5-2017

Average Frobenius Distributions for Elliptic Curves: Extremal Primes and Koblitz's Conjecture

Luke M. Giberson
Clemson University, lgibers@g.clemson.edu

Average Frobenius Distributions for Elliptic Curves: Extremal Primes and Koblitz's Conjecture

---

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
Luke M. Giberson
May 2017

Accepted by:
Dr. Kevin James, Committee Chair
Dr. Jim Brown
Dr. Hui Xue
Dr. Michael Burr

Abstract

Let $E/\mathbb{Q}$ be an elliptic curve, and let p be a rational prime of good reduction. Let $a_p(E)$ denote the trace of the Frobenius endomorphism of E at the prime p, and let $\#E(\mathbb{F}_p)$ be the number of $\mathbb{F}_p$-rational points on E. In this dissertation we investigate two different questions regarding the statistical distribution of these two quantities.

We say p is a *champion prime of* E if $a_p(E) = -\big[\big|2\sqrt{p}\big|\big]$, which occurs precisely when the group of $\mathbb{F}_p$-rational points is as large as possible in accordance with the Hasse bound. In a similar vein, we say p is a *trailing prime of* E if $a_p(E) = +\big[\big|2\sqrt{p}\big|\big]$, which occurs precisely when the group of $\mathbb{F}_p$-rational points is as small as possible in accordance with the Hasse bound. Together, we say that these primes constitute the *extremal primes of* E. The first result of this dissertation establishes that the number of elliptic curve champion primes that are less than X is asymptotically equal to $\frac{8}{3\pi} \cdot X^{1/4}/\log X$ in an average sense. As an immediate corollary, we also gain asymptotics on the average number of trailing primes less than X and the average number of extremal primes less than X.

In 1988, Koblitz conjectured that for any real number X

$$\#\{p < X : p \text{ prime and } \#E(\mathbb{F}_p) \text{ prime}\} \sim C_E \cdot \frac{X}{\log^2 X},$$

where C_E is an explicit constant depending on E. Balog, Cojocaru, and David have proved that Koblitz's conjecture is true on average for rational elliptic curves. The second result of this dissertation generalizes their average result to elliptic curves over certain higher number fields.

Acknowledgments

Throughout my life as a student I've been blessed with a number of excellent educators who inspired me along the way. First and foremost, I'd like to thank Kevin James for his guidance and advice throughout my entire graduate career. At the beginning he led me along the way of becoming a researcher, and at the end he encouraged me to follow my own research directions. As such his influence on me as a professional mathematician cannot be overstated. I'm also grateful for the members of my committee – for Jim Brown, whose teaching style resonated with me like none before; for Hui Xue, whose in-class tangents led to some of the most memorable mathematical discussions; and for Michael Burr, whose care for his students' well-being goes above and beyond what I've seen in my education. Lastly I'd like to thank my middle-school math teacher Wade Zwingler, who surely laid the seeds of this dissertation fifteen years ago; my calculus teacher Jon Barker, who instilled confidence in my mathematical abilities; my undergraduate advisor Joe Wagner, who never had an opportunity to teach me math but certainly taught me life; my algebra professor Dena Morton, whose enthusiasm for math is unparalleled; and finally my senior project advisor Bernd Rossa, who had little interest in chess engines but plenty of interest in helping me forge my own path.

I'd like to thank my family, who supported me with steadfast patience and emotional reassurance throughout this journey. In particular, I appreciate Mom and Dad, Wujek and Thea, Alan, and Cindy – though your names won't be found in any of this work, none of this would have been possible without your encouragement and belief in me. Lastly I'd like to thank my life-long friends Brian, Kevin, and Jaime, as well as all my co-workers and peers I met and with whom I worked throughout my career.

Table of Contents

Chapter 1

Introduction

This dissertation is the culmination of three years of graduate research in a subfield of analytic number theory and arithmetic geometry known as Frobenius distributions. In this chapter, we discuss the motivation and results of this work and subsequently discuss future extensions and generalizations. In the second chapter we state a variety of known number-theoretic results and conclude with an important lemma bridging the gap between arithmetic geometry and analytic number theory. The third and fourth chapters are proofs of the two main theorems of this dissertation.

Most notation will be developed as we go, however there are a few conventions we establish here that hold throughout the paper. All logarithms are assumed to be natural. The variables p and ℓ are reserved for prime numbers; summations or products over these variables are always assumed to be over the set of primes. Summations over $d \mid n$ are sums over all positive divisors of the integer n; summations over $m \leq M$ are assumed to begin at $m = 1$. Summations over $a \pmod q$ run over a complete set of residues modulo q, while summations over $a \pmod q^{\times}$ run over only those invertible residues modulo q.

For two functions $f(t)$ and $g(t)$, we write $f(t) = \mathrm{O}(g(t))$ or $f(t) \ll g(t)$ to mean that there is an absolute constant C such that $|f(t)| \leq C \cdot g(t)$ for all t sufficiently large. In such a case, we say that *f is asymptotically less than or equal to g*. On the other hand we write $f(t) \sim g(t)$ whenever the ratio $f(t)/g(t)$ tends to 1 as t grows without bound. In this case we say that *f is asymptotic to g*.

This preliminary chapter serves as an overview of the results found in this dissertation in an attempt to clearly display the main theorems proved herein. Therefore in order to fully understand

this chapter, the reader may need to consult the second chapter for definitions of objects with which he or she is unfamiliar.

1.1 Motivation

In a big picture sense, a rational elliptic curve E can be reduced modulo all but finitely many primes to yield a sequence of elliptic curves over finite fields. Each of these curves yields two important integer-valued quantities: the number of $\mathbb{F}_p$-rational points on the curve, denoted $\#E(\mathbb{F}_p)$, and the trace of the Frobenius endomorphism, denoted $a_p(E)$. Therefore for every rational elliptic curve we get the arithmetic sequences $\{\#E(\mathbb{F}_p)\}$ and $\{a_p(E)\}$, both indexed by the primes.

Of interest is to determine the distributional and statistical information about these sequences. For example, the *Sato-Tate conjecture* was recently proven by Taylor in conjunction with Clozel, Harris, and Shepherd-Barron in [Tay08, CHT08, HSBT10, BLGHT11]. If we normalize the trace of Frobenius by setting $b_p(E) := a_p(E)/2\sqrt{p}$, then it is appropriate to count the number of primes such that $b_p(E) \in [a, b]$ for a fixed subinterval $[a, b] \subset [-1, 1]$. These authors showed that for a rational elliptic curve E without complex multiplication the asymptotic density of such primes amongst all primes is

$$\frac{\#\{p < X : b_p(E) \in [a, b]\}}{\#\{p < X\}} \sim \frac{2}{\pi} \cdot \int_a^b \sqrt{1 - t^2}\, \mathrm{d}t, \tag{1.1.1}$$

as X grows without bound. Other questions remain open, such as a conjecture of Lang and Trotter in [LT76] regarding how often $a_p(E) = r$ for a fixed integer r.

In this dissertation, we examine two different topics in Frobenius distributions: one on the number of extremal primes of an elliptic curve and one on an open conjecture of Koblitz on the primality of $\#E(\mathbb{F}_p)$. Both results provide evidence for unproven conjectures by showing that the conjectures are true "on average" over a collection of elliptic curves. In this way both results are very similar in spirit and technique not only to one another but also to established results in the literature such as in [FM96, DP99, BCD11].

1.2 Extremal Primes

For a rational elliptic curve E, the Hasse bound gives the inequality $|a_p(E)| \leq 2\sqrt{p}$ for any trace of Frobenius $a_p(E)$ at a prime of good reduction p. The first result of this dissertation investigates the frequency at which the trace of Frobenius $a_p(E)$ is maximal or minimal inside the Hasse interval. We make the following definitions:

1. p is a *champion prime of* E if $a_p(E) = -\big[\big|2\sqrt{p}\big|\big]$,
2. p is a *trailing prime of* E if $a_p(E) = +\big[\big|2\sqrt{p}\big|\big]$,
3. p is an *extremal prime of* E if $a_p(E) = \pm\big[\big|2\sqrt{p}\big|\big]$,

where $[|a|]$ denotes the integer floor function.

The study of extremal primes was initiated by Hedetniemi, James, and Xue in [HJX14]. They proved the following theorem, which establishes that "almost all" rational elliptic curves have at least one champion prime (and hence at least one extremal prime). In fact, the same method also establishes that "almost all" rational elliptic curves have at least one trailing prime.

Theorem 1.2.1 ([HJX14])**.** *Let X be a positive real number, and let $A := A(X)$ and $B := B(X)$ be positive parameters depending only on X. For any $\epsilon > 0$, take*

$$\begin{aligned} A, B &\geq \exp((1/4+\epsilon)X), \\ AB &\geq \exp((5/4+\epsilon)X). \end{aligned}$$

For any $a, b \in \mathbb{Z}$ such that $4a^3 + 27b^2 \neq 0$, let $E_{a,b}$ be the elliptic curve given by the affine equation $y^2 = x^3 + ax + b$. Define sets

$$\begin{aligned} \mathcal{E}(A,B) &= \{E_{a,b} : |a| \leq A, |b| \leq B\} \\ \mathcal{E}^-(A,B) &= \{E_{a,b} \in \mathcal{E}(A,B) : E_{a,b} \text{ has a champion prime}\}. \end{aligned}$$

Then $\#\mathcal{E}^-(A,B) \sim \#\mathcal{E}(A,B)$ as $X \to \infty$.

In [JTT+16], the authors established an asymptotic on the number of champion primes up to X for a elliptic curve $E/\mathbb{Q}$ with complex multiplication (CM), but this result was conditional on

the assumption of the Riemann Hypothesis for certain Hecke L-functions. A recent paper of James and Pollack has removed this assumption.

Theorem 1.2.2 ([JP17, Theorem 1])**.** *Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication. The number of champion primes $p < X$ is asymptotically $\frac{2X^{3/4}}{3\pi \log X}$. The number of trailing primes $p < X$ has an identical asymptotic.*

For an elliptic curve $E/\mathbb{Q}$ and a positive real number X, we define

$$\pi_E^{\text{Champ}}(X) = \#\{p < X : \ E \text{ of good reduction of } p \text{ and } a_p(E) = -[|2\sqrt{p}|]\}.$$

Apart from Theorem 1.2.1 nothing is known about extremal primes on non-CM curves. Because the Sato-Tate distribution (see (1.1.1)) is much different in the CM versus the non-CM case, the predicted asymptotic for the non-CM case is much smaller than the asymptotic obtained by James and Pollack in Theorem 1.2.2. For a non-CM elliptic curve E, we can interpret the "probability" that $a_p(E) = -\left[\left|2\sqrt{p}\right|\right]$ as the likelihood that the normalized trace $b_p(E)$ lies in the real interval $\left[-1, -1 + \frac{\{2\sqrt{p}\}}{2\sqrt{p}}\right]$, where $\{x\}$ denotes the fractional part of a real number x. Seeing as $\frac{\{2\sqrt{p}\}}{2\sqrt{p}} = \mathrm{O}\left(\frac{1}{\sqrt{p}}\right)$, arguing heuristically with the Sato-Tate theorem gives that the "probability" that p is a champion prime of E is approximately

$$\begin{aligned}
\frac{2}{\pi} \int_{-1}^{-1+\mathrm{O}\left(\frac{1}{\sqrt{p}}\right)} \sqrt{1-t^2}\ \mathrm{d}t &= \frac{2}{\pi} \int_{-1}^{-1+\mathrm{O}\left(\frac{1}{\sqrt{p}}\right)} \left(\sqrt{2}(1-t)^{1/2} + \mathrm{O}((1-t)^{3/2}))\right)\ \mathrm{d}t \\
&= \frac{2}{\pi}\left(\frac{2\sqrt{2}}{3}\left(\frac{1}{2\sqrt{p}}\right)^{3/2}\right) + \mathrm{O}(p^{-5/4}) \\
&= \frac{2}{3\pi} p^{-3/4} + \mathrm{O}(p^{-5/4}).
\end{aligned}$$

Assuming independence and summing over all primes while ignoring error terms gives the expectation that

$$\pi_E^{\text{Champ}}(X) \sim \frac{2}{3\pi} \sum_{p<X} p^{-3/4} \sim \frac{8X^{1/4}}{3\pi \log X}.$$

The first result of this dissertation indicates that this heuristic is correct on average.

Theorem 1.2.3. *For all positive real numbers X and $Z := Z(X)$, we have*

$$\frac{1}{4Z^2}\sum_{\substack{|a|\leq Z\\|b|\leq Z}}\pi^{\text{Champ}}_{E_{a,b}}(X) = \frac{8X^{1/4}}{3\pi\log X} + \mathrm{O}\left(\frac{X^{3/2}\log X}{Z} + \frac{X^{1/4}}{\log^2 X}\right).$$

The same result holds when counting trailing primes on average. Since extremal primes are the disjoint union of champion primes and trailing primes, when counting extremal primes on average we get a constant of $16/3\pi$ in the asymptotic.

Corollary 1.2.4. *Taking $Z > X^{5/4}\log^3 X$ in Theorem 1.2.3 and letting $X \to \infty$ gives*

$$\frac{1}{4Z^2}\sum_{\substack{|a|\leq Z\\|b|\leq Z}}\pi^{\text{Champ}}_{E(a,b)}(X) \sim \frac{8X^{1/4}}{3\pi\log X}.$$

The same result holds when counting trailing primes on average. Since extremal primes are the disjoint union of champion primes and trailing primes, when counting extremal primes on average we get a constant of $16/3\pi$ in the asymptotic.

1.3 Koblitz's Conjecture

Let $E/\mathbb{Q}$ be an elliptic curve. Motivated by interest in elliptic curve cryptosystems, in 1988 Koblitz conjectured in [Kob88] that

$$\#\{p < X : p \text{ prime of good reduction of } E \text{ and } \#E(\mathbb{F}_p) \text{ prime}\} \sim C_E \cdot \frac{X}{\log^2 X}, \tag{1.3.1}$$

for an explicit constant C_E.

From the theory of elliptic curves we know that $\#E(\mathbb{F}_p) = p+1-a_p(E)$, and in particular in conjunction with the Hasse bound $|a_p(E)| \leq 2\sqrt{p}$, this implies that $\#E(\mathbb{F}_p) = p+\mathrm{O}(\sqrt{p})$. Therefore Koblitz's conjecture (which asks how often both p and $p+1+a_p(E)$ are simultaneously prime) is similar in spirit to the classical twin primes conjecture (which asks how often both p and $p+2$ are simultaneously prime). For this reason Koblitz's conjecture is sometimes referred to as the twin prime conjecture for elliptic curves.

Partial progress towards Koblitz's conjecture for a single curve has typically used sieve-

theoretic methods (see [MM01, SW05, DW12] for example), typically attaining results on how often $\#E(\mathbb{F}_p)$ has no more than k distinct prime divisors. Let

$$A_E(X) := \{\#E(\mathbb{F}_p) : p < X \text{ of good reduction of } E\}.$$

When $E/\mathbb{Q}$ has complex multiplication, Cojocaru showed in [Coj05] that $\#(A_E(X) \cap P_4) \gg X/\log^2 X$, where P_k is the set of integers with at most k distinct prime factors. The most accurate asymptotic lower bound is due to Iwaniec and Jiménez Urroz who showed in [IJU10] that $\#(A_E(X) \cap P_2) \gg X/\log^2 X$ for the particular CM-curve $E : y^2 = x^3 - x$. With respect to upper bounds, Cojocaru showed in [Coj05] that unconditionally for $E/\mathbb{Q}$ without complex multiplication that we have $\#(A_E(X) \cap P_1) \ll X/(\log X \cdot \log\log\log X)$. In the same paper she showed that for $E/\mathbb{Q}$ with complex multiplication we have $\#(A_E(X) \cap P_1) \ll X/\log^2 X$ conditionally on an assumption similar to the Generalized Riemann Hypothesis.

All of this is to say that there is only partial progress towards Koblitz's conjecture, and in fact the asymptotic conjectured in (1.3.1) has not been shown for even a single rational elliptic curve. For a family of rational elliptic curves $\mathcal{C}$ that grows with the parameter X, Balog, Cojocaru, and David prove in [BCD11] that Koblitz's conjecture is true "on average", that is

$$\frac{1}{\#\mathcal{C}} \sum_{E \in \mathcal{C}} \#\{p < X : p \text{ prime of good reduction of } E \text{ and } \#E(\mathbb{F}_p) \text{ prime}\} \sim \mathfrak{C} \cdot \frac{X}{\log^2 X},$$

where

$$\mathfrak{C} := \frac{2}{3} \prod_{\ell \neq 2} \frac{\ell^4 - 2\ell^3 - \ell^2 + 3\ell}{(\ell-1)^3(\ell+1)}. \tag{1.3.2}$$

Jones showed in [Jon09] that conditional on a question of Serre, the average of the conjectured constants C_E from (1.3.1) across the curves appearing in the family $\mathcal{C}$ is indeed the average constant $\mathfrak{C}$ seen above. It is in this way that such a result lends credence to the truth of Koblitz's conjecture.

In this dissertation we work towards a generalization of the above result to Koblitz's conjecture for elliptic curves defined over abelian number fields with square-free conductor. Such generalizations to curves over number fields have been seen in the literature for similar problems in Frobenius distributions, for instance beginning in [DP99] and then subsequently continuing in [DP04, FJKP11, JS11, JS13].

Fix an abelian number field K of degree $d := [K : \mathbb{Q}]$ with square-free conductor Q and ideal

norm $N(\cdot)$. Let $\mathcal{O}_K$ be the ring of integers of K with a fixed integral basis $\mathcal{B} = \{e_1, \dots, e_d\} \subset \mathcal{O}_K$. For each element $a \in \mathcal{O}_K$ we can write $a = \sum_{j \le d} c_j e_j$, where each c_j is a rational integer. Therefore the supremum norm

$$||a|| := \max_{1 \le i \le d} \{|c_i|\}, \tag{1.3.3}$$

is well-defined with respect to the fixed basis $\mathcal{B}$. For a real number X and an elliptic curve E/K with discriminant $\Delta(E)$ we define a counting function

$$\pi_E^{\text{twin}}(X) := \#\{\mathfrak{p} \text{ prime in } \mathcal{O}_K : N(\mathfrak{p}) < X;\ \mathfrak{p} \nmid \Delta(E);\ \#E(\mathbb{F}_\mathfrak{p}) \text{ is prime}\},$$

where $\#E(\mathbb{F}_\mathfrak{p})$ denotes the number of points on the reduction of E modulo $\mathfrak{p}$. The following theorem is the other major result in this dissertation.

Theorem 1.3.1. *Let X and $Z := Z(X)$ be positive real numbers. Let $\mathcal{C}_Z$ denote the set of models of elliptic curves*

$$E_{a,b} : y^2 = x^3 + ax + b$$

with $||a||, ||b|| \le Z$. We have

$$\frac{1}{\#\mathcal{C}_Z} \sum_{E \in \mathcal{C}_Z} \pi_E^{twin}(X) = d\mathfrak{B}_K \mathfrak{C} \cdot \frac{X}{\log^2 X} + \mathrm{O}\left(\frac{X}{\log^3 X} + \frac{X^2 \log X}{Z}\right),$$

where $\mathfrak{C}$ is defined as in (1.3.2) and $\mathfrak{B}_K$ is a constant depending only on the number field K. In particular, if $\mathcal{V}$ is the set of residues modulo Q such that a rational prime p splits completely in K if and only if $p \equiv v \pmod{Q}$ for some $v \in \mathcal{V}$, then the constant $\mathfrak{B}_K$ is

$$\mathfrak{B}_K = \sum_{v \in \mathcal{V}} \prod_{\substack{\ell \neq 2 \\ \ell | Q}} \frac{\left(\ell^2 - \ell - \left[1 + \left(\frac{(v-1)^2}{\ell}\right)\right]\right)}{\ell^3 - 2\ell^2 - \ell + 3},$$

where $\left(\frac{\cdot}{\ell}\right)$ is the Legendre symbol.

