$. Summing over $U = Q2^{-k}$, we have

$$\begin{aligned}\sum_{Q_1<q\leq Q} \frac{1}{\varphi(q)} \left(\log \frac{2Q}{q}\right) \sum_{\chi\in\mathcal{X}^*(q)} |\theta'_K(x,\chi\circ\mathrm{N})|^2 &\ll x\log x \sum_{k=1}^{\left\lfloor \frac{\log(Q/Q_1)}{\log 2}\right\rfloor} (x2^kQ^{-1} + Q2^{-k}) \\ &\ll x^2Q_1^{-1}(\log x)\log Q + xQ\log x \\ &\ll xQ\log x \qquad (4.11)\end{aligned}$$

if $x(\log x)^{-M} \leq Q \leq x$ and $Q_1 = (\log x)^{M+1}$.

We now turn to the small values of q. Applying Lemma 4.2.7, we have

$$\begin{aligned}\sum_{q\leq Q_1} \frac{1}{\varphi(q)} \left(\log \frac{2Q}{q}\right) \sum_{\chi\in\mathcal{X}^*(q)} |\theta'_K(x,\chi\circ\mathrm{N})|^2 &\ll Q_1(\log Q)\left(x\exp\left\{-C\sqrt{\log x}\right\}\right)^2 \\ &\ll x^2(\log x)^{-M} \ll xQ\log x. \qquad (4.12)\end{aligned}$$

Combining (4.11) and (4.12), the theorem follows. □

4.2.3 Comparison with GRH

Using the bound on the analytic conductor of the L-function $L(s,\chi\circ\mathrm{N})$ given in [IK04, p. 129], GRH implies

$$\begin{aligned}\sum_{q\leq Q}\sum_{a\in G_q} E_K(x;q,a)^2 &= \sum_{q\leq Q} \frac{1}{\varphi(q)} \sum_{\chi\in\mathcal{X}(q)} \left|\theta'_K(x,\chi\circ\mathrm{N})\right|^2 \\ &\ll (\sqrt{x}(\log x)^2)^2 \sum_{q\leq Q}\frac{1}{\varphi(q)} \sum_{\chi\in\mathcal{X}(q)} 1 \\ &= xQ(\log x)^4.\end{aligned}$$

See [IK04, Thm. 5.15, p. 114] for this implication of GRH.

4.3 An Asymptotic Formula for the Mean Square Error

The remainder of this chapter will be dedicated to proving the following more refined version of Theorem 4.2.1.

Theorem 4.3.1. *For any fixed $M > 0$,*

$$\sum_{q \le x} \sum_{a \in G_q} \left(\theta_K(x; q, a) - \frac{x}{\varphi_K(q)} \right)^2 = [K : \mathbb{Q}] x^2 \log x + D_1 x^2 + O\left(\frac{x^2}{(\log x)^M} \right); \qquad (4.13)$$

and if $1 \le Q \le x$,

$$\sum_{q \le Q} \sum_{a \in G_q} \left(\theta_K(x; q, a) - \frac{x}{\varphi_K(q)} \right)^2 = [K : \mathbb{Q}] x Q \log x - \frac{\varphi(m_K)}{\varphi_K(m_K)} x Q \log(x/Q) + D_2 Q x + O\left(x^{3/4} Q^{5/4} + \frac{x^2}{(\log x)^M} \right), \qquad (4.14)$$

where D_1, D_2 are constants and m_K is an integer defined in the first paragraph of Section 4.3.1.

Remark 4.3.2. The constants D_1, D_2 appearing in the statement of the theorem depend on K and may be given explicitly. However, the expressions are somewhat messy. For example, D_1 is given by

$$D_1 = F(1)\zeta'(2) + F(1)\frac{(2\gamma - 3)\pi^2}{12} + F(1)F'(1)\frac{\pi^2}{6} - [K : \mathbb{Q}].$$

Here, $\zeta(s)$ denotes the Riemann zeta function, $\gamma \approx 0.577$ is the Euler-Mascheroni constant, and $F(s) := h(s) \prod_{\ell | m_K} G_{K,\ell}(s)$. The functions $h(s)$ and $G_{K,\ell}(s)$ are described in Section 4.3.1.

Remark 4.3.3. In the case that $K/\mathbb{Q}$ is Abelian, it turns out that $\frac{\varphi(m_K)}{\varphi_K(m_K)} = [K : \mathbb{Q}]$. See the first paragraph of Section 4.3.1. Thus, in this case, equation (4.14) simplifies to

$$\sum_{q\le Q}\sum_{a\in G_q}\left(\theta_K(x;q,a)-\frac{x}{\varphi_K(q)}\right)^2=[K:\mathbb{Q}]xQ\log Q+D_2Qx+O\left(x^{3/4}Q^{5/4}+\frac{x^2}{(\log x)^M}\right).$$

Our proof of Theorem 4.3.1 very closely follows Hooley's proof of the theorem for the case $K=\mathbb{Q}$. See [Hoo75, pp. 209-212]. The proof will be carried out in Section 4.3.2.

4.3.1 Analysis of the Arithmetic Function $\varphi_K(q)$

Before proceeding with the proof of Theorem 4.3.1, we first analyze the arithmetic function $\varphi_K(q)$. Let $\mathbb{Q}^{\text{cyc}} := \bigcup_{q>1}\mathbb{Q}(\zeta_q)$, and let $\mathcal{A} := \mathbb{Q}^{\text{cyc}}\cap K$. Then $\mathcal{A}$ is an Abelian extension of $\mathbb{Q}$ of finite degree. In particular, $\mathcal{A}$ is the maximal Abelian subfield of K. By the Kronecker-Weber Theorem, there exists a smallest integer m_K such that $\mathcal{A}\subseteq\mathbb{Q}(\zeta_{m_K})$ See, for example, [Lan94, p. 210]. Recall that for each integer $q>0$, we defined the intersection field $A_q = K\cap\mathbb{Q}(\zeta_q)$. Whence, via restriction maps, $\text{Gal}(K(\zeta_q)/K)\cong\text{Gal}(\mathbb{Q}(\zeta_q)/A_q)$. See the field diagram (4.3). Thus, it is clear that if q is coprime to m_K, then $\varphi_K(q)=\varphi(q)$. In any case, $\varphi_K(q)$ is multiplicative and divides $\varphi(q)$. For each prime divisor ℓ of m_K, we make the definition $b_\ell := \text{ord}_\ell(m_K)$.

Lemma 4.3.4. *For a prime ℓ, $\varphi_K(\ell)$ is a divisor of $\ell-1$. In general, we have*

$$\varphi_K(q)=\prod_{\substack{\ell^\alpha\|q\\ \ell\nmid m_K}}\ell^{\alpha-1}(\ell-1)\prod_{\substack{\ell^\alpha\|q\\ \ell\mid m_K\\ \alpha\ge b_\ell}}\ell^{\alpha-b_\ell}\varphi_K(\ell)\prod_{\substack{\ell^\alpha\|q\\ \ell\mid m_K\\ \alpha<b_\ell}}\varphi_K(\ell).$$

Proof. The first statement is trivial as G_q is a subgroup of $(\mathbb{Z}/q\mathbb{Z})^*$. Since $\varphi_K(q)$ is multiplicative and $\varphi_K(q)=\varphi(q)$ for $(q,m_K)=1$, we restrict attention to primes dividing m_K.

Suppose that ℓ is a prime dividing m_K. Then $A_{\ell^{b_\ell+k}}=A_{\ell^{b_\ell}}$ for all integers $k\ge 0$. Thus, we immediately see that

$$\varphi_K(\ell^{b_\ell+k})=|\text{Gal}(\mathbb{Q}(\zeta_{\ell^{b_\ell+k}})/\mathbb{Q}(\zeta_{\ell^{b_\ell}}))|\cdot|\text{Gal}(\mathbb{Q}(\zeta_{\ell^{b_\ell}})/A_{\ell^{b_\ell}})|=\ell^k\varphi_K(\ell^{b_\ell}). \tag{4.15}$$

We claim that

$$\varphi_K(\ell^j) = \varphi_K(\ell) \text{ for } 1 \leq j \leq b_\ell. \tag{4.16}$$

If $b_\ell = 1$, the statement is trivial. Assume then that $b_\ell \geq 2$, and consider the following field diagram.

$$\begin{tikzcd}
& \mathbb{Q}(\zeta_{\ell^{b_\ell}}) \arrow[dl, dash, "\ell^{b_\ell-1}"'] \arrow[dr, dash, "\varphi_K(\ell^{b_\ell})"] & \\
\mathbb{Q}(\zeta_\ell) \arrow[dr, dash, "\varphi_K(\ell)"'] & & A_{\ell^{b_\ell}} \arrow[dl, dash] \\
& A_\ell &
\end{tikzcd} \tag{4.17}$$

Observe that $A_\ell = K \cap \mathbb{Q}(\zeta_\ell) = A_{\ell^{b_\ell}} \cap \mathbb{Q}(\zeta_\ell)$. Since the compositum $A_{\ell^{b_\ell}}\mathbb{Q}(\zeta_\ell)$ is the smallest field containing both $A_{\ell^{b_\ell}}$ and $\mathbb{Q}(\zeta_\ell)$, we have that $\mathbb{Q}(\zeta_{\ell^{b_\ell}}) \supseteq A_{\ell^{b_\ell}}\mathbb{Q}(\zeta_\ell) \supseteq \mathbb{Q}(\zeta_\ell)$. The Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^{b_\ell}})/\mathbb{Q}(\zeta_\ell))$ is cyclic of order $\ell^{b_\ell-1}$. We deduce then that $A_{\ell^{b_\ell}}\mathbb{Q}(\zeta_\ell) = \mathbb{Q}(\zeta_{\ell^{j_0}})$ for some $1 \leq j_0 \leq b_\ell - 1$. However, since m_K is minimal, b_ℓ must be minimal as well. Therefore, we must have that $A_{\ell^{b_\ell}} \not\subseteq \mathbb{Q}(\zeta_{\ell^{b_\ell-1}})$. This implies that $A_{\ell^{b_\ell}}\mathbb{Q}(\zeta_\ell) = \mathbb{Q}(\zeta_{\ell^{b_\ell}})$. Thus, from the diagram (4.17), we see that $\varphi_K(\ell) = \varphi_K(\ell^{b_\ell})$. The claim in (4.16) follows since $\varphi_K(\ell^j)$ divides $\varphi_K(\ell^{j+1})$ for all $j \geq 1$. The lemma follows by combining (4.15) with (4.16). □

The final goal of this section is to study the Dirichlet generating function

$$G_K(s) := \sum_{n=1}^{\infty} \frac{1}{\varphi_K(n)n^{s-1}}$$

and use it to prove two asymptotic identities involving the function $\varphi_K(n)$. Since $\varphi_K(n)$ agrees with $\varphi(n)$ for $(n, m_K) = 1$, we begin with the Dirichlet series

$$G(s) := \sum_{n=1}^{\infty} \frac{1}{\varphi(n)n^{s-1}}$$

and introduce finitely many correction factors to obtain $G_K(s)$. Let $h(s)$ denote the Euler product

$$h(s) := \prod_{\ell} \left\{ 1 + \frac{1}{\ell^{s+2}} \left(1 - \frac{1}{\ell^s}\right) \left(1 - \frac{1}{\ell}\right)^{-1} \right\};$$

and observe that, for any $\epsilon > 0$, $h(s)$ is holomorphic and bounded for $\Re(s) > -\frac{1}{2} + \epsilon$. Using the product formula for Euler's φ function, we factor $G(s)$ as

$$G(s) = \prod_{\ell} \left\{ 1 + \frac{1}{\ell^s} \left(1 - \frac{1}{\ell}\right)^{-1} \left(1 - \frac{1}{\ell^s}\right)^{-1} \right\} = \zeta(s)\zeta(s+1)h(s), \tag{4.18}$$

where again $\zeta(s)$ is the Riemann zeta function.

We now return to the Dirichlet series $G_K(s)$. In light of (4.18) and Lemma 4.3.4, for each prime ℓ dividing m_K, we define the correction factor

$$G_{K,\ell}(s) := \frac{\left\{ 1 + \frac{1}{\varphi_K(\ell)\ell^{s-1}} \left(\frac{1 - \left(\frac{1}{\ell^{s-1}}\right)^{b_\ell - 1}}{1 - \frac{1}{\ell^{s-1}}} \right) + \frac{1}{\varphi_K(\ell)} \left(\frac{1}{\ell^{s-1}}\right)^{b_\ell} \left(1 - \frac{1}{\ell^s}\right)^{-1} \right\}}{\left\{ 1 + \frac{1}{\ell^s} \left(1 - \frac{1}{\ell}\right)^{-1} \left(1 - \frac{1}{\ell^s}\right)^{-1} \right\}},$$

which has removable singularities at $s = 0, 1$ and is analytic elsewhere. We also define $G_{K,\ell}(0)$ (resp. $G_{K,\ell}(1)$) to be the limit of $G_{K,\ell}(s)$ as s approaches 0 (resp. 1). In particular, we note that

$$G_{K,\ell}(0) = \lim_{s \to 0} G_{K,\ell}(s) = \frac{\varphi(\ell^{b_\ell})}{\varphi_K(\ell)} = \frac{\varphi(\ell^{b_\ell})}{\varphi_K(\ell^{b_\ell})}. \tag{4.19}$$

Finally, from (4.18), we observe that $G_K(s)$ may be factored as

$$G_K(s) = \zeta(s)\zeta(s+1)h(s) \prod_{\ell \mid m_K} G_{K,\ell}(s). \tag{4.20}$$

Lemma 4.3.5. *For a fixed number field K, we have*

$$\sum_{n<x} \left(1 - \frac{n}{x}\right)^2 \frac{1}{\varphi_K(n)} = C_1 \log x + C_2 + \frac{\varphi(m_K)}{\varphi_K(m_K)} \frac{\log x}{x} + \frac{C_3}{x} + O\left(x^{-\frac{5}{4}}\right); \tag{4.21}$$

$$\sum_{n \le x} \frac{1}{\varphi_K(n)} = C_1 \log x + C_4 + O\left(\frac{1}{x}\right), \tag{4.22}$$

where $C_1 = \frac{\zeta(2)\zeta(3)}{\zeta(6)} \prod_{\ell | m_K} G_{K,\ell}(1)$*, and* C_2, C_3, C_4 *are constants.*

Proof. We begin with the proof of (4.21). For $c > 0$,

$$\begin{aligned}\frac{1}{2}\sum_{n<x}\left(1-\frac{n}{x}\right)^2\frac{1}{\varphi_K(n)} &= \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} G_K(s+1)\frac{x^s}{s(s+1)(s+2)}ds \\ &= R_0 + R_{-1} + \frac{1}{2\pi i}\int_{-\frac{5}{4}-i\infty}^{-\frac{5}{4}+i\infty} G_K(s+1)\frac{x^s}{s(s+1)(s+2)}ds,\end{aligned}$$

where R_0 and R_{-1} are the residues of the integrand at $s = 0$ and $s = -1$ respectively. See [Mur01, Exercise 4.1.9, p. 57] for example. Using (4.20), we calculate the residues as follows:

$$\begin{aligned} R_0 &= \frac{\zeta(2)h(1)\prod_{\ell|m_K} G_{K,\ell}(1)}{2}\log x + \frac{1}{2}C_2 = \frac{C_1}{2}\log x + \frac{1}{2}C_2; \\ R_{-1} &= \frac{-\zeta(0)h(0)\prod_{\ell|m_K} G_{K,\ell}(0)\log x}{x} + \frac{C_3}{2x} = \frac{\varphi(m_K)}{\varphi_K(m_K)}\frac{\log x}{2x} + \frac{C_3}{2x}, \end{aligned}$$

where we have applied (4.19) to compute $\prod_{\ell|m_K} G_{K,\ell}(0)$ The remaining integral is clearly $O(x^{-5/4})$.

For the proof of (4.22), we begin with the formula

$$\sum_{n\le x}\frac{1}{\varphi_K(n)} = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} G_K(s+1)\frac{x^s}{s}ds$$

and proceed in a manner similar to the proof of (4.21). □

4.3.2 Proof of the Asymptotic Formula for the Mean Square Error

Let $\theta_K(x) := \sum_{\mathrm{N}\mathfrak{p}\le x} \log \mathrm{N}\mathfrak{p}$. We will frequently make use of the formula

$$\theta_K(x) = x + O(x/(\log x)^M). \tag{4.23}$$

The formula follows from (4.5) for example. We will need the following lemma in order to complete the proof of Theorem 4.3.1.