Corollary 1.3.2. *Upon taking $Z \ge X \log^4 X$ in Theorem 1.3.1, we obtain*

$$\frac{1}{\#\mathcal{C}_Z} \sum_{E \in \mathcal{C}_Z} \pi_E^{twin}(X) \sim d\mathfrak{B}_K \mathfrak{C} \cdot \frac{X}{\log^2 X}.$$

It is worth giving at least one explicit example of the previous theorem. For a prime $p > 2$,

suppose $K/\mathbb{Q}$ is the p^{th} cyclotomic field, that is, $K = \mathbb{Q}(\zeta_p)$ for some primitive p^{th} root-of-unity ζ_p. Cyclotomic fields are the quintessential examples of abelian number fields – in particular the Galois group of $K/\mathbb{Q}$ is the multiplicative group of integers modulo p and K has conductor p. The minimal polynomial for ζ_p is the p^{th} cyclotomic polynomial, which has degree $\phi(p) = p - 1$, so the extension $K/\mathbb{Q}$ has degree $d = p - 1$. From [Was97, Theorem 2.13], we know that the rational primes that split completely in K are precisely the primes that are 1 modulo p. As a result the asymptotic in this case is

$$\frac{1}{\#\mathcal{C}_Z} \sum_{E \in \mathcal{C}_Z} \pi_E^{\text{twin}}(X) \sim \mathfrak{C} \cdot \frac{p^3 - 2p^2 + 1}{p^3 - 2p^2 - p + 3} \cdot \frac{X}{\log^2 X}.$$

1.4 Future Work

A glaring issue in both results is the rather large size of the averaging family $\mathcal{C}_Z$; in particular we are forced to take $Z \gg X$ in both theorems. These results can be improved by using more precise character sum approximations and therefore more precise curve-counting arguments as in [Bai07, JS11]. In the future publication of this work we will use the state-of-the-art estimates in that realm and significantly reduce the size of the family $\mathcal{C}_Z$.

With respect to extremal primes, there are several interesting directions to pursue in order to further the results presented here. Almost all rational elliptic curves are torsion-free, however the presence of torsion on a curve inflicts a divisibility condition on the trace of Frobenius through the underlying Galois representations. This is to say that restricting the averaging family to only curves with say, m-torsion, should affect the constant in the resulting asymptotic. This type of work has been done in other problems, such as in [Jam04] and [BBIJ05], so it would be interesting to see a similar analysis for extremal primes. Alternatively, one could pursue counting primes that are "almost" extremal, for instance primes such that $a_p(E) = -\left[\left|2\sqrt{p}\right|\right] + f(p)$ for a small function $f(p)$.

On the side of Koblitz's conjecture, the most obvious generalizations are to abelian number fields of arbitrary conductor (not just squarefree) or even a general finite Galois number field as in [JS11]. One could also attempt to prove a similar theorem for only the primes of some fixed degree as in [DP04] or [JS13]; this would be a notable improvement from the work here as this result only notices the contribution of the primes of degree one.

The final generalization comes from Zywina, who has generalized Koblitz's conjecture to the setting of elliptic curves over number fields in [Zyw11]. His work corrects the initial constant

predicted by Koblitz, extends the conjecture to curves over an arbitrary number field, and allows for an additional divisibility condition on $\#E(\mathbb{F}_{\mathfrak{p}})$. Let E be an elliptic curve defined over a number field K, and let t be a fixed integer. There is an explicit constant $C_{E,t} \geq 0$ so that

$$\#\{\mathfrak{p} \text{ prime in } \mathcal{O}_K : N(\mathfrak{p}) < X;\ \mathfrak{p} \nmid \Delta(E);\ \#E^{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})/t \text{ is prime}\} \sim C_{E,t} \cdot \frac{X}{\log^2 X}.$$

The constant $C_{E,t}$ arises from the Galois representations associated to the curve E and is explicitly defined in [Zyw11]. Following the work in [Jon09], it would be interesting to see if the average of the constants $C_{E,t}$ over the family of elliptic curves coming from $\mathcal{C}_Z$ is indeed the average constant discovered in Theorem 1.3.1.

Chapter 2

Tools from Number Theory

In this chapter, we discuss some pertinent objects and results from number theory that will be especially useful in the main theorems of this dissertation. For the elementary results we give explicit proofs; for deeper results we give references. We invite the interested reader to consult [Mur01, Chapters 1-2], [IR90, Chapters 5, 12-13, 16], [Coh08, Chapters 2-3], [Dav00], and [Apo76] for more detailed information.

2.1 Multiplicative Functions

Any function from the positive integers to the complex numbers is called an *arithmetic function*. Some arithmetic functions inherently carry more structure than others; it is possible for such a function to preserve some portion of the multiplicative structure of the integers. We say an arithmetic function f is *multiplicative* if for any pair of coprime integers m and n we have $f(mn) = f(m) \cdot f(n)$. The primary advantage of a multiplicative function is that its evaluation is dependent only on its evaluation on prime powers due to the fundamental theorem of arithmetic.

Example 2.1.1. Upon fixing one of its arguments, the greatest common divisor function $(a, b) := \gcd(a, b)$ is multiplicative in the other variable. Using multiplicativity and the fundamental theorem of arithmetic, for any integers a, b, c we have

$$(a, bc) = (a, b) \cdot \prod_{\ell | c} \frac{(a, bc)_\ell}{(a, b)_\ell}, \tag{2.1.1}$$

where $(a,b)_\ell$ is the largest prime power ℓ^e that divides (a,b). We also know from elementary number theory that there is a relationship between the greatest common divisor and the least common multiple of a pair of numbers, namely

$$(a,b) = \frac{ab}{[a,b]}, \tag{2.1.2}$$

where $[a,b]$ denotes the least common multiple between a and b.

Example 2.1.2. Let p be a prime, e be a positive integer, and a, b, and c be arbitrary positive integers. The *Euler totient* function, denoted $\phi(\cdot)$, is the multiplicative function generated by

$$\phi(p^e) := (p-1)\cdot p^{e-1} = p^e(1-1/p).$$

Equivalently, $\phi(n)$ counts the number of positive integers less than n that are coprime to n, that is it is precisely the order of the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$. Immediately from the definition we obtain the Euler product formula

$$\phi(n) = n\prod_{\ell \mid n}(1-1/\ell)\,.$$

The Euler product expression for $\phi(n)$ is the key ingredient in obtaining the identity

$$\phi(ab) = \phi(a)\cdot\phi(b)\cdot\frac{(a,b)}{\phi((a,b))}. \tag{2.1.3}$$

Finally, the combination of (2.1.2) and (2.1.3) yields

$$\phi([a,bc]) = \frac{\phi(ab)\cdot\phi(c)\cdot(ab,c)}{(a,bc)\cdot\phi((ab,c))}. \tag{2.1.4}$$

Example 2.1.3. Let p be a prime and e be a positive integer. The *Möbius function*, denoted $\mu(\cdot)$, is the multiplicative function generated by

$$\mu(p^e) := \begin{cases} -1 & \text{if } e = 1, \\ 0 & \text{if } e \geq 2. \end{cases}$$

Since the Möbius function vanishes on any integer that is not square-free, it can be used as a

square-free indicator function, namely

$$\mu^2(n) = \begin{cases} 1 & \text{if } n \text{ is square-free,} \\ 0 & \text{otherwise.} \end{cases} \tag{2.1.5}$$

Example 2.1.4. Perhaps the most important example of multiplicative functions in this paper are the *Legendre symbol*, the *Jacobi symbol*, and the *Kronecker symbol*. These objects are ordered in order of increasing generalization, and so we methodically build up from the former to the latter. Let p be an odd prime and let a be an integer. The *Legendre symbol*, denoted $(a|p)$ or as below, is defined by

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if } a \text{ is a non-zero quadratic residue modulo } p, \\ 0 & \text{if } a \equiv 0 \pmod{p}, \\ -1 & \text{if } a \text{ is not a non-zero quadratic residue modulo } p. \end{cases}$$

The Jacobi symbol is the natural multiplicative extension of the Legendre symbol. For any integer a and any odd positive integer $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, we generalize the Legendre symbol by defining $(a|1) := 1$, $(1|n) := 1$, and

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} \dots \left(\frac{a}{p_k}\right)^{e_k}.$$

If we additionally define

$$\left(\frac{a}{2}\right) := \begin{cases} 1 & \text{if } a \equiv \pm 1 \pmod{8}, \\ 0 & \text{if } a \equiv 0 \pmod{2}, \\ -1 & \text{if } a \equiv \pm 3 \pmod{8}, \end{cases}$$

then the multiplicative extension of the Legendre symbol applies to $(a|n)$ where n is now any non-zero integer – this is the Kronecker symbol.

These three symbols have tremendous importance in number theory. Not only do they encode the law of quadratic reciprocity, but they are more generally in the ubiquitous family of Dirichlet characters. The results below are stated precisely for their use in this paper and make no attempt at being as general as possible.

Fact 2.1.5. *Upon fixing one of the arguments in the Kronecker symbol, we say the symbol has* conductor N *if and only if* N *is smallest positive integer such that the Kronecker symbol has period*

N in its free variable.

1. *Upon fixing a positive integer n, the Kronecker symbol $(\cdot|n)$ has conductor n.*

2. *Upon fixing an integer a, the Kronecker symbol $(a|\cdot)$ has conductor either $|a|$ or $4|a|$.*

Proof. See [IK04, p.52]. □

Lemma 2.1.6. *Let q be an odd prime. The Legendre symbol $(a|q)$ satisfies the orthogonality relation*

$$\sum_{a \pmod q} \left(\frac{a}{q}\right) = 0.$$

Proof. From the theory of quadratic residues, we know that inside the residue classes modulo q we have precisely $(q-1)/2$ quadratic non-residues and $(q-1)/2$ non-zero quadratic residues; the contributions from these two groups negate themselves. Since additionally $(0|q) = 0$, this sum completely vanishes. □

Lemma 2.1.7. *Let q be an odd prime, and let $f(z) = z^2 + bz + c$ have integer coefficients. Set $\Delta = b^2 - 4c$. Then*

$$S := \sum_{a \pmod q} \left(\frac{f(a)}{q}\right) = \begin{cases} -1 & \text{if } q \nmid \Delta, \\ q-1 & \text{if } q \mid \Delta. \end{cases}$$

Proof. Since the character $(4|q) = 1$ for all odd primes q, we have

$$S = \sum_{a \pmod q} \left(\frac{4}{q}\right)\left(\frac{f(a)}{q}\right) = \sum_{a \pmod q} \left(\frac{(2a+b)^2 - \Delta}{q}\right) = \sum_{a \pmod q} \left(\frac{a^2 - \Delta}{q}\right),$$

where the final equality holds because the map $a \mapsto 2a+b$ is an automorphism of the ring of integers modulo q. Obviously we have $|S| \leq q$. On the other hand using Euler's criterion we can reduce modulo q to obtain

$$S \equiv \sum_{a \pmod q} (a^2 - \Delta)^{(q-1)/2} \equiv: \sum_{a \pmod q} \sum_{j=0}^{q-1} b_j a^j \equiv \sum_{j=0}^{q-1} b_j \sum_{a \pmod q} a^j \pmod q, \tag{2.1.6}$$

for the appropriate coefficients b_j depending on Δ. The only coefficient that will matter for our purposes is $b_{q-1} \equiv 1 \pmod q$.

To proceed, we require an understanding of the quantity

$$S_n :\equiv \sum_{a \pmod q} a^n \pmod q$$

for $n \geq 1$. Suppose a_0 is a non-zero element modulo q such that $a_0^n \neq 1$. This implies $a_0^n S_n = S_n$, since multiplication by a_0^n is an automorphism of the ring of integers modulo q. As $a_0^n \neq 1$, it must be that $S_n \equiv 0 \pmod q$. On the other hand no such element a_0 exists if and only if $q-1 \mid n$. In such a case we have $S_n = 0 + (q-1) \equiv -1 \pmod q$ by Fermat's little theorem.

We can now complete the proof of the lemma. Continuing modulo q from (2.1.6) with the help of the observations on S_n above we have

$$S \equiv \sum_{j=0}^{q-1} b_j S_j \equiv -b_{q-1} \equiv -1 \pmod q .$$

Now $|S| \leq q$ and $S \equiv -1 \pmod q$ allows only the possibilities that $S = -1$ or $S = q-1$. The latter case occurs if and only if all but one term in the sum S is 1 and precisely one term is 0. The summand that vanishes corresponds to a particular residue a_0 modulo q such that $a_0^2 - \Delta \equiv 0 \pmod q$. However if this is the case for a_0 it is also the case for $-a_0$. Since only one residue modulo q can satisfy such an equality, it must be that $a_0 \equiv 0 \pmod q$ and so $q \mid \Delta$. Hence we have shown $S = q-1$ if and only if $q \mid \Delta$, which completes the proof. □

As is evident from the previous two lemmas, summing character values is a recurring theme in analytic number theory. For a fixed integer a, consider the character sum $\sum_{n \leq N} \left(\frac{a}{n}\right)$. From Fact 2.1.5, the function $\left(\frac{a}{\cdot}\right)$ is $4|a|$-periodic. Since $|\left(\frac{a}{n}\right)| \leq 1$, we have a trivial upper bound of $\sum_{n \leq N} \left(\frac{a}{n}\right) \ll |a|$. In taking absolute values of the summands we immediately lose any potential cancellation in the sum, so the following theorem improves significantly on this naïve result.

Theorem 2.1.8 (Polya-Vinogradov)**.** *Let q be an integer, and let $\chi(n) := (q|n)$. We have the uniform bound*

$$\max_{M,N \in \mathbb{Z}} \left| \sum_{M < a < M+N} \chi(a) \right| \ll \sqrt{q} \log q.$$

Proof. See [Dav00, Section 23]. □

2.2 Analytic Results on Primes

We begin this section by stating the crown jewel of analytic number theory: the prime number theorem. We have known since Euclid that there are infinitely many primes, but a rigorous result describing how the prime-counting function grows eluded mathematicians until 1896. As the asymptotic answer to the question "how many primes are there less than X?", it is of fundamental importance throughout this paper. For technical reasons related to how primes interact with the Riemann zeta function, it is more convenient to count primes with a logarithmic weight.

Theorem 2.2.1 (Hadamard, de la Vallée-Poussin)**.** *For a positive real number X, define*

$$\psi(X) := \sum_{p<X} \log p.$$

As X grows without bound we have $\psi(X) \sim X$.

Proof. See [Apo76, Chapter 13]. □

Among the many generalizations of the prime number theorem, one of the most significant for this paper is the adaptation of the prime number theorem to the distribution of primes across arithmetic progressions. It is possible to show using elementary means, for example, that there are infinitely many primes of the form $4k + 1$. To generalize this, let a and q be integers and consider counting primes of the form $p = kq + a$ for some integer k. Obviously if $(a, q) > 1$ there is at most one prime of this form. In 1837, Dirichlet showed that this coprimality condition is the only obstacle to finding an infinite number of primes in an arithmetic progression. Although he died in 1859, the advent of the prime number theorem in 1896 extends Dirichlet's result to a statement about the equidistribution of primes among residue classes. For this reason, the following theorem is typically attributed to Dirichlet himself.

Theorem 2.2.2 (Dirichlet)**.** *For a positive real number X and coprime integers a and q, define*

$$\psi(X; q, a) := \sum_{\substack{p<X \\ p\equiv a \pmod{q}}} \log p.$$

As X grows without bound we have $\psi(X; q, a) \sim X/\phi(q)$.

Proof. See [Apo76, Chapter 7]. □

The other generalization of the prime number theorem that will be significant in this work is the study of generalized twin primes. Although some recent work (see [Zha14, Pol14, May15], [Pol14]) has made outstanding progress in this area, the conjecture is still unresolved. For our purposes it is of interest to study the distribution of generalized twin primes across arithmetic progressions, for which Hardy and Littlewood made the following hypothesis.

Conjecture 2.2.3 ([HL23, Conjecture B])**.** *For a positive real number X and integers a, q, and r, define*

$$\psi_r(X;q,a) := \sum_{\substack{p<X \\ p\equiv a \pmod q \\ p-r \text{ prime}}} \log p \cdot \log(p-r).$$

It is believed that as X grows without bound we have

$$\psi_r(X;q,a) \sim \mathfrak{S}(r;q,a)X,$$

where

$$\mathfrak{S}(r;q,a) := \begin{cases} \dfrac{2C_2}{\phi(q)} \cdot \displaystyle\prod_{\substack{\ell\neq 2 \\ \ell\mid r}} \frac{\ell-1}{\ell-2} & \text{if } r \text{ is even and } (a,q) = (a-r,q) = 1, \\ 0 & \text{otherwise,} \end{cases}$$

and $C_2 := \prod_{\ell\neq 2} \frac{\ell(\ell-2)}{(\ell-1)^2}$ is the classical twin prime constant.

Asymptotic equivalence says nothing about absolute error, and so in general we should never expect, for example, that $X/\phi(q)$ is an accurate approximation for $\psi(X;q,a)$. However in this paper we will indeed approximate certain prime counting functions using the asymptotics above and then control the resulting error term in making such an approximation. In particular for real numbers X and h and integers a and q we define

$$\begin{aligned} E(X,h;q,a) &:= [\psi(X+h,q,a) - \psi(X,q,a)] - \frac{h}{\phi(q)}, \\ E(X,h;q) &:= \max_{(a,q)=1} |E(X,h;q,a)|, \\ E_r(X,h;q,a) &:= [\psi_r(X+h;q,a) - \psi_r(X;q,a)] - \mathfrak{S}(r;q,a)h. \end{aligned}$$

Obtaining the best possible estimates of these error terms on their own is akin to proving an appropriate version of the Generalized Riemann Hypothesis (GRH), which is of course a significant

obstacle to cross. In this work we require bounds on these terms of strength comparable to that gained by assuming GRH, so it appears we have arrived at an impasse.

It is a general principle in analytic number theory that an estimate that seems to be unobtainable point-wise is almost certainly more accessible on average. For instance, there is little to no chance of obtaining an asymptotic on the Möbius function $\mu(n)$ on its own, however an asymptotic on $\sum_{n\leq X}\mu(n)$ is equivalent to the prime number theorem. In this dissertation we will be averaging such error terms over many moduli q or over many intervals of the form $[X, X+h]$ for fixed h. As a result we are able to achieve GRH-like bounds unconditionally. The following two results are of utmost importance for this work; without them we would need to assume GRH.

Theorem 2.2.4 ([Kou15, Theorem 1.1]). *Fix $A \geq 1$ and $\epsilon > 0$. Let $2 \leq h \leq X$ be real numbers. For any real number Q satisfying $1 \leq Q^2 \leq h/X^{1/6+\epsilon}$, we have*

$$\int_X^{2X} \sum_{q\leq Q} E(y;h,q)\ \mathrm{d}y \ll \frac{hX}{\log^A X}.$$

Theorem 2.2.5 ([BCD11, Theorem 3]). *Fix $A \geq 1$ and $\epsilon > 0$. Let X be a positive real number, and let x, y be real numbers such that $2 \leq x+y \leq X$. Let R be a real number such that $X^{1/3+\epsilon} \leq R \leq X$. Provided $Q \leq X\log^{-(A+3)} X$, we have*

$$\sum_{0<|r|\leq R}\sum_{q\leq Q}\sum_{a\pmod q}|E_r(X,h;q,a)|^2 \ll \frac{RX^2}{\log^A X}.$$

2.3 Dirichlet L-Series

Fix an integer q and let $\chi(n) := (q|n)$ denote the Kronecker symbol. The *Dirichlet L-series associated to* χ is the function

$$L(s,\chi) := \sum_{n\geq 1}\frac{\chi(n)}{n^s} = \prod_{\ell}\left(1-\frac{\chi(\ell)}{\ell^s}\right)^{-1}, \tag{2.3.1}$$

where s is a complex variable with $\mathrm{Re}(s) > 1$. In this paper we will encounter the special values $L(1,\chi)$ for various symbols χ. It is not immediately clear that such a value is even well-defined, however the non-vanishing of $L(s,\chi)$ when $s = 1$ is the fundamental lemma in proving Dirichlet's theorem on primes in arithmetic progressions (see Theorem 2.2.2).

Even though these special values arise in both main theorems, the ways in which they are handled are vastly different in each argument. The proof of Theorem 1.2.3 uses the Polya-Vinogradov inequality (see Theorem 2.1.8) to truncate each special value uniformly while incurring an error.

Lemma 2.3.1. *Let $\chi(n) := (q|n)$ denote the Kronecker symbol. For any real number N we have*

$$L(1,\chi) = \sum_{n<N} \frac{\chi(n)}{n} + \mathrm{O}\left(\frac{\sqrt{q}\log q}{N}\right).$$

In particular, upon taking $N = \sqrt{q}$ we obtain the bound $L(1,\chi) \ll \log q$.

Proof. Let $N' \geq N$, and set $A(M) = \sum_{m\leq M} \chi(m) \ll \sqrt{q}\log q$ by Theorem 2.1.8. Using partial summation on the function $f(t) = 1/t$ yields

$$\sum_{N\leq n\leq N'} \frac{\chi(n)}{n} \quad = \quad \frac{A(N')}{N'} - \frac{A(N)}{N} + \int_N^{N'} \frac{A(t)\ \mathrm{d}t}{t^2} \quad \ll \quad \frac{\sqrt{q}\log q}{N'} + \frac{\sqrt{q}\log q}{N},$$

which approaches $\frac{\sqrt{q}\log q}{N}$ as N' increases without bound. □

The proof of Theorem 1.3.1 also involves truncating the special L-values, however the uniform estimate obtained by using the Polya-Vinogradov inequality is not tight enough to adequately control resulting error terms. Instead we truncate "most" special L-values in an even more powerful way than Lemma 2.3.1 and argue that the L-values we cannot control are rather sporadic. To make all this rigorous, we let $P^+(n)$ denote the largest prime dividing n and define the truncated Euler product

$$L(s,\chi;w) = \prod_{\ell\leq w} \left(1 - \frac{\chi(\ell)}{\ell^s}\right)^{-1}.$$

The following theorem is a specialization of one due to a combination of Elliott, Granville, Soundararajan, and the authors in [CDKS16].

Theorem 2.3.2 ([GS03, Proposition 2.2] and [CDKS16, Lemmas 2.3 and 2.4])**.**
Let $\alpha \geq 1$ and $H \geq 3$. For convenience in notation set $z := \log H$. There is a set of integers $\mathcal{E}_\alpha(H) \subset [1,H]$ of size at most $H^{2/\alpha}$ such that if $\chi(n) := (a|n)$ is a Kronecker symbol of conductor $q \leq H$ with $q \notin \mathcal{E}_\alpha(H)$, then

$$L(1,\chi) = L(1,\chi;z^{8\alpha^2})\left[1 + \mathrm{O}\left(\frac{1}{z^\alpha}\right)\right].$$

Moreover, for any $u \geq 1$ and $w \geq 10$ the evaluation of $L(1, \chi; w)$ for such symbols is

$$L(1, \chi; w) = \sum_{\substack{n \leq w^u \\ P^+(n) \leq w}} \frac{\chi(n)}{n} + \mathrm{O}\left(\frac{\log w}{e^u}\right).$$

Lemma 2.3.3. *Let $\chi(n) := (q|n)$ denote the Kronecker symbol. For any real number w we have $L(1, \chi; w) \ll \log w$.*

Proof. We first observe that a Taylor expansion of $-\log(1-t)$ yields the bound

$$-\sum_{\ell \leq w} \log\left(1 - \frac{\chi(\ell)}{\ell}\right) \ll \sum_{\ell \leq w} \frac{1}{\ell} \ll \log\log w,$$

where the final inequality follows from Mertens' second theorem (see [Mer74]). As a result we have

$$L(1, \chi; w) = \exp\left(-\sum_{\ell \leq w} \log\left(1 - \frac{\chi(\ell)}{\ell}\right)\right) \ll \log w.$$

□

2.4 Quadratic Forms and Class Numbers

For a fixed positive integer D, let

$$\mathcal{Q}_D^{\mathrm{prim}} := \{Q(x,y) = ax^2 + bxy + cy^2 : a, b, c \in \mathbb{Z};\ a > 0;\ b^2 - 4ac = -D;\ (a,b,c) = 1\}$$

denote the set of positive-definite integral binary quadratic forms that are primitive and have discriminant $-D$. Notice that this set is empty unless $-D \equiv 0, 1 \pmod 4$. The group $\Gamma := \mathrm{SL}_2(\mathbb{Z})$ acts on $\mathcal{Q}_D^{\mathrm{prim}}$ in its classical way; for $\gamma = \left(\begin{smallmatrix} \gamma_{11} & \gamma_{12} \\ \gamma_{21} & \gamma_{22} \end{smallmatrix}\right) \in \Gamma$ and $Q(x,y) \in \mathcal{Q}_D^{\mathrm{prim}}$, we define

$$\gamma \cdot Q(x,y) := Q(\ \gamma_{11}x + \gamma_{12}y\ ,\ \gamma_{21}x + \gamma_{22}y\ ). \tag{2.4.1}$$

To see that this is a valid group action, we first show that the resulting form on the right-hand side of the equality in (2.4.1) actually lives in $\mathcal{Q}_D^{\mathrm{prim}}$. Writing $Q(x,y) = ax^2 + bxy + cy^2$, we

compute

$$Q(\ \gamma_{11}x+\gamma_{12}y\ ,\ \gamma_{21}x+\gamma_{22}y\ ) = dx^2+exy+fy^2, \tag{2.4.2}$$

where

$$\begin{aligned} d &:= a\gamma_{11}^2+b\gamma_{11}\gamma_{21}+c\gamma_{21}^2 \\ e &:= 2a\gamma_{11}\gamma_{12}+b(\gamma_{11}\gamma_{22}+\gamma_{12}\gamma_{21})+2c\gamma_{21}\gamma_{22} \\ f &:= a\gamma_{12}^2+b\gamma_{12}\gamma_{22}+c\gamma_{22}^2 \end{aligned}$$

Obviously the coefficients d, e, and f are all integers. Completing the square in the coefficient d gives

$$d = a\left(\gamma_{11}+\frac{b}{2a}\gamma_{21}\right)^2-(b^2-4ac)\left(\frac{\gamma_{21}}{2a}\right)^2,$$

which is necessarily positive because $a>0$ and $b^2-4ac=-D<0$. A direct (but incredibly messy) computation on e^2-4df using the facts that $\det\gamma=1$ and $b^2-4ac=-D$ leads immediately to $e^2-4df=-D$. Lastly to see that $(d,e,f)=1$, notice from (2.4.2) that (d,e,f) divides $\gamma\cdot Q(x,y)$ for any choice of integers x and y. Therefore using the fact that $\det\gamma=1$ we can compute

$$\begin{aligned} a &= Q(1,0)=\gamma\cdot Q(\gamma_{22},-\gamma_{21}), \\ c &= Q(0,1)=\gamma\cdot Q(-\gamma_{12},\gamma_{11}), \\ b &= Q(1,1)-a-c=\gamma\cdot Q(\gamma_{22}+\gamma_{12},\gamma_{21}+\gamma_{11})-a-c. \end{aligned}$$

Since (d,e,f) divides the right-hand side of each equation above, it also divides the left-hand side of each equation above. As a result, we have deduced that $(d,e,f)\mid(a,b,c)=1$. Therefore we have shown $(d,e,f)=1$, which completes the proof that the form $\gamma\cdot Q(x,y)$ lives in $\mathcal{Q}_D^{\text{prim}}$.

It remains to be shown that the binary operation defined in (2.4.2) is an action which respects the group structure of $\mathrm{SL}_2(\mathbb{Z})$. First note that immediately from the definition the identity matrix $I_2\in\Gamma$ fixes each $Q\in\mathcal{Q}_D^{\text{prim}}$. Furthermore for any two matrices $A=\left(\begin{smallmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{smallmatrix}\right)$, $B=\left(\begin{smallmatrix}b_{11}&b_{12}\\b_{21}&b_{22}\end{smallmatrix}\right)\in\Gamma$ set

$$\begin{pmatrix}\gamma_{11}&\gamma_{12}\\ \gamma_{21}&\gamma_{22}\end{pmatrix} := AB$$

For an arbitrary form $Q(x,y) \in \mathcal{Q}_D^{\text{prim}}$ we have

$$[AB] \cdot Q(x,y) \quad = \quad Q(\ \gamma_{11}x + \gamma_{12}y\ ,\ \gamma_{21}x + \gamma_{22}y\ ).$$

Expanding the coefficients γ_{ij} according to the a_{ij} and b_{ij} while regrouping gives the quantity above as

$$Q(\ a_{11}(b_{11}x + b_{12}y) + a_{12}(b_{21}x + b_{22}y)\ ,\ a_{21}(b_{11}x + b_{12}y) + a_{22}(b_{21}x + b_{22}y)\ ),$$

which is

$$A \cdot Q(\ b_{11}x + b_{12}y\ ,\ b_{21}x + b_{22}y\ ) = A \cdot [B \cdot Q(x,y)].$$

Having shown that the operation defined in (2.4.2) is a valid group action, the number of orbits of this action is known as the *form class number* and is denoted $h(-D)$. It's important to note that the form class number is finite (see [Cox89, Theorem 2.13]). In fact we know $h(-3) = h(-4) = 1$, and for $-D < -4$ we have the explicit formula (see [IK04, p. 38])

$$h(-D) = \frac{\sqrt{D} \cdot L(1,\chi)}{\pi}, \tag{2.4.3}$$

where $\chi := (-D|\cdot)$ is the Kronecker symbol.

Although the action in (2.4.2) is defined only for primitive forms, it is straightforward to extend the action to the non-primitive forms as well. Let $\mathcal{Q}_D$ denote the space of all integral positive-definite binary quadratic forms of discriminant $-D$. The number of orbits in the action of Γ on $\mathcal{Q}_D$ is denoted $H(-D)$ and called the *Kronecker class number*. Our goal is to relate the form class number and the Kronecker class number.

Let $\overline{Q}$ be an orbit of the action of Γ on $\mathcal{Q}_D$. Choose a representative $Q(x,y) = ax^2+bxy+cy^2$ from the orbit $\overline{Q}$. We can factor $Q = (a,b,c)Q_0$, where $Q_0(x,y)$ is a primitive integral positive-definite binary quadratic form of discriminant $-D/(a,b,c)^2$. In this way, every orbit of the action of Γ on $\mathcal{Q}_D$ corresponds to an orbit of the action of Γ on $\mathcal{Q}_{D/f^2}^{\text{prim}}$ for some divisor f^2 of D with $f > 0$.

Therefore we have

$$H(-D) = \sum_{\Gamma/\overline{Q}\in\mathcal{Q}_D/\Gamma} 1 = \sum_{f^2|D} \left(\sum_{\overline{Q}_0\in\mathcal{Q}_D^{\text{prim}}/\Gamma} 1 \right) = \sum_{f^2|D} h(-D/f^2) = \sum_{\substack{f^2|D \\ \frac{-D}{f^2}\equiv 0,1 \pmod 4}} h(-D/f^2),$$

where the final equality holds because Q_{D/f^2}^{prim} is empty if and only if $-D/f^2 \not\equiv 0, 1 \pmod 4$. For all but two divisors $f^2 \mid D$, we can apply the class number formula in (2.4.3) to $h(-D/f^2)$. If they exist, divisors f^2 such that $-D/f^2 \in \{3, 4\}$ contribute $h(-3) = h(-4) = 1$. Therefore upon applying (2.4.3) we have the useful analytic expression

$$H(-D) = \frac{1}{\pi} \sum_{\substack{f^2|D \\ \frac{-D}{f^2}\equiv 0,1 \pmod 4}} \frac{\sqrt{D} \cdot L(1,\chi)}{f} \quad + \quad \mathrm{O}(1), \tag{2.4.4}$$

where the error term has no dependence on D and $\chi := (-D|\cdot)$ is the Kronecker symbol. Using the bound $L(1,\chi) \ll \log D$ from Lemma 2.3.1, we conclude the section by recording the naïve asymptotic upper-bound

$$H(-D) \ll \sqrt{D} \log^2 D.$$

In particular for any integers r and f satisfying $-D = r^2 - 4p^f < -1$, we have

$$H(r^2 - 4p^f) \ll p^{f/2} \log^2 p. \tag{2.4.5}$$

2.5 Algebraic Number Theory

A *number field* is a finite algebraic extension over the field of rational numbers. Let $F/\mathbb{Q}$ be a number field, and let $\mathrm{Aut}(F/\mathbb{Q})$ be the group of automorphisms of the field F that fix each rational number point-wise. If there is a one-to-one and order-reversing correspondence between subfields of $F/\mathbb{Q}$ and subgroups of $\mathrm{Aut}(F/\mathbb{Q})$, we say the number field $F/\mathbb{Q}$ is *Galois over* $\mathbb{Q}$ (or simply *Galois* if the base field is understood). If $F/\mathbb{Q}$ is Galois, then the group $\mathrm{Aut}(F/\mathbb{Q})$ is subsequently denoted $\mathrm{Gal}(F/\mathbb{Q})$ and called the *Galois group of* F *over* $\mathbb{Q}$.

Let $F/\mathbb{Q}$ be a number field. The *ring of integers of* F, denoted $\mathcal{O}_F$, is the ring of all elements of F that are solutions to some monic polynomial with rational integer coefficients. Since

every number field is a finite extension over the field of rational numbers, it is not difficult to show that $\mathcal{O}_F$ is finitely-generated as a $\mathbb{Z}$-module. Such a set of generators for $\mathcal{O}_F$ over the integers is known as an *integral basis of* $\mathcal{O}_F$. Furthermore $\mathcal{O}_F$ is a *Dedekind domain*, which among other things means that $\mathcal{O}_F$ has Krull dimension one and every ideal of $\mathcal{O}_F$ factors uniquely into prime ideals.

Let p be a rational prime, and consider the ideal $p\mathcal{O}_F \subset \mathcal{O}_F$. Since $\mathcal{O}_F$ is a Dedekind domain we can factor this ideal uniquely as

$$p\mathcal{O}_F = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\dots\mathfrak{p}_g^{e_g},$$

where each $\mathfrak{p}_j$ is a distinct prime ideal of $\mathcal{O}_F$ and each e_j is a positive integer. We say the prime ideal $\mathfrak{p}$ *lies above* the rational prime p if $\mathfrak{p} \cap \mathbb{Z} = (p)$; similarly the rational prime p *lies below* any ideal $\mathfrak{p}$ appearing in the ideal factorization of $p\mathcal{O}_F$.

Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_F$ lying above the rational prime p; say $\mathfrak{p}^e$ occurs in the factorization of the ideal $p\mathcal{O}_F$. We say the exponent e is the *ramification index of* $\mathfrak{p}$ *over* p. Since $\mathcal{O}_F$ is one-dimensional every prime ideal is maximal; therefore the quotient $\mathbb{F}_\mathfrak{p} := \mathcal{O}_F/\mathfrak{p}$ is known as the *residue field of* $\mathfrak{p}$. In fact such a field is finite and contains $\mathbb{Z}/p\mathbb{Z}$, so it is isomorphic to the field with p^f elements for some integer $f \geq 1$ known as the *(inertia) degree of* $\mathfrak{p}$. The *norm of the ideal* $\mathfrak{p}$ is $N(\mathfrak{p}) := p^f$. Lastly we note the relationship $[F : \mathbb{Q}] = \sum_{j=1}^{g} e_j f_j$.

For a general number field $F/\mathbb{Q}$, the ramification indices and inertia degrees can vary considerably upon looking through all prime ideals lying above a fixed rational prime. However if $F/\mathbb{Q}$ is Galois, the situation simplifies considerably. In this case the group $\mathrm{Gal}(F/\mathbb{Q})$ acts transitively on the set of prime ideals lying above a fixed rational prime p (see [ME06, 11.3.1]), leading to the fact that the factorization of the ideal $p\mathcal{O}_F$ is simply

$$p\mathcal{O}_F = \mathfrak{p}_1^e\mathfrak{p}_2^e\dots\mathfrak{p}_g^e,$$

for a unique integer e depending only on the rational prime p. Furthermore the inertia degrees are identical as well – for each prime ideal $\mathfrak{p}_j$ lying above p the residue field $\mathbb{F}_{\mathfrak{p}_j}$ is isomorphic to the field with p^f elements for a unique integer f depending only on the rational prime p. As a result we have the very simple relationship $[F : \mathbb{Q}] = efg$.

Let $F/\mathbb{Q}$ be a Galois number field of degree $d := [F : \mathbb{Q}]$, and let p be a fixed rational

prime with ramification index e and inertia degree f. Since $[F : \mathbb{Q}] = efg$, the rational prime p lies below precisely $g = d/ef$ distinct prime ideals of $\mathcal{O}_K$, each with ramification index e and inertia degree f. If $g = d$, then we say the prime p *splits completely in* F. The typical way to determine the splitting behavior of a prime p in a Galois number field is to study the factorization of the polynomial that defines the algebraic number field modulo the prime p. In certain cases, however, the splitting behavior of a prime can be made more explicit.

An *abelian number field* is a Galois number field with an abelian Galois group. For example, the cyclotomic field $\mathbb{Q}(\zeta_m)$ where ζ_m is a primitive m^{th} root of unity is an abelian number field with Galois group $(\mathbb{Z}/m\mathbb{Z})^\times$. In a way this is the quintessential example of abelian number fields; the Kronecker-Weber theorem (see [Rib01, Chapter 15] for a proof) states that every abelian number field can be realized as the subfield of a cyclotomic field. The *conductor of an abelian number field* $K/\mathbb{Q}$ is the smallest integer Q such that K is a subfield of the Q^{th} cyclotomic field $\mathbb{Q}(\zeta_Q)$. The following theorem from class field theory is the tool that allows us to explicitly characterize the splitting of rational primes in an abelian number field.

Theorem 2.5.1. *Let K be an abelian number field of conductor Q. There is a unique set $\mathcal{V}$ of residues modulo Q such that the rational prime p splits completely in K if and only if $p \equiv v \pmod{Q}$ for some $v \in \mathcal{V}$.*

Proof. See [Was97, Theorem 3.7]. □

2.6 Elliptic Curves

In this section we study elliptic curves just enough so as to gather their arithmetic information and then to pass to the techniques of analytic number theory. As such, we state and define only what we need to prove the main theorems of this dissertation; for a more general treatment or for further detail, the reader is invited to consult [Sil86, Kna92, ST94] as well as [Kob12, Ch.1-2].

Let K be a field with $\text{char}(K) \neq 2, 3$. An *elliptic curve* is a pair (E, O), where E is a smooth projective variety over K of genus one and O is a distinguished base point on E. We will also use the notation E/K when the base point O is understood or irrelevant. Using the Riemann-Roch theorem (see [Sil86, II.5]), every elliptic curve over K can be modeled by an affine *Weierstrass equation*

$$E_{a,b} : y^2 = x^3 + ax + b, \tag{2.6.1}$$

where $a, b \in K$. The distinguished point O corresponds to the projective point [0:1:0] upon homogenizing the equation $E_{a,b}$. Associated to such an equation is the *discriminant* $\Delta(E_{a,b}) = -16(4a^3 + 27b^2)$, which encodes the smoothness of the curve. For any $u \in K^\times$ the change of variables

$$\begin{aligned} x &= u^2\bar{x} \\ y &= u^3\bar{y}, \end{aligned} \tag{2.6.2}$$

leads to the new Weierstrass equation

$$E_{\frac{a}{u^4},\frac{b}{u^6}} : \bar{y}^2 = \bar{x}^3 + \frac{a}{u^4}\bar{x} + \frac{b}{u^6}$$

for the same elliptic curve. These are said to be *isomorphic models* of the same curve, however note that the respective discriminants differ by a factor of $1/u^{12}$.

Let E/K be an elliptic curve with Weierstrass equation $E_{a,b}$ and discriminant $\Delta := \Delta(E_{a,b})$. Upon applying the changes of variables as described in (2.6.2) we may always assume that $E_{a,b}$ and Δ are defined over the ring of integers $\mathcal{O}_K$. Let $\mathfrak{p}$ be a prime from $\mathcal{O}_K$. We say that this Weierstrass equation is *minimal at* $\mathfrak{p}$ if the order of divisibility of $\mathfrak{p}$ in the ideal $\Delta\mathcal{O}_K$ is minimal amongst all isomorphic models of E arising from the admissible changes of variables described in (2.6.2). If the Weierstrass equation $E_{a,b}$ is indeed a minimal model for E with respect to the prime $\mathfrak{p}$, we define the *reduction of E modulo $\mathfrak{p}$* as the elliptic curve $E^{\mathfrak{p}}/\mathbb{F}_{\mathfrak{p}}$ modeled by the Weierstrass equation

$$E^{\mathfrak{p}}_{a,b} : y^2 = x^3 + ax + b \pmod{\mathfrak{p}}, \tag{2.6.3}$$

where a and b are now interpreted as elements of $\mathbb{F}_{\mathfrak{p}}$. For this reduction to yield an elliptic curve over this finite field we insist $\mathfrak{p} \nmid \Delta\mathcal{O}_K$ so that the reduced curve $E^{\mathfrak{p}}/\mathbb{F}_{\mathfrak{p}}$ is nonsingular.

Lemma 2.6.1. *Let $E_{a,b}$ be a model for an elliptic curve $E/\mathbb{F}_{p^f}$. The number of models $E_{a',b'}$ isomorphic to $E_{a,b}$ over the field $\mathbb{F}_{p^f}$ is*

$$\#\mathcal{I}(E_{a,b}) := \begin{cases} \dfrac{p^f-1}{6} & \text{if } a \equiv 0 \pmod{p^f} \text{ and } p^f \equiv 1 \pmod 3, \\ \dfrac{p^f-1}{4} & \text{if } b \equiv 0 \pmod{p^f} \text{ and } p^f \equiv 1 \pmod 4, \\ \dfrac{p^f-1}{2} & \text{otherwise.} \end{cases}$$

Proof. Recall from (2.6.2) that the model $E_{a,b}$ is $\mathbb{F}_{p^f}$-isomorphic to a model $E_{a',b'}$ if and only if there is a non-zero element $u \in \mathbb{F}_{p^f}^{\times}$ such that $a \equiv u^4 a'$ and $b \equiv u^6 b'$ both modulo p^f. Note that if such an element u indeed satisfies both congruences above then $-u$ will satisfy both as well. Therefore to prove this lemma it suffices to understand how much we "overcount" as we run through the elements of $\mathbb{F}_{p^f}^{\times}$ based on how many roots of unity we see in $\mathbb{F}_{p^f}^{\times}$. We use the fact from finite group theory that the group $\mathbb{F}_{p^f}^{\times}$ contains 4^{th} roots of unity (denoted Z_4) if and only if $p^f \equiv 1 \pmod 4$ and $\mathbb{F}_{p^f}^{\times}$ contains 3^{rd} roots of unity (denoted Z_3) if and only if $p^f \equiv 1 \pmod 3$.