Lemma 4.3.6. *For any $M > 0$,*

$$\sum_{\mathrm{N}\mathfrak{p}\le x} \sum_{\mathrm{N}\mathfrak{p}'=\mathrm{N}\mathfrak{p}} (\log \mathrm{N}\mathfrak{p})^2 = [K:\mathbb{Q}](x\log x - x) + O\left(\frac{x}{(\log x)^M}\right).$$

Proof. First, note that since only finitely many rational primes may ramify in K, we only introduce an error of $O(1)$ by restricting our sum to prime ideals which do not lie above a rational prime ramifying in K. For a rational prime p, let g_p denote the number of primes lying above p, let f_p denote the degree of any prime lying above p, and let e_p denote the ramification index of p in K. Note that e_p and f_p are well-defined since $K/\mathbb{Q}$ is Galois. Recall that if p does not ramify in K, then we have $[K:\mathbb{Q}] = g_p f_p$. Thus, partial summation and (4.23) yield

$$\begin{aligned}\sum_{\mathrm{N}\mathfrak{p}\le x} \sum_{\mathrm{N}\mathfrak{p}'=\mathrm{N}\mathfrak{p}} (\log \mathrm{N}\mathfrak{p})^2 &= [K:\mathbb{Q}] \sum_{\substack{p^{f_p}\le x \\ e_p=1}} g_p f_p (\log p)^2 + O(1) \\ &= [K:\mathbb{Q}] \log x\,(\theta_K(x) + O(1)) - [K:\mathbb{Q}] \int_1^x \frac{\theta_K(t)+O(1)}{t}dt + O(1) \\ &= [K:\mathbb{Q}](x\log x - x) + O\left(x(\log x)^{-M}\right).\end{aligned}$$

□

Proof of Theorem 4.3.1. First, define

$$S(x;Q_1,Q_2) := \sum_{Q_1<q\le Q_2} \sum_{a\in G_q} \left(\theta_K(x;q,a) - \frac{x}{\varphi_K(q)}\right)^2.$$

If $Q \le x(\log x)^{-(M+1)}$, then Theorem 4.2.1 implies that $S(x;0,Q) \ll x^2(\log x)^{-M}$, and hence Theorem 4.3.1 follows since the error term dominates in this case. Thus, it suffices to consider the case when $Q > x(\log x)^{-(M+1)}$. Therefore, for the remainder of the proof, we will write $Q_1 := x(\log x)^{-(M+1)}$, and assume that $Q_1 < Q_2 \le x$. By Theorem 4.2.1, we have

$$S(x;0,Q_2) = S(x;Q_1,Q_2) + O\left(x^2(\log x)^{-M}\right). \tag{4.24}$$

For Q_1, Q_2 as above,

$$\begin{aligned}S(x;Q_1,Q_2) &= \sum_{Q_1<q\le Q_2}\sum_{a\in G_q}\left\{\theta_K(x;q,a)^2 - \frac{2x}{\varphi_K(q)}\theta_K(x;q,a) + \frac{x^2}{\varphi_K(q)^2}\right\}\\ &= \sum_{Q_1<q\le Q_2}\left\{\sum_{a\in G_q}\theta_K(x;q,a)^2 - \frac{x}{\varphi_K(q)}\left(2\theta_K(x) - 2\sum_{\substack{\mathrm{N}\mathfrak{p}\le x\\ (\mathrm{N}\mathfrak{p},q)>1}}\log \mathrm{N}\mathfrak{p} - x\right)\right\}\\ &= \sum_{Q_1<q\le Q_2}\sum_{a\in G_q}\theta_K(x;q,a)^2 - x^2\sum_{Q_1<q\le Q_2}\frac{1}{\varphi_K(q)} + O\left(\frac{x^2}{(\log x)^M}\right). \qquad (4.25)\end{aligned}$$

Now, observe that

$$\begin{aligned}\sum_{a\in G_q}\theta_K(x;q,a)^2 &= \sum_{\substack{\mathrm{N}\mathfrak{p},\mathrm{N}\mathfrak{p}'\le x\\ \mathrm{N}\mathfrak{p}\equiv\mathrm{N}\mathfrak{p}' \pmod q\\ (\mathfrak{p}\mathfrak{p}',q\mathcal{O}_K)=\mathcal{O}_K}}\log \mathrm{N}\mathfrak{p}\log \mathrm{N}\mathfrak{p}'\\ &= \sum_{\substack{\mathrm{N}\mathfrak{p}=\mathrm{N}\mathfrak{p}'\le x\\ (\mathfrak{p}\mathfrak{p}',q\mathcal{O}_K)=\mathcal{O}_K}}(\log \mathrm{N}\mathfrak{p})^2 + \sum_{\substack{\mathrm{N}\mathfrak{p},\mathrm{N}\mathfrak{p}'\le x;\ \mathrm{N}\mathfrak{p}\ne\mathrm{N}\mathfrak{p}',\\ \mathrm{N}\mathfrak{p}\equiv\mathrm{N}\mathfrak{p}' \pmod q}}\log \mathrm{N}\mathfrak{p}\log \mathrm{N}\mathfrak{p}'.\end{aligned}$$

Thus, we define

$$\begin{aligned}H(x;Q_1,Q_2) &:= \sum_{Q_1<q\le Q_2}\sum_{\substack{\mathrm{N}\mathfrak{p}=\mathrm{N}\mathfrak{p}'\le x\\ (\mathfrak{p}\mathfrak{p}',q\mathcal{O}_K)=\mathcal{O}_K}}(\log \mathrm{N}\mathfrak{p})^2;\\ J(x;Q_1,Q_2) &:= \sum_{Q_1<q\le Q_2}\sum_{\substack{\mathrm{N}\mathfrak{p},\mathrm{N}\mathfrak{p}'\le x;\ \mathrm{N}\mathfrak{p}\ne\mathrm{N}\mathfrak{p}',\\ \mathrm{N}\mathfrak{p}\equiv\mathrm{N}\mathfrak{p}' \pmod q}}\log \mathrm{N}\mathfrak{p}\log \mathrm{N}\mathfrak{p}'.\end{aligned}$$

Now (4.25) may be rewritten as

$$\begin{aligned}S(x;Q_1,Q_2) &= H(x;Q_1,Q_2) + J(x;Q_1,Q_2)\\ &\qquad - C_1x^2\log(Q_2/Q_1) + O\left(\frac{x^2}{(\log x)^M}\right). \qquad (4.26)\end{aligned}$$

Note that we have applied the second part of Lemma 4.3.5 to the second term of (4.25).

Removing the condition $(\mathfrak{p}\mathfrak{p}', q\mathcal{O}_K) = 1$ from the inner sum of $H(x;Q_1,Q_2)$ introduces an error which is $O\left((\log x)^2\right)$. Thus, we may apply Lemma 4.3.6 to obtain

$$\begin{aligned} H(x;Q_1,Q_2) &= \{Q_2 - Q_1 + O(1)\}\left\{[K:\mathbb{Q}](x\log x - x) + O\left(x(\log x)^{-M}\right)\right\} \\ &= [K:\mathbb{Q}]xQ_2\log x - [K:\mathbb{Q}]xQ_2 + O\left(\frac{x^2}{(\log x)^M}\right). \end{aligned} \tag{4.27}$$

Now, define $J(x;Q) := J(x;Q,x)$, so that $J(x;Q_1,Q_2) = J(x;Q_1) - J(x;Q_2)$. Then

$$\begin{aligned} J(x;Q) = 2\sum_{\substack{\mathrm{N}\mathfrak{p}'<\mathrm{N}\mathfrak{p}\le x \\ \mathrm{N}\mathfrak{p}-\mathrm{N}\mathfrak{p}'=kq \\ Q<q\le x}} \log \mathrm{N}\mathfrak{p}\log\mathrm{N}\mathfrak{p}' &= 2\sum_{k<x/Q}\sum_{\substack{\mathrm{N}\mathfrak{p}\equiv\mathrm{N}\mathfrak{p}' \pmod k \\ \mathrm{N}\mathfrak{p}\le x;\mathrm{N}\mathfrak{p}-\mathrm{N}\mathfrak{p}'>kQ}} \log \mathrm{N}\mathfrak{p}\log\mathrm{N}\mathfrak{p}' \\ &= 2\sum_{k<x/Q}\sum_{a\in G_k}\sum_{\substack{\mathrm{N}\mathfrak{p}'<x-kQ \\ \mathrm{N}\mathfrak{p}'\equiv a \pmod k}} \log\mathrm{N}\mathfrak{p}' \sum_{\substack{kQ+\mathrm{N}\mathfrak{p}'<\mathrm{N}\mathfrak{p}\le x \\ \mathrm{N}\mathfrak{p}\equiv a \pmod k}} \log\mathrm{N}\mathfrak{p}. \end{aligned}$$

Since $Q \ge Q_1 = x/(\log x)^{M+1}$, we have $k < x/Q \le (\log x)^{M+1}$ and $kQ \ge x/(\log x)^{M+1}$. Thus, we may apply (4.5) and write

$$\theta_K(x;k,a) - \theta_K(kQ+\mathrm{N}\mathfrak{p}';k,a) = \frac{x-kQ-\mathrm{N}\mathfrak{p}'}{\varphi_K(k)} + O\left(\frac{x}{(\log x)^{2M+1}}\right)$$

for the innermost sum above. This gives

$$\begin{aligned} J(x,Q) &= 2\sum_{k<\frac{x}{Q}}\frac{1}{\varphi_K(k)}\sum_{\substack{\mathrm{N}\mathfrak{p}'<x-kQ \\ (\mathrm{N}\mathfrak{p}',k)=1}}(x-kQ-\mathrm{N}\mathfrak{p}')\log\mathrm{N}\mathfrak{p}' + O\left(\frac{x}{(\log x)^{2M+1}}\sum_{k<\frac{x}{Q}}\theta_K(x)\right) \\ &= 2\sum_{k<\frac{x}{Q}}\frac{\int_1^{x-kQ}\theta_K(t)dt}{\varphi_K(k)} + O\left(x\sum_{k<\frac{x}{Q}}\frac{\log k}{\varphi_K(k)}\right) + O\left(\frac{x^3}{Q(\log x)^{2M+1}}\right), \end{aligned}$$

where the last line follows by partial summation applied to the inner sum of the main term. Therefore, by (4.23), we have

$$J(x,Q) = x^2\sum_{k<\frac{x}{Q}}\left(1-\frac{kQ}{x}\right)^2\frac{1}{\varphi_K(k)} + O\left(\frac{x^2}{(\log x)^M}\right).$$

Following Hooley [Hoo75, p. 212], we consider two different cases for the treatment of $J(x; Q_1, Q_2)$. First, if $Q_2 = x$, then

$$\begin{aligned} J(x; Q_1, Q_2) &= J(x; Q_1) \\ &= x^2 \left\{ C_1 \log(x/Q_1) + C_2 + O\left(\frac{\log(x/Q_1)}{x/Q_1} \right) \right\} + O\left(\frac{x^2}{(\log x)^M} \right) \\ &= C_1 x^2 \log(Q_2/Q_1) + C_2 x^2 + O\left(\frac{x^2}{(\log x)^M} \right). \end{aligned} \tag{4.28}$$

In the case that $Q_2 \leq x$ (including the previous case), we may write

$$\begin{aligned} J(x; Q_1, Q_2) =& J(x; Q_1) - J(x; Q_2) \\ =& C_1 x^2 \log(Q_2/Q_1) - \frac{\varphi(m_K)}{\varphi_K(m_K)} x Q_2 \log(x/Q_2) - C_3 x Q_2 \\ &+ O\left(x^{3/4} Q_2^{5/4} \right) + O\left(\frac{x^2}{(\log x)^M} \right). \end{aligned} \tag{4.29}$$

Theorem 4.3.1 now follows by combining (4.24), (4.26), (4.27), (4.28), and (4.29). □

Chapter 5

Average Frobenius Distribution for Elliptic Curves over Galois Number Fields

Recall that if E is a fixed elliptic curve defined over a number field K, r is any integer, and f is a positive integer, then we define the prime counting function $\pi_E^{r,f}(x)$ by

$$\pi_E^{r,f}(x) := \{\mathrm{N}\mathfrak{p} \leq x : a_{\mathfrak{p}}(E) = r, \deg \mathfrak{p} = f\}. \tag{5.1}$$

Now, recall the Lang-Trotter Conjecture for elliptic curves defined over number fields.

Conjecture 5.0.7. *Let E be a fixed elliptic curve defined over K, and let r be a fixed integer. In the case that $r = 0$, assume further that E does not possess complex multiplication. Let f be a positive integer. Then there exists a positive constant $C_{E,r,f}$ such that*

$$\pi_E^{r,f}(x) \sim C_{E,r,f} \begin{cases} \frac{\sqrt{x}}{\log x}, & f = 1, \\ \log\log x, & f = 2, \\ 1, & f \geq 3. \end{cases}$$

Recall that in the case $K = \mathbb{Q}$, all primes have degree 1, and hence we suppress the f. For more details on the conjecture, see Section 1.2.4 of this thesis.

The theme of studying the Lang-Trotter Conjecture "on average" was initiated by Fouvry and Murty in [FM96] where they studied the case when $K = \mathbb{Q}$ and $r = 0$. Their work was generalized by David and Pappalardi in [DP99] who showed the following.

Theorem 5.0.8 (David-Pappalardi)**.** *For $a, b \in \mathbb{Z}$, let $E_{a,b}$ denote the elliptic curve given by $Y^2 = X^3 + aX + b$. Let $\epsilon > 0$. Then, if $A, B > x^{1+\epsilon}$, we have*

$$\frac{1}{4AB} \sum_{\substack{|a|<A, \\ |b|<B}} \pi^r_{E_{a,b}}(x) \sim C_r \frac{\sqrt{x}}{\log x},$$

where C_r is the convergent infinite product defined by

$$C_r := \frac{2}{\pi} \prod_{\ell | r} \left(1 - \frac{1}{\ell^2}\right)^{-1} \prod_{\ell \nmid r} \frac{\ell(\ell^2 - \ell - 1)}{(\ell - 1)(\ell^2 - 1)}.$$

This result has been improved by Baier [Bai07] in the sense that he showed that one may relax the growth conditions on A and B to $A, B > x^{1/2+\epsilon}$ and $AB > x^{3/2+\epsilon}$. In [Jam04], James considered the average over the family of elliptic curves admitting a rational 3-torsion point. The work was extended in [BBIJ05], where the average was taken over families of curves with various torsion structure.

The average Lang-Trotter problem was studied in the number field case first by David and Pappalardi [DP04] where they considered the case $K = \mathbb{Q}(i)$ and $f = 2$. This work has very recently been extended by Faulkner and James [FJ] to the setting of an arbitrary number field assumed to be Abelian over $\mathbb{Q}$. They, in fact, consider all f dividing $[K : \mathbb{Q}]$. We will state their theorem in the next section after we have introduced the necessary notation.

In this chapter, we will show that the conjecture holds on average for the case $f = 1$ under the assumption that $K/\mathbb{Q}$ is Galois. That is, for the case of degree one primes, we will remove the strigent requirement that $\mathrm{Gal}(K/\mathbb{Q})$ be Abelian from the main result of [FJ]. See Theorem 5.1.2 below. A major ingredient in the proof will be a version of the mean square error bound for the Chebotarëv Density Theorem given in Chapter 4. See Remark 4.2.2 following Theorem 4.2.1 on page 76.

5.1 The Lang-Trotter Conjecture for Number Fields "on Average"

For the remainder of this chapter, we assume that K is a fixed Galois extension of $\mathbb{Q}$ with group G. We denote the discriminant of the field by Δ_K and the degree of extension by $n_K := [K : \mathbb{Q}]$. Recall that the ring of integers $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n_K, and let $\mathcal{B} = \{\alpha_i\}_{i=1}^{n_K}$ be an integral basis for $\mathcal{O}_K$. We denote the coordinate map for the basis $\mathcal{B}$ by

$$[\cdot]_{\mathcal{B}} : \mathcal{O}_K \xrightarrow{\sim} \bigoplus_{i=1}^{n_K} \mathbb{Z}\alpha_i \cong \mathbb{Z}^{n_K}.$$

Given an algebraic integer α, we let $|||\alpha|||$ denote the absolute value of the maximum entry in the coordinate vector $[\alpha]_{\mathcal{B}}$. Given two algebraic integers $\alpha, \beta \in \mathcal{O}_K$, we write $E_{\alpha,\beta}$ for the model

$$E_{\alpha,\beta} : Y^2 = X^3 + \alpha X + \beta,$$

and we write $\Delta(E_{\alpha,\beta})$ for the discriminant of the equation. For a positive real number t, we define a "box of elliptic curves" by

$$\mathcal{C}_t := \{E_{\alpha,\beta} : |||\alpha|||, |||\beta||| \leq t; \Delta(E_{\alpha,\beta}) \neq 0\}.$$

Recall that

$$\pi_{1/2}(x) = \int_2^x \frac{dt}{2\sqrt{t}\log t} \sim \frac{\sqrt{x}}{\log x}.$$

See Remark 1.2.26 on page 22. We now state the main result of Faulkner and James [FJ].

Theorem 5.1.1 (Faulkner-James)**.** *Suppose that* $G = \mathrm{Gal}(K/\mathbb{Q})$ *is Abelian and that* r *is a* *fixed odd integer. Then there exist explicit constants $D_{r,1,K}$ and $D_{r,2,K}$ such that*

$$\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,f}(x)\sim\begin{cases}D_{r,1,K}\pi_{1/2}(x) & \text{if } f=1, t\gg x^{3/2}\log x,\\ D_{r,2,K}\log\log x & \text{if } f=2, t\gg\sqrt{x}\log x.\end{cases}$$

Furthermore,

$$\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,f}(x)<\infty,$$

provided that

$$t\gg\begin{cases}x^{1/6}\log x & \text{if } f=3,\\ (\log x)^2\log\log x & \text{if } f=4,\\ (\log x)^2 & \text{if } f\geq 5.\end{cases}$$

Faulkner and James give explicit descriptions of the constants $D_{r,1,K}$ and $D_{r,2,K}$ both as convergent infinite series and as convergent infinite products. For the sake of comparison, we will state the series form of $D_{r,1,K}$ in the next section.

In what follows, we will improve Theorem 5.1.1 for the case $f=1$ in two ways. First, we will define a more general "box of elliptic curves." This will lead to an improvement in the sense that we will be able to show the result still holds for boxes growing in "volume" slightly less rapidly with respect to x. The second improvement is that we remove the assumption that $G=\text{Gal}(K/\mathbb{Q})$ is a Abelian.

For a vector $\mathbf{v}=(v_1,\ldots,v_m)\in\mathbb{R}^m$, we define the quantities

$$\begin{aligned}P_0(\mathbf{v}) &:= \prod_{i=1}^{m} v_i,\\ P_1(\mathbf{v}) &:= \max_{1\leq i\leq m}\prod_{\substack{j=1,\\ j\neq i}}^{m} v_j, \qquad (5.2)\\ \mathbf{v}_{\min} &:= \min_{1\leq i\leq m}\{v_i\}.\end{aligned}$$

Given another vector $\mathbf{w}=(w_1,\ldots,w_m)\in\mathbb{R}^m$, by $\mathbf{v}\leq\mathbf{w}$, we mean $v_i\leq w_i$ for all

$1 \leq i \leq m$. Also, if $\mathbf{v} = (v_1, \ldots, v_{2m}) \in \mathbb{R}^{2m}$, then we write $\mathbf{v}_1 := (v_1, \ldots v_m)$ for the vector consisting of the first m components and $\mathbf{v}_2 := (v_{m+1}, \ldots v_{2m})$ for the vector consisting of the last m components of $\mathbf{v}$. Given vectors $\mathbf{a} = (a_1, \ldots a_{n_K}), \mathbf{t} = (t_1, \ldots t_{n_K}) \in \mathbb{R}^{n_K}$, we define a "box" of algebraic integers in K by

$$\mathcal{B}(\mathbf{a}, \mathbf{t}) = \{\alpha \in \mathcal{O}_K : \mathbf{a} < [\alpha]_{\mathcal{B}} \leq \mathbf{a} + \mathbf{t}\}. \tag{5.3}$$

Given vectors $\mathbf{a}, \mathbf{t} \in \mathbb{R}^{2n_K}$ with $\mathbf{t} \geq \mathbf{0}$, we define our general box of elliptic curves $\mathcal{C}_{\mathbf{a},\mathbf{t}}$ by

$$\mathcal{C}_{\mathbf{a},\mathbf{t}} := \{E_{\alpha,\beta} : \alpha \in \mathcal{B}(\mathbf{a}_1, \mathbf{t}_1), \beta \in \mathcal{B}(\mathbf{a}_2, \mathbf{t}_2); \Delta(E_{\alpha,\beta}) \neq 0\}. \tag{5.4}$$

We now state the main results of this chapter. First, we give the average order of $\pi_E^{r,1}(x)$.

Theorem 5.1.2. *Let r be a fixed integer, and let K be a fixed number field, assumed to be Galois over $\mathbb{Q}$. Then there exists a constant $C_{K,r,1}$ such that*

$$\frac{1}{|\mathcal{C}_{\mathbf{a},\mathbf{t}}|} \sum_{E \in \mathcal{C}_{\mathbf{a},\mathbf{t}}} \pi_E^{r,1}(x) \sim C_{K,r,1}\pi_{1/2}(x),$$

provided that $P_0(\mathbf{t}) \gg x^{2n_K - 1/2}(\log x)^{2n_K+1+c}$, $P_0(\mathbf{t}_1), P_0(\mathbf{t}_2) \gg x^{n_K-1/2}(\log x)^{n_K+1+c}$ and $\mathbf{t}_{\min} \gg (\log x)^c$, where c is any positive constant.