First assume $b \equiv 0 \pmod{p^f}$. Any model that is $\mathbb{F}_{p^f}$-isomorphic to $E_{a,0}$ must be of the form $E_{au^4,0}$. For $\zeta \in Z_4$ and $u \in \mathbb{F}_{p^f}^{\times}$, the elements u and ζu will yield identical Weierstrass models because $au^4 \equiv a(\zeta u)^4 \pmod{p^f}$. Therefore since $\#Z_4 = 4$ when $p^f \equiv 1 \pmod 4$ and $\#Z_4 = 2$ otherwise, in the case that $b \equiv 0 \pmod{p^f}$ we have

$$\#\mathcal{I}(E_{a,b}) = \sum_{u \in \mathbb{F}_{p^f}^{\times}} \frac{1}{\#Z_4} = \begin{cases} \dfrac{p^f - 1}{2} & \text{if } p^f \not\equiv 1 \pmod 4, \\ \dfrac{p^f - 1}{4} & \text{if } p^f \equiv 1 \pmod 4. \end{cases}$$

Next assume $a \equiv 0 \pmod{p^f}$. Any model that is $\mathbb{F}_{p^f}$-isomorphic to $E_{0,b}$ must be of the form E_{0,bu^6}. Let Z_6 denote the sixth roots of unity in $\mathbb{F}_{p^f}^{\times}$. Note that -1 is a sixth root of unity which always exists in $\mathbb{F}_{p^f}^{\times}$, so $\#Z_6 = 2$ or $\#Z_6 = 6$ depending on whether or not $\mathbb{F}_{p^f}^{\times}$ contains Z_3 or not. For $\zeta \in Z_6$ and $u \in \mathbb{F}_{p^f}^{\times}$, the elements u and ζu will yield identical Weierstrass models because $bu^6 \equiv b(\zeta u)^6 \pmod{p^f}$. Therefore in the case that $a \equiv 0 \pmod{p^f}$ we have

$$\#\mathcal{I}(E_{a,b}) = \sum_{u \in \mathbb{F}_{p^f}^{\times}} \frac{1}{\#Z_6} = \begin{cases} \dfrac{p^f - 1}{2} & \text{if } p^f \not\equiv 1 \pmod 3, \\ \dfrac{p^f - 1}{6} & \text{if } p^f \equiv 1 \pmod 3. \end{cases}$$

In the case that both a and b are non-zero in $\mathbb{F}_{p^f}$, the only time that E_{au^4,bu^6} is the same model as E_{av^4,bv^6} is if $u \equiv -v \pmod{p^f}$. Therefore in the generic case we have

$$\#\mathcal{I}(E_{a,b}) = \sum_{u \in \mathbb{F}_{p^f}^{\times}} \frac{1}{\#Z_2} = \frac{p^f - 1}{2},$$

which completes the proof.

□

Let $E^{\mathfrak{p}}/\mathbb{F}_{\mathfrak{p}}$ be an elliptic curve with base point O and Weierstrass equation $E^{\mathfrak{p}}_{a,b}$. The $\mathbb{F}_{\mathfrak{p}}$-*rational points of* E is the locus of points

$$E(\mathbb{F}_{\mathfrak{p}}) := \{(x,y) \in \mathbb{F}_{\mathfrak{p}}^2 : (x,y) \in E^{\mathfrak{p}}_{a,b}\} \cup \{O\}.$$

Since $\mathbb{F}_{\mathfrak{p}}$ is a finite field (in particular it is isomorphic to the finite field $\mathbb{F}_{N(\mathfrak{p})}$), the number of $\mathbb{F}_{\mathfrak{p}}$-rational points is finite. From the theory of quadratic residues, it is reasonable to expect that $\#E(\mathbb{F}_{\mathfrak{p}}) \approx N(\mathfrak{p}) + 1$, and so we define the integer-valued quantity $a_{\mathfrak{p}}(E)$ known as the *trace of Frobenius of* E *at* $\mathfrak{p}$ such that

$$\#E(\mathbb{F}_{\mathfrak{p}}) = N(p) + 1 - a_{\mathfrak{p}}(E),$$

which satisfies the Hasse bound $|a_{\mathfrak{p}}(E)| \leq 2\sqrt{N(\mathfrak{p})}$ (see [Sil86, V.1]).

2.7 A Curve-Counting Lemma

In this section, we prove an important lemma which allows us to pass from elliptic curves to analytic number theory. Given a family of elliptic curves $\mathcal{F}$ defined over a Galois number field K, of interest is to reduce these curves modulo many primes $\mathfrak{p}$ from $\mathcal{O}_K$ and count how often the trace of Frobenius at that prime $\mathfrak{p}$ is precisely equal to some fixed integer r. Since these traces are preserved by isomorphism class over $\mathbb{F}_{\mathfrak{p}}$, we will rely heavily on the following classical theorem of Waterhouse and Deuring.

Theorem 2.7.1 ([Deu41] or [Wat69, Section 4])**.** *Let p be a rational prime, and let f be a positive integer. For any integer r coprime to p which satisfies $r^2 \leq 4p^f$, there are precisely $H(r^2 - 4p^f)$ isomorphism classes of elliptic curves over $\mathbb{F}_{p^f}$ with $p^f + 1 - r$ points, where $H(-D)$ is the Kronecker class number associated to the discriminant $-D$.*

Let K be a number field of degree d with ring of integers $\mathcal{O}_K$. Fix an integral basis $\mathcal{B} = \{e_1, e_2, \ldots, e_d\}$ for $\mathcal{O}_K$ and the supremum norm $||\cdot||$ on $\mathcal{O}_K$ described in (1.3.3) with respect to this basis. For any positive real number Z, let $\mathcal{C}_Z$ be the set of models of elliptic curves $E_{a,b}$ defined over K such that $||a||, ||b|| \leq Z$. For a fixed prime $\mathfrak{p}$ of degree f in $\mathcal{O}_K$ and a fixed integer r, of interest is to study

$$\#\{E_{a,b} \in \mathcal{C}_Z : a_{\mathfrak{p}}(E) = r\}.$$

There are approximately $(2Z)^{2d}$ models in the family $\mathcal{C}_Z$, however if we find a model $E_{a,b}$ that satisfies $a_{\mathfrak{p}}(E) = r$ then we can find several more. More explicitly, two distinct models $E_{a,b}$ and $E_{a',b'}$ are identical modulo $\mathfrak{p}$ if and only if both $a \equiv a' \pmod{\mathfrak{p}}$ and $b \equiv b' \pmod{\mathfrak{p}}$. Since the residue field $\mathcal{O}_K/\mathfrak{p}$ has size p^f, as a' and b' run through $\mathcal{O}_K$ we expect $E_{a',b'}$ and $E_{a,b}$ to be identical modulo $\mathfrak{p}$ once out of every $(p^f)^2 = p^{2f}$ models we see. From this we see that it suffices to only count models of elliptic curves over $\mathbb{F}_{\mathfrak{p}}$ such that $a_{\mathfrak{p}}(E) = r$. From Lemma (2.6.1) the number of models over $\mathbb{F}_{\mathfrak{p}}$ isomorphic to a fixed model is typically about $p^f/2$; from Theorem 2.7.1 the number of isomorphism classes of elliptic curves over $\mathbb{F}_{\mathfrak{p}}$ with trace r is $H(r^2 - 4p^f)$. Making this argument rigorous leads to the following lemma.

Lemma 2.7.2. *For a fixed integer r and a fixed prime $\mathfrak{p}$ of $\mathcal{O}_K$ of degree f over a rational prime $p > 5$ satisfying both $r^2 - 4p^f \leq -1$ and $p \nmid r$, we have*

$$\#\{E_{a,b} \in \mathcal{C}_Z : a_{\mathfrak{p}}(E) = r\} = (2Z)^{2d} \cdot \frac{H(r^2 - 4p^f)}{2p^f} + \mathrm{O}\left(\frac{Z^{2d}}{p^f} + \log^2 p \cdot \left[\frac{Z^{2d-1}}{p^{f/2-1}} + \frac{Z^{2d}}{p^{17f/2}}\right]\right).$$

Proof. Let $N_{\mathfrak{p},r}(Z)$ denote the quantity in question. Since $a_{\mathfrak{p}}(E)$ is preserved by $\mathbb{F}_{\mathfrak{p}}$-isomorphisms, we can count the number of models $E_{a,b} \in \mathcal{C}_Z$ with the particular trace $a_{\mathfrak{p}}(E) = r$ by partitioning the curves into isomorphism classes. Regrouping according to all models $E_{a,b} \in \mathcal{C}_Z$ that are isomorphic to a fixed model $E'_{a',b'}/\mathbb{F}_{\mathfrak{p}}$, we obtain

$$N_{\mathfrak{p},r}(Z) = \sum_{\substack{E'_{a',b'}/\mathbb{F}_{\mathfrak{p}} \\ a_{\mathfrak{p}}(E')=r}} \sum_{\substack{E_{a,b} \in \mathcal{C}_Z \\ E \cong_{\mathfrak{p}} E'}} 1. \tag{2.7.1}$$

Fix a model $E'_{a',b'}/\mathbb{F}_{\mathfrak{p}}$, and consider only the inner-most sum of (2.7.1). Since reduction modulo $\mathfrak{p}$ is only defined on minimal models with respect to the prime $\mathfrak{p}$, we have

$$\sum_{\substack{E_{a,b} \in \mathcal{C}_Z \\ E \cong_{\mathfrak{p}} E'}} 1 = \sum_{\substack{a,b \in \mathcal{O}_K \\ ||a||,||b|| \leq Z \\ a \equiv a' \pmod{\mathfrak{p}} \\ b \equiv b' \pmod{\mathfrak{p}}}} 1 \quad + \quad \mathrm{O}(\#\{\text{models in } \mathcal{C}_Z \text{ that are not minimal at } \mathfrak{p}\}). \tag{2.7.2}$$

Since $p\mathcal{O}_K \subset \mathfrak{p} \subset \mathcal{O}_K$, we may partition the elements of $\mathfrak{p}$ into the left cosets of $p\mathcal{O}_K$ in $\mathfrak{p}$. In doing so we will pass from the modulo $\mathfrak{p}$ condition to the easier-to-handle modulo p condition. Since $[\mathcal{O}_K : \mathfrak{p}] = p^f$ and $[\mathcal{O}_K : p\mathcal{O}_K] = p^d$, we know that there are p^{d-f} such cosets. Therefore we can

choose coset representatives $r_1, r_2, \ldots, r_{p^{d-f}} \subset p\mathcal{O}_K$ such that

$$\begin{aligned} a \equiv a' \pmod{\mathfrak{p}} \quad &\text{if and only if} \quad a \equiv a' + r_i \pmod{p\mathcal{O}_K} \text{ for some } r_i, \\ b \equiv b' \pmod{\mathfrak{p}} \quad &\text{if and only if} \quad b \equiv b' + r_j \pmod{p\mathcal{O}_K} \text{ for some } r_j. \end{aligned}$$

Using the integral basis $\mathcal{B} = \{e_1, e_2, \ldots, e_d\}$ for $\mathcal{O}_K$, we can uniquely write

$$\begin{aligned} a' + r_i &=: \sum_{j=1}^{d} c_{i,j} e_j, \\ b' + r_i &=: \sum_{j=1}^{d} d_{i,j} e_j, \end{aligned}$$

for appropriate rational integers $c_{i,j}$ and $d_{i,j}$. With this characterization we can now express

$$\begin{aligned} a \equiv a' \pmod{\mathfrak{p}} \quad &\text{if and only if} \quad a \equiv \sum_{j=1}^{d} c_{i,j} e_j \pmod{p\mathcal{O}_K}, \\ b \equiv b' \pmod{\mathfrak{p}} \quad &\text{if and only if} \quad b \equiv \sum_{j=1}^{d} d_{i,j} e_j \pmod{p\mathcal{O}_K}. \end{aligned}$$

Therefore the main term of (2.7.2) is

$$\begin{aligned} \sum_{\substack{a,b \in \mathcal{O}_K \\ ||a||, ||b|| \le Z \\ a \equiv a' \pmod{\mathfrak{p}} \\ b \equiv b' \pmod{\mathfrak{p}}}} 1 &= \sum_{i \le p^{d-f}} \left(\sum_{\substack{a \in \mathcal{O}_K \\ ||a|| \le Z \\ a \equiv \sum_{j=1}^{d} c_{i,j} e_j \pmod{p\mathcal{O}_K}}} 1 \right) \sum_{i \le p^{d-f}} \left(\sum_{\substack{b \in \mathcal{O}_K \\ ||b|| \le Z \\ b \equiv \sum_{j=1}^{d} d_{i,j} e_j \pmod{p\mathcal{O}_K}}} 1 \right) \\ &= \sum_{i \le p^{d-f}} \left(\sum_{\substack{v \in \mathbb{Z}^d \\ ||v||_\infty \le Z \\ v_j \equiv c_{i,j} \pmod{p} \text{ for all } j \le d}} 1 \right) \sum_{i \le p^{d-f}} \left(\sum_{\substack{w \in \mathbb{Z}^d \\ ||w||_\infty \le Z \\ w_j \equiv d_{i,j} \pmod{p} \text{ for all } j \le d}} 1 \right) \\ &= \sum_{i \le p^{d-f}} \left(\frac{2Z+1}{p} + \mathrm{O}(1) \right)^d \cdot \sum_{i \le p^{d-f}} \left(\frac{2Z+1}{p} + \mathrm{O}(1) \right)^d \end{aligned}$$

which is

$$\frac{(2Z)^{2d}}{p^{2f}} + \mathrm{O}\left(\frac{Z^{2d-1}}{p^{2f-1}} \right).$$

With respect to the error term of (2.7.2), we know from [Sil86, p.172] that for a prime $\mathfrak{p}$

lying above a rational prime $p > 5$ the model $E_{a,b}$ is minimal at $\mathfrak{p}$ if and only if $a \notin \mathfrak{p}^4$ or $b \notin \mathfrak{p}^6$. Using an identical argument as above on the ideals $\mathfrak{p}^4$ and $\mathfrak{p}^6$, the error term in (2.7.2) is bounded above by

$$\sum_{\substack{a,b\in\mathcal{O}_K \\ ||a||,||b||\leq Z \\ a\equiv 0 \pmod{\mathfrak{p}^4} \\ b\equiv 0 \pmod{\mathfrak{p}^6}}} 1 = \sum_{i\leq p^{d-f}} \left(\frac{2Z+1}{p^{4f}} + \mathrm{O}(1)\right)^d \sum_{i\leq p^{d-f}} \left(\frac{2Z+1}{p^{6f}} + \mathrm{O}(1)\right)^d \ll \frac{Z^{2d}}{p^{10f}}.$$

Having evaluated both terms in (2.7.2), we can now express the quantity in (2.7.1) as

$$N_{\mathfrak{p},r}(Z) = \left[\frac{(2Z)^{2d}}{p^{2f}} + \mathrm{O}\left(\frac{Z^{2d-1}}{p^{2f-1}} + \frac{Z^{2d}}{p^{10f}}\right)\right] \sum_{\substack{E_{a,b}/\mathbb{F}_{\mathfrak{p}} \\ a_{\mathfrak{p}}(E)=r}} 1. \tag{2.7.3}$$

We now turn our attention to the inner-most sum of (2.7.3), which counts the number of models of elliptic curves over a finite field with fixed trace. Since the trace of Frobenius at $\mathfrak{p}$ is preserved by $\mathbb{F}_{\mathfrak{p}}$-isomorphism, for each $\mathbb{F}_{\mathfrak{p}}$-isomorphism class $\tilde{E}/\mathbb{F}_{\mathfrak{p}}$ we may choose a representative model $E_{a,b}$. Note that from Lemma (2.6.1) there are at most $10 = \mathrm{O}(1)$ isomorphism classes that have a representative model $E_{a,b}$ with either $a \equiv 0 \pmod{\mathfrak{p}}$ or $b \equiv 0 \pmod{\mathfrak{p}}$. As a result, letting $\mathcal{I}(E_{a,b})$ represent the set of all models isomorphic to $E_{a,b}$, we can sum over all isomorphism classes to yield

$$\sum_{\substack{E_{a,b}/\mathbb{F}_{\mathfrak{p}} \\ a_{\mathfrak{p}}(E)=r}} 1 = \sum_{\substack{\tilde{E}/\mathbb{F}_{\mathfrak{p}} \\ a_{\mathfrak{p}}(E)=r}} \#\mathcal{I}(E_{a,b}) = \sum_{\substack{\tilde{E}/\mathbb{F}_{\mathfrak{p}} \\ a_{\mathfrak{p}}(E)=r}} \frac{p^f-1}{2} \quad + \quad \mathrm{O}\left(10p^f\right),$$

Recalling that we are assuming $r^2 - 4p^f < -1$ and $(p, r) = 1$, Theorem 2.7.1 gives that the number of $\mathbb{F}_{\mathfrak{p}}$-isomorphism classes of elliptic curves over $\mathbb{F}_{\mathfrak{p}}$ with precisely $p^f + 1 - r$ points is $H(r^2 - 4p^f)$, where $H(-D)$ is the Kronecker class number associated to the discriminant $-D$. As a result the inner-most sum of (2.7.3) is

$$\frac{p^f-1}{2} H(r^2 - 4p^f) + \mathrm{O}\left(p^f\right).$$

Upon applying this substitution into (2.7.3) and simplifying the resulting error terms using the bound in (2.4.5) we obtain the desired result.

□

Chapter 3

Extremal Primes of Elliptic Curves

In this chapter, we study the number of extremal primes of an elliptic curve on average and prove Theorem 1.2.3. For a positive real number X and a parameter $Z := Z(X)$, the quantity of interest is

$$\frac{1}{4Z^2}\sum_{\substack{|a|\leq Z\\|b|\leq Z}}\pi^{\text{Champ}}_{E_{a,b}}(X).$$

In Section 3.1 we pass from a sum on elliptic curves to a sum on rational primes. In Section 3.2, we prove the main theorem conditional on technical lemmas proved in Sections 3.3, 3.4, and 3.5.

3.1 Reducing to an Average of Special L-Values

We begin by switching the sums and writing

$$\frac{1}{4Z^2}\sum_{\substack{|a|\leq Z\\|b|\leq Z}}\pi^{\text{Champ}}_{E_{a,b}}(X) = \frac{1}{4Z^2}\sum_{3<p<X}\#\{E_{a,b} : |a|,|b|\leq Z \text{ and } a_p(E) = [|-2\sqrt{p}|]\}.$$

For convenience, set $\Delta_p = \left[\left|2\sqrt{p}\right|\right]^2 - 4p$. The quantity inside the sum above was studied in Lemma 2.7.2; applying that result here gives

$$\frac{1}{4Z^2}\sum_{\substack{|a|\leq Z\\|b|\leq Z}}\pi^{\text{Champ}}_{E(a,b)}(X) = \sum_{3<p<X}\frac{H(\Delta_p)}{2p} + \mathrm{O}\left(\log\log X + \frac{X^{3/2}\log X}{Z}\right),$$

where the estimates on the error terms are obtained using partial summation in conjunction with the prime number theorem. It is worth noting that studying the trailing primes of elliptic curves (those primes such that $a_p(E) = [|2\sqrt{p}|]$) would lead to an identical expression because we are squaring the trace in each case. In this way, studying champion primes and trailing primes will each lead to an identical asymptotic. In cooperation with the analytic expression of the Kronecker class number seen in (2.4.4), in total we have

$$\frac{1}{4Z^2}\sum_{\substack{|a|\leq Z\\|b|\leq Z}}\pi^{\text{Champ}}_{E(a,b)}(X)=\frac{1}{2\pi}\sum_{3<p<X}\frac{\sqrt{|\Delta_p|}}{p}\sum_{\substack{f^2|\Delta_p\\ \frac{\Delta_p}{f^2}\equiv 0,1 \pmod 4}}\frac{L(1,\chi_{p;f})}{f}\ +\ \mathrm{O}\left(\log\log X+\frac{X^{3/2}\log X}{Z}\right), \tag{3.1.1}$$

where $\chi_{p;f} := (\Delta_p/f^2|\cdot)$ is the Kronecker symbol.

For the time-being we focus only on the main term of (3.1.1). As a function of a positive real variable t, the function $|\Delta_t| = 4t-[|2\sqrt{t}|]^2$ is sawtooth; it has zeros whenever t or $t/4$ is a square and is linear with slope 4 between these zeros. With this in mind we define intervals

$$I_k := \left(\frac{k^2}{4}, \frac{(k+1)^2}{4}\right],$$

where we note that for $t \in I_k$ we have $|\Delta_t| = |\Delta_{t,k}| := |k^2 - 4t|$ and also

$$|\Delta_{t,k}| \leq 2k+1 \text{ for all } t \in I_k, \tag{3.1.2}$$

which we will use repeatedly. Furthermore, since we are only concerned with the primes in the real interval $(3, X)$, it suffices to look at the union of intervals I_k from $k = 4$ to $k = [|2\sqrt{X}|]$. Partitioning in this manner allows us to write the main term in (3.1.1) as

$$\frac{1}{2\pi}\sum_{3<k<2X^{1/2}}\sum_{p\in I_k}\frac{\sqrt{|\Delta_{p,k}|}}{p}\sum_{\substack{f^2|\Delta_{p,k}\\ \frac{\Delta_{p,k}}{f^2}\equiv 0,1 \pmod 4}}\frac{L(1,\chi_{p,k;f})}{f}+\mathrm{O}(\log^2 X),$$

where $\chi_{p,k;f} := (\Delta_{p,k}/f^2|\cdot)$ is the same Kronecker symbol as above. The error term arises from potential overcounting in the interval $I_{[|2\sqrt{X}|]}$ since the parameter $2\sqrt{X}$ may not be an integer; it was bounded using Lemma 2.3.1 and (3.1.2). Switching the order of summation gives the quantity

above as

$$\frac{1}{2\pi}\sum_{3<k<2X^{1/2}}\sum_{f\leq\sqrt{2k+1}}\frac{1}{f}\sum_{p\in\mathcal{S}_f(I_k)}\frac{\sqrt{|\Delta_{p,k}|}}{p}L\left(1,\chi_{p,k;f}\right)+\mathrm{O}(\log^2 X), \tag{3.1.3}$$

where we have defined

$$\mathcal{S}_f(I_k):=\left\{p\in I_k:\Delta_{p,k}\equiv 0\pmod{f^2}\,;\frac{\Delta_{p,k}}{f^2}\equiv 0,1\pmod 4\right\}.$$

The upper bound of $f\leq\sqrt{2k+1}$ arises because if $f>\sqrt{2k+1}$ then the set $\mathcal{S}_f(I_k)$ is empty due to the condition that $f^2\mid\Delta_{p,k}$ and (3.1.2).

Theorem 3.1.1. *For any real number $U\geq 4$ and with the notation as established in this section, set*

$$\mathfrak{D}(U):=\sum_{U\leq k<2U}\sum_{f\leq\sqrt{2k+1}}\frac{1}{f}\sum_{p\in\mathcal{S}_f(I_k)}\frac{\sqrt{|\Delta_{p,k}|}}{p}L\left(1,\chi_{p,k;f}\right).$$

We have that

$$\mathfrak{D}(U)=\frac{2\sqrt{2}}{3}\int_U^{2U}\frac{\mathrm{d}t}{t^{1/2}\log t}+\mathrm{O}\left(\frac{U^{1/2}}{\log^2 U}\right).$$

Theorem 1.2.3 now follows from the result stated above. To see this, substituting (3.1.3) back into the main term of (3.1.1) and using the notation $\mathfrak{D}(U)$ gives

$$\frac{1}{4Z^2}\sum_{\substack{|a|\leq Z\\|b|\leq Z}}\pi^{\mathrm{Champ}}_{E(a,b)}(X)=\frac{1}{2\pi}\sum_{\substack{j\leq\log(X^{1/2})\\(U=2^j)}}\mathfrak{D}(U)\ +\ \mathrm{O}\left(\log^2 X+\frac{X^{3/2}\log X}{Z}\right),$$

the main term of which, in conjunction with Theorem 3.1.1 and standard integration, is

$$\frac{2\sqrt{2}}{3\pi}\int_4^{2X^{1/2}}\frac{\mathrm{d}t}{t^{1/2}\log t}\ +\ \mathrm{O}\left(\frac{X^{1/4}}{\log^2 X}\right)=\frac{8X^{1/4}}{3\pi\log X}+\mathrm{O}\left(\frac{X^{1/4}}{\log^2 X}\right),$$

as desired. It is for this reason the remainder of this chapter is a proof of Theorem 3.1.1.

3.2 Outlining the Proof of Theorem 3.1.1

For simplicity in notation, we let $\chi:=\chi_{p,k;f}=(\Delta_{p,k}/f^2|\cdot)$. We begin our study of $\mathfrak{D}(U)$ by noting that for any real number $p\in I_k$, we can write $p=k^2/4+\mathrm{O}(k)$ and therefore a Taylor series

approximation gives

$$\frac{1}{p\log p} = \frac{1}{\frac{k^2}{4}\log\frac{k^2}{4}} + \mathrm{O}\left(\frac{1}{k^3\log k}\right).$$

Using this estimate gives

$$\mathfrak{D}(U) = \sum_{U\le k<2U} \frac{1}{\frac{k^2}{4}\log\frac{k^2}{4}} \sum_{f\le\sqrt{2k+1}} \frac{1}{f} \sum_{p\in\mathcal{S}_f(I_k)} \sqrt{|\Delta_{p,k}|}\log p\cdot L\left(1,\chi\right) + \mathrm{O}(\log^2 U), \tag{3.2.1}$$

where the error term was obtained using Lemma 2.3.1 and (3.1.2).

We truncate the sum over integers $f \le \sqrt{2k+1} \le 3\sqrt{U}$ at a parameter $F := F(U)$ to be determined later. Using Lemma 2.3.1, (3.1.2), and the naive bound $\#\mathcal{S}_f(I_k) \ll k/f^2$ to bound the tail, the inner sums over $f \le \sqrt{2k+1}$ and $p \in \mathcal{S}_f(I_k)$ of (3.2.1) contribute

$$\sum_{f\le F} \frac{1}{f} \sum_{p\in\mathcal{S}_f(I_k)} \sqrt{|\Delta_{p,k}|}\log p\cdot L(1,\chi) + \mathrm{O}\left(\frac{k^{3/2}\log^2 k}{F^2}\right).$$

Therefore, we have

$$\mathfrak{D}(U) = \sum_{U\le k<2U} \frac{1}{\frac{k^2}{4}\log\frac{k^2}{4}} \sum_{f\le F} \frac{1}{f} \sum_{p\in\mathcal{S}_f(I_k)} \sqrt{|\Delta_{p,k}|}\log p\cdot L\left(1,\chi\right) + \mathrm{O}\left(\log^2 U + \frac{U^{1/2}\log^2 U}{F^2}\right), \tag{3.2.2}$$

whereupon taking $F \ge \log^2 U$ gives this error as $\mathrm{O}(U^{1/2}/\log^2 U)$.

Next, we aim to replace the special L-value $L(1,\chi)$ with an appropriate truncated L-value $L(1,\chi;w)$ for most Kronecker symbols χ. We recall from Fact 2.1.5 that the conductor of $\chi = (\Delta_{p,k}/f^2|\cdot)$, denoted here as N_χ, is at most $4|\Delta_{p,k}/f^2|$; therefore using (3.1.2) we see that $N_\chi \le 17U$. Set $H := 17U$ and $\alpha := 4$, and let $\mathcal{E}_4(H)$ be the set of exceptional conductors as guaranteed by Theorem 2.3.2. For convenience, set $z := \log H$. For a prime $p \in \mathcal{S}_f(I_k)$, if $N_\chi \in \mathcal{E}_4(H)$ then by Lemma 2.3.1 we have

$$L(1,\chi) - L(1,\chi;z^{128}) \ll \log p \ll \log U.$$

On the other hand, if $N_\chi \notin \mathcal{E}_4(H)$ then by the second claim in Theorem 2.3.2 and the estimate in Lemma 2.3.3 we have

$$L(1,\chi) - L(1,\chi,z^{128}) \ll \frac{L(1,\chi;z^{128})}{z^4} \ll \frac{\log z}{z^4} \ll \frac{1}{\log^3 U}.$$

Lastly, we note that as p runs through $\mathcal{S}_f(I_k)$, we never see the same conductor N_χ more than twice. To see this, note from Fact 2.1.5 that the conductor of the character $(a|\cdot)$ is either $|a|$ or $4|a|$. So as a result we have

$$\sum_{\substack{p\in\mathcal{S}_f(I_k)\\ N_\chi=e}} 1 \leq \sum_{\substack{m\in I_k\\ (4m-k^2)/f^2=e}} 1 + \sum_{\substack{m\in I_k\\ 4(4m-k^2)/f^2=e}} 1 \leq 2.$$

Therefore, for a fixed integer k satisfying $U \leq k < 2U$ and a fixed integer $f < F$ we have

$$\begin{aligned}
&\sum_{p\in\mathcal{S}_f(I_k)} \sqrt{|\Delta_{p,k}|}\log p \cdot \left[L\left(1,\chi\right) - L\left(1,\chi;z^{128}\right)\right] \\
&\qquad \ll \sqrt{U}\log U\left[\sum_{\substack{p\in\mathcal{S}_f(I_k)\\ N_\chi\in\mathcal{E}_4(H)}} \log U + \sum_{\substack{p\in\mathcal{S}_f(I_k)\\ N_\chi\notin\mathcal{E}_4(H)}} \frac{1}{\log^3 U}\right] \\
&\qquad \ll \sqrt{U}\log U\left[H^{1/2}\log U + \frac{U}{\log^3 U}\right],
\end{aligned}$$

where we rely on the bound $\#\mathcal{E}_4(H) \ll H^{1/2}$ coming from Theorem 2.3.2. Recalling that $H \ll U$ gives the entire error above is $\mathrm{O}(U^{3/2}/\log^2 U)$. Therefore we have shown

$$\mathfrak{D}(U) = \sum_{U\leq k<2U} \frac{1}{\frac{k^2}{4}\log\frac{k^2}{4}} \sum_{f\leq F}\frac{1}{f}\sum_{p\in\mathcal{S}_f(I_k)} \sqrt{|\Delta_{p,k}|}\log p\cdot L\left(1,\chi;z^{128}\right) + \mathrm{O}\left(\frac{U^{1/2}}{\log^2 U}\right). \tag{3.2.3}$$

With $z = \log(17U)$, one can check that $z^{128} \geq 10$ for any $U \geq 1$. Therefore, by Theorem 2.3.2 with a parameter $v := v(U) \geq 4\log\log U$, we have

$$L\left(1,\chi;z^{128}\right) = \sum_{\substack{n\leq z^{128v}\\ P^+(n)\leq z^{128}}} \frac{\chi(n)}{n} + \mathrm{O}\left(\frac{1}{\log^3 U}\right).$$

As a result we obtain

$$\mathfrak{D}(U) = \sum_{U\leq k<2U} \frac{1}{\frac{k^2}{4}\log\frac{k^2}{4}} \sum_{\substack{f\leq F\\ n\leq z^{128v}\\ P^+(n)\leq z^{128}}} \frac{1}{nf}\sum_{p\in\mathcal{S}_f(I_k)} \sqrt{|\Delta_{p,k}|}\log p\cdot\chi(n) + \mathrm{O}\left(\frac{U^{1/2}}{\log^2 U}\right). \tag{3.2.4}$$

For now we solely investigate the main term of (3.2.4). From Fact 2.1.5, for fixed n the Kronecker symbol $\chi(n) = (\cdot|n)$ is $4n$-periodic in the top argument. Furthermore, the conditions $p \in \mathcal{S}_f(I_k)$ and $\Delta_{p,k}/f^2 \equiv a \pmod{4n}$ are equivalent to $p \in I_k$, $4p \equiv (k^2 - af^2) \pmod{4nf^2}$, and

$a \equiv 0, 1 \pmod 4$. In this way, the main term of (3.2.4) is

$$\sum_{U \le k < 2U} \frac{1}{\frac{k^2}{4} \log \frac{k^2}{4}} \sum_{\substack{f \le F \\ n \le z^{128v} \\ P^+(n) \le z^{128}}} \frac{1}{nf} \sum_{\substack{a \in \mathbb{Z}/4n\mathbb{Z} \\ a \equiv 0,1 \pmod 4 \\ (k^2 - af^2, 4nf^2) = 4}} \left(\frac{a}{n}\right) \sum_{\substack{p \in I_k \\ p \equiv \frac{k^2 - af^2}{4} \pmod{nf^2}}} \sqrt{|\Delta_{p,k}|} \log p, \tag{3.2.5}$$

where the condition $(k^2 - af^2, 4nf^2) = 4$ is a necessary condition when the inner sum over primes is non-zero.

The innermost sum counts primes in a short arithmetic progressions with an awkward weighting function. For $p \in I_k$, the function $\sqrt{|\Delta_{p,k}|}$ grows to be about $(2k+1)^{1/2}$ and the length of the interval I_k is essentially $2k+1$. Since such primes are expected to be equally distributed amongst the $\phi(nf^2)$ primitive residue classes modulo nf^2, we expect the innermost sum in (3.2.5) to be about $(2k+1)^{3/2}/\phi(nf^2)$. Inspired by this intuition, the following result is proved in Section 3.3.

Lemma 3.2.1. *Let b and q be coprime integers, and fix an integer k satisfying $U \le k < 2U$. For any integer h with $q \le h \le U/4$, we have*

$$\sum_{\substack{p \in I_k \\ p \equiv b \pmod q}} \sqrt{|\Delta_{p,k}|} \cdot \log p = \frac{(2k+1)^{3/2}}{6\phi(q)} + \mathrm{O}\left(\frac{U^{1/2}}{h} \int_{I_k} E(y, h; q, b) \, \mathrm{d}y + \frac{hU^{1/2} \log U}{q}\right).$$

Applying the result of Lemma 3.2.1 and (3.2.5) in the context of (3.2.4) while also rearranging some finite sums gives the expression

$$\mathfrak{D}(U) = \frac{1}{6} \sum_{U \le k < 2U} \frac{(2k+1)^{3/2}}{\frac{k^2}{4} \log \frac{k^2}{4}} \left[\sum_{\substack{f \le F \\ n \le z^{128v} \\ P^+(n) \le z^{128}}} \frac{1}{nf\phi(nf^2)} \sum_{\substack{a \in \mathbb{Z}/4n\mathbb{Z} \\ a \equiv 0,1 \pmod 4 \\ (k^2 - af^2, 4nf^2) = 4}} \left(\frac{a}{n}\right) \right] + E_1 + E_2 + E_3, \tag{3.2.6}$$

where

$$\begin{aligned}
E_1 &\ll \frac{U^{1/2}}{h}\sum_{U\le k<2U}\frac{1}{k^2\log k}\sum_{\substack{f\le F\\ n\le z^{128v}\\ P^+(n)\le z^{128}}}\frac{1}{nf}\sum_{\substack{a\in\mathbb{Z}/4n\mathbb{Z}\\ a\equiv 0,1 \pmod 4\\ (k^2-af^2,4nf^2)=4}}\int_{I_k} E\left(y,h;nf^2,\frac{k^2-af^2}{4}\right)\mathrm{d}y,\\
E_2 &\ll hU^{1/2}\log U\sum_{U\le k<2U}\frac{1}{k^2\log k}\sum_{\substack{f\le F\\ n\le z^{128v}\\ P^+(n)\le z^{128}}}\frac{1}{n^2f^3}\sum_{\substack{a\in\mathbb{Z}/4n\mathbb{Z}\\ a\equiv 0,1 \pmod 4\\ (k^2-af^2,4nf^2)=4}}1,\\
E_3 &\ll \frac{U^{1/2}}{\log^2 U}.
\end{aligned}$$

Since $v \ge 4\log\log U$, the E_2 term can be immediately bounded above by

$$\frac{h}{U^{1/2}}\sum_{\substack{n\le z^{128v}\\ P^+(n)\le z^{128}}}\frac{1}{n}\sum_{f<F}\frac{1}{f^3} \ll \frac{hv\log z}{U^{1/2}} \ll \frac{h(\log\log U)^2}{U^{1/2}},$$

so if we take $h \le U/\log^4 U$ then this error is $\mathrm{O}(U^{1/2}/\log^2 U)$.

The E_1 term can be bounded using Theorem 2.2.4. Since for $U \le k < 2U$ the function $1/(k^2\log k) = \mathrm{O}(1/(U^2\log U))$, we have

$$E_1 \ll \frac{1}{hU^{3/2}\log U}\sum_{U\le k<2U}\sum_{\substack{f<F\\ n\le z^{128v}\\ P^+(n)\le z^{128}}}\frac{1}{nf}\sum_{\substack{a\in\mathbb{Z}/4n\mathbb{Z}\\ a\equiv 0,1 \pmod 4\\ (k^2-af^2,4nf^2)=4}}\int_{I_k} E\left(y,h;nf^2,\frac{k^2-af^2}{4}\right)\,\mathrm{d}y.$$

Since $E(y,h;q,b) \le \max_{(a,q)=1}|E(y,h;q,a)| =: E(y,h;q)$, we subsequently obtain

$$E_1 \ll \frac{1}{hU^{3/2}\log U}\sum_{U\le k<2U}\sum_{\substack{f<F\\ n\le z^{128v}\\ P^+(n)\le z^{128}}}\frac{1}{f}\int_{I_k} E\left(y,h;nf^2\right)\,\mathrm{d}y,$$

where now as all summands are positive we may relax the conditions on the sum over integers n to give

$$E_1 \ll \frac{1}{hU^{3/2}\log U}\sum_{U\le k<2U}\sum_{\substack{f<F\\ n\le z^{128v}}}\frac{1}{f}\int_{I_k} E\left(y,h;nf^2\right)\,\mathrm{d}y.$$

Switching sums and integrals is valid as these are all finite quantities. Furthermore, we recall that the intervals $I_U, I_{U+1}, \dots, I_{2U-1}$ partition the real interval $[U^2/4, U^2]$. Lastly, upon fixing an f as

n runs in the interval $n \leq z^{128v}$ we see moduli of the form $nf^2 \leq z^{128v} f^2$. Since all summands are positive we may extend the sum to all moduli $q \leq z^{128v} f^2$. With all these observations, we continue with

$$E_1 \ll \frac{1}{hU^{3/2} \log U} \sum_{f<F} \frac{1}{f} \int_{U^2/4}^{U^2} \sum_{q<z^{128v} f^2} E\left(y, h; q\right) \, \mathrm{d}y.$$

We recall that our current error bounds rely on the parameters $h \leq U/\log^4 U$, $F \geq \log^2 U$, $z = \log\left(17U\right)$, and $v \geq 4 \log\log U$. As such, $(z^{128v} f^2)^2 \ll U^{\delta}$ for any $\delta > 0$, and therefore the necessary condition $(z^{128v} f^2)^2 \leq h/U^{1/6+\epsilon}$ for some $\epsilon > 0$ in Theorem 2.2.4 holds comfortably upon taking F and v as small as possible and h as large as possible in accordance with this necessary condition. Therefore applying Theorem 2.2.4 with $A = 2$ to this quantity gives the desired bound

$$E_1 \ll \frac{1}{hU^{3/2} \log U} \cdot \frac{hU^2}{\log^2 U} \sum_{f<F} \frac{1}{f} \ll \frac{U^{1/2}}{\log^2 U}.$$

Returning to (3.2.6) with our updated error bounds gives

$$\mathfrak{D}(U) = \frac{1}{6} \sum_{U \leq k < 2U} \frac{(2k+1)^{3/2}}{\frac{k^2}{4} \log \frac{k^2}{4}} \left[\sum_{\substack{f \leq F \\ n \leq z^{128v} \\ P^+(n) \leq z^{128}}} \frac{1}{nf\phi(nf^2)} \sum_{\substack{a \in \mathbb{Z}/4n\mathbb{Z} \\ a \equiv 0,1 \pmod 4 \\ (k^2 - af^2, 4nf^2) = 4}} \left(\frac{a}{n}\right) \right] + \mathrm{O}\left(\frac{U^{1/2}}{\log^2 U}\right). \quad (3.2.7)$$

The quantity in square brackets in (3.2.7) has significant multiplicative structure and can be transformed into an Euler product. The proof of the following lemma is quite short as this expression is very similar to one studied in [DP99]; its proof can be found in Section 3.4.