Remark 5.1.3. We say that the *average order* of $\pi_E^{r,1}(x)$ is $C_{K,r,1}\pi_{1/2}(x)$.

Remark 5.1.4. A more precise statement of this result together with an explicit description of the constant $C_{K,r,1}$ is given in the next section.

Remark 5.1.5. Note that the conditions on t in Theorem 5.1.1 imply $P_0(\mathbf{t}) \gg x^{3n_K}(\log x)^{2n_K}$.

We also prove the following bound on the variance, which allows us to show that the *normal order* of $\pi_E^{r,1}(x)$ is also $C_{K,r,1}\pi_{1/2}(x)$.

Theorem 5.1.6. *Let $c > 0$. Then*

$$\frac{1}{|\mathcal{C}_{\mathbf{a},\mathbf{t}}|} \sum_{E \in \mathcal{C}_{\mathbf{a},\mathbf{t}}} \left|\pi_E^{r,1}(x) - C_{K,r,1}\pi_{1/2}(x)\right|^2 \ll \frac{x}{(\log x)^{2+c}},$$

provided that $P_0(\mathbf{t}) \gg x^{4n_K-1}(\log x)^{2(2n_K+1)+c}$*,* $P_0(\mathbf{t}_1), P_0(\mathbf{t}_2) \gg x^{2n_K-1}(\log x)^{2(n_K+1)+c}$*, and* $\mathbf{t}_{\min} \gg (\log x)^c$*.*

The Turán normal order method supplies us with the following corollary. The corollary may be interpreted as saying that $\pi_E^{r,1}(x) \sim C_{K,r,1}\pi_{1/2}(x)$ for "almost all" elliptic curves $E \in \mathcal{C}_{\mathbf{a},\mathbf{t}}$.

Corollary 5.1.7. *Let* $c, \epsilon > 0$ *be fixed with* $c > 2\epsilon$*. If* $\mathbf{t} \in \mathbb{R}^{2n_K}$ *satisfies the conditions of Theorem 5.1.6, then for all* $E \in \mathcal{C}_{\mathbf{a},\mathbf{t}}$ *with at most* $O\left(P_0(\mathbf{t})(\log x)^{2\epsilon-c}\right)$ *exceptions, we have*

$$|\pi_E^{r,1}(x) - C_{K,r,1}\pi_{1/2}(x)| < \frac{\sqrt{x}}{(\log x)^{1+\epsilon}}. \tag{5.5}$$

Proof. Let $\mathcal{C}^{\mathrm{e}}_{\mathbf{a},\mathbf{t}}$ denote the subset of $\mathcal{C}_{\mathbf{a},\mathbf{t}}$ consisting of all exceptions to the inequality (5.5), and let $N_{\mathrm{e}} = |\mathcal{C}^{\mathrm{e}}_{\mathbf{a},\mathbf{t}}|$. Then by Theorem 5.1.6, we have

$$\frac{x}{(\log x)^{2+c}} \gg \frac{1}{|\mathcal{C}_{\mathbf{a},\mathbf{t}}|}\sum_{E \in \mathcal{C}^{\mathrm{e}}_{\mathbf{a},\mathbf{t}}} \left|\pi_E^{r,1}(x) - C_{K,r,1}\pi_{1/2}(x)\right|^2 \geq \frac{1}{|\mathcal{C}_{\mathbf{a},\mathbf{t}}|}N_{\mathrm{e}}\frac{x}{(\log x)^{2+2\epsilon}}.$$

Hence, $N_{\mathrm{e}} \ll P_0(\mathbf{t})(\log x)^{2\epsilon-c}$ since, by Lemma 5.3.1 on page 102, we have $|\mathcal{C}_{\mathbf{a},\mathbf{t}}| = P_0(\mathbf{t}) + O\left(P_1(\mathbf{t})\right)$. □

5.2 More Precise Statements of the Main Theorems

In this section, we state the series form of the constant $D_{r,1,K}$ of Theorem 5.1.1 as well as a more precise statement of Theorem 5.1.2. We also give an explicit description of the constant $C_{K,r,1}$ both as an infinite series and as an infinite product. See Theorems 5.2.1 and 5.2.5 below.

Before proceeding further, we must first recall some of the notation of the previous chapter. As in Chapter 4, ζ_q will always denote a primitive q-th root of unity, and G_q will denote the image of the natural map

$$\mathrm{Gal}(K(\zeta_q)/K) \hookrightarrow (\mathbb{Z}/q\mathbb{Z})^*. \tag{5.6}$$

In [FJ], Faulkner and James note that, by the Kronecker-Weber Theorem [Lan94, p. 210], every Abelian extension K of $\mathbb{Q}$ is contained in some cyclotomic extension of $\mathbb{Q}$. Hence, the splitting of rational primes in K is completely determined by congruence conditions. See Example 1.1.5 on page 4. We note here that we may further assume that the cyclotomic extension is taken to be as small as possible. That is, we may choose a smallest integer m_K so that $K \subseteq \mathbb{Q}(\zeta_{m_K})$. Thus, there exist a list of congruences modulo m_K such that a rational prime splits completely in K if and only if it satisfies exactly one congruence on the list. We now observe that this list of congruences is precisely the elements of the group G_{m_K}. In order to see this, recall that a rational prime p splits completely in K if and only if the Frobenius $\left(\frac{K/\mathbb{Q}}{p}\right)$ is trivial. Thus, it follows that G_{m_K} is the correct set of congruences since in the case $K/\mathbb{Q}$ is Abelian, $\mathbb{Q}(\zeta_{m_K}) = K(\zeta_{m_K})$ and $G = \mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/m_K\mathbb{Z})^*/G_{m_K}$. Given this notation, we now state the series form of constant $D_{r,1,K}$:

$$D_{1,r,K} = \frac{2n_K}{\pi}\left(\sum_{b\in G_{m_K}}\sum_{k=1}^{\infty}\frac{1}{k}\sum_{n=1}^{\infty}\frac{c_k^{r,b,m_K}(n)}{\varphi([m_K,nk^2])n}\right), \tag{5.7}$$

where

$$c_k^{r,b,m_K}(n) := \sum_{\substack{a\in(\mathbb{Z}/4n\mathbb{Z})^* \\ a\equiv 0,1 \pmod 4 \\ (r^2-ak^2,4nk^2)=4 \\ 4b\equiv r^2-ak^2 \pmod{(4m_K,4nk^2)}}} \left(\frac{a}{n}\right). \tag{5.8}$$

We now recall some more notation from Chapter 4 and then give the more precise statement of Theorem 5.1.2. We continue to assume that $K/\mathbb{Q}$ is Galois, but not necessarily Abelian. Recall the definitions $\mathbb{Q}^{\mathrm{cyc}} := \bigcup_{q>1}\mathbb{Q}(\zeta_q)$ and $\mathcal{A} := K \cap \mathbb{Q}^{\mathrm{cyc}}$, and note again that $\mathcal{A}$ is the maximal Abelian subfield of K. Further, put $n_K' := [\mathcal{A} : \mathbb{Q}]$.

Theorem 5.2.1. *Let r be a fixed integer, and let K be a fixed number field, assumed to be Galois over $\mathbb{Q}$. Further, let*

$$C_{K,r,1} := \frac{2n_K'}{\pi}\left(\sum_{b\in G_{m_K}}\sum_{k=1}^{\infty}\frac{1}{k}\sum_{n=1}^{\infty}\frac{c_k^{r,b,m_K}(n)}{\varphi([m_K,nk^2])n}\right). \tag{5.9}$$

Then $C_{K,r,1}$ is absolutely convergent. Furthermore, for any fixed $c > 0$,

$$\frac{1}{|\mathcal{C}_{\mathbf{a},\mathbf{t}}|}\sum_{E\in\mathcal{C}_{\mathbf{a},\mathbf{t}}}\pi_E^{r,1}(x) = C_{K,r,1}\pi_{1/2}(x) + E(x;\mathbf{t}),$$

where

$$E(x;\mathbf{t}) \ll \frac{\sqrt{x}}{(\log x)^{1+c}} + \frac{\sqrt{x}/\log x}{\mathbf{t}_{\min}} + \left(\frac{1}{P_0(\mathbf{t}_1)} + \frac{1}{P_0(\mathbf{t}_2)}\right)(x\log x)^{n_K} + \frac{(x\log x)^{2n_K}}{P_0(\mathbf{t})}.$$

Remark 5.2.2. Theorem 5.1.2 is an immediate corollary of Theorem 5.2.1.

Remark 5.2.3. Observe that in the case $K/\mathbb{Q}$ is Abelian, we have $\mathcal{A} = K$, and hence $n_K' = n_K = [K : \mathbb{Q}]$. Therefore, in this case, the constants $D_{1,r,K}$ and $C_{K,r,1}$ agree.

Remark 5.2.4. In the case that $r = 0$, a discussion of the contribution made by complex multiplication curves is warranted. However, one may follow the argument in [Jam04] to show that this contribution is dominated by the error term.

As in [FJ], we also describe our constant $C_{K,r,1}$ as an infinite product over primes. This requires some considerable notation, which we now define. For $b \in G_{m_K}$, let $\Delta^{r,b} := r^2 - 4b$, and define the following sets of primes:

$$\mathscr{L}_{r,b,m_K}^{<} := \{\ell > 2 : \ell | m_K, \ell \nmid r, \mathrm{ord}_\ell(\Delta^{r,b}) < \mathrm{ord}_\ell(m_K)\}, \tag{5.10}$$

$$\mathscr{L}_{r,b,m_K}^{\geq} := \{\ell > 2 : \ell | m_K, \ell \nmid r, \mathrm{ord}_\ell(\Delta^{r,b}) \geq \mathrm{ord}_\ell(m_K)\}. \tag{5.11}$$

Also make the definition

$$\Gamma_\ell := \begin{cases} \left(\frac{\Delta^{r,b}/\ell^{\mathrm{ord}_\ell(\Delta^{r,b})}}{\ell}\right) & \text{if } \mathrm{ord}_\ell(\Delta^{r,b}) \text{ is even, positive, and finite,} \\ 0 & \text{otherwise.} \end{cases} \tag{5.12}$$

Finally, let $F(r, b, m_K)$ denote the following finite product over the primes dividing m_K:

$$F_2(r,b,m_K) \prod_{\substack{\ell \neq 2 \\ \ell \mid m_K \\ \ell \mid r}} \frac{\ell\left(\ell + \left(\frac{-b}{\ell}\right)\right)}{\ell^2 - 1} \prod_{\ell \in \mathscr{L}^{\geq}_{r,b,m_K}} \left(\frac{\ell^{\left\lfloor \frac{\operatorname{ord}_\ell(m_K)+1}{2} \right\rfloor} - 1}{\ell^{\left\lfloor \frac{\operatorname{ord}_\ell(m_K)-1}{2} \right\rfloor}(\ell - 1)} + \frac{\ell^{\operatorname{ord}_\ell(m_K)+2}}{\ell^{3\left\lfloor \frac{\operatorname{ord}_\ell(m_K)+1}{2} \right\rfloor}(\ell^2 - 1)} \right)$$

$$\cdot \prod_{\ell \in \mathscr{L}^{<}_{r,b,m_K}} \left(1 + \frac{\ell\left(\frac{\Delta^{r,b}}{\ell}\right) + \left(\frac{\Delta^{r,b}}{\ell}\right)^2 + \frac{\ell\Gamma_\ell + \ell^2\Gamma_\ell^2}{\ell^{\operatorname{ord}_\ell(\Delta^{r,b})/2}}}{\ell^2 - 1} + \frac{\Gamma_\ell^2\left(\ell^{\left\lfloor \frac{\operatorname{ord}_\ell(\Delta^{r,b})-1}{2} \right\rfloor} - 1\right)}{\ell^{\left\lfloor \frac{\operatorname{ord}_\ell(\Delta^{r,b})-1}{2} \right\rfloor}(\ell - 1)} \right), \tag{5.13}$$

where the definition of $F_2(r, b, m_K)$ is given on the following page.

Theorem 5.2.5. *As an infinite product over primes, the constant $C_{K,r,1}$ may be written as*

$$C_{K,r,1} = \left(\frac{2n'_K}{\pi\varphi(m_K)} \prod_{\substack{\ell \neq 2 \\ \ell \nmid m_K \\ \ell \nmid r}} \frac{\ell(\ell^2 - \ell - 1)}{(\ell+1)(\ell-1)^2} \prod_{\substack{\ell \neq 2 \\ \ell \nmid m_K \\ \ell \mid r}} \frac{\ell^2}{\ell^2 - 1} \right) \sum_{b \in G_{m_K}} F(r, b, m_K). \tag{5.14}$$

$$F_2(r,b,m_K) := \begin{cases} 2/3 & \text{if } 2 \nmid r; \\ 4/3 & \text{if } 2|r, 4 \nmid m_K; \\ 2 - \frac{2}{3\cdot 2^{\lfloor \mathrm{ord}_2(m_K)/2 \rfloor}} & \text{if } r \equiv 2 \pmod{4}, 2 \leq \mathrm{ord}_2(m_K) \leq \mathrm{ord}_2(\Delta^{r,b}) - 2; \\ 2 - \frac{4}{3\cdot 2^{\frac{\mathrm{ord}_2(m_K)-1}{2}}} & \text{if } r \equiv 2 \pmod{4}, \mathrm{ord}_2(m_K) = \mathrm{ord}_2(\Delta^{r,b}) - 1, \\ & \quad 2|\mathrm{ord}_2(\Delta^{r,b}); \\ 2 - \frac{2}{2^{\mathrm{ord}_2(m_K)/2}} & \text{if } r \equiv 2 \pmod{4}, \mathrm{ord}_2(m_K) = \mathrm{ord}_2(\Delta^{r,b}) - 1, \\ & \quad 2 \nmid \mathrm{ord}_2(\Delta^{r,b}); \\ 2 - \frac{2}{3\cdot 2^{\mathrm{ord}_2(m_K)/2}} & \text{if } r \equiv 2 \pmod{4}, \mathrm{ord}_2(m_K) = \mathrm{ord}_2(\Delta^{r,b}), \\ & \quad 2|\mathrm{ord}_2(\Delta^{r,b}), \frac{\Delta^{r,b}}{2^{\mathrm{ord}_2(\Delta^{r,b})}} \equiv 1 \pmod{4}; \\ 2 - \frac{2}{2^{\lfloor \mathrm{ord}_2(m_K)/2 \rfloor}} & \text{if } r \equiv 2 \pmod{4}, \mathrm{ord}_2(m_K) = \mathrm{ord}_2(\Delta^{r,b}), \\ & \quad \left[2 \nmid \mathrm{ord}_2(\Delta^{r,b}) \textbf{ OR } \frac{\Delta^{r,b}}{2^{\mathrm{ord}_2(\Delta^{r,b})}} \equiv 3 \pmod{4} \right]; \\ 2 & \text{if } r \equiv 2 \pmod{4}, \mathrm{ord}_2(m_K) > \mathrm{ord}_2(\Delta^{r,b}), \\ & \quad 2|\mathrm{ord}_2(\Delta^{r,b}), \frac{\Delta^{r,b}}{2^{\mathrm{ord}_2(\Delta^{r,b})}} \equiv 1 \pmod{8}; \\ 2 - \frac{4}{3\cdot 2^{\mathrm{ord}_2(\Delta^{r,b})/2}} & \text{if } r \equiv 2 \pmod{4}, \mathrm{ord}_2(m_K) > \mathrm{ord}_2(\Delta^{r,b}), \\ & \quad 2|\mathrm{ord}_2(\Delta^{r,b}), \frac{\Delta^{r,b}}{2^{\mathrm{ord}_2(\Delta^{r,b})}} \equiv 5 \pmod{8}; \\ 2 - \frac{2}{2^{\mathrm{ord}_2(\Delta^{r,b})/2}} & \text{if } r \equiv 2 \pmod{4}, \mathrm{ord}_2(m_K) > \mathrm{ord}_2(\Delta^{r,b}), \\ & \quad \left[2 \nmid \mathrm{ord}_2(\Delta^{r,b}) \textbf{ OR } \frac{\Delta^{r,b}}{2^{\mathrm{ord}_2(\Delta^{r,b})}} \equiv 3 \pmod{8} \right]; \\ \frac{5}{3} & \text{if } r \equiv 0 \pmod{4}, \mathrm{ord}_2(m_K) = 2, b \equiv 3 \pmod{4}; \\ 2 & \text{if } r \equiv 0 \pmod{4}, 8|m_K, b \equiv 3 \pmod{4}, \\ & \quad \frac{\Delta^{r,b}}{4} \equiv 1 \pmod{8}; \\ \frac{4}{3} & \text{if } r \equiv 0 \pmod{4}, 8|m_K, b \equiv 3 \pmod{4}, \\ & \quad \frac{\Delta^{r,b}}{4} \equiv 5 \pmod{8}; \\ 1 & \text{if } r \equiv 0 \pmod{4}, 4|m_K, b \equiv 1 \pmod{4}. \end{cases}$$

Theorem 5.2.6. *For every $c > 0$,*

$$\frac{1}{|\mathcal{C}_{\mathbf{a},\mathbf{t}}|} \sum_{E \in \mathcal{C}_{\mathbf{a},\mathbf{t}}} \left| \pi_E^{r,1}(x) - C_{K,r,1}\pi_{1/2}(x) \right|^2 \ll \frac{x}{(\log x)^{2+c}} + E_1(x, \mathbf{t}),$$

where

$$E_1(x,\mathbf{t}) = \frac{\sqrt{x}\log\log x}{\log x} + \frac{x/(\log x)^2}{\mathbf{t}_{\min}} + \left(\frac{1}{P_0(\mathbf{t}_1)} + \frac{1}{P_0(\mathbf{t}_2)}\right)(x\log x)^{2n_K} + \frac{(x\log x)^{4n_K}}{P_0(\mathbf{t})}.$$

Remark 5.2.7. Note that Theorem 5.1.6 is an immediate corollary of Theorem 5.2.6.

The next two sections will be concerned with the statements and proofs of several intermediate results. The proofs of Theorems 5.2.1 and 5.2.6 will be carried out in Sections 5.5 and 5.7 respectively.

5.3 Counting Elliptic Curves over K

Let $\mathbf{a} = (a_1, \dots, a_{2n_K}), \mathbf{t} = (t_1, \dots, t_{2n_K}) \in \mathbb{R}^{2n_K}$. Then $\mathbf{a}_1 = (a_1, \dots, a_{n_K}), \mathbf{a}_2 = (a_{n_K+1}, \dots, a_{2n_K})$ and $\mathbf{t}_1 = (t_1, \dots, t_{n_K}), \mathbf{t}_2 = (t_{n_K+1}, \dots, t_{2n_K})$. Our initial step is to compute the volume of the box of elliptic curves $\mathcal{C}_{\mathbf{a},\mathbf{t}}$ defined in (5.4). Using the notation of (5.2), we first observe that the volume of a box of algebraic integers, as defined in (5.3), is

$$\#\mathcal{B}(\mathbf{a}_i, \mathbf{t}_i) = P_0(\mathbf{t}_i) + O(P_1(\mathbf{t}_i)) \tag{5.15}$$

for $i = 1, 2$.

Lemma 5.3.1. *Let $\mathbf{a} = (a_1, \dots a_{2n_K}), \mathbf{t} = (t_1, \dots, t_{2n_K}) \in \mathbb{R}^{2n_K}$ with $\mathbf{t} \geq \mathbf{1}$, Then*

$$|\mathcal{C}_{\mathbf{a},\mathbf{t}}| = P_0(\mathbf{t}) + O\left(P_1(\mathbf{t})\right),$$

and hence

$$\frac{1}{|\mathcal{C}_{\mathbf{a},\mathbf{t}}|} = \frac{1}{P_0(\mathbf{t})} + O\left(\frac{P_1(\mathbf{t})}{P_0(\mathbf{t})^2}\right).$$

Proof. First, we observe that

$$\#\mathcal{B}(\mathbf{a}_1,\mathbf{t}_1)\cdot\#\mathcal{B}(\mathbf{a}_2,\mathbf{t}_2)=\#\left\{E_{\alpha,\beta}:\alpha\in\mathcal{B}(\mathbf{a}_1,\mathbf{t}_1),\beta\in\mathcal{B}(\mathbf{a}_2,\mathbf{t}_2)\right\},$$

where we are careful to note that we are counting singular curves as well as nonsingular curves on the right. Thus, by (5.3), we have

$$\begin{aligned}\#\left\{E_{\alpha,\beta}:\alpha\in\mathcal{B}(\mathbf{a}_1,\mathbf{t}_1),\beta\in\mathcal{B}(\mathbf{a}_2,\mathbf{t}_2)\right\}&=\left(P_0(\mathbf{t}_1)+O(P_1(\mathbf{t}_1))\right)\left(P_0(\mathbf{t}_2)+O(P_1(\mathbf{t}_2))\right)\\&=P_0(\mathbf{t})+O(P_1(\mathbf{t})).\end{aligned}$$

Finally, we compute that

$$\begin{aligned}\#\left\{E_{\alpha,\beta}:\alpha\in\mathcal{B}(\mathbf{a}_1,\mathbf{t}_1),\beta\in\mathcal{B}(\mathbf{a}_2,\mathbf{t}_2);\Delta(E_{\alpha,\beta})=0\right\}&=\sum_{\alpha\in\mathcal{B}(\mathbf{a}_1,\mathbf{t}_1)}\sum_{\substack{\beta\in\mathcal{B}(\mathbf{a}_2,\mathbf{t}_2),\\4\alpha^3+27\beta^2=0}}1\ll\sum_{\alpha\in\mathcal{B}(\mathbf{a}_1,\mathbf{t}_1)}1\\&\ll\prod_{i=1}^{n_K}t_i\leq P_1(\mathbf{t}).\end{aligned}$$

The desired result now follows. □

Let $\mathfrak{p}$ be a degree one prime of $\mathcal{O}_K$ not containing 6. Then any elliptic curve over $\mathcal{O}_K/\mathfrak{p}$ may be realized as $E_{a,b}:Y^2=X^3+aX+b$ with $a,b\in\mathcal{O}_K/\mathfrak{p}$. Given such a curve, we will need an estimate on the number of curves in $\mathcal{C}_{\mathbf{a},\mathbf{t}}$ that reduce modulo $\mathfrak{p}$ to a member of the same isomorphism class as $E_{a,b}$. That is, we need to estimate the size of

$$\mathcal{C}_{\mathbf{a},\mathbf{t}}(E_{a,b};\mathfrak{p}):=\{E\in\mathcal{C}_{\mathbf{a},\mathbf{t}}:E^{\mathfrak{p}}\cong E_{a,b}\}.$$

In addition, if $\mathfrak{p}$ and $\mathfrak{p}'$ do not lie above the same rational prime, we will also need an estimate for the size of

$$\mathcal{C}_{\mathbf{a},\mathbf{t}}(E_{a,b},E_{a',b'};\mathfrak{p},\mathfrak{p}'):=\{E\in\mathcal{C}_{\mathbf{a},\mathbf{t}}:E^{\mathfrak{p}}\cong_{\mathbb{F}_p}E_{a,b};E^{\mathfrak{p}'}\cong_{\mathbb{F}_{p'}}E_{a',b'}\}.$$

Lemma 5.3.2. *Let $\mathfrak{p}$ be a prime of K such that $\deg \mathfrak{p} = 1$, $\mathfrak{p} \nmid 6$, and $\mathfrak{p} \nmid \prod_{j=1}^{n_K} \alpha_j$. Also, let p be the unique rational prime lying below $\mathfrak{p}$. Then, for any fixed elliptic curve $E_{a,b} : Y^2 = X^3 + aX + b$ defined over $\mathbb{F}_p$, we have*

$$\begin{aligned}|\mathcal{C}_{\mathbf{a},\mathbf{t}}(E_{a,b};\mathfrak{p})| =& \frac{p-1}{c_p(a,b)p^2} P_0(\mathbf{t}) + O\left(p^{2n_K-3/2}(\log p)^{2n_K}\right) \\ &+ O\left(\left[P_0(\mathbf{t}_1) + P_0(\mathbf{t}_2)\right] p^{n_K-3/2}(\log p)^{n_K} + \frac{P_1(\mathbf{t})}{p}\right),\end{aligned}$$

where

$$c_p(a,b) := \begin{cases} 2, & ab \neq 0 \\ (4, p-1), & a \neq 0, b = 0 \\ (6, p-1), & a = 0, b \neq 0. \end{cases}$$

Proof. First, we identify $\mathcal{O}_K/\mathfrak{p}$ with $\mathbb{F}_p$ and recall some facts about additive characters on $\mathbb{F}_p$. We write ψ_0 for the trivial additive character. Given a fixed nontrivial additive character ψ of $\mathbb{F}_p$, every other additive character is of the form $\psi_h(c) = \psi(hc)$ with $h \in \mathbb{F}_p$. Moreover, $\psi(c) = e(c/p)$ is a nontrivial additive character of $\mathbb{F}_p$, where $e(z) := \exp(2\pi i z)$.

We will need estimates for sums of the form $\sum_{c=u}^{u+t} \psi(c)$. The sum is clearly bounded by t since $|\psi(c)| \leq 1$ for all c. If $\psi \neq \psi_0$, we can sometimes do better. In particular, since $\psi(c) = e(hc/p)$ for some $1 \leq h \leq p-1$, we have

$$\sum_{c=u}^{u+t} \psi(c) \ll \int_u^{u+t} e(hx/p)dx \ll \frac{p}{h}.$$

Thus, we also have

$$\sum_{\psi \neq \psi_0} \left| \sum_{c=u}^{u+t} \psi(c) \right| \ll \sum_{h=1}^{p-1} \min\{t, p/h\} \ll p \log p. \tag{5.16}$$

By Remark 1.2.3, the only curves of the form $E_{a',b'} : Y^2 = X^3 + a'X + b'$ which are isomorphic to $E_{a,b}$ are given by $a' = u^4 a, b' = u^6 b$ for $u \in (\mathcal{O}_K/\mathfrak{p})^*$. We first observe that

$c_p(a,b) = \#\left\{u \in (\mathcal{O}_K/\mathfrak{p})^* : a \equiv au^4 \pmod{\mathfrak{p}}, b \equiv bu^6 \pmod{\mathfrak{p}}\right\}$. Therefore,

$$|\mathcal{C}_{\mathbf{a},\mathbf{t}}(E_{a,b};\mathfrak{p})| = \frac{1}{c_p(a,b)} \sum_{u \in (\mathcal{O}_K/\mathfrak{p})^*} \sum_{\substack{\alpha \in \mathcal{B}(\mathbf{a}_1,\mathbf{t}_1) \\ \mathfrak{p} | (\alpha - au^4)}} \sum_{\substack{\beta \in \mathcal{B}(\mathbf{a}_2,\mathbf{t}_2) \\ \mathfrak{p} | (\beta - bu^6) \\ \Delta(E_{\alpha,\beta}) \neq 0}} 1.$$

Now, since $E_{a,b}$ is assumed to be an elliptic curve over $\mathbb{F}_p$, the discriminant $\Delta(E_{a,b}) \neq 0$. Thus, if $E_{\alpha,\beta}$ reduces to a curve isomorphic to $E_{a,b}$ modulo $\mathfrak{p}$, then $\mathfrak{p} \nmid \Delta(E_{\alpha,\beta}^{\mathfrak{p}})$; and hence $\Delta(E_{\alpha,\beta}) \neq 0$. Therefore, we may remove the nonsingularity condition from the above and write

$$\frac{1}{c_p(a,b)} \sum_{u \in (\mathcal{O}_K/\mathfrak{p})^*} \sum_{\substack{\alpha \in \mathcal{B}(\mathbf{a}_1,\mathbf{t}_1) \\ \mathfrak{p} | (\alpha - au^4), \\ \beta \in \mathcal{B}(\mathbf{a}_2,\mathbf{t}_2) \\ \mathfrak{p} | (\beta - bu^6)}} 1 = \frac{1}{c_p(a,b)} \sum_{u \in (\mathcal{O}_K/\mathfrak{p})^*} \sum_{\substack{\alpha \in \mathcal{B}(\mathbf{a}_1,\mathbf{t}_1) \\ \beta \in \mathcal{B}(\mathbf{a}_2,\mathbf{t}_2)}} \frac{1}{p^2} \sum_{\psi,\psi'} \psi(\alpha - au^4)\psi'(\beta - bu^6),$$

where the innermost sum is over all pairs (ψ, ψ') of additive characters on $\mathcal{O}_K/\mathfrak{p}$. The main term comes from $\psi = \psi' = \psi_0$, which contributes $\frac{p-1}{c(a,b)p^2} P_0(\mathbf{t}) + O\left(\frac{P_1(\mathbf{t})}{p}\right)$. The remaining terms are bounded by

$$\frac{1}{p^2 c_p(a,b)} \sum_{(\psi,\psi') \neq (\psi_0,\psi_0)} \left| \sum_{u \in (\mathcal{O}_K/\mathfrak{p})^*} \overline{\psi}(au^4)\overline{\psi'}(bu^6) \right| \left| \sum_{\alpha \in \mathcal{B}(\mathbf{a}_1,\mathbf{t}_1)} \psi(\alpha) \right| \left| \sum_{\beta \in \mathcal{B}(\mathbf{a}_2,\mathbf{t}_2)} \psi'(\beta) \right|. \quad (5.17)$$

In (5.17), at least one of ψ and ψ' is nontrivial. Without loss of generality, assume $\psi \neq \psi_0$. By our above observations concerning additive characters, we have

$$\overline{\psi}(au^4)\overline{\psi}'(bu^6) = \overline{\psi}(au^4 + mbu^6)$$

for some $m \in \mathcal{O}_K/\mathfrak{p}$. We think of $au^4 + mbu^6$ as a polynomial in u over $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_p$ of degree either 4 or 6. Thus, since $\mathfrak{p} \nmid 6$, we may apply Weil's Theorem [LN97, Thm. 5.38, p. 223], which yields

$$\left| \sum_{u \in (\mathcal{O}_K/\mathfrak{p})^*} \overline{\psi}\left(au^4 + mbu^6\right) \right| \ll \sqrt{p}.$$

Now, if $\psi = \psi_0$, we have

$$\left|\sum_{\alpha\in\mathcal{B}(\mathbf{a}_1,\mathbf{t}_1)} \psi(\alpha)\right| = P_0(\mathbf{t}_1) + O(P_1(\mathbf{t}_1)).$$

Similarly, if $\psi' = \psi_0$,

$$\left|\sum_{\beta\in\mathcal{B}(\mathbf{a}_2,\mathbf{t}_2)} \psi'(\beta)\right| = P_0(\mathbf{t}_2) + O(P_1(\mathbf{t}_2)).$$

It remains to bound $\sum_{\psi\neq\psi_0}\left|\sum_{\alpha\in\mathcal{B}(\mathbf{a}_1,\mathbf{t}_1)}\psi(\alpha)\right|$ since the corresponding sum for β in (5.17) is estimated in the same manner. We write each $\alpha \in \mathcal{B}(\mathbf{a}_1,\mathbf{t}_1)$ in terms of our fixed basis $\mathcal{B} = \{\alpha_1,\ldots,\alpha_{n_K}\}$ as $\alpha = \sum_{j=1}^{n_K} c_j\alpha_j$. Since $\mathfrak{p} \nmid \prod_{j=1}^{n_K}\alpha_j$, each of the α_j are nonzero modulo $\mathfrak{p}$, and hence $\psi_{\alpha_j} \neq \psi_0$ whenever $\psi \neq \psi_0$. Thus,

$$\begin{aligned}\sum_{\psi\neq\psi_0}\left|\sum_{\alpha\in\mathcal{B}(\mathbf{a}_1,\mathbf{t}_1)}\psi(\alpha)\right| &= \sum_{\psi\neq\psi_0}\left|\sum_{\alpha\in\mathcal{B}(\mathbf{a}_1,\mathbf{t}_1)}\prod_{j=1}^{n_K}\psi(c_j\alpha_j)\right| \\ &= \sum_{\psi\neq\psi_0}\prod_{j=1}^{n_K}\left|\sum_{c_j=\lceil a_j\rceil}^{\lfloor a_j+t_j\rfloor}\psi_{\alpha_j}(c_j)\right| \\ &\leq \prod_{j=1}^{n_K}\sum_{\psi\neq\psi_0}\left|\sum_{c_j=\lceil a_j\rceil}^{\lfloor a_j+t_j\rfloor}\psi_{\alpha_j}(c_j)\right| \\ &\ll p^{n_K}(\log p)^{n_K}\end{aligned}$$

by the estimate of (5.16). Therefore, (5.17) is bounded in absolute value by a constant times

$$p^{n_K-3/2}(\log p)^{n_K}\left(P_0(\mathbf{t}_1) + P_0(\mathbf{t}_2) + p^{n_K}(\log p)^{n_K}\right).$$

□

Lemma 5.3.3. *Suppose $\mathfrak{p}$ and $\mathfrak{p}'$ are degree one primes not lying above the same rational prime. Further, suppose that neither contains 6 or any element of our fixed basis $\{\alpha_j\}_{j=1}^{n_K}$. Let p be the unique rational prime number lying below $\mathfrak{p}$, and let p' be the unique rational prime number lying below $\mathfrak{p}'$. Fix elliptic curves $E_{a,b}$ and $E_{a',b'}$ defined over $\mathcal{O}_K/\mathfrak{p}$ and*

$\mathcal{O}_K/\mathfrak{p}'$ respectively. Then

$$\left|\mathcal{C}_{\mathbf{a},\mathbf{t}}(E_{a,b},E_{a',b'};\mathfrak{p},\mathfrak{p}')\right| = \frac{(p-1)(p'-1)}{c_p(a,b)c_{p'}(a',b')(pp')^2}P_0(\mathbf{t}) + O\left((pp')^{2n_K-3/2}(\log(pp'))^{2n_K}\right)$$
$$+ O\left(\left[P_0(\mathbf{t}_1)+P_0(\mathbf{t}_2)\right](pp')^{n_K-3/2}(\log(pp'))^{n_K} + \frac{P_1(\mathbf{t})}{pp'}\right).$$

Proof. As in the proof of Lemma 5.3.2, we use character sums to see that $\left|\mathcal{C}_{\mathbf{a},\mathbf{t}}(E_{a,b},E_{a',b'};\mathfrak{p},\mathfrak{p}')\right|$ is equal to

$$\frac{1}{c_p(a,b)c_{p'}(a',b')} \sum_{\substack{u\in(\mathcal{O}_K/\mathfrak{p})^*,\\ v\in(\mathcal{O}_K/\mathfrak{p}')^*}} \sum_{\substack{\alpha\in\mathcal{B}(\mathbf{a}_1,\mathbf{t}_1)\\ \beta\in\mathcal{B}(\mathbf{a}_2,\mathbf{t}_2)}} \frac{1}{(pp')^2}$$
$$\cdot \sum_{\substack{\psi,\chi\\ \psi',\chi'}} \psi(\alpha-au^4)\chi(\beta-bu^6)\psi'(\alpha-a'v^4)\chi'(\beta-b'v^6),$$

where ψ,χ each range over all additive characters of $\mathcal{O}_K/\mathfrak{p}$ and ψ',χ' each range over all additive characters of $\mathcal{O}_K/\mathfrak{p}'$. As before, the main term arises when all four characters are trivial and contributes

$$\frac{(p-1)(p'-1)}{c_p(a,b)c_{p'}(a',b')(pp')^2}P_0(\mathbf{t}) + O\left(\frac{P_1(\mathbf{t})}{pp'}\right).$$

We again apply Weil's Theorem to find that the remainder is bounded by a constant multiple of

$$\frac{\sqrt{pp'}}{(pp')^2}\sum_{\substack{\psi,\chi\\ \psi',\chi'}}{}' \left|\sum_{\alpha\in\mathcal{B}(\mathbf{a}_1,\mathbf{t}_1)}\psi(\alpha)\psi'(\alpha)\right|\left|\sum_{\beta\in\mathcal{B}(\mathbf{a}_2,\mathbf{t}_2)}\chi(\beta)\chi'(\beta)\right|,$$

where the prime on the outer sum means that we omit the term where all four characters are trivial. By the Chinese Remainder Theorem, this expression is equal to

$$\frac{\sqrt{pp'}}{(pp')^2}\sum_{\lambda,\tau}{}' \left|\sum_{\alpha\in\mathcal{B}(\mathbf{a}_1,\mathbf{t}_1)}\lambda(\alpha)\right|\left|\sum_{\beta\in\mathcal{B}(\mathbf{a}_2,\mathbf{t}_2)}\tau(\beta)\right|,$$

where λ,τ each range over all additive characters of $\mathcal{O}_K/\mathfrak{p}\mathfrak{p}'$. The prime on the outer sum again means that we omit the term where both λ and τ are trivial. Observe that $\mathcal{O}_K/\mathfrak{p}\mathfrak{p}' \cong \mathbb{Z}/pp'\mathbb{Z}$ since $p \neq p'$. The additive characters of $\mathbb{Z}/pp'\mathbb{Z}$ are all of the $\lambda(c) = e(hc/pp')$ for some $0 \leq h < pp'$. Thus, arguing as in the proof of Lemma 5.3.2, we obtain the desired result. □

5.4 A Weighted Average of Special Values of L-functions

In this section, we compute a certain weighted average of special values of L-functions. This average is interesting in its own right, but will also figure as a key ingredient in the proofs of Theorems 5.2.1 and 5.2.6. Recall that given a Dirichlet character χ, for $\Re(s)$ sufficiently large, the L-function associated to χ is defined by $L(s,\chi) := \sum_{n\geq 1} \frac{\chi(n)}{n^s}$.