Lemma 3.2.2. *Let $U \leq k < 2U$. For any parameters F, z, and v, we have that*

$$\sum_{\substack{f \leq F \\ n \leq z^{128v} \\ P^+(n) \leq z^{128}}} \frac{1}{nf\phi(nf^2)} \sum_{\substack{a \in \mathbb{Z}/4n\mathbb{Z} \\ a \equiv 0,1 \ (mod\ 4) \\ (k^2 - af^2, 4nf^2) = 4}} \left(\frac{a}{n}\right) = C \cdot C(k) + \mathrm{O}\left(\frac{1}{F^2} + \frac{1}{z^{64v}} + \frac{1}{z^{64}}\right),$$

where

$$C \cdot C(k) := \prod_{\ell} \frac{\ell(\ell^2 - \ell - 1)}{(\ell - 1)(\ell^2 - 1)} \cdot \prod_{\ell \mid k} \frac{\ell(\ell - 1)}{\ell^2 - \ell - 1}.$$

Note that our choice of $F = \log^2 U$, $v = 4 \log\log U$, and $z = \log 17U$ implies the entire error

of Lemma 3.2.2 is $\mathrm{O}(1/\log^4 U)$. As a result, we apply Lemma 3.2.2 to (3.2.7) to obtain

$$\mathfrak{D}(U) = \frac{C}{6} \sum_{U \le k < 2U} \frac{(2k+1)^{3/2}}{\frac{k^2}{4} \log \frac{k^2}{4}} \cdot C(k) + \mathrm{O}\left(\frac{U^{1/2}}{\log^2 U}\right).$$

Taylor series approximations allow us to write

$$\begin{aligned} (2k+1)^{3/2} &= 2\sqrt{2}k^{3/2} + \mathrm{O}(k^{1/2}), \\ \frac{1}{\log \frac{k^2}{4}} &= \frac{1}{2\log k} + \mathrm{O}\left(\frac{1}{k \log k}\right). \end{aligned}$$

Therefore we have

$$\mathfrak{D}(U) = \frac{2\sqrt{2}C}{3} \sum_{U \le k < 2U} \frac{C(k)}{k^{1/2} \log k} + \mathrm{O}\left(\frac{U^{1/2}}{\log^2 U}\right). \tag{3.2.8}$$

It remains to study the partial sums of the multiplicative function $C(k)$. The function $C(k)$ is a product of several factors just slightly larger than 1, and therefore we expect $C(k) \approx 1$. This is the intuition for the final technical lemma of this section; a proof can be found in Section 3.5.

Lemma 3.2.3. *Let U be a real number, and let K be any real number satisfying $U \le K < 2U$. We have*

$$S(U,K) := \sum_{U \le k < K} C(k) = C^{-1}(K-U) + \mathrm{O}(\log K),$$

where

$$C^{-1} := \prod_{\ell} \left(1 + \frac{1}{\ell^3 - \ell^2 - 1}\right).$$

Since $CC^{-1} = 1$, applying partial summation and then Lemma 3.2.3 to the main term of (3.2.8) gives

$$\begin{aligned} \frac{2\sqrt{2}C}{3} & \left[\frac{S(1,2U)}{(2U)^{1/2}\log 2U} - \frac{S(1,U)}{(U)^{1/2}\log U} - \int_U^{2U} \frac{\mathrm{d}}{\mathrm{d}t}\left(\frac{1}{t^{1/2}\log t}\right) S(1,t)\ \mathrm{d}t\right] \\ &= \frac{2\sqrt{2}}{3}\left[\frac{2U}{(2U)^{1/2}\log 2U} - \frac{U}{(U)^{1/2}\log U} - \int_U^{2U} \frac{\mathrm{d}}{\mathrm{d}t}\left(\frac{1}{t^{1/2}\log t}\right) t\ \mathrm{d}t\right] \end{aligned}$$

with a negligible error of $\mathrm{O}(1/U^{1/2})$. Integration by parts implies the quantity above is

$$\frac{2\sqrt{2}}{3} \int_U^{2U} \frac{\mathrm{d}t}{t^{1/2}\log t},$$

which completes the proof of Theorem 3.1.1 conditional on the lemmas used in the proof.

3.3 Counting Primes with a Strange Weight

In this section we prove Lemma 3.2.1, which examines the quantity

$$\Lambda(k; q, b) := \sum_{\substack{p \in I_k \\ p \equiv b \pmod{q}}} \sqrt{|\Delta_{p,k}|} \cdot \log p,$$

where $U \leq k < 2U$ and the integers b and q are coprime. We define the notation

$$\ell_k := \frac{2k+1}{4}, \quad I_k^+ := \frac{(k+1)^2}{4}, \quad I_k^- := \frac{k^2}{4},$$

which represent the length, upper endpoint, and lower endpoints (respectively) of the interval I_k.

The proof in this section is inspired by that in [CDKS16, Lemma 7.1]. We begin by peeling off a small amount from each end of the interval I_k. Let $q \leq h \leq U/4$. Since $U \leq k < 2U$, we know that $I_k^- + 2h \leq I_k^- + U/2 < \ell_k$. Using the naive bound $\#\{p \in (y, y+z) : p \equiv b \pmod{q}\} \ll z/q$, we have

$$\Lambda(k; q, b) = \sum_{\substack{I_k^- + h < p \leq I_k^+ - h \\ p \equiv b \pmod{q}}} \sqrt{|\Delta_{p,k}|} \cdot \log p + \mathrm{O}(F_1), \tag{3.3.1}$$

where

$$F_1 \ll \frac{h\sqrt{k} \log k}{q} \ll \frac{h\sqrt{U} \log U}{q}. \tag{3.3.2}$$

For any prime p satisfying $I_k^- + h < p \leq I_k^+ - h$, we can write $p = I_k^- + p_0 \cdot \ell_k$ for some real number p_0 satisfying $\frac{h}{\ell_k} < p_0 \leq 1 - \frac{h}{\ell_k}$. Therefore, for such primes we have

$$\sqrt{|\Delta_{p,k}|} = \sqrt{2k+1} \cdot \sqrt{p_0}.$$

Set $\eta := h/\ell_k$. For any $t = t_0 + \mathrm{O}(\eta)$, a Taylor series approximation gives

$$\int_{t_0 - \eta}^{t_0} \sqrt{t} \, \mathrm{d}t = \eta\sqrt{t_0} + \mathrm{O}\left(\frac{\eta^2}{\sqrt{t_0}}\right).$$

Therefore for the primes described above, we have

$$\sqrt{|\Delta_{p,k}|} = \frac{(2k+1)^{3/2}}{4h} \int_{\frac{p-I_k^-}{\ell_k} - h}^{\frac{p-I_k^-}{\ell_k}} \sqrt{t}\ \mathrm{d}t + \mathrm{O}\left(\frac{\eta}{\sqrt{\frac{p-I_k^-}{\ell_k}}}\right).$$

In this way, we have replaced the awkward prime-weight of $\sqrt{\Delta_{p,k}}$ with a smooth integral weight. Upon putting this work into (3.3.1), we obtain

$$\Lambda(k;q,b) = \frac{(2k+1)^{3/2}}{4h} \sum_{\substack{I_k^- + h < p \le I_k^+ - h \\ p \equiv b \pmod q}} \log p \left[\int_{\frac{p-I_k^-}{\ell_k} - h}^{\frac{p-I_k^-}{\ell_k}} \sqrt{t}\ \mathrm{d}t \right] + \mathrm{O}(F_1 + F_2),$$

where

$$F_2 \ll \frac{h \log k}{\sqrt{k}} \sum_{\substack{I_k^- + h < p \le I_k^+ - h \\ p \equiv b \pmod q}} \frac{1}{\sqrt{p - I_k^-}} \ll \frac{\sqrt{hU}\log U}{q}. \tag{3.3.3}$$

In comparison to F_1 we see that $F_2 \ll F_1$, and so we omit F_2 going forward. Switching the sum and integral in the previous expression of $\Lambda(k;q,b)$ gives

$$\Lambda(k;q,b) = \frac{(2k+1)^{3/2}}{4h} \int_0^{1-\eta} \sqrt{t} \left[\sum_{\substack{I_k^- + h < p \le I_k^+ - h \\ I_k^- + t\ell_k < p < I_k^- + t\ell_k + h \\ p \equiv b \pmod q}} \log p \right] \mathrm{d}t + \mathrm{O}(F_1). \tag{3.3.4}$$

We aim to extend the limits of the integration to the full interval $[0,1]$. For t satisfying $\eta < t < 1 - 2\eta$, the first condition in the summation is implied by the second condition. For $t \in [0,1] \backslash (\eta, 1-2\eta)$, we have

$$\sqrt{t} \left[\sum_{\substack{I_k^- + h < p \le I_k^+ - h \\ I_k^- + t\ell_k < p < I_k^- + t\ell_k + h \\ p \equiv b \pmod q}} \log p \right] \le \sum_{\substack{I_k^- + t\ell_k < p < I_k^- + t\ell_k + h \\ p \equiv b \pmod q}} \log p \ \ll\ \frac{h \log k}{q},$$

and so the full contribution for $t \in [0,1]\backslash(\eta, 1-2\eta)$ is

$$\frac{(2k+1)^{3/2}}{4h} \int\limits_{[0,1]\backslash(\eta,1-2\eta)} \frac{h\log k}{q}\, \mathrm{d}t \ll \frac{k^{1/2}h\log k}{q} \ll \frac{U^{1/2}h\log U}{q},$$

which is the same size as F_1. Returning to (3.3.4), we now have the expression

$$\Lambda(k;q,b) = \frac{(2k+1)^{3/2}}{4h}\int_0^1 \sqrt{t}\left[\sum_{\substack{I_k^- + t\ell_k < p < I_k^- + t\ell_k + h \\ p \equiv b \pmod q}} \log p\right] \mathrm{d}t + \mathrm{O}(F_1). \tag{3.3.5}$$

The sum in square brackets above counts log-weighted primes in a short arithmetic progression. Using the notation defined in Section 2.2, we have

$$\Lambda(k;q,b) = \frac{(2k+1)^{3/2}}{4h}\int_0^1 \sqrt{t}\left[\frac{h}{\phi(q)} + E(I_k^- + t\ell_k, h; q, b)\right] \mathrm{d}t + \mathrm{O}(F_2),$$

which is

$$\frac{(2k+1)^{3/2}}{6\phi(q)} + \frac{(2k+1)^{3/2}}{4h}\int_0^1 \sqrt{t}\cdot E(I_k^- + t\ell_k, h; q, b)\, \mathrm{d}t + \mathrm{O}(F_1).$$

Upon applying the change of variables $y := I_k^- + t\ell_k$, the absolute value of the second term is no larger than

$$\frac{k^{3/2}}{h}\int_0^1 E(I_k^- + t\ell_k, h; q, b)\, \mathrm{d}t \ll \frac{U^{1/2}}{h}\int_{I_k} E(y, h; q, b)\, \mathrm{d}y,$$

which completes the proof.

3.4 Averaging a Character Sum

In this section we prove Lemma 3.2.2 by fixing $U \le k < 2U$ and studying the quantity

$$D(k) := \sum_{\substack{f \le F \\ n \le z^{128v} \\ P^+(n) \le z^{128}}} \frac{1}{nf\phi(nf^2)} \sum_{\substack{a \in \mathbb{Z}/4n\mathbb{Z} \\ a \equiv 0,1 \pmod 4 \\ (k^2 - af^2, 4nf^2) = 4}} \left(\frac{a}{n}\right).$$

We will use the notation introduced in [DP99] by defining

$$c_f^k(n) := \sum_{\substack{a \in \mathbb{Z}/4n\mathbb{Z} \\ a \equiv 0,1 \pmod 4 \\ (k^2 - af^2, 4nf^2) = 4}} \left(\frac{a}{n}\right),$$

and we also define a multiplicative function $\kappa(n)$ generated on prime powers by

$$\kappa(\ell^\alpha) = \begin{cases} \ell & \alpha \text{ is odd,} \\ 1 & \alpha \text{ is even.} \end{cases}$$

The analysis of $D(k)$ is almost identical to a similar quantity investigated in [DP99, Section 3]. The only difference in the two terms is our additional constraint of $P^+(n) \leq z^{128}$. As such, we will state facts proven in [DP99] without proof and give full credit to the authors of that paper for this slightly modified proof. In particular, the following theorem is a conglomeration of results found in [DP99, Lemma 3.3, Lemma 3.4, Equation 22, Lemma 4.1].

Theorem 3.4.1.

1. *For every n, we have the bound $|c_f^k(n)| \leq n/\kappa(n)$.*

2. *For any parameter T, we have*
$$\sum_{n>T} \frac{1}{\kappa(n)\phi(n)} \ll \frac{1}{\sqrt{T}}.$$

3. *For any parameters T and F, we have*
$$\sum_{\substack{n<T \\ f<F}} \frac{c_f^k(n)}{nf\phi(nf^2)} = C \cdot C(k) + \mathrm{O}\left(\frac{1}{F^2} + \frac{1}{\sqrt{T}}\right),$$
where
$$C \cdot C(k) := \prod_{\ell} \frac{\ell(\ell^2 - \ell - 1)}{(\ell - 1)(\ell^2 - 1)} \cdot \prod_{\ell | k} \frac{\ell(\ell - 1)}{\ell^2 - \ell - 1}.$$

We begin by writing $D(k)$ as

$$D(k) = \sum_{\substack{f \leq F \\ n \leq z^{128v}}} \frac{c_f^k(n)}{nf\phi(nf^2)} - \sum_{\substack{f \leq F \\ n \leq z^{128v} \\ P^+(n) > z^{128}}} \frac{c_f^k(n)}{nf\phi(nf^2)}.$$

Since $\phi(nf^2) \geq \phi(n) \cdot \phi(f^2)$ and the constraint $P^+(n) > z^{128}$ means that $n > z^{128}$, we can use (1) and (2) from Theorem 3.4.1 to show that the second term above is bounded above by

$$\sum_{f \leq F} \frac{1}{f\phi(f^2)} \sum_{z^{128} < n \leq z^{128v}} \frac{1}{\kappa(n)\phi(n)} \ll \frac{1}{z^{64}}.$$

Therefore, we have

$$D(k) = \sum_{\substack{f \leq F \\ n \leq z^{128v}}} \frac{c_f^k(n)}{nf\phi(nf^2)} + \mathrm{O}\left(\frac{1}{z^{64}}\right).$$

Applying (3) from Theorem 3.4.1 gives

$$D(k) = C \cdot C(k) + \mathrm{O}\left(\frac{1}{F^2} + \frac{1}{z^{64v}} + \frac{1}{z^{64}}\right),$$

which is the desired result.

3.5 Summing a Multiplicative Function

In this section we study the quantity

$$S(U, K) := \sum_{U \leq k < K} C(k) = \sum_{U \leq k < K} \left(\prod_{\ell \mid k} \frac{\ell(\ell-1)}{\ell^2 - \ell - 1} \right),$$

however to prove Lemma 3.2.2 it suffices to prove

$$S(K) := \sum_{k < K} C(k) = C^{-1}K + \mathrm{O}(\log K), \tag{3.5.1}$$

where C^{-1} is defined in the statement of the lemma, as then $S(U, K) = S(K) - S(U)$ gives the desired result.

We begin by noting that $C(k)$ is not just multiplicative but also prime-power-invariant, and so the identity

$$C(k) = \sum_{d \mid k} \mu^2(d) \prod_{\ell \mid d} \frac{1}{\ell^2 - \ell - 1}$$

can be checked by computing on prime powers. With this in tow, we sum over all $k < K$ to obtain

$$\begin{aligned} S(K) &= \sum_{k<K} C(k) \\ &= \sum_{k<K} \sum_{d|k} \mu^2(d) \prod_{\ell|d} \frac{1}{\ell^2-\ell-1} \\ &= \sum_{de<K} \mu^2(d) \prod_{\ell|d} \frac{1}{\ell^2-\ell-1} \\ &= \sum_{d<K} \mu^2(d) \prod_{\ell|d} \frac{1}{\ell^2-\ell-1} \left[\sum_{e<K/d} 1 \right] \\ &= K \sum_{d<K} \frac{\mu^2(d)}{d^3} \prod_{\ell|d} \frac{\ell^2}{\ell^2-\ell-1} - \sum_{d<K} \left\{ \frac{K}{d} \right\} \frac{\mu^2(d)}{d^2} \prod_{\ell|d} \frac{\ell^2}{\ell^2-\ell-1}, \end{aligned}$$

where $\{a\}$ denotes the fractional part of a real number a.

Let $\nu(m)$ count the number of prime divisors of m without multiplicity. We remark that since $1 < \ell^2/(\ell^2-\ell-1) \le 9/5$ for any odd prime ℓ, the fractional part $\{K/d\} \le 1$, and the arithmetic function $\nu(d) \le \log d$, the second term above can be bounded above by

$$\sum_{d<K} \frac{\mu^2(d)}{d^2} \left[4 \cdot \left(\frac{9}{5} \right)^{\nu(d)} \right] \ll \sum_{d<K} \frac{\mu^2(d)}{d^2} \cdot \left(\frac{9}{5} \right)^{\log d} \ll \sum_{d<K} \frac{1}{d^2} \cdot d \ll \log K.$$

For the main term, we extend the sum over all integers $d \ge 1$ and estimate the tail similarly as

$$K \sum_{d \ge K} \frac{\mu^2(d)}{d^3} \prod_{\ell|d} \frac{\ell^2}{\ell^2-\ell-1} \ll K \sum_{d \ge K} \frac{\mu^2(d)}{d^3} \left(\frac{9}{5} \right)^{\nu(d)} \ll K \sum_{d \ge K} \frac{1}{d^2} \ll 1.$$

As a result, in full we have

$$\begin{aligned} S(K) &= K \sum_{d=1}^{\infty} \frac{\mu^2(d)}{d^3} \prod_{\ell|d} \frac{\ell^2}{\ell^2-\ell-1} + \mathrm{O}(\log K) \\ &= K \prod_{l} \sum_{\alpha=0}^{\infty} \frac{\mu^2(\ell^\alpha)}{\ell^{3\alpha}} \prod_{p|\ell^\alpha} \frac{p^2}{p^2-p-1} + \mathrm{O}(\log K) \\ &= K \prod_{\ell} \left(1 + \frac{1}{\ell^3} \cdot \frac{\ell^2}{\ell^2-\ell-1} \right) + \mathrm{O}(\log K) \\ &= C^{-1} K + \mathrm{O}(\log K), \end{aligned}$$

which completes the proof of (3.5.1).

Chapter 4

Koblitz's Conjecture over Abelian Number Fields

The focus of this chapter is Theorem 1.3.1, which states that Koblitz's conjecture holds on average for elliptic curves defined over an abelian number field with square-free conductor. In particular, the quantity of interest is

$$\sum_{E \in \mathcal{C}_Z} \pi_E^{\text{twin}}(X),$$

for positive real numbers X and Z and the family of curves $\mathcal{C}_Z$.

Throughout this portion of the paper, $K/\mathbb{Q}$ is an abelian number field of degree d and Q is the square-free conductor of $K/\mathbb{Q}$. We begin by reducing Theorem 1.3.1 to Theorem 4.1.1, which is a statement about rational primes. Section 4.2 is a sketch of the proof of this reduction, conditional on various lemmas proved in Sections 4.3, 4.4, and 4.5.

4.1 Reducing to a Sum on Rational Primes

Since $K/\mathbb{Q}$ is Galois, every rational prime p of degree f has precisely $g(p) := d/f$ distinct primes in $\mathcal{O}_K$ which lie above p. Therefore we begin by rewriting the sum over primes of $\mathcal{O}_K$ as a

sum over rational primes; in particular we have

$$\sum_{E\in\mathcal{C}_Z}\pi_E^{\text{twin}}(X) \;:=\; \sum_{E\in\mathcal{C}_Z}\left(\sum_{f=1}^{d}\sum_{\substack{N(\mathfrak{p})<X\\ \deg_K(\mathfrak{p})=f\\ \mathfrak{p}\nmid\Delta(E)\\ \#E(\mathbb{F}_{\mathfrak{p}})\text{ prime}}}1 \;+\; \mathrm{O}(1)\right) \;=\; \sum_{f=1}^{d}\sum_{\substack{5<p<X^{1/f}\\ g(p)=d/f\\ |r|\le 2p^{f/2}\\ p^f+1-r\text{ prime}}}\frac{d}{f}\sum_{\substack{E\in\mathcal{C}_Z\\ a_{\mathfrak{p}}(E)=r}}1 \;+\; \mathrm{O}(Z^2), \quad (4.1.1)$$

where the error term arises from the finite number of primes lying above the rational primes 2, 3, and 5, in addition to the finite number of primes of bad reduction for each curve. We note that for $p>5$, it is necessary that r is odd if we are to have p^f+1-r prime. The inner-most sum over models of elliptic curves was studied in Lemma 2.7.2; applying its result here and then switching the order of the finite sums allows us to write the main term of (4.1.1) as

$$\frac{d(2Z)^{2d}}{2}\sum_{f=1}^{d}\frac{1}{f}\sum_{\substack{5<p<X^{1/f}\\ g(p)=d/f\\ |r|\le 2p^{f/2};\ r\text{ odd}\\ p^f+1-r\text{ prime}}}\frac{H(r^2-4p^f)}{p^f} \quad+\quad \mathrm{O}\left(Z^{2d}\left[X^{1/2}+\frac{X^2\log X}{Z}+\log^2 X\right]\right).$$

As a result, upon averaging across the family $\mathcal{C}_Z$ of size $\mathcal{C}_Z=(2Z)^{2d}+\mathrm{O}(Z^{2d-1})$ we obtain

$$\frac{1}{\#\mathcal{C}_Z}\sum_{E\in\mathcal{C}_Z}\pi_E^{\text{twin}}(X)=\frac{d}{2}\sum_{f=1}^{d}\frac{1}{f}\sum_{\substack{5<p<X^{1/f}\\ g(p)=d/f\\ |r|\le 2p^{f/2};\ r\text{ odd}\\ p^f+1-r\text{ prime}}}\frac{H(r^2-4p^f)}{p^f} \;+\; \mathrm{O}\left(X^{1/2}+\frac{X^2\log X}{Z}+\log^2 X\right). \quad (4.1.2)$$

In inspecting (4.1.2), we notice that the contribution from the high-degree primes is negligible in comparison to the contribution from the primes that split completely in $\mathcal{O}_K$. Indeed, consider only the portion of (4.1.2) with $f>1$. Using (2.4.5) this quantity is asymptotically-bounded above by

$$\sum_{f=2}^{d}\frac{1}{f}\sum_{\substack{p<X^{1/f}\\ |r|\le 2p^{f/2}}}\frac{H(r^2-4p^f)}{p^f} \;\ll\; \sum_{f=2}^{d}\sum_{\substack{p<X^{1/f}\\ |r|\le 2p^{f/2}}}\frac{\log^2 p}{p^{f/2}} \;\ll\; d\cdot\log^2 X\sum_{p<X^{1/2}}1\ll X^{1/2}\log X,$$

which, though larger than the existing error terms in (4.1.2), is significantly smaller than the expected main term. Having now seen that the high degree primes have no significant effect on the quantity

in question, we return to (4.1.2) to simplify

$$\frac{1}{\#\mathcal{C}_Z}\sum_{E\in\mathcal{C}_Z}\pi_E^{\text{twin}}(X)=\frac{d}{2}\sum_{\substack{5<p<X\\ g(p)=d\\ |r|\leq 2\sqrt{p};\ r\text{ odd}\\ p+1-r\text{ prime}}}\frac{H(\Delta_{p,r})}{p}\quad+\quad \mathrm{O}\left(\frac{X^2\log X}{Z}+X^{1/2}\log^2 X\right), \tag{4.1.3}$$

where as in Chapter 3 we use the notation $\Delta_{p,r}:=r^2-4p$.

Rather than look at all primes up to the parameter X simultaneously, it will be helpful to partition the primes in the interval $(5,X)$ into $J(X)+1:=[|\log^8 X|]+1$ subintervals of length $Y(X):=X/\log^8 X$. Set $X_j:=jY$. In this way, we can write the main term in (4.1.3) as

$$\frac{d}{2}\sum_{j=1}^{J}\sum_{\substack{X_j<p\leq X_j+Y\\ g(p)=d\\ |r|\leq 2\sqrt{p};\ r\text{ odd}\\ p+1-r\text{ prime}}}\frac{H(\Delta_{p,r})}{p}+\mathrm{O}\left(\frac{X}{\log^6 X}\right),$$

where the error term comes from potential overcounting in the top interval and the contribution from the first interval $(0,Y]$. For each $1\leq j\leq J$, the contribution from values of r satisfying $2X_j^{1/2}\leq|r|\leq 2\sqrt{p}$ in the quantity above is also negligible. Using (2.4.5) and the convexity bound $\sqrt{a+b}-\sqrt{a}\leq\sqrt{b}$ for positive real numbers a and b, indeed the contribution from such r is asymptotically less than

$$\sum_{j=1}^{J}\sum_{\substack{X_j<p\leq X_j+Y\\ 2X_j^{1/2}\leq|r|\leq 2\sqrt{p}}}\frac{p^{1/2}\log^2 p}{p}\ll\sum_{j=1}^{J}\sum_{X_j<p\leq X_j+Y}\frac{\log^2 p}{p^{1/2}}\cdot\sqrt{Y}\ \ll\ \sqrt{YX}\log X\ \ll\ \frac{X}{\log^3 X}.$$

Returning to (4.1.3), the previous two lines have allowed us to write

$$\frac{1}{\#\mathcal{C}_Z}\sum_{E\in\mathcal{C}_Z}\pi_E^{\text{twin}}(X)=\frac{d}{2}\sum_{j=1}^{J}\sum_{\substack{|r|<2X_j^{1/2}\\ r\text{ odd}}}\left[\sum_{\substack{X_j<p\leq X_j+Y\\ g(p)=d\\ p+1-r\text{ prime}}}\frac{H(\Delta_{p,r})}{p}\right]+\mathrm{O}\left(\frac{X}{\log^3 X}+\frac{X^2\log X}{Z}\right). \tag{4.1.4}$$

For the time-being we will focus solely on the quantity in square brackets (4.1.4) above. To this end fix an interval $(X_j,X_j+Y]$ and an odd integer $|r|<2X_j^{1/2}$. With the analytic expression

of the Hurwitz class number in (2.4.4), this term is

$$\frac{1}{\pi}\sum_{\substack{X_j<p\le X_j+Y\\ g(p)=d\\ p+1-r \text{ prime}}}\frac{1}{p}\sum_{\substack{f^2\mid\Delta_{p,r}\\ \frac{\Delta_{p,r}}{f^2}\equiv 0,1 \pmod 4}}\frac{\sqrt{\Delta_{p,r}}}{f}L(1,\chi_{p,r;f}),$$

where as we saw in Chapter 3, $\chi_{p,r;f}$ is the Kronecker symbol $(\Delta_{p,r}/f^2|\cdot)$. Note that as $p \le X$, the constraint $f^2 \mid \Delta_{p,r}$ is satisfied only if $f \le 2\sqrt{X}$. Furthermore since r is odd, $f^2 \mid \Delta_{p,r}$ is only possible for odd f. Hence, we must have $\Delta_{p,r}/f^2 \equiv 1 \pmod 4$. With these observations in mind, switching the order of summation gives the quantity above as

$$\frac{1}{\pi}\sum_{f\le 2\sqrt{X}}\frac{1}{f}\sum_{p\in\mathcal{S}_f(X_j,Y;r)}\frac{\sqrt{\Delta_{p,r}}}{p}L(1,\chi_{p,r;f}), \tag{4.1.5}$$

where we have defined the set

$$\mathcal{S}_f(X_j,Y;r)=\left\{X_j<p\le X_j+Y:\begin{array}{l} g(p)=d,\\ p+1-r \text{ prime},\\ f^2\mid\Delta_{p,r},\\ \frac{\Delta_{p,r}}{f^2}\equiv 1 \pmod 4\end{array}\right\}.$$

We now work to change the weighting function on the sum over primes in (4.1.5). Since we are attempting to identify not just when p is prime but also when $p+1-r$ is prime, we are aiming for a prime weight of $\log p \cdot \log(p+1-r)$. Since $|r| < 2X_j^{1/2} \ll Y$, Taylor approximations for $X_j < p \le X_j + Y$ give

$$\begin{aligned}\frac{1}{p} &= \frac{1}{X_j}+\mathrm{O}\left(\frac{Y}{X_j^2}\right),\\ \sqrt{4p-r^2} &= \sqrt{4X_j-r^2}+\mathrm{O}\left(\frac{Y}{\sqrt{4X_j-r^2}}\right),\\ \log(p+\mathrm{O}(r)) &= \log X_j+\mathrm{O}\left(\frac{Y}{X_j}\right).\end{aligned}$$

Therefore since $Y \leq X_j$ and $4X_j - r^2 \ll X_j$ we have

$$\begin{aligned}\frac{\sqrt{4p-r^2}}{p} &= \frac{\sqrt{4X_j-r^2}}{X_j} + \mathrm{O}\left(\frac{Y}{X_j\sqrt{4X_j-r^2}}\right),\\ \frac{\log p \log(p+1-r)}{\log^2 X_j} &= 1 + \mathrm{O}\left(\frac{Y}{X_j \log X_j}\right),\end{aligned}$$

and so subsequently

$$\frac{\sqrt{4p-r^2}}{p} = \frac{\sqrt{4X_j-r^2}}{X_j \log^2 X_j} \cdot \log p \log(p+1-r) + \mathrm{O}\left(\frac{Y}{X_j\sqrt{4X_j-r^2}}\right). \tag{4.1.6}$$

Inputting the new weighting function derived in (4.1.6) back into (4.1.5) and simplifying the resulting error term using Lemma 2.3.1 and the trivial bound $\#\mathcal{S}_f(X_j, Y; r) \ll Y$ gives

$$\frac{\sqrt{4X_j-r^2}}{\pi X_j \log^2 X_j} \sum_{f \leq 2\sqrt{X}} \frac{1}{f} \sum_{p \in \mathcal{S}_f(X_j,Y;r)} \log p \cdot \log(p+1-r) \cdot L(1, \chi_{p,r;f}) + \mathrm{O}\left(\frac{Y^2 \log^2 X}{X_j\sqrt{4X_j-r^2}}\right). \tag{4.1.7}$$

Recall that the quantity above is an alternative expression of the term surrounded by square brackets in (4.1.4). When we make the substitution, the contribution of the error term can be bounded above by

$$Y \log^2 X \sum_{j=1}^{J} \frac{Y}{X_j} \int_0^{2X_j^{1/2}} \frac{\mathrm{d}r}{\sqrt{4X_j-r^2}} \ \ll\ Y \log^2 X \sum_{j=1}^{J} \frac{1}{j} \ \ll\ \frac{X}{\log^6 X} \cdot \log J \ \ll\ \frac{X}{\log^5 X},$$

which is smaller than the pre-existing error term in (4.1.4). Therefore upon making the full substitution of (4.1.7) into (4.1.4) we obtain

$$\begin{aligned}\frac{1}{\#\mathcal{C}_Z} \sum_{E \in \mathcal{C}_Z} \pi_E^{\mathrm{twin}}(X) &= \frac{d}{2\pi} \sum_{j=1}^{J} \frac{1}{X_j \log^2 X_j} \sum_{\substack{|r|<2X_j^{1/2}\\ r \text{ odd}}} \sqrt{4X_j-r^2} \cdot \mathfrak{D}(X_j, Y; r)\\ &\quad + \mathrm{O}\left(\frac{X}{\log^3 X} + \frac{X^2 \log X}{Z}\right),\end{aligned} \tag{4.1.8}$$

where we have defined the new notation

$$\mathfrak{D}(X_j, Y; r) := \sum_{f \leq 2\sqrt{X}} \frac{1}{f} \sum_{p \in \mathcal{S}_f(X_j,Y;r)} \log p \cdot \log(p+1-r) \cdot L(1, \chi_{p,r;f}).$$

The expression in (4.1.8) lends itself to summation by parts on the integers $|r| < 2X_j^{1/2}$ with the function $f(r) = \sqrt{4X_j - r^2}$. Notice in particular that $\sqrt{4X_j - [|2X_j^{1/2}|]^2} \ll X_j^{1/4}$ and $\mathfrak{D}(X_j, Y; r) \ll Y \log^4 X$, so one term in the partial summation will be negligible. For a fixed $1 \leq j \leq J$, abelian summation yields

$$\sum_{\substack{|r|<2X_j^{1/2} \\ r \text{ odd}}} \sqrt{4X_j - r^2} \cdot \mathfrak{D}(X_j, Y; r) = \int_0^{2X_j^{1/2}} \frac{R \, \mathrm{d}R}{\sqrt{4X_j - R^2}} \sum_{\substack{|r|<R \\ r \text{ odd}}} \mathfrak{D}(X_j, Y; r) \quad + \quad \mathrm{O}\left(Y X_j^{3/4} \log^4 X\right).$$

Putting the expression above back into (4.1.8) gives

$$\begin{aligned} \frac{1}{\#\mathcal{C}_Z} \sum_{E \in \mathcal{C}_Z} \pi_E^{\text{twin}}(X) \quad &= \quad \frac{d}{2\pi} \sum_{j=1}^{J} \frac{1}{X_j \log^2 X_j} \int_0^{2X_j^{1/2}} \frac{R \, \mathrm{d}R}{\sqrt{4X_j - R^2}} \sum_{\substack{|r|<R \\ r \text{ odd}}} \mathfrak{D}(X_j, Y; r) \\ &\quad + \mathrm{O}\left(\frac{X}{\log^3 X} + \frac{X^2 \log X}{Z}\right), \end{aligned}$$

where the resulting error of $\mathrm{O}(X^{3/4} \log^3 X)$ from this substitution has been swallowed into the existing error term. Lastly we remark that contribution of the integral over $[0, 2X_j^{2/5}]$ is negligible. To see this we use the bound $\mathfrak{D}(X_j, Y; r) \ll Y \log^4 X$ and compute

$$\int_0^{2X_j^{2/5}} \frac{R \, \mathrm{d}R}{\sqrt{4X_j - R^2}} \cdot RY \log^4 X \ll X_j^{2/5} Y \log^4 X \int_{4X_j - X_j^{4/5}}^{4X_j} \frac{\mathrm{d}u}{\sqrt{u}} \ll X_j^{7/10} Y \log^4 X. \tag{4.1.9}$$

As a result, we have

$$\begin{aligned} \frac{1}{\#\mathcal{C}_Z} \sum_{E \in \mathcal{C}_Z} \pi_E^{\text{twin}}(X) \quad &= \quad \frac{d}{2\pi} \sum_{j=1}^{J} \frac{1}{X_j \log^2 X_j} \int_{2X_j^{2/5}}^{2X_j^{1/2}} \frac{R \, \mathrm{d}R}{\sqrt{4X_j - R^2}} \sum_{\substack{|r|<R \\ r \text{ odd}}} \mathfrak{D}(X_j, Y; r) \\ &\quad + \mathrm{O}\left(\frac{X}{\log^3 X} + \frac{X^2 \log X}{Z} + X^{7/10} \log^5 X\right). \end{aligned} \tag{4.1.10}$$

It is now clear that in order to move forward we need to understand the partial sums

$$\Lambda(X_j, Y; R) := \sum_{\substack{|r|<R \\ r \text{ odd}}} \mathfrak{D}(X_j, Y; r) = \sum_{\substack{|r|<R \\ r \text{ odd}}} \sum_{f \leq 2\sqrt{X}} \frac{1}{f} \sum_{p \in \mathcal{S}_f(X_j, Y; r)} \log p \cdot \log(p + 1 - r) \cdot L(1, \chi_{p,r;f}).$$

The remainder of the chapter is aimed at proving the following asymptotic, after which Theorem 1.3.1 follows immediately.

Theorem 4.1.1. *For a positive real number X, let x and y be such that $x + y \leq X$ with $y = X/\log^8 X$, and let R be a real number such that $2x^{2/5} \leq |R| < 2x^{1/2}$. Under these conditions we have*

$$\Lambda(x, y; R) = 2\mathfrak{C} \cdot \mathfrak{B}_K \cdot Ry + \mathrm{O}\left(\frac{Ry}{\log X}\right),$$

where $\mathfrak{C}$ and $\mathfrak{B}_K$ are defined in Theorem 1.3.1.

Before proving the theorem above, we explain how Theorem 1.3.1 follows from the theorem above. With this simpler expression of $\Lambda(X_j, Y; R)$ in hand, the main term of (4.1.10) can be written

$$\frac{d\mathfrak{B}_K\mathfrak{C}}{2\pi} \sum_{j=1}^{J} \frac{Y}{X_j \log^2 X_j} \int_{2X_j^{2/5}}^{2X_j^{1/2}} \frac{2R\,\mathrm{d}R}{\sqrt{4X_j - R^2}} \left[R + \mathrm{O}\left(R/\log X\right)\right].$$

From (4.1.9) we see that upon reintroducing the contribution of $0 \leq R \leq 2X_j^{2/5}$ we get

$$\int_{2X_j^{2/5}}^{2X_j^{1/2}} \frac{2R\,\mathrm{d}R}{\sqrt{4X_j - R^2}} \cdot R = \int_{0}^{2X_j^{1/2}} \frac{2R\,\mathrm{d}R}{\sqrt{4X_j - R^2}} \cdot R \quad + \quad \mathrm{O}(X_j^{7/10}),$$

whereupon applying standard integration techniques we obtain

$$\int_{0}^{2X_j^{1/2}} \frac{2R\,\mathrm{d}R}{\sqrt{4X_j - R^2}} \cdot [R + \mathrm{O}(R/\log X)] = 2\pi X_j \quad + \quad \mathrm{O}(X_j/\log X).$$

Therefore the main term of (4.1.10) is

$$d\mathfrak{B}_K\mathfrak{C} \sum_{j=1}^{J} \frac{Y}{\log^2 X_j} + \mathrm{O}\left(\frac{1}{\log X} \sum_{j=1}^{J} \frac{Y}{\log^2 X_j}\right).$$

All that remains is to use the definitions of Y and J and substitute the quantity above back into (4.1.10) which subsequently yields the desired result of

$$\frac{1}{\#\mathcal{C}_Z} \sum_{E \in \mathcal{C}_Z} \pi_E^{\mathrm{twin}}(X) = d\mathfrak{B}_K\mathfrak{C} \cdot \frac{X}{\log^2 X} + \mathrm{O}\left(\frac{X}{\log^3 X} + \frac{X^2 \log X}{Z}\right).$$

4.2 Outlining the Proof of Theorem 4.1.1

Consider truncating the outer sum of $\Lambda(x, y; R)$ over integers $f \leq 2\sqrt{X}$ at a parameter $F \leq 2\sqrt{X}$ to be determined later. Using (2.3.1) and the naive bound $\#\{x < m \leq x + y : f^2 \mid 4m - r^2\} \ll y/f^2$, the tail of this sum in $\Lambda(x, y; R)$ is asymptotically bounded above by

$$\log^3 X \sum_{|r|\leq R} \sum_{f\geq F} \frac{1}{f} \sum_{p\in\mathcal{S}_f(x,y;r)} 1 \ll \frac{Ry \log^3 X}{F^2}.$$

The special L-value occurring in $\Lambda(X_j, Y; R)$ can be treated using the Polya-Vinogradov inequality as we did in Lemma 2.3.1. Applying this result for an unspecified parameter N in conjunction with the truncation of the sum over integers $f < F$ allows us to write

$$\Lambda(x, y; R) = \sum_{\substack{|r|<R \\ r \text{ odd}}} \sum_{\substack{n<N \\ f<F}} \frac{1}{nf} \sum_{p\in\mathcal{S}_f(x,y;r)} \log p \cdot \log(p + 1 - r) \cdot \chi_{p,r;f}(n) + \mathrm{O}\left(Ry \log^3 X \left[\frac{1}{F^2} + \frac{X^{1/2}}{N}\right]\right),$$

where the error in truncating the special L-value contributes no more than

$$\log^2 X \sum_{|r|<R} \sum_{f<F} \frac{1}{f} \sum_{p\in\mathcal{S}_f(x,y;r)} \frac{p^{1/2} \log p}{N} \ll \frac{RyX^{1/2} \log^3 X}{N}.$$

Notice by taking $F \geq \log^2 X$ and $N \geq X^{1/2} \log^4 X$ the total error above becomes $\mathrm{O}(Ry/\log X)$; we will assume we choose our parameters to satisfy these bounds. Lastly, as in Chapter 3 we exploit the $4n$-periodicity of the character $\chi_{p,r;f}(n) = (\Delta_{p,r}/f^2|n)$. In this case, the conditions $\Delta_{p,r}/f^2 \equiv 1 \pmod 4$ and $a \equiv \Delta_{p,r}/f^2 \pmod{4n}$ are equivalent to $a \equiv 1 \pmod 4$ and $4p \equiv r^2 - af^2 \pmod{4nf^2}$. As a result we have

$$\Lambda(x, y; R) = \sum_{\substack{|r|<R \\ r \text{ odd} \\ n<N \\ f<F}} \frac{1}{nf} \sum_{\substack{a \pmod{4n} \\ a\equiv 1 \pmod 4 \\ (r^2-af^2, 4nf^2)=4 \\ ((r-2)^2-af^2, 4nf^2)=4}} \left(\frac{a}{n}\right) \sum_{\substack{x<p\leq x+y \\ g(p)=d \\ p+1-r \text{ prime} \\ 4p\equiv r^2-af^2 \pmod{4nf^2}}} \log p \cdot \log(p + 1 - r) + \mathrm{O}\left(\frac{Ry}{\log X}\right), \quad (4.2.1)$$

where the condition $(r^2 - af^2, 4nf^2) = 4$ is a necessary condition in order to have a non-negligible number of primes in the arithmetic progression $p \equiv (r^2 - af^2)/4 \pmod{nf^2}$, and where the condition $((r - 2)^2 - af^2, 4nf^2) = 4$ is a necessary condition in order to have $p \equiv (r^2 - af^2)/4 \pmod{nf^2}$ and $p + 1 - r$ prime.