We begin by making a few elementary observations and by defining some more notation. Since only finitely many primes of K may ramify in $K(\zeta_{m_K})$, there exists an integer r_K such that if $\mathfrak{p}$ is a prime of K with $\mathrm{N}\mathfrak{p} > r_K$, then $\mathfrak{p}$ does not ramify in $K(\zeta_{m_K})$. Hence, if $\mathfrak{p}$ is a prime of K with $\mathrm{N}\mathfrak{p} > r_K$, then $\mathrm{N}\mathfrak{p} \equiv a \pmod{m_K}$ for some $a \in G_{m_K}$. Similarly, there are only finitely many primes containing an element of the basis $\mathcal{B}$. Thus, there exists an integer r_K' such that if $\mathrm{N}\mathfrak{p} > r_K'$, then $\mathfrak{p} \nmid \prod_{j=1}^{n_K} \alpha_j$. Given a fixed integer r, we make the definition $B(r) := \max\{5, r^2/4, \Delta_K, r_K, r_K'\}$.

Throughout the remainder of the chapter, given an integer D, we write χ_D for the Legendre symbol $\left(\frac{D}{\cdot}\right)$. Given a prime of K, say $\mathfrak{p}$, we will write p for the unique rational prime lying below $\mathfrak{p}$. We also put $d_k(p) := (r^2-4p)/k^2$ if $k^2|(r^2-4p)$. Finally, we define the following set of rational primes:

$$S_k(r,f,K,x) := \left\{B(r) < p \leq x : f_p(K) = f, k^2|(4p^f - r^2), \text{and } d_k(p) \equiv 0, 1 \pmod 4\right\}.$$

Proposition 5.4.1. *Let*

$$A(r,1,K,x) := n_K \sum_{\substack{k \leq 2\sqrt{x},\\ (k,2r)=1}} \frac{1}{k} \sum_{p \in S_k(r,1,K,x)} L(1, \chi_{d_k(p)}) \log p.$$

Then for any fixed $c > 0$,

$$A(r, 1, K, x) = C'_{K,r,1}x + O\left(\frac{x}{(\log x)^c}\right),$$

where

$$C'_{K,r,1} := n'_K \sum_{b \in G_{m_K}} \sum_{k=1}^{\infty} \frac{1}{k} \sum_{n=1}^{\infty} \frac{c_k^{r,b,m_K}(n)}{n\varphi([m_K, nk^2])}$$

is a convergent double sum.

Before proceeding with the proof of Proposition 5.4.1, we need two preliminary results. The first result is essentially Theorem 4.2.1 of Chapter 4. In fact, it is precisely the version described in Remark 4.2.2 immediately following the statement of Theorem 4.2.1. For convenience, we state this alternate version here. Let

$$\theta_{K,1}(x; q, a) := \sum_{\substack{\mathrm{N}\mathfrak{p} \leq x \\ \deg \mathfrak{p} = 1 \\ \mathrm{N}\mathfrak{p} \equiv a \pmod q}} \log \mathrm{N}\mathfrak{p}, \tag{5.18}$$

and let

$$E_{K,1}(x; q, a) := \theta_{K,1}(x; q, a) - x/\varphi_K(q), \tag{5.19}$$

where $\varphi_K(q) = |G_q|$.

Theorem 5.4.2. *For any fixed $M > 0$,*

$$\sum_{q \leq Q} \sum_{a \in G_q} E_{K,1}(x; q, a)^2 \ll xQ \log x,$$

provided that $x(\log x)^{-M} \leq Q \leq x$.

Remark 5.4.3. To obtain a proof, one may adapt the proof of Theorem 4.2.1 given in Chapter 4.

Our second preliminary result is a careful application of the Chebotarëv Density Theorem.

Lemma 5.4.4. *For fixed integers n and k,*

$$n_K \sum_{p \in S_k(r,1,K,x)} \left(\frac{d_k(p)}{n}\right) \log p = \frac{x}{\varphi_K\left([m_K, nk^2]\right)} \sum_{b \in G_{m_K}} c_k^{r,b,m_K}(n) + O\left(\log n + \frac{1}{k^2}\right)$$
$$+ O\left(\sum_{h \in G_{m_K nk^2}} \left|E_{K,1}(x; m_K nk^2, h)\right|\right). \tag{5.20}$$

Proof. First, note that

$$\theta_{K,1}(x;q,a) = n_K \sum_{\substack{p \le x \\ g_p(K)=1 \\ p \equiv a \pmod q}} \log p.$$

Since $\left(\frac{\cdot}{n}\right)$ is periodic modulo $4n$ (in fact, modulo n) and since $d_k(p)$ must be restricted to values that are 0 and 1 modulo 4, we have

$$n_K \sum_{p \in S_k(r,1,K,x)} \left(\frac{d_k(p)}{n}\right) \log p = n_K \sum_{\substack{a \in (\mathbb{Z}/4n\mathbb{Z})^* \\ a \equiv 0,1 \pmod 4}} \left(\frac{a}{n}\right) \sum_{\substack{p \in S_k(r,1,K,x) \\ d_k(p) \equiv a \pmod{4n}}} \log p. \tag{5.21}$$

Now, the conditions $k^2|(r^2-4p)$ and $d_k(p) \equiv a \pmod{4n}$ are equivalent to the one condition $r^2 - 4p \equiv ak^2 \pmod{4nk^2}$, which we want to solve for p. Rearranging, we find that this is equivalent to $4p \equiv r^2 - ak^2 \pmod{4nk^2}$, which is equivalent to $p \equiv (r^2-ak^2)/4 \pmod{nk^2}$. Thus, (5.21) becomes

$$n_K \sum_{p \in S_k(r,1,K,x)} \left(\frac{d_k(p)}{n}\right) \log p = n_K \sum_{\substack{a \in (\mathbb{Z}/4n\mathbb{Z})^* \\ a \equiv 0,1 \pmod 4 \\ 4|(r^2-ak^2)}} \left(\frac{a}{n}\right) \sum_{\substack{B(r) < p \le x \\ f_p(K)=1 \\ p \equiv \frac{r^2-ak^2}{4} \pmod{nk^2}}} \log p. \tag{5.22}$$

Recall the definition of r_K on page 108. In particular, recall that if $\mathfrak{p}$ is a prime of K with $\mathrm{N}\mathfrak{p} > r_K$, then $\mathrm{N}\mathfrak{p} \equiv b \pmod{m_K}$ for some $b \in G_{m_K}$. Thus, since $B(r) \ge r_K$, (5.22) is equal to

$$\sum_{\substack{a\in(\mathbb{Z}/4n\mathbb{Z})^* \\ a\equiv 0,1 \pmod 4 \\ 4|(r^2-ak^2)}} \left(\frac{a}{n}\right) \sum_{b\in G_{m_K}} \sum_{\substack{B(r)<\mathrm{N}\mathfrak{p}\le x \\ \deg\mathfrak{p}=1 \\ \mathrm{N}\mathfrak{p}\equiv(r^2-ak^2)/4 \pmod{nk^2} \\ \mathrm{N}\mathfrak{p}\equiv b \pmod{m_K}}} \log \mathrm{N}\mathfrak{p}. \tag{5.23}$$

By the Chebotarëv Density Theorem, there are infinitely many degree 1 primes of K satisfying the conditions $\mathrm{N}\mathfrak{p}\equiv b \pmod{m_K}$ and $\mathrm{N}\mathfrak{p}\equiv(r^2-ak^2)/4 \pmod{nk^2}$ provided that the two conditions do not directly conflict and the integers $(r^2-ak^2)/4$ and nk^2 are coprime. If the conditions conflict with one another, then there can be no primes with that property. We will deal with this situation later. If $(r^2-ak^2)/4$ is not coprime to nk^2, then there can be at most one prime satisfying these conditions. Furthermore, this can only happen when the greatest common divisor of nk^2 and the least positive residue of $(r^2-ak^2)/4$ is itself a prime ℓ and $\mathrm{N}\mathfrak{p}=\ell$. Now, if $\ell|k$, then ℓ^2 divides both $(r^2-ak^2)/4$ and nk^2. Thus, we need only consider those primes dividing n. Therefore, the expression in (5.23) is equal to

$$\sum_{\substack{a\in(\mathbb{Z}/4n\mathbb{Z})^* \\ a\equiv 0,1 \pmod 4 \\ \left(r^2-ak^2,4nk^2\right)=4}} \left(\frac{a}{n}\right) \sum_{b\in G_{m_K}} \sum_{\substack{B(r)<\mathrm{N}\mathfrak{p}\le x \\ \deg\mathfrak{p}=1 \\ \mathrm{N}\mathfrak{p}\equiv(r^2-ak^2)/4 \pmod{nk^2} \\ \mathrm{N}\mathfrak{p}\equiv b \pmod{m_K}}} \log \mathrm{N}\mathfrak{p} + O\left(\sum_{\substack{\ell|n \\ \ell \text{ prime}}} \log\ell\right). \tag{5.24}$$

Now, we interchange the sum on a with the sum on b. We note that the conditions

$$\mathrm{N}\mathfrak{p}\equiv(r^2-ak^2)/4 \pmod{nk^2}, \tag{5.25}$$

$$\mathrm{N}\mathfrak{p}\equiv b \pmod{m_K} \tag{5.26}$$

are contradictory unless $4b\equiv r^2-ak^2 \pmod{(4m_K,nk^2)}$. In the case that $4b\equiv r^2-ak^2 \pmod{(4m_K,nk^2)}$, the two conditions (5.25) and (5.26) are equivalent to the single condition

$$\mathrm{N}\mathfrak{p}\equiv h_{b,r,a,n,k} \pmod{[m_K,nk^2]}, \tag{5.27}$$

where $h_{b,r,a,n,k} := bnk^2 + m_K(r^2 - ak^2)/4$ and $[m_K, nk^2]$ denotes the least common multiple of m_K and nk^2. Thus, we have that (5.24) is equal to

$$\sum_{b \in G_{m_K}} c_k^{r,b,m_K}(n)\theta_{K,1}\left(x; [m_K, nk^2], h_{b,r,a,n,k}\right) + O\left(\log n\right) + O\left(\frac{1}{k^2}\right), \tag{5.28}$$

where the function $c_k^{r,b,m_K}(n)$ was defined in (5.8) on page 98, and the second big-O term comes from the primes of norm less than or equal to $B(r)$.

We now apply the Chebotarëv's theorem to estimate $\theta_{K,1}\left(x; [m_K, nk^2], h_{b,r,a,n,k}\right)$. The result is that (5.28) is equal to

$$\begin{aligned} &\frac{x}{\varphi_K\left([m_K, nk^2]\right)} \sum_{b \in G_{m_K}} c_k^{r,b,m_K}(n) + O\left(\log n + \frac{1}{k^2}\right) \\ &\qquad + O\left(\sum_{b \in G_{m_K}} \sum_{\substack{a \in (\mathbb{Z}/4n\mathbb{Z})^* \\ (r^2 - ak^2, 4nk^2) = 4}} \left|E_{K,1}(x; [m_K, nk^2], h_{b,r,a,n,k})\right|\right). \end{aligned} \tag{5.29}$$

For a fixed $b \in G_{m_K}$, we note that $h_{b,r,a,n,k}$ ranges over some subset of $G_{[m_K,nk^2]}$ as a ranges over $(\mathbb{Z}/4n\mathbb{Z})^*$. Thus, since G_{m_K} is a finite group, we have

$$\sum_{h \in G_{m_K}} \sum_{\substack{a \in (\mathbb{Z}/4n\mathbb{Z})^* \\ (r^2 - ak^2, 4nk^2) = 4}} \left|E_{K,1}(x; [m_K, nk^2], h_{b,r,a,n,k})\right| \ll \sum_{h \in G_{[m_K,nk^2]}} \left|E_{K,1}(x; [m_K, nk^2], h)\right|.$$

Facts from Galois theory imply that $G_{[m_K,nk^2]}$ is a quotient of $G_{m_K nk^2}$ by a group of size (m_K, nk^2); which, via the triangle inequality, implies that

$$\sum_{h \in G_{[m_K,nk^2]}} \left|E_{K,1}(x; [m_K, nk^2], h)\right| \le \sum_{h \in G_{m_K nk^2}} \left|E_{K,1}(x; m_K nk^2, h)\right|.$$

This concludes the proof. □

We now proceed with the proof of Proposition 5.4.1.

Proof of Proposition 5.4.1. Let U be a parameter to be chosen later. We begin with the integral identity

$$\sum_{n\geq 1}\left(\frac{d_k(p)}{n}\right)\frac{e^{-n/U}}{n} = L\left(1,\chi_{d_k(p)}\right) + \int_{\Re(s)=-1/2} L\left(s+1,\chi_{d_k(p)}\right)\Gamma(s+1)\frac{U^s}{s}ds,$$

where $\Gamma(s)$ is the Gamma function defined by

$$\Gamma(s) := \int_0^\infty t^{s-1}e^{-t}dt.$$

Compare with [Mur01, Exer. 6.6.3, p. 99]. We estimate the integral with Burgess' bound, which says $L\left(1/2+it,\chi_{d_k(p)}\right) \ll |t||d_k(p)|^{7/32}$. See [Bur63, Thm. 3]. This yields the identity

$$L(1,\chi_{d_k(p)}) = \sum_{n\geq 1}\left(\frac{d_k(p)}{n}\right)\frac{1}{n} = \sum_{n\geq 1}\left(\frac{d_k(p)}{n}\right)\frac{e^{-n/U}}{n} + O\left(\frac{|d_k(p)|^{7/32}}{U^{1/2}}\right).$$

Now, $|d_k(p)|^{7/32} = |\frac{r^2-4p}{k^2}|^{7/32} \ll (\frac{p}{k^2})^{7/32}$, which gives

$$\begin{aligned}\sum_{k\leq 2\sqrt{x}}\frac{1}{k}\sum_{p\in S_k(r,1,K,x)}\frac{p^{7/32}\log p}{k^{7/16}U^{1/2}} &\ll \frac{1}{\sqrt{U}}\sum_{p\leq x}p^{7/32}\log p\\ &\ll \frac{1}{\sqrt{U}}x^{7/32}\log x\frac{x}{\log x}\\ &\ll \frac{x^{39/32}}{\sqrt{U}}.\end{aligned}$$

Thus, if

$$U \geq x^{7/16}(\log x)^{2c}, \tag{5.30}$$

then we have

$$A(r,1,K,x) = n_K\sum_{k\leq 2\sqrt{x}}\frac{1}{k}\sum_{n\geq 1}\frac{e^{-n/U}}{n}\sum_{p\in S_k(r,1,K,x)}\left(\frac{d_k(p)}{n}\right)\log p + O\left(\frac{x}{(\log x)^c}\right). \tag{5.31}$$

Let V be a parameter to be chosen later. We now dispense with the large values of

k and n in (5.31). First, observe that

$$\begin{aligned}\sum_{V<k\leq 2\sqrt{x}} \frac{1}{k} \sum_{n\geq 1} \frac{e^{-n/U}}{n} \sum_{p\in S_k(r,1,K,x)} \left(\frac{d_k(p)}{n}\right) \log p &\ll \log x \sum_{n\geq 1} \frac{e^{-n/U}}{n} \sum_{V<k\leq 2\sqrt{x}} \frac{1}{k} \sum_{\substack{m\leq x,\\ k^2|(4m-r^2)}} 1 \\ &\ll x\log x \sum_{n\geq 1} \frac{e^{-n/U}}{n} \sum_{V<k\leq 2\sqrt{x}} \frac{1}{k^3} \\ &\ll (x\log x)V^{-2} \sum_{n\geq 1} \frac{e^{-n/U}}{n}.\end{aligned}$$

By Alternating Series Estimation Theorem, we have $1-e^{-z} > z - \frac{1}{2}z^2$. Whence, for $U>1$,

$$\sum_{n\geq 1} \frac{e^{-n/U}}{n} = -\log(1-e^{-1/U}) \leq -\log\left(\frac{1}{U} - \frac{1}{2U^2}\right) \ll \log U.$$

So, in particular, if

$$V \geq (\log x)^{(c+2)/2}, \tag{5.32}$$

$$U \ll x, \tag{5.33}$$

then

$$\sum_{V<k\leq 2\sqrt{x}} \frac{1}{k} \sum_{n\geq 1} \frac{e^{-n/U}}{n} \sum_{p\in S_k(r,1,K,x)} \left(\frac{d_k(p)}{n}\right) \log p \ll \frac{x\log x}{V^2} \log U \ll \frac{x}{(\log x)^c}.$$

Hence (5.31) becomes

$$A(r,1,K,x) = n_K \sum_{k\leq V} \frac{1}{k} \sum_{n\geq 1} \frac{e^{-n/U}}{n} \sum_{p\in S_k(r,1,K,x)} \left(\frac{d_k(p)}{n}\right) \log p + O\left(\frac{x}{(\log x)^c}\right). \tag{5.34}$$

Observe that

$$\sum_{n\geq U\log U} \frac{e^{-n/U}}{n} \ll \frac{1}{U\log U} \int_{U\log U}^{\infty} e^{-x/U} dx = \frac{1}{U\log U}.$$

Thus, assuming that U satisfies (5.30), we have

$$\sum_{\substack{k\le V,\\(k,2r)=1}}\frac{1}{k}\sum_{n>U\log U}\frac{e^{-n/U}}{n}\sum_{p\in S_k(r,1,K,x)}\left(\frac{d_k(p)}{n}\right)\log p \ll \frac{\log x}{U\log U}\sum_{\substack{k\le V,\\(k,2r)=1}}\frac{1}{k}\sum_{\substack{m\le x,\\k^2|(4m-r^2)}}1$$

$$\ll \frac{x\log x}{U\log U}\ll\frac{x}{(\log x)^c}.$$

Therefore, (5.34) becomes

$$A(r,1,K,x)=n_K\sum_{k\le V}\frac{1}{k}\sum_{n\le U\log U}\frac{e^{-n/U}}{n}\sum_{p\in S_k(r,1,K,x)}\left(\frac{d_k(p)}{n}\right)\log p+O\left(\frac{x}{(\log x)^c}\right). \quad (5.35)$$

By Lemma 5.4.4, n_K times the innermost sum may be written as

$$n_K\sum_{p\in S_k(r,1,K,x)}\left(\frac{d_k(p)}{n}\right)\log p=\frac{x}{\varphi_K([m_K,nk^2])}\sum_{b\in G_{m_K}}c_k^{r,b,m_K}(n)+O\left(\log n+\frac{1}{k^2}\right)$$
$$+O\left(\sum_{h\in G_{m_Knk^2}}\left|E_{K,1}(x;m_Knk^2,h)\right|\right).$$
$$(5.36)$$

We first turn our attention to the last O-term in (5.36) and sum over n and k. Applying the Cauchy-Schwarz inequality, we have

$$\sum_{k\le V}\frac{1}{k}\left[\sum_{n\le U\log U}\left(\sum_{h\in G_{m_Knk^2}}\frac{e^{-n/U}}{n}\left|E_{K,1}(x;m_Knk^2,h)\right|\right)\right]$$
$$\le\sum_{k\le V}\frac{1}{k}\left[\sum_{n\le U\log U}\frac{\varphi_K(m_Knk^2)}{n^2}\right]^{1/2}\left[\sum_{n\le U\log U}\sum_{h\in G_{m_Knk^2}}E_{K,1}\left(x;m_Knk^2,h\right)^2\right]^{1/2}$$
$$\ll V\sqrt{\log U}\left[\sum_{q\le m_KV^2U\log U}\sum_{h\in G_q}E_{K,1}(x;q,h)^2\right]^{1/2}.$$
$$(5.37)$$

We now choose

$$U = \frac{x}{(\log x)^{(5c+15)}}, \tag{5.38}$$

$$V = (\log x)^{(c+3)/2}. \tag{5.39}$$

Note that this choice is in accord with (5.30), (5.32), and (5.33). We also observe that $x \gg V^2 U \log U \gg x(\log x)^{-M}$, for say $M = 4c + 11$. Thus, Theorem 5.4.2 applies, and we have

$$\left(\sum_{q \le m_K V^2 U \log U} \sum_{h \in G_m} E_{K,1}(x; q, h)^2 \right)^{1/2} \ll \sqrt{x V^2 U \log U \log x} \ll \frac{x}{(\log x)^{2c+5}}. \tag{5.40}$$

Whence, we see that (5.37) is bounded by a constant times $x/(\log x)^c$.

Now, we concentrate on the first O-term in (5.36) and sum over n and k, to find

$$\sum_{k \le V} \frac{1}{k} \sum_{n < U \log U} \frac{e^{-n/U}}{n} \left(\log n + \frac{1}{k^2} \right) \ll \log V (\log U)^2 \ll \frac{x}{(\log x)^c}.$$

Combining (5.35), (5.36), (5.37), and (5.40), we have

$$A(r, 1, K, x) = x \sum_{b \in G_{m_K}} \sum_{\substack{k \le V, \\ n \le U \log U}} \frac{e^{-n/U} c_k^{r,b,m_K}(n)}{nk\varphi_K([m_K, nk^2])} + O\left(\frac{x}{(\log x)^c} \right), \tag{5.41}$$

where $c_k^{r,b,m_K}(n)$ is defined as in (5.8).

Observe that since $m_K | [m_K, nk^2]$, $\mathcal{A} = \mathbb{Q}^{\text{cyc}} \cap K = \mathbb{Q}(\zeta_{m_K}) \cap K \subseteq \mathbb{Q}(\zeta_{[m_K, nk^2]})$. Thus, we have the isomorphism $G_{[m_K, nk^2]} \cong \text{Gal}(\mathbb{Q}(\zeta_{[m_K, nk^2]})/\mathcal{A})$. Recalling the definition $n'_K = [\mathcal{A} : \mathbb{Q}]$, we have $\varphi([m_K, nk^2]) = n'_K \varphi_K([m_K, nk^2])$. Therefore, we may rewrite (5.41) as

$$A(r, 1, K, x) = x n'_K \sum_{b \in G_{m_K}} \sum_{\substack{k \le V, \\ n \le U \log U}} \frac{e^{-n/U} c_k^{r,b,m_K}(n)}{nk\varphi([m_K, nk^2])} + O\left(\frac{x}{(\log x)^c} \right). \tag{5.42}$$

We now proceed with removing the parameters U and V. Observe that

$$\sum_{\substack{k\leq V,\\ n\leq U\log U}} \frac{e^{-n/U}c_k^{r,b,m_K}(n)}{nk\varphi([m_K,nk^2])} = \sum_{\substack{k\geq 1,\\ n\leq U\log U}} \frac{e^{-n/U}c_k^{r,b,m_K}(n)}{nk\varphi([m_K,nk^2])} + O\left(\sum_{\substack{k>V,\\ n\leq U\log U}} \frac{e^{-n/U}\varphi(n)}{nk\varphi([m_K,nk^2])}\right).$$

Elementary properties of the Euler φ function imply

$$\varphi([m_K,nk^2]) = \frac{\varphi(m_Knk^2)}{(m_K,nk^2)} \geq \frac{\varphi(m_K)\varphi(n)\varphi(k^2)}{m_K} \geq \varphi(n)k\varphi(k),$$

and

$$\frac{1}{\varphi(k)} = \frac{1}{k}\prod_{\ell|k}\frac{\ell}{\ell-1} \leq \frac{1}{k}\prod_{\ell|k}2 \leq \frac{2^{\nu(k)}}{k}.$$

Hence,

$$\sum_{\substack{k>V,\\ n\leq U\log U}} \frac{e^{-n/U}\varphi(n)}{nk\varphi([m_K,nk^2])} \ll \sum_{n\leq U\log U}\frac{1}{n}\sum_{k>V}\frac{1}{k^2\varphi(k)} \ll \log U\sum_{k>V}\frac{2^{\nu(k)}}{k^3},$$

and partial summation yields

$$\begin{aligned}\sum_{k>V}\frac{2^{\nu(k)}}{k^3} &= \lim_{X\to\infty}\left(\frac{1}{X^3}\sum_{k=1}^{X}2^{\nu(k)} + \int_V^X \frac{\sum_{k=1}^t 2^{\nu(k)}}{3t^2}dt - \frac{1}{(V+1)^3}\sum_{k=1}^{V}2^{\nu(k)}\right)\\ &\ll \frac{\log V}{V^2} \ll \frac{1}{(\log x)^c}\end{aligned}$$

since $\sum_{k=1}^X 2^{\nu(k)} \ll X\log X$. See [Mur01, Exer. 4.4.18, p. 68] for example. Therefore,

$$\sum_{\substack{k\leq V,\\ n\leq U\log U}} \frac{e^{-n/U}c_k^{r,b,m_K}(n)}{nk\varphi([m_K,nk^2])} = \sum_{\substack{k\geq 1,\\ n\leq U\log U}} \frac{e^{-n/U}c_k^{r,b,m_K}(n)}{nk\varphi([m_K,nk^2])} + O\left(\frac{1}{(\log x)^c}\right).$$

Furthermore,

$$\begin{aligned}\sum_{\substack{k\geq 1,\\ n\leq U\log U}} \frac{e^{-n/U}c_k^{r,b,m_K}(n)}{nk\varphi([m_K,nk^2])} &= \sum_{\substack{k\geq 1,\\ n\geq 1}} \frac{e^{-n/U}c_k^{r,b,m_K}(n)}{nk\varphi([m_K,nk^2])} + O\left(\sum_{\substack{k\geq 1,\\ n> U\log U}} \frac{e^{-n/U}c_k^{r,b,m_K}(n)}{nk\varphi([m_K,nk^2])}\right)\\ &= \sum_{\substack{k\geq 1,\\ n\geq 1}} \frac{e^{-n/U}c_k^{r,b,m_K}(n)}{nk\varphi([m_K,nk^2])} + O\left(\frac{1}{(\log x)^c}\right),\end{aligned}$$

since

$$\begin{aligned}\sum_{\substack{k\geq 1,\\ n> U\log U}} \frac{e^{-n/U}c_k^{r,b,m_K}(n)}{nk\varphi([m_K,nk^2])} &\ll \int_{U\log U}^{\infty} \frac{e^{-t/U}}{t}dt \ll \frac{1}{U\log U}\int_{U\log U}^{\infty} e^{-t/U}dt\\ &\ll \frac{1}{U^3\log U} \ll \frac{1}{(\log x)^c}.\end{aligned}$$

Therefore,

$$A(r,1,K,x) = xn_K'\sum_{b\in G_{m_K}}\sum_{\substack{k\geq 1,\\ n\geq 1}} \frac{e^{-n/U}c_k^{r,b,m_K}(n)}{nk\varphi([m_K,nk^2])} + O\left(\frac{x}{(\log x)^c}\right). \tag{5.43}$$

The final step of the proof is to show that

$$\sum_{\substack{k\geq 1,\\ n\geq 1}} \frac{e^{-n/U}c_k^{r,b,m_K}(n)}{nk\varphi([m_K,nk^2])} = \sum_{\substack{k\geq 1,\\ n\geq 1}} \frac{c_k^{r,b,m_K}(n)}{nk\varphi([m_K,nk^2])} + O\left(\frac{1}{(\log x)^c}\right) \tag{5.44}$$

and that double sum on the right is convergent. To do this, we begin by considering the Dirichlet series

$$D_k(s) := \sum_{n=1}^{\infty} \frac{c_k^{r,b,m_K}(n)}{\varphi([m_K,nk^2])}n^{-s}, \tag{5.45}$$

which we claim converges for $\Re(s) > 1/2$. To demonstrate this, we first note that

$$D_k(s) = \sum_{n=1}^{\infty} \frac{(m_K,nk^2)c_k^{r,b,m_K}(n)}{k\varphi([m_K,nk])}n^{-s} \ll \frac{1}{k\varphi(k)}\sum_{n=1}^{\infty} \frac{c_k^{r,b,m_K}(n)}{\varphi(n)}n^{-s}. \tag{5.46}$$

We prove the convergence of $D_k(s)$ for $\Re(s) > 1/2$ by showing that $\sum_{n\geq 1} \frac{c_k^{r,b,m_K}(n)}{\varphi(n)} n^{-s}$ converges for $\Re(s) > 1/2$. Note that this also implies that $D_k(1) \ll \frac{1}{k\varphi(k)}$, and hence the double sum on the right hand side of (5.44) converges.

Now, let $\kappa(n)$ denote the multiplicative function whose value on prime powers is determined by the definition

$$\kappa(\ell^m) := \begin{cases} \ell, & 2 \nmid m, \\ 1, & 2|m. \end{cases} \tag{5.47}$$

Then Lemma 2.6 of [Jam05] states that $c_k^{r,b,m_K}(n) \leq n/\kappa(n)$ for all n. Thus,

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{c_k^{r,b,m_K}(n)}{\varphi(n) n^s} &\leq \prod_{\ell} \left[1 + \sum_{j=1}^{\infty} \left(\frac{\ell^{2j}/\kappa(\ell^{2j})}{\varphi(\ell^{2j})\ell^{2js}} + \frac{\ell^{2j-1}/\kappa(\ell^{2j-1})}{\varphi(\ell^{2j-1})\ell^{(2j-1)s}} \right) \right] \\ &= \prod_{\ell} \left[1 + \frac{\ell}{\ell-1} \sum_{j=1}^{\infty} \left(\frac{1}{\ell^{2s}} \right)^j + \frac{\ell^s}{\ell-1} \sum_{j=1}^{\infty} \left(\frac{1}{\ell^{2s}} \right)^j \right] \\ &= \prod_{\ell} \left[1 + \left(\frac{1}{1-\frac{1}{\ell^{2s}}} \right) \left(\frac{\ell^s+\ell}{\ell^{2s}(\ell-1)} \right) \right] \\ &= \prod_{\ell} \left[1 + \frac{\ell}{\ell-1} \left(\frac{\ell^{s-1}+1}{\ell^{2s}-1} \right) \right]. \end{aligned}$$

The infinite product converges for $\Re(2s) - \max\{0, \Re(s-1)\} > 1$, i.e., for $\Re(s) > 1/2$.

For any $\epsilon > 0$, we apply [Mur01, Exer. 6.6.3, p. 99] to obtain the identity

$$\sum_{n\geq 1} \frac{e^{-n/U} c_k^{r,b,m_K}(n)}{n\varphi([m_K, nk^2])} = D_k(1) + \int_{\Re(s)=-1/2+\epsilon} \Gamma(s+1) D_k(s+1) \frac{U^s}{s} ds. \tag{5.48}$$

The integral is then bounded by a constant times $\frac{1}{k} U^{-1/2+\epsilon}$. Summing over k, we have

$$\sum_{k\geq 1} \frac{1}{k} \sum_{n\geq 1} \frac{e^{-n/U} c_k^{r,b,m_K}(n)}{n\varphi([m_K, nk^2])} = \sum_{k\geq 1} \frac{1}{k} \sum_{n\geq 1} \frac{c_k^{r,b,m_K}(n)}{n\varphi([m_K, nk^2])} + O\left(U^{-1/2+\epsilon} \sum_{k\geq 1} \frac{1}{k^2} \right),$$

which completes the proof since $U = x/(\log x)^{5c+15}$ implies that $U^{-1/2+\epsilon} \ll (\log x)^{-c}$ for ϵ small enough. □

5.5 The Average Order of $\pi_E^{r,1}(x)$

We break our computation of the average order of $\pi_E^{r,1}(x)$ into two steps. We record these two steps as separate propositions since the second step will also be useful in bounding the size of the variance of $\pi_E^{r,1}(x)$. Theorem 5.2.1 will follow immediately by combining the results of the two propositions. As our first step in computing the average order, we convert the average into a weighted sum of Hurwitz class numbers.

Proposition 5.5.1. *Let r be a fixed integer. Then*

$$\frac{1}{|\mathcal{C}_{\mathbf{a},\mathbf{t}}|}\sum_{E\in\mathcal{C}_{\mathbf{a},\mathbf{t}}}\pi_E^{r,1}(x)=\frac{n_K}{2}\sum_{\substack{B(r)<p\le x\\ f_p(K)=1}}\frac{H(4p-r^2)}{p}+E_0(x;\mathbf{t}),$$

where

$$E_0(x;\mathbf{t})\ll\log\log x+\frac{\sqrt{x}/\log x}{\mathbf{t}_{\min}}+\left(\frac{1}{P_0(\mathbf{t}_1)}+\frac{1}{P_0(\mathbf{t}_2)}\right)(x\log x)^{n_K}+\frac{(x\log x)^{2n_K}}{P_0(\mathbf{t})}.$$

Proof. Since there are only finitely many primes of K with norm less than $B(r)$, we have

$$\begin{aligned}\frac{1}{|\mathcal{C}_{\mathbf{a},\mathbf{t}}|}\sum_{E\in\mathcal{C}_{\mathbf{a},\mathbf{t}}}\pi_E^{r,1}(x)&=\frac{1}{|\mathcal{C}_{\mathbf{a},\mathbf{t}}|}\sum_{E\in\mathcal{C}_{\mathbf{a},\mathbf{t}}}\sum_{\substack{B(r)<\mathrm{N}\mathfrak{p}\le x\\ \deg\mathfrak{p}=1\\ a_{\mathfrak{p}}(E)=r}}1+O(1)=\frac{1}{|\mathcal{C}_{\mathbf{a},\mathbf{t}}|}\sum_{\substack{B(r)<\mathrm{N}\mathfrak{p}\le x\\ \deg\mathfrak{p}=1}}\sum_{\substack{E\in\mathcal{C}_{\mathbf{a},\mathbf{t}}\\ a_{\mathfrak{p}}(E)=r}}1+O(1)\\&=\frac{1}{|\mathcal{C}_{\mathbf{a},\mathbf{t}}|}\sum_{\substack{B(r)<\mathrm{N}\mathfrak{p}\le x\\ \deg\mathfrak{p}=1}}\left[\sum_{\substack{\tilde{E}/\mathbb{F}_p\\ \#E(\mathbb{F}_p)=p+1-r}}|\mathcal{C}_{\mathbf{a},\mathbf{t}}(E;\mathfrak{p})|+O\left(\sum_{\substack{E\in\mathcal{C}_{\mathbf{a},\mathbf{t}}\\ E^{\mathfrak{p}}\text{ sing.}}}1\right)\right]+O(1),\end{aligned}\tag{5.49}$$

where the sum in first O-term in the last line of (5.49) is over all elliptic curves in $\mathcal{C}_{\mathbf{a},\mathbf{t}}$ whose reductions are singular modulo $\mathfrak{p}$.

We now concentrate on estimating $1/|\mathcal{C}_{\mathbf{a},\mathbf{t}}|$ times the bracketed expression in the last line of (5.49). Arguing as in the proof of Lemma 5.3.2, we have

$$\frac{1}{|\mathcal{C}_{\mathbf{a},\mathbf{t}}|}\sum_{\substack{E\in\mathcal{C}_{\mathbf{a},\mathbf{t}}\\ E^{\mathfrak{p}}\text{ sing.}}} 1 = \frac{1}{|\mathcal{C}_{\mathbf{a},\mathbf{t}}|}\sum_{\substack{a,b\in\mathcal{O}_K/\mathfrak{p}\\ 4a^3+27b^2=0}}\frac{1}{p^2}\sum_{\alpha\in\mathcal{B}(\mathbf{a}_1,\mathbf{t}_1)}\sum_{\beta\in\mathcal{B}(\mathbf{a}_2,\mathbf{t}_2)}\sum_{\psi}\psi(\alpha-a)\sum_{\psi'}\psi'(\beta-b)$$
$$\ll \frac{1}{p}+\left(\frac{1}{P_0(\mathbf{t}_1)}+\frac{1}{P_0(\mathbf{t}_2)}\right)\frac{(p\log p)^{n_K}}{p}+\left(\frac{1}{P_0(\mathbf{t})}\right)\frac{(p\log p)^{2n_K}}{p}. \quad (5.50)$$

Further, since there are at most 10 isomorphism classes $\tilde{E}_{a,b}$ over $\mathbb{F}_p$ with $ab=0$ and since $p=\mathrm{N}\mathfrak{p}>B(r)$, we may apply Deuring's Theorem (Theorem 1.2.21), Lemma 5.3.1, and Lemma 5.3.2, to obtain

$$\frac{1}{|\mathcal{C}_{\mathbf{a},\mathbf{t}}|}\sum_{\substack{\tilde{E}/\mathbb{F}_p\\ \#E(\mathbb{F}_p)=p+1-r}}|\mathcal{C}_{\mathbf{a},\mathbf{t}}(E;\mathfrak{p})| = \frac{H(4p-r^2)}{2p}+O\left(\frac{1}{p}+\frac{H(4p-r^2)}{p}\frac{1}{\mathbf{t}_{\min}}\right)$$
$$+O\left(p^{n_K-3/2}(\log p)^{n_K}H(4p-r^2)\left[\frac{1}{P_0(\mathbf{t}_1)}+\frac{1}{P_0(\mathbf{t}_2)}\right]\right)$$
$$+O\left(\frac{p^{2n_K-3/2}(\log p)^{2n_K}H(4p-r^2)}{P_0(\mathbf{t})}\right), \quad (5.51)$$

where $H(4p-r^2)$ is the Hurwitz class number of discriminant r^2-4p. Substituting equations (5.50) and (5.51) back into (5.49) and writing $E_0(x;\mathbf{t})$ for the error term, we have

$$\frac{1}{|\mathcal{C}_{\mathbf{a},\mathbf{t}}|}\sum_{E\in\mathcal{C}_{\mathbf{a},\mathbf{t}}}\pi_E^{r,1}(x) = \frac{n_K}{2}\sum_{\substack{p\le x\\ f_p(K)=1}}\frac{H(4p-r^2)}{p}+E_0(x;\mathbf{t}). \quad (5.52)$$

We now turn to bounding the error term $E_0(x;\mathbf{t})$. It is well known that

$$\sum_{p\le x}\frac{1}{p}\sim\log\log x.$$

See [Dav80, eqn. (5), p. 56] for example. Also, by [DP99, eqn. (32), p. 179], we have

$$\sum_{p\le x}\frac{H(4p-r^2)}{p}\ll\frac{\sqrt{x}}{\log x}. \quad (5.53)$$

It remains then to bound

$$\sum_{p\le x} p^{n_K-3/2}(\log p)^{2n_K} H(4p-r^2) \tag{5.54}$$

since $\displaystyle\sum_{p\le x} p^{2n_K-3/2}(\log p)^{n_K} H(4p-r^2)$ may be bounded in a similar manner. The key to bounding both is in bounding $\sum_{p\le x} H(4p-r^2)$. We do this as follows.

The class number formula applied to the imaginary quadratic order of discriminant $-d<0$ has the simple form

$$L\left(1,\left(\frac{-d}{\cdot}\right)\right) = \frac{2\pi h(-d)}{w(-d)\sqrt{d}}. \tag{5.55}$$

See [IK04, eqn. (22.59), p. 513] and [Cox89, Cor. 7.28] for example. Thus, by definition of the Hurwitz class number, we have

$$\begin{aligned} H(4p-r^2) &= 2\sum_{\substack{k^2|(r^2-4p)\\ d_k(p)\equiv 0,1 \pmod 4}} \frac{h((r^2-4p)/k^2)}{w((r^2-4p)/k^2)}\\ &= \sum_{\substack{k^2|(r^2-4p)\\ d_k(p)\equiv 0,1 \pmod 4}} \frac{\sqrt{4p-r^2}L(1,\chi_{d_k(p)})}{\pi k}, \end{aligned} \tag{5.56}$$

recalling that $d_k(p)=(r^2-4p)/k^2$. We also have the bound

$$L\left(1,\left(\frac{-d}{\cdot}\right)\right) \ll \log d. \tag{5.57}$$

See [IK04, Exer. 9, p. 120]. Hence $H(4p-r^2) \ll \sqrt{p}\log p\sum_{k^2|(r^2-4p)}\frac{1}{k}$. As in [DP99, p.

178], we apply the Brun-Titchmarsh Theorem , which gives

$$\begin{aligned}\sum_{p\leq x} H(4p-r^2) &\ll \sqrt{x}\log x \sum_{p\leq x}\sum_{k^2|(r^2-4p)} \frac{1}{k} = \sqrt{x}\log x \sum_{k\leq 2\sqrt{x}} \frac{1}{k} \sum_{\substack{p\leq x\\ k^2|(r^2-4p)}} 1 \\ &\leq \sqrt{x}\log x \sum_{k\leq 2\sqrt{x}} \frac{1}{k} \sum_{\substack{p\leq 4e^2x\\ k^2|(r^2-4p)}} 1 \ll \sqrt{x}\log x \sum_{k\leq 2\sqrt{x}} \frac{1}{k}\frac{x}{\varphi(k)k\log(4e^2x/k^2)}.\end{aligned}$$

See [IK04, Thm. 6.6, p. 167] for a statement of the Brun-Titchmarsh Theorem. As a function of k on the interval $[1, 2\sqrt{x}]$, the expression $k\log(4e^2x/k^2)$ is minimized at $k=1$. Thus, we have $\log x \leq \log(4e^2x) < k\log(4e^2/k^2)$, and hence

$$\sum_{p\leq x} H(4p-r^2) \ll \sqrt{x}\log x \sum_{k\leq 2\sqrt{x}} \frac{1}{k}\frac{x}{\varphi(k)\log x} \ll x^{3/2}. \tag{5.58}$$

If $n_K \geq 2$, the expression in (5.54) is bounded by a constant multiple of

$$x^{n_K-3/2}(\log x)^{n_K} \sum_{p\leq x} H(4p-r^2) \ll (x\log x)^{n_K}.$$

If $n_K = 1$ (i.e., if $K=\mathbb{Q}$), we use partial summation together with (5.58) to bound (5.54) by $x\log x$. Therefore,

$$E_0(x;\mathbf{t}) \ll \log\log x + \frac{\sqrt{x}/\log x}{\mathbf{t}_{\min}} + \left(\frac{1}{P_0(\mathbf{t}_1)} + \frac{1}{P_0(\mathbf{t}_2)}\right)(x\log x)^{n_K} + \frac{(x\log x)^{2n_K}}{P_0(\mathbf{t})}.$$

□

As our second step in computing the average order of $\pi_E^{r,1}(x)$, we estimate the weighted sum of Hurwitz class numbers appearing in Proposition 5.5.1.

Proposition 5.5.2. *For every $c > 0$,*

$$\frac{n_K}{2} \sum_{\substack{B(r)<p\leq x\\ f_p(K)=1}} \frac{H(4p-r^2)}{p} = C_{K,r,1}\pi_{1/2}(x) + O\left(\frac{\sqrt{x}}{(\log x)^{1+c}}\right).$$

Proof. Using (5.56), we have that

$$\frac{n_K}{2}\sum_{\substack{B(r)<p\le x\\ f_p(K)=1}}\frac{H(4p-r^2)}{p}=\frac{n_K}{2}\sum_{\substack{B(r)<p\le x\\ f_p(K)=1}}\sum_{\substack{k^2|(4p-r^2)\\ d_k(p)\equiv 0,1\pmod 4}}\frac{\sqrt{4p-r^2}}{\pi kp}L\left(1,\chi_{d_k(p)}\right).$$

Rearranging the order of summation and noticing that we need only consider $k\le 2\sqrt{x}$, this becomes

$$\frac{n_K}{2}\sum_{\substack{B(r)<p\le x\\ f_p(K)=1}}\frac{H(4p-r^2)}{p}=\frac{n_K}{2\pi}\sum_{k\le 2\sqrt{x}}\frac{1}{k}\sum_{p\in S_k(r,1,K,x)}\frac{\sqrt{4p-r^2}}{p}L\left(1,\chi_{d_k(p)}\right).$$

From the bound (5.57) and the fact that $\sqrt{4p-r^2}=2\sqrt{p}+O(1/\sqrt{p})$, we obtain

$$\frac{n_K}{2}\sum_{\substack{B(r)<p\le x\\ f_p(K)=1}}\frac{H(4p-r^2)}{p}=\frac{n_K}{\pi}\sum_{k\le 2\sqrt{x}}\frac{1}{k}\sum_{p\in S_k(r,1,K,x)}\frac{L\left(1,\chi_{d_k(p)}\right)}{\sqrt{p}}$$
$$+O\left(\sum_{p\le x}\frac{\log p}{p^{3/2}}\sum_{k^2|(4p-r^2)}1\right).$$

Since $\sum_{k^2|(4p-r^2)}1\ll p^{\epsilon}$ for every $\epsilon>0$, the big-O term is bounded. Thus,

$$\frac{n_K}{2}\sum_{\substack{B(r)<p\le x\\ f_p(K)=1}}\frac{H(4p-r^2)}{p}=\frac{n_K}{\pi}\sum_{k\le 2\sqrt{x}}\frac{1}{k}\sum_{p\in S_k(r,1,K,x)}\frac{L\left(1,\chi_{d_k(p)}\right)}{\sqrt{p}}+O(1). \tag{5.59}$$

Partial summation applied to the inner sum yields

$$\sum_{p\in S_k(r,1,K,x)}\frac{L\left(1,\chi_{d_k(p)}\right)}{\sqrt{p}}=\frac{1}{\sqrt{x}\log x}\sum_{p\in S_k(r,1,K,x)}L\left(1,\chi_{d_k(p)}\right)\log p$$
$$+\int_{B(r)}^{x}\frac{\sum_{p\in S_k(r,1,K,x)}L\left(1,\chi_{d_k(p)}\right)\log p}{2t^{3/2}\log t+t^{3/2}(\log t)^2}dt.$$

Let $c > 0$ be fixed. Applying Proposition 5.4.1, we have

$$\frac{n_K}{\pi\sqrt{x}\log x}\sum_{k\leq 2\sqrt{x}}\frac{1}{k}\sum_{p\in S_k(r,1,K,x)} L\left(1,\chi_{d_k(p)}\right)\log p = \frac{C'_{K,r,1}}{\pi}\frac{\sqrt{x}}{\log x} + O\left(\frac{\sqrt{x}}{(\log x)^{c+1}}\right),$$

and

$$\begin{aligned}\frac{n_K}{\pi}\sum_{k\leq 2\sqrt{x}}\frac{1}{k}\int_{B(r)}^{x}\frac{\sum_{p\in S_k(r,1,K,x)} L\left(1,\chi_{d_k(p)}\right)\log p}{2t^{3/2}\log t + t^{3/2}(\log t)^2}dt &= \frac{C'_{K,r,1}}{\pi}\int_2^x \frac{dt}{2\sqrt{t}\log t + \sqrt{t}(\log t)^2}\\ &\quad + O\left(\int_{B(r)}^{x}\frac{dt}{\sqrt{t}(\log t)^{c+1}}\right).\end{aligned}$$

Substituting all of this back into (5.59) yields

$$\begin{aligned}\frac{n_K}{2}\sum_{\substack{B(r)<p\leq x\\ f_p(K)=1}}\frac{H(4p-r^2)}{p} &= \frac{C'_{K,r,1}}{\pi}\left[\frac{\sqrt{x}}{\log x} + \int_2^x\frac{dt}{\sqrt{t}(\log t)^2} + \int_2^x\frac{dt}{2\sqrt{t}\log t}\right]\\ &\quad + O\left(\frac{\sqrt{x}}{(\log x)^{c+1}}\right)\end{aligned} \tag{5.60}$$

since integration by parts gives

$$\int_2^x\frac{dt}{\sqrt{t}(\log t)^{c+1}} = \frac{2\sqrt{x}}{(\log x)^{c+1}} + O\left(\int_2^x\frac{dt}{\sqrt{t}(\log t)^{c+2}}\right) \ll \frac{\sqrt{x}}{(\log x)^{c+1}}.$$

This completes the proof since $C_{K,r,1} = \frac{2}{\pi}C'_{K,r,1}$ and integrating by parts gives

$$\pi_{1/2}(x) = \int_2^x\frac{dt}{2\sqrt{t}\log t} = \frac{\sqrt{x}}{\log x} + \int_2^x\frac{dt}{\sqrt{t}(\log t)^2}. \tag{5.61}$$

□

5.6 The Product Formula for the Constant $C_{K,r,1}$

We now compute the product formula for the constant $C_{K,r,1}$. That is, we prove Theorem 5.2.5.

Proof of Theorem 5.2.5. First, we break the constant $C'_{K,r,1}$ into smaller pieces. In particular, for a fixed $b \in G_{m_K}$, we make the definition

$$C_{K,r,1}^{b,m_K} := n'_K \sum_{k=1}^{\infty} \frac{1}{k} \sum_{n=1}^{\infty} \frac{c_k^{r,b,m_K}(n)}{n\varphi([m_K, nk^2])}. \tag{5.62}$$

Comparing Theorem 1.1 and Proposition 2.1 of [Jam05], we see that James proves that

$$\frac{C_{K,r,1}^{b,m_K}}{n'_K} = \frac{F(r,b,m_K)}{\varphi(m_K)} \prod_{\substack{\ell \neq 2 \\ \ell \nmid m_K \\ \ell \nmid r}} \frac{\ell(\ell^2 - \ell - 1)}{(\ell+1)(\ell-1)^2} \prod_{\substack{\ell \neq 2 \\ \ell \nmid m_K \\ \ell \mid r}} \frac{\ell^2}{\ell^2 - 1},$$

where $F(r,b,m_K)$ is defined as in (5.13). Thus, summing over all $b \in G_{m_K}$ and factoring appropriately, we have

$$\begin{aligned} C_{K,r,1} &= \frac{2}{\pi} C'_{K,r,1} = \frac{2}{\pi} \sum_{b \in G_{m_K}} C_{K,r,1}^{b,m_K} \\ &= \left(\frac{2n'_K}{\pi\varphi(m_K)} \prod_{\substack{\ell \neq 2 \\ \ell \nmid m_K \\ \ell \nmid r}} \frac{\ell(\ell^2 - \ell - 1)}{(\ell+1)(\ell-1)^2} \prod_{\substack{\ell \neq 2 \\ \ell \nmid m_K \\ \ell \mid r}} \frac{\ell^2}{\ell^2 - 1} \right) \sum_{b \in G_{m_K}} F(r,b,m_K) \end{aligned} \tag{5.63}$$

as desired. □

5.7 The Variance of $\pi_E^{r,1}(x)$

In this section, we prove the bound on the variance of $\pi_E^{r,1}(x)$ given in Theorem 5.2.6.

Proof of Theorem 5.2.6. In general, if $\mu = \frac{1}{N}\sum_{n=1}^{N} \lambda_n$, then

$$\frac{1}{N} \sum_{n=1}^{N} (\lambda_n - \mu)^2 = \frac{1}{N} \left(\sum_{n=1}^{N} \lambda_n^2 \right) - \mu^2.$$

Whence,

$$\frac{1}{|\mathcal{C}_{\mathbf{a},\mathbf{t}}|}\sum_{E\in\mathcal{C}_{\mathbf{a},\mathbf{t}}}\left|\pi_E^{r,1}(x)-C_{K,r,1}\pi_{1/2}(x)\right|^2=\frac{1}{|\mathcal{C}_{\mathbf{a},\mathbf{t}}|}\sum_{E\in\mathcal{C}_{\mathbf{a},\mathbf{t}}}\left[\pi_E^{r,1}(x)\right]^2-\left[C_{K,r,1}\pi_{1/2}(x)\right]^2. \tag{5.64}$$

Concentrating on the first term on the right hand side of (5.64), we have

$$\frac{1}{|\mathcal{C}_{\mathbf{a},\mathbf{t}}|}\sum_{E\in\mathcal{C}_{\mathbf{a},\mathbf{t}}}[\pi_E^{r}(x)]^2=\frac{1}{|\mathcal{C}_{\mathbf{a},\mathbf{t}}|}\sum_{E\in\mathcal{C}_{\mathbf{a},\mathbf{t}}}\left[\sum_{\substack{\mathrm{N}\mathfrak{p},\mathrm{N}\mathfrak{p}'\leq x\\ \mathrm{N}\mathfrak{p}=\mathrm{N}\mathfrak{p}'\\ a_{\mathfrak{p}}(E)=a_{\mathfrak{p}'}(E)=r\\ \deg\mathfrak{p}=\deg\mathfrak{p}'=1}}1+\sum_{\substack{\mathrm{N}\mathfrak{p},\mathrm{N}\mathfrak{p}'\leq x\\ \mathrm{N}\mathfrak{p}\neq\mathrm{N}\mathfrak{p}'\\ a_{\mathfrak{p}}(E)=a_{\mathfrak{p}'}(E)=r\\ \deg\mathfrak{p}=\deg\mathfrak{p}'=1}}1\right]. \tag{5.65}$$

Let $c>0$ be given. We bound the sum over primes of equal norm by noting that

$$\frac{1}{|\mathcal{C}_{\mathbf{a},\mathbf{t}}|}\sum_{E\in\mathcal{C}_{\mathbf{a},\mathbf{t}}}\sum_{\substack{\mathrm{N}\mathfrak{p},\mathrm{N}\mathfrak{p}'\leq x\\ \mathrm{N}\mathfrak{p}=\mathrm{N}\mathfrak{p}'\\ a_{\mathfrak{p}}(E)=a_{\mathfrak{p}'}(E)=r\\ \deg\mathfrak{p}=\deg\mathfrak{p}'=1}}1\leq\frac{1}{|\mathcal{C}_{\mathbf{a},\mathbf{t}}|}\sum_{E\in\mathcal{C}_{\mathbf{a},\mathbf{t}}}\sum_{\substack{\mathrm{N}\mathfrak{p}\leq x\\ a_{\mathfrak{p}}(E)=r\\ \deg\mathfrak{p}=1}}n_K=n_K\frac{1}{|\mathcal{C}_{\mathbf{a},\mathbf{t}}|}\sum_{E\in\mathcal{C}_{\mathbf{a},\mathbf{t}}}\pi_E^{r,1}(x).$$

Applying Theorem 5.2.1, we have

$$\frac{1}{|\mathcal{C}_{\mathbf{a},\mathbf{t}}|}\sum_{E\in\mathcal{C}_{\mathbf{a},\mathbf{t}}}\sum_{\substack{\mathrm{N}\mathfrak{p},\mathrm{N}\mathfrak{p}'\leq x\\ \mathrm{N}\mathfrak{p}=\mathrm{N}\mathfrak{p}'\\ a_{\mathfrak{p}}(E)=a_{\mathfrak{p}'}(E)=r\\ \deg\mathfrak{p}=\deg\mathfrak{p}'=1}}1\ll\frac{\sqrt{x}}{\log x}+E(x;\mathbf{t}). \tag{5.66}$$

For the primes of unequal norm, we argue as in the proof of Proposition 5.5.1 and write

$$\begin{aligned}\frac{1}{|\mathcal{C}_{\mathbf{a},\mathbf{t}}|}\sum_{E\in\mathcal{C}_{\mathbf{a},\mathbf{t}}}\sum_{\substack{\mathrm{N}\mathfrak{p},\mathrm{N}\mathfrak{p}'\leq x\\ \mathrm{N}\mathfrak{p}\neq\mathrm{N}\mathfrak{p}'\\ a_{\mathfrak{p}}(E)=a_{\mathfrak{p}'}(E)=r\\ \deg\mathfrak{p}=\deg\mathfrak{p}'=1}} 1 &= \frac{1}{|\mathcal{C}_{\mathbf{a},\mathbf{t}}|}\sum_{\substack{B(r)<\mathrm{N}\mathfrak{p},\mathrm{N}\mathfrak{p}'\leq x\\ \mathrm{N}\mathfrak{p}\neq\mathrm{N}\mathfrak{p}'\\ \deg\mathfrak{p}=\deg\mathfrak{p}'=1}}\sum_{\substack{E\in\mathcal{C}_{\mathbf{a},\mathbf{t}}\\ a_{\mathfrak{p}}(E)=a_{\mathfrak{p}'}(E')=r}} 1\\
&=\frac{1}{|\mathcal{C}_{\mathbf{a},\mathbf{t}}|}\sum_{\substack{B(r)<\mathrm{N}\mathfrak{p},\mathrm{N}\mathfrak{p}'\leq x\\ \mathrm{N}\mathfrak{p}\neq\mathrm{N}\mathfrak{p}'\\ \deg\mathfrak{p}=\deg\mathfrak{p}'=1}}\sum_{\substack{\tilde{E}/\mathbb{F}_p,\tilde{E}'/\mathbb{F}_{p'}\\ \#E(\mathbb{F}_p)=p+1-r\\ \#E'(\mathbb{F}_{p'})=p'+1-r}}\left|\mathcal{C}_{\mathbf{a},\mathbf{t}}(E,E';\mathfrak{p},\mathfrak{p}')\right|\\
&\quad+O\left(\frac{1}{|\mathcal{C}_{\mathbf{a},\mathbf{t}}|}\sum_{\substack{B(r)<\mathrm{N}\mathfrak{p},\mathrm{N}\mathfrak{p}'\leq x\\ \mathrm{N}\mathfrak{p}\neq\mathrm{N}\mathfrak{p}'\\ \deg\mathfrak{p}=\deg\mathfrak{p}'=1}}\sum_{\substack{E\in\mathcal{C}_{\mathbf{a},\mathbf{t}}\\ E^{\mathfrak{p}}\text{ or }E^{\mathfrak{p}'}\text{ sing.}}} 1\right).\end{aligned}$$

Thus, applying Lemma 5.3.3 on page 106 and arguing as in the proof of Proposition 5.5.1, we obtain

$$\frac{1}{|\mathcal{C}_{\mathbf{a},\mathbf{t}}|}\sum_{E\in\mathcal{C}_{\mathbf{a},\mathbf{t}}}\sum_{\substack{\mathrm{N}\mathfrak{p},\mathrm{N}\mathfrak{p}'\leq x\\ \mathrm{N}\mathfrak{p}\neq\mathrm{N}\mathfrak{p}'\\ a_{\mathfrak{p}}(E)=a_{\mathfrak{p}'}(E)=r\\ \deg\mathfrak{p}=\deg\mathfrak{p}'=1}} 1=\frac{n_K^2}{4}\sum_{\substack{B(r)<p,p'\leq x\\ p\neq p'\\ f_p(K)=f_{p'}(K)=1}}\frac{H(4p-r^2)H(4p'-r^2)}{pp'}+O\left(E_1(x,\mathbf{t})\right), \tag{5.67}$$

where

$$E_1(x,\mathbf{t})=\frac{\sqrt{x}\log\log x}{\log x}+\frac{x/(\log x)^2}{\mathbf{t}_{\min}}+\left[\frac{1}{P_0(\mathbf{t}_1)}+\frac{1}{P_0(\mathbf{t}_2)}\right](x\log x)^{2n_K}+\frac{(x\log x)^{4n_K}}{P_0(\mathbf{t})}.$$

By Proposition 5.5.2, the double sum over primes in (5.67) is equal to

$$\left[\frac{n_K}{2}\sum_{\substack{B(r)<p\leq x\\ f_p(K)=1}}\frac{H(4p-r^2)}{p}\right]^2-\frac{n_K^2}{4}\sum_{\substack{B(r)<p\leq x\\ f_p(K)=1}}\frac{H(4p-r^2)^2}{p^2}=\left[C_{K,r,1}\pi_{1/2}(x)\right]^2+O\left(\frac{x}{(\log x)^{2+c}}\right).$$

Combining this with equations (5.65), (5.66), and (5.67), we have

$$\frac{1}{|\mathcal{C}_{\mathbf{a},\mathbf{t}}|}\sum_{E\in\mathcal{C}_{\mathbf{a},\mathbf{t}}}[\pi_E^r(x)]^2=\left[C_{K,r,1}\pi_{1/2}(x)\right]^2+O\left(\frac{x}{(\log x)^{2+c}}+E_1(x;\mathbf{t})\right);$$

and substituting this into (5.64), we obtain the desired result. □

Chapter 6

Conclusions and Future Work

In this thesis, four different number theoretic problems were discussed. In Chapter 2, Hurwitz class number identities of a certain type were stated and proved. In particular, three different techniques were demonstrated. The first involved counting elliptic curves over finite fields; the second involved expressing the sums of interest as the coefficients of a certain modular form; and the third involved manipulations of the Eichler-Selberg Trace Formula. The tables of Section 2.5 state many conjectures which remain open. In the future, it would be appropriate to pursue proofs of these conjectures. We also note that several of the entries in the table of Conjecture 2.5.2 are empty. We believe that this is due to the prescence of cusp forms in the associated space of modular forms. William Duke has pointed out to us that the contribution of these cusp forms may be estimated as in [Duk97, Jon08]. However, it may be interesting to study the specific cusp forms that appear to see if anything more can be said in special cases.

In Chapter 3, we studied the problem of generating large order elements in finite fields. The technique for generation involved explicit equations for modular towers discovered by Elkies [Elk98]. However, the proofs never used this interpretation, but rather relied on elementary manipulations. It would be interesting to see if using the modular interpretation of these equations could lead to better bounds. However, the author admits that he has no idea how to begin such a project. Other potentially useful projects include using

Elkies "recipe" to "cook up" more examples of explicit equations for modular towers or seeing if his techinque applies to the case of the curves $X_1(N)$ in addition to his description for the curves $X_0(N)$.

The Chebotarëv Density Theorem is a powerful and beautiful tool. In Chapter 4, we studied the error in the approximation given by the Chebotarëv Density Theorem. The best known bounds on the error in the approximation are given by Lagarias and Odlyzko [LO77] who give both unconditional bounds and stronger bounds under the assumption of GRH. Estimates on the error term are useful when one needs to control the error incurred by invoking the theorem. However, for many applications, such as in the proof of Proposition 5.4.1 on page 108, it is often sufficient to obtain bounds in some average sense. In fact, one can often produce better bounds on average that what is "naïvely predicted" by GRH. In Chapter 4, we studied the mean square error for the Chebotarëv Density Theorem when averaging over cyclotomic extensions of a fixed number field. In particular, we showed that that the mean square error is small and gave an asymptotic formula for it as well. These results are related to the classical Barban-Davenport-Halberstam Theorem and its variants.

With respect to future work, two ideas readily come to mind. The first comes from noting that the ray class fields of $\mathbb{Q}$ are precisely the cyclotomic extensions of $\mathbb{Q}$ [Cox89, p. 164]. Thus, we may interpret the original Barban-Davenport-Halberstam Theorem (see Theorem 4.1.1) as the mean square error for the Chebotarëv Density Theorem when average over all ray class fields of $\mathbb{Q}$. In light of this new interpretation, it would be interesting to obtain this result for the number field setting, where the ray class fields are not necessarily the cyclotomic extensions of K. The second idea for future work would involve studying the mean square error in estimating the sum

$$\sum_{\substack{p \leq x \\ p \equiv a \pmod q \\ \left(\frac{K/\mathbb{Q}}{p}\right) = C}} \log p \tag{6.1}$$

by the Chebotarëv Density Theorem. Here, we would assume that K is a fixed Galois extension of $\mathbb{Q}$ of finite degree, linearly disjoint from $\mathbb{Q}(\zeta_q)$, and C is a fixed conjugacy class of $\mathrm{Gal}(K/\mathbb{Q})$. A result of this type would be useful in extending the work of Faulkner and James on the average Lang-Trotter problem for primes of degree 2 to certain non-Abelian Galois extensions of $\mathbb{Q}$. We note that though only stated for finite Abelian extensions of $\mathbb{Q}$, the work of Faulkner and James [FJ] on the average Lang-Trotter problem for primes of degree greater than 2 actually goes through for finite Galois extensions of $\mathbb{Q}$ more generally. The Bombieri-Vinogradov type average error (see [Dav80, p. 161]) for the sum (6.1) has already been studied by Murty and Murty in [MM87].

Finally, in Chapter 5, we studied the Lang-Trotter Conjecture in number fields. In particular, we extended and improved a recent result of Faulkner and James [FJ] on the average problem for the case of degree 1 primes. The improvement involved showing that the result holds for averages over "smaller boxes" of elliptic curves. The extension involved showing that the assumption that the number field is Abelian over $\mathbb{Q}$ may be relaxed to Galois over $\mathbb{Q}$. Provided that one can obtain the proper Barban-Davenport-Halberstam variant, extending this work to the case of degree 2 primes would be very natural. We note that the Barban-Davenport-Halberstam variant associated to the sum (6.1) discussed above should be enough to extend the result to any Galois number field with no nontrivial intersection with $\mathbb{Q}^{\mathrm{cyc}}$. In particular, this would apply to any Galois extension with a simple, non-Abelian Galois group (e.g., an A_5-extension).

Bibliography

[Bai07] Stephan Baier. The Lang-Trotter conjecture on average. *J. Ramanujan Math. Soc.*, 22(4):299–314, 2007.

[Bar64] M.B. Barban. On the distribution of primes in arithmetic progressions "on average". *Dokl. Akad. Nauk UzSSR*, 5:5–7, 1964. (Russian).

[BBIJ05] Jonathan Battista, Jonathan Bayless, Dmitriy Ivanov, and Kevin James. Average Frobenius distributions for elliptic curves with nontrivial rational torsion. *Acta Arith.*, 119(1):81–91, 2005.

[BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939 (electronic), 2001.

[BCF$^+$08] Brittany Brown, Neil J. Calkin, Timothy B. Flowers, Kevin James, Ethan Smith, and Amy Stout. Elliptic curves, modular forms, and sums of Hurwitz class numbers. *J. Number Theory*, 128(6):1847–1863, 2008.

[BCG$^+$09] Jessica Burkhart, Neil J. Calkin, Shuhong Gao, Justine Hyde-Volpe, Kevin James, Hiren Maharaj, Shelly Manber, Jared Ruiz, and Ethan Smith. Finite field elements of high order arising from modular curves. *Des. Codes Cryptogr.*, 51(3):301–314, 2009.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[Bur63] D. A. Burgess. On character sums and L-series. II. *Proc. London Math. Soc. (3)*, 13:524–536, 1963.

[Che05] Qi Cheng. On the construction of finite field elements of large order. *Finite Fields Appl.*, 11(3):358–366, 2005.

[Che07] Qi Cheng. Constructing finite field extensions with large order elements. *SIAM J. Discrete Math.*, 21(3):726–730, 2007.

[Coh75] Henri Cohen. Sums involving the values at negative integers of L-functions of quadratic characters. *Math. Ann.*, 217(3):271–285, 1975.

[Coh96] Henri Cohen. *A Course in Computational Algebraic Number Theory.* Springer-Verlag, New York, 1996.

[Con01] Alessandro Conflitti. On elements of high order in finite fields. In *Cryptography and computational number theory (Singapore, 1999)*, volume 20 of *Progr. Comput. Sci. Appl. Logic*, pages 11–14. Birkhäuser, Basel, 2001.

[Cox89] David A. Cox. *Primes of the form* $x^2 + ny^2$. A Wiley-Interscience Publication. John Wiley & Sons Inc., New York, 1989. Fermat, class field theory and complex multiplication.

[Cro75] M. J. Croft. Square-free numbers in arithmetic progressions. *Proc. London Math. Soc. (3)*, 30:143–159, 1975.

[Dav80] Harold Davenport. *Multiplicative Number Theory.* Springer-Verlag, New York, 1980.

[Deu41] Max Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ.*, 14:197–272, 1941.

[DH66] H. Davenport and H. Halberstam. Primes in arithmetic progressions. *Michigan Math. J.*, 13:485–489, 1966.

[DH68] H. Davenport and H. Halberstam. Corrigendum: “Primes in arithmetic progression”. *Michigan Math. J.*, 15:505, 1968.

[DP99] Chantal David and Francesco Pappalardi. Average Frobenius distributions of elliptic curves. *Internat. Math. Res. Notices*, 1999(4):165–183, 1999.

[DP04] Chantal David and Francesco Pappalardi. Average Frobenius distribution for inerts in $\mathbb{Q}(i)$. *J. Ramanujan Math. Soc.*, 19(3):181–201, 2004.

[DS05] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 2005.

[Duk97] William Duke. Elliptic curves with no exceptional primes. *C. R. Acad. Sci. Paris Sér. I Math.*, 325(8):813–818, 1997.

[Eic55] Martin Eichler. On the class of imaginary quadratic fields and the sums of divisors of natural numbers. *J. Indian Math. Soc. (N.S.)*, 19:153–180 (1956), 1955.

[Elk98] Noam D. Elkies. Explicit modular towers. In *Proceedings of the Thirty-Fifth Annual Allerton Conference on Communication, Control and Computing.* Univ. of Illinois at Urbana-Champaign, 1998.

[FJ] Bryan Faulkner and Kevin James. Average Frobenius distributions for elliptic curves over Abelian extensions. (preprint).

[FM96] Etienne Fouvry and M. Ram Murty. On the distribution of supersingular primes. *Canad. J. Math.*, 48(1):81–104, 1996.

[Fre94] Gerhard Frey. Construction and arithmetical applications of modular forms of low weight. In *Elliptic curves and related topics*, volume 4 of *CRM Proc. Lecture Notes*, pages 1–21. Amer. Math. Soc., Providence, RI, 1994.

[Gao99] Shuhong Gao. Elements of provable high orders in finite fields. *Proc. Amer. Math. Soc.*, 127(6):1615–1623, 1999.

[Gol70] Larry Joel Goldstein. A generalization of the Siegel-Walfisz theorem. *Trans. Amer. Math. Soc.*, 149:417–429, 1970.

[GS95a] Arnaldo Garcia and Henning Stichtenoth. A tower of Artin-Schreier extensions of function fields attaining the Drinfel′d-Vlăduţ bound. *Invent. Math.*, 121(1):211–222, 1995.

[GS95b] Joachim von zur Gathen and Igor Shparlinski. Orders of Gauss periods in finite fields. In *Algorithms and computations (Cairns, 1995)*, volume 1004 of *Lecture Notes in Comput. Sci.*, pages 208–215. Springer, Berlin, 1995. Also appeared as Orders of Gauss periods in finite fields. Applicable Algebra in Engineering, Communication and Computing, 9 (1998), 15-24.

[GS96] Arnaldo Garcia and Henning Stichtenoth. Asymptotically good towers of function fields over finite fields. *C. R. Acad. Sci. Paris Sér. I Math.*, 322(11):1067–1070, 1996.

[GS01] Joachim von zur Gathen and Igor Shparlinski. Gauß periods in finite fields. In *Finite fields and applications (Augsburg, 1999)*, pages 162–177. Springer, Berlin, 2001.

[GV95] Shuhong Gao and Scott A. Vanstone. On orders of optimal normal basis generators. *Math. Comp.*, 64(211):1227–1233, 1995.

[GvzGP98] Shuhong Gao, Joachim von zur Gathen, and Daniel Panario. Gauss periods: orders and cryptographical applications. *Math. Comp.*, 67(221):343–352, 1998. With microfiche supplement.

[Hin81] Jürgen G. Hinz. On the theorem of Barban and Davenport-Halberstam in algebraic number fields. *J. Number Theory*, 13(4):463–484, 1981.

[Hoo75] Christopher Hooley. On the Barban-Davenport-Halberstam theorem. I. *J. Reine Angew. Math.*, 274/275:206–223, 1975. Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday, III.

[HPS89] Hiroaki Hijikata, Arnold K. Pizer, and Thomas R. Shemanske. The basis problem for modular forms on $\Gamma_0(N)$. *Mem. Amer. Math. Soc.*, 82(418):vi+159, 1989.

[Hun74] Thomas W. Hungerford. *Algebra*. Springer-Verlag, New York, 1974.

[HZ76] F. Hirzebruch and D. Zagier. Intersection numbers of curves on Hilbert modular surfaces and modular forms of Nebentypus. *Invent. Math.*, 36:57–113, 1976.

[IK04] Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[IR90] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*. Springer-Verlag, New York, 2 edition, 1990.

[Jam04] Kevin James. Average Frobenius distributions for elliptic curves with 3-torsion. *J. Number Theory*, 109(2):278–298, 2004.

[Jam05] Kevin James. Averaging special values of Dirichlet L-series. *Ramanujan J.*, 10(1):75–87, 2005.

[Jon08] Nathan Jones. Trace formulas and class number sums. *Acta Arith.*, 132(4):301–313, 2008.

[Kna92] Anthony W. Knapp. *Elliptic Curves*. Princeton University Press, Princeton, 1992.

[Kob93] Neal Koblitz. *Introduction to Elliptic Curves and Modular Forms*. Springer-Verlag, New York, 1993.

[Lan94] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[Lan02] Serge Lang. *Algebra*. Springer-Verlag, New York, 3 edition, 2002.

[Len87] Jr. H. W. Lenstra. Factoring integers with elliptic curves. *Ann. of Math. (2)*, 126(3):649–673, 1987.

[Liu08] H.-Q. Liu. Barban-Davenport-Halberstam average sum and exceptional zero of L-functions. *J. Number Theory*, 121(4):1044–1059, 2008.

[LN97] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn.

[LO77] J. C. Lagarias and A. M. Odlyzko. Effective versions of the Chebotarev density theorem. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 409–464. Academic Press, London, 1977.

[LT76] Serge Lang and Hale Trotter. *Frobenius distributions in* GL_2*-extensions*. Lecture Notes in Mathematics, Vol. 504. Springer-Verlag, Berlin, 1976. Distribution of Frobenius automorphisms in GL_2-extensions of the rational numbers.

[Mar77] Daniel A. Marcus. *Number fields*. Universitext. Springer-Verlag, New York, 1977.

[Miy89] Toshitsune Miyake. *Modular Forms*. Springer-Verlag, New York, 1989.

[MM87] M. Ram Murty and V. Kumar Murty. A variant of the Bombieri-Vinogradov theorem. In *Number theory (Montreal, Que., 1985)*, volume 7 of *CMS Conf. Proc.*, pages 243–272. Amer. Math. Soc., Providence, RI, 1987.

[Mon70] H. L. Montgomery. Primes in arithmetic progressions. *Michigan Math. J.*, 17:33–39, 1970.

[Mur01] M. Ram Murty. *Problems in analytic number theory*, volume 206 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2001. Readings in Mathematics.

[Mur02] V. Kumar Murty. Splitting of primes in infinite extensions. In *Number theory for the millennium, III (Urbana, IL, 2000)*, pages 23–41. A K Peters, Natick, MA, 2002.

[Ono04] Ken Ono. *The web of modularity: arithmetic of the coefficients of modular forms and q-series*, volume 102 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC, 2004.

[Sch87] René Schoof. Nonsingular plane cubic curves over finite fields. *J. Combin. Theory Ser. A*, 46(2):183–211, 1987.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[Ser98] Jean-Pierre Serre. *Abelian l-adic representations and elliptic curves*, volume 7 of *Research Notes in Mathematics*. A K Peters Ltd., Wellesley, MA, 1998. With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original.

[Sil86] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 1986.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[SL96] P. Stevenhagen and H. W. Lenstra, Jr. Chebotarëv and his density theorem. *Math. Intelligencer*, 18(2):26–37, 1996.

[Smia] Ethan Smith. A Barban-Davenport-Halberstam asymptotic for number fields. (preprint).

[Smib] Ethan Smith. A generalization of the Barban-Davenport-Halberstam theorem to number fields. (to appear in *J. Number Theory*).

[SS77] J.-P. Serre and H. M. Stark. Modular forms of weight 1/2. In *Modular functions of one variable, VI (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, pages 27–67. Lecture Notes in Math., Vol. 627. Springer, Berlin, 1977.

[Tay] Richard Taylor. Automorphy for some l-adic lifts of automorphic mod l galois representations. ii. (preprint).

[TW95] Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.

[Vol07] José Felipe Voloch. On the order of points on curves over finite fields. *Integers*, 7:A49, 4, 2007.

[Wil69] Robin J. Wilson. The large sieve in algebraic number fields. *Mathematika*, 16:189–204, 1969.

[Wil95] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

INDEX

SYMBOL INDEX