By assumption, $K/\mathbb{Q}$ is abelian with square-free conductor Q, we can apply Lemma 2.5.1 to obtain a set $\mathcal{V}$ of residues modulo Q such that a rational prime p splits completely in K if and only if $p \equiv v \pmod{Q}$ for some $v \in \mathcal{V}$. In order for this to happen for a prime p, it must be that $(Q, v) = 1$ for all $v \in \mathcal{V}$. Furthermore, if both $p \equiv v \pmod{Q}$ and $p+1-r$ is prime, then it must be that $(v+1-r, Q) = 1$ as well. Also we remark that given r is necessarily odd and $a \equiv 1 \pmod{4}$, the condition $4 \mid r^2 - af^2$ holds only if f is odd. With these observations in place, we can write $\Lambda(x, y; R)$ as

$$\Lambda(x,y;R) = \sum_{\substack{v\in\mathcal{V}\\ |r|<R\\ r \text{ odd; } r\neq 1\\ n<N\\ f<F;\ f \text{ odd}\\ (v+1-r,Q)=1}} \frac{1}{nf} \sum_{\substack{a \pmod{4n}\\ a\equiv 1 \pmod 4\\ (r^2-af^2,4nf^2)=4\\ ((r-2)^2-af^2,4nf^2)=4}} \left(\frac{a}{n}\right) \sum_{\substack{x<p\leq x+y\\ p\equiv v \pmod Q\\ p+1-r \text{ prime}\\ 4p\equiv r^2-af^2 \pmod{4nf^2}}} \log p \cdot \log(p+1-r) + \mathrm{O}\left(\frac{Ry}{\log X}\right),$$

where we have omitted the contribution from $r = 1$ of $\mathrm{O}(y \log^3 X)$ since it is swamped by the existing error term.

By the Chinese Remainder Theorem, the two congruence conditions on the primes in the inner-most sum simultaneously hold if and only if $4v \equiv r^2 - af^2 \pmod{4(v, nf^2)}$, in which case p falls into the unique residue class b modulo $[Q, nf^2]$ such that both $b \equiv v \pmod{Q}$ and $4b \equiv r^2 - af^2 \pmod{4nf^2}$. In this way, we have

$$\Lambda(x,y;R) = \sum_{\substack{v\in\mathcal{V}\\ |r|<R\\ r \text{ odd; } r\neq 1\\ n<N\\ f<F;\ f \text{ odd}\\ (v+1-r,Q)=1}} \frac{1}{nf} \sum_{\substack{a \pmod{4n}\\ a\equiv 1 \pmod 4\\ 4v\equiv r^2-af^2 \pmod{4(Q,nf^2)}\\ (r^2-af^2,4nf^2)=4\\ ((r-2)^2-af^2,4nf^2)=4}} \left(\frac{a}{n}\right) \sum_{\substack{x<p\leq x+y\\ p+1-r \text{ prime}\\ p\equiv b \pmod{[Q,nf^2]}\\ (r^2-af^2,4nf^2)=4\\ ((r-2)^2-af^2,4nf^2)=4}} \log p \cdot \log(p-(r-1)) + \mathrm{O}\left(\frac{Ry}{\log X}\right). \tag{4.2.2}$$

The sum on primes in (4.2.2) concerns how primes spaced precisely $r-1$ apart are distributed in arithmetic progressions. Recalling the discussion and notation in and after Conjecture 2.2.3 regarding the functions $\mathfrak{S}(w, q, a)$, C_2, and $E_r(x, h; q, a)$, we will replace the sum on primes in (4.2.2) with an approximation and control the resulting error term. First note that since the quantity

$\mathfrak{S}(w,q,a)$ is q-periodic as a function of a, we see that

$$\mathfrak{S}(r-1,[Q,nf^2],b)=\begin{cases}\dfrac{2C_2}{\phi([Q,nf^2])}\displaystyle\prod_{\substack{\ell\neq 2\\ \ell\mid(r-1)[Q,nf^2]}}\dfrac{\ell-1}{\ell-2} & \text{if } r \text{ is odd,}\\ & \text{and } (r^2-af^2,4nf^2)=4,\\ & \text{and } ((r-2)^2-af^2,4nf^2)=4,\\ 0 & \text{otherwise.}\end{cases}$$

Therefore upon making the approximation discussed in Conjecture 2.2.3, the main term in (4.2.2) is

$$\begin{aligned}\Lambda(x,y;R) &= 2C_2y\sum_{\substack{v\in\mathcal{V}\\ |r|<R\\ r\text{ odd; }r\neq 1\\ n<N\\ f<F;\ f\text{ odd}\\ (v+1-r,Q)=1}}\frac{1}{nf\phi([Q,nf^2])}\left(\prod_{\substack{\ell\neq 2\\ \ell\mid(r-1)[Q,nf^2]}}\frac{\ell-1}{\ell-2}\right)\sum_{\substack{a\pmod{4n}\\ a\equiv 1\pmod 4\\ 4v\equiv r^2-af^2\pmod{4(Q,nf^2)}\\ (r^2-af^2,4nf^2)=4\\ ((r-2)^2-af^2,4nf^2)=4}}\left(\frac{a}{n}\right)\\ &\quad+\sum_{\substack{v\in\mathcal{V}\\ |r|<R\\ r\text{ odd; }r\neq 1\\ n<N\\ f<F;\ f\text{ odd}\\ (v+1-r,Q)=1}}\frac{1}{nf}\sum_{\substack{a\pmod{4n}\\ a\equiv 1\pmod 4\\ 4v\equiv r^2-af^2\pmod{4(Q,nf^2)}}}\left(\frac{a}{n}\right)E_{r-1}(x,y;[Q,nf^2],b)\\ &\quad+\mathrm{O}\left(\frac{Ry}{\log X}\right).\end{aligned}\tag{4.2.3}$$

The entire proof of this result rests on the fact that we can control the second term occurring in (4.2.3). As we will see we can indeed control it using Theorem 2.2.5. Taking absolute values, weakening constraints, and applying Cauchy-Schwarz to this quantity gives an upper of

$$\left(\sum_{\substack{|r|<R\\ v\in\mathcal{V}\\ n<N\\ f<F\\ a\pmod{4n}}}\frac{1}{n^2f^2}\right)^{1/2}\left(\sum_{\substack{|r|<R;\ r\neq 1\\ v\in\mathcal{V}\\ n<N\\ f<F\\ a\pmod{4n}}}E_{r-1}^2(x,y;[Q,nf^2],b)\right)^{1/2}\tag{4.2.4}$$

Since $\#\mathcal{V}\ll Q\ll 1$, the first factor in (4.2.4) is simply $\mathrm{O}(R^{1/2}\log^{1/2}N)$.

To understand the second factor in (4.2.4), recall that b is the unique residue modulo $[Q,nf^2]$ that satisfies both $b\equiv v\pmod Q$ and $4b\equiv r^2-af^2\pmod{4nf^2}$. As a cycles through the residue classes modulo $4n$, we see $b\equiv(r^2-af^2)/4\pmod{nf^2}$ at most once. Therefore since all summands are positive we can in fact sum over all residues classes c modulo $[Q,nf^2]$ and then make the change

of variables $w = r - 1$ to bound this term asymptotically above by

$$\sum_{\substack{0<|w|<R-1\\ n<N\\ f<F\\ c \pmod{[Q,nf^2]}}} E_w^2(x,y;[Q,nf^2],c) \quad \ll \quad \sum_{f<F} \sum_{\substack{0<|w|<R-1\\ q<[Q,Nf^2]\\ c \pmod{q}}} E_w^2(x,y;q,c)$$

Considering only the inner sum above, we now invoke Theorem 2.2.5 which gives that for any $A > 0$ this inner sum is asymptotically bounded above by $RX^2/\log^A X$ provided we choose N and F to satisfy $X/\log^A X \leq Nf^2 \leq X$ for any $f < F$. In particular, taking $F := \log^2 X$ and $N = X/\log^{41} X$ satisfies the prior constraints on N and F and satisfies the hypotheses in Theorem 2.2.5. As a result the entire second term of (4.2.3) is asymptotically bounded above by

$$R^{1/2}\log^{1/2} N \cdot \frac{R^{1/2}XF}{\log^{39/2} X} \ll \frac{RX}{\log^{17} X} \ll \frac{Ry}{\log X}.$$

Upon returning to (4.2.3) we have shown

$$\Lambda(x,y;R) = 2C_2 y \sum_{\substack{v\in\mathcal{V}\\ |r|<R\\ r \text{ odd; } r\neq 1\\ n<N\\ f<F;\ f \text{ odd}\\ (v+1-r,Q)=1}} \frac{c_{f,v}^r(n)}{nf\phi([Q,nf^2])} \left(\prod_{\substack{\ell\neq 2\\ \ell \mid (r-1)[Q,nf^2]}} \frac{\ell-1}{\ell-2} \right) + \mathrm{O}\left(\frac{Ry}{\log X}\right), \tag{4.2.5}$$

where we have defined the notation

$$c_{f,v}^r(n) := \sum_{\substack{a \pmod{4n}\\ a\equiv 1 \pmod 4\\ 4v\equiv r^2-af^2 \pmod{4(Q,nf^2)}\\ (r^2-af^2,4nf^2)=4\\ ((r-2)^2-af^2,4nf^2)=4}} \left(\frac{a}{n}\right).$$

The character sum $c_{f,v}^r(n)$ is very familiar not only to the work in [BCD11] but also in similar problems in Frobenius distributions such as in [DP99] and [Jam05]. The key idea is that this sum is multiplicative in the variable n, which means we need only evaluate it on prime powers. The techniques which establish the following lemma are standard; we spend all of Section 4.3 proving it.

Lemma 4.2.1. *Let r and f be odd positive integers, and let v be coprime to an integer Q with $(v+1-r,Q) = 1$. We have that $c_{f,v}^r(n) = 0$ if either $(r,f) \neq 1$, $(r-2,f) \neq 1$, or $(Q,f^2) \nmid \Delta_{v,r}$. If*

we assume $(r,f)=(r-2,f)=1$, *and* $(Q,f^2)\mid\Delta_{v,r}$, *then all of the following are true:*

1. *For odd* n, *we have*
$$c_{f,v}^r(n)=\sum_{\substack{a\ (mod\ n)\\(r^2-af^2,n)=1\\((r-2)^2-af^2,n)=1\\ \frac{\Delta_{v,r}}{(Q,f^2)}\equiv\frac{af^2}{(Q,f^2)}\ \left(mod\ \left(\frac{Q}{(Q,f^2)},n\right)\right)}}\left(\frac{a}{n}\right).$$

2. *The function* $c_{f,v}^r(n)$ *is multiplicative in* n.

3. *Let* e *be a positive integer. Then* $c_{f,v}^r(2^e)=(-1)^e\cdot 2^{e-1}$.

4. *Let* e *be a positive integer, and let* q *be an odd prime dividing* f. *Then we have*
$$c_{f,v}^r(q^e)=\begin{cases}\phi(q^e) & \text{if } e \text{ is even,}\\ 0 & \text{if } e \text{ is odd.}\end{cases}$$

5. *Let* e *be a positive integer, and let* q *be an odd prime that does not divide* f. *Then we have*
$$c_{f,v}^r(q^e)=\begin{cases}\left(\frac{\Delta_{v,r}}{q}\right)^e q^{e-1} & \text{if } q\mid Q,\\ q^{e-1}(q-2) & \text{if } q\nmid Q,\ e \text{ even, and } q\mid r(r-1)(r-2),\\ q^{e-1}(q-3) & \text{if } q\nmid Q,\ e \text{ even, and } q\nmid r(r-1)(r-2),\\ -q^{e-1} & \text{if } q\nmid Q,\ e \text{ odd, and } q\mid r(r-1)(r-2),\\ -2q^{e-1} & \text{if } q\nmid Q,\ e \text{ odd, and } q\nmid r(r-1)(r-2).\end{cases}$$

In Lemma 4.2.1 we gained some non-vanishing conditions of $c_{f,v}^r(n)$, and so for completeness we include them in rewriting the main term of (4.2.5) as

$$2C_2y\sum_{\substack{|r|<R\\ r\text{ odd; }r\neq 1\\ v\in\mathcal{V}\\ (v+1-r,Q)=1}}\ \sum_{\substack{n<N\\ f<F\\ f\text{ odd}\\ (f,r)=(f,r-2)=1\\ (Q,f^2)\mid\Delta_{v,r}}}\frac{c_{f,v}^r(n)}{\phi([Q,nf^2])nf}\left(\prod_{\substack{\ell\neq 2\\ \ell\mid(r-1)[Q,nf^2]}}\frac{\ell-1}{\ell-2}\right). \tag{4.2.6}$$

Since $c_{f,v}^r(n)$ is multiplicative in n, we work towards exploiting this characteristic. In particular, we no longer need to keep the sums over integers $n\leq N$ and $f\leq F$ truncated. Using a technique

identical to [DP99, Lemma 3.4] we can extend the sums above to sums over all integers $n \geq 1$ and $f \geq 1$ and incur a small error. In particular the quantity in (4.2.6) is

$$2C_2 y \sum_{\substack{|r|<R \\ r \text{ odd; } r\neq 1 \\ v\in\mathcal{V} \\ (v+1-r,Q)=1}} \sum_{\substack{n\geq 1 \\ f\geq 1 \\ f \text{ odd} \\ (f,r)=(f,r-2)=1 \\ (Q,f^2)\mid \Delta_{v,r}}} \frac{c_{f,v}^r(n)}{\phi([Q,nf^2])nf} \left(\prod_{\substack{\ell\neq 2 \\ \ell\mid (r-1)[Q,nf^2]}} \frac{\ell-1}{\ell-2} \right) + \mathrm{O}\left(\frac{Ry}{F^2} + \frac{Ry}{\sqrt{N}} \right). \tag{4.2.7}$$

Recalling that we have set $F = \log^2 X$ and $N = X/\log^{41} X$, the contribution of the error term above is certainly $\mathrm{O}(Ry/\log X)$. For simplicity going forward set

$$D_v^r := \sum_{\substack{n\geq 1 \\ f\geq 1 \\ f \text{ odd} \\ (f,r)=(f,r-2)=1 \\ (Q,f^2)\mid \Delta_{v,r}}} \frac{c_{f,v}^r(n)}{\phi([Q,nf^2])nf} \left(\prod_{\substack{\ell\neq 2 \\ \ell\mid (r-1)[Q,nf^2]}} \frac{\ell-1}{\ell-2} \right),$$

so that we have

$$\Lambda(x,y;R) = 2C_2 y \sum_{\substack{|r|<R \\ r \text{ odd; } r\neq 1 \\ v\in\mathcal{V} \\ (v+1-r,Q)=1}} D_v^r \quad + \quad \mathrm{O}\left(\frac{Ry}{\log X} \right). \tag{4.2.8}$$

As we see from the following lemma, the quantity D_v^r is filled with multiplicative structure. The proof of the next result is relegated to Section 4.4.

Lemma 4.2.2. *Let r be an odd integer, and fix $v \in \mathcal{V}$ coprime to Q with $(v+1-r, Q) = 1$. Then we have*

$$D_v^r = \frac{2}{3\phi(Q)} \prod_{\substack{\ell\neq 2 \\ \ell\mid Q}} \frac{\ell-1}{\ell-2} \prod_{\ell\nmid 2Q} \frac{\ell(\ell^2-2\ell-2)}{(\ell-2)(\ell^2-1)} \prod_{\ell\neq 2} \left(1 + e_v^r(\ell)\right),$$

where

$$e_v^r(\ell) = \begin{cases} \dfrac{\ell+1}{\ell^2-2\ell-2} & \text{if } \ell\nmid Q \text{ and } \ell \mid r-1, \\ \dfrac{1}{\ell^2-2\ell-2} & \text{if } \ell\nmid Q \text{ and } \ell \mid r(r-2), \\ \dfrac{\ell\left(\frac{\Delta_{v,r}}{\ell}\right)+1}{\ell^2-1} & \text{if } \ell \mid Q, \\ 0 & \text{otherwise.} \end{cases}$$

Upon applying the result of Lemma 4.2.2 into the quantity in (4.2.8) we obtain

$$\Lambda(x,y;R) = \frac{4C_2 y}{3\phi(Q)} \prod_{\substack{\ell\neq 2\\ \ell\mid Q}} \frac{\ell-1}{\ell-2} \prod_{\ell\nmid 2Q} \frac{\ell(\ell^2-2\ell-2)}{(\ell-2)(\ell^2-1)} \sum_{\substack{|r|<R\\ r \text{ odd; } r\neq 1\\ v\in\mathcal{V}\\ (v+1-r,Q)=1}} \prod_{\ell\neq 2} (1+e_v^r(\ell)) + \mathrm{O}\left(\frac{Ry}{\log X}\right). \tag{4.2.9}$$

All that remains is to sum the Euler products appearing in (4.2.9). In Section 4.5 we prove the final technical lemma of this chapter.

Lemma 4.2.3. *Let v be coprime to Q. We have*

$$\sum_{\substack{|r|<R\\ r \text{ odd; } r\neq 1\\ (v+1-r,Q)=1}} \prod_{\ell\neq 2} (1+e_v^r(\ell)) = R \prod_{\ell\nmid 2Q} \frac{\ell^3-2\ell^2-\ell+3}{\ell(\ell^2-2\ell-2)} \prod_{\substack{\ell\neq 2\\ \ell\mid Q}} k_v(\ell) + \mathrm{O}\left(\log^2 R\right),$$

where

$$k_v(\ell) := \frac{\ell^2-\ell-\left[1+\left(\frac{(v-1)^2}{\ell}\right)\right]}{\ell^2-1}.$$

So using the definition $C_2 = \prod_{\ell\neq 2} \frac{\ell(\ell-2)}{(\ell-1)^2}$, we may apply the previous lemma to the expression of $\Lambda(x,y;R)$ given in (4.2.9). Upon doing so we obtain

$$\Lambda(x,y;R) \;=\; \frac{4Ry}{3} \prod_{\ell\neq 2} \frac{\ell(\ell^3-2\ell^2-\ell+3)}{(\ell+1)(\ell-1)^3} \sum_{v\in\mathcal{V}} \prod_{\substack{\ell\neq 2\\ \ell\mid Q}} \frac{\left(\ell^2-\ell-\left[1+\left(\frac{(v-1)^2}{\ell}\right)\right]\right)}{\ell^3-2\ell^2-\ell+3} + \mathrm{O}\left(\frac{Ry}{\log X}\right).$$

This completes the proof of Theorem 4.1.1 conditional on the lemmas proven in Sections 4.3, 4.4, and 4.5.

4.3 Evaluating a Character Sum

In this section we consider properties of the character sum

$$c_{f,v}^r(n) := \sum_{\substack{a \pmod{4n}\\ a\equiv 1 \pmod 4\\ 4v\equiv r^2-af^2 \pmod{4(Q,nf^2)}\\ (r^2-af^2,4nf^2)=4\\ ((r-2)^2-af^2,4nf^2)=4}} \left(\frac{a}{n}\right), \tag{4.3.1}$$

and we prove Lemma 4.2.1. Throughout this section we fix r and f as odd positive integers, and $v \in \mathcal{V}$ coprime to Q satisfying $(Q, v+1-r) = 1$.

We begin by establishing some necessary conditions for the non-vanishing of this character sum. Since r and f are both odd, the condition that $(r^2 - af^2, 4nf^2) = 4$ holds only if $(r, f) = 1$. That is, if $(r, f) \neq 1$, then the sum necessarily vanishes. So assuming $(r, f) = 1$, multiplicativity establishes the equivalence

$$(r^2 - af^2, 4nf^2) = 4 \Longleftrightarrow (r^2 - af^2, 4n) = 4.$$

A similar analysis on the condition $((r-2)^2 - af^2), 4nf^2) = 4$ leads to the necessity for non-vanishing that $(r-2, f) = 1$ and the equivalence of conditions

$$((r-2)^2 - af^2, 4nf^2) = 4 \Longleftrightarrow ((r-2)^2 - af^2, 4n) = 4.$$

Lastly, we remark that the congruence condition in $c^r_{f,v}(n)$ holds only if $(Q, f^2) \mid \Delta_{v,r}$. Assuming this divisibility requirement, the final equivalence relation in the character sum holds if and only if

$$\frac{\Delta_{v,r}}{(Q,f^2)} \equiv \frac{af^2}{(Q,f^2)} \pmod{4\left(\frac{Q}{(Q,f^2)}, n\right)}.$$

Therefore

$$c^r_{f,v}(n) = \begin{cases} \displaystyle\sum_{\substack{a \pmod{4n}^\times \\ a \equiv 1 \pmod 4 \\ (r^2-af^2, 4n)=4 \\ ((r-2)^2-af^2, 4n)=4 \\ \frac{\Delta_{v,r}}{(Q,f^2)} \equiv \frac{af^2}{(Q,f^2)} \left(\mathrm{mod}\ 4\left(\frac{Q}{(Q,f^2)}, n\right)\right)}} \left(\frac{a}{n}\right) & \text{if } (r,f) = (r-2,f) = 1 \text{ and } (Q,f^2) \mid \Delta_{v,r} \\ 0 & \text{otherwise.} \end{cases} \tag{4.3.2}$$

We are now ready to prove Lemma 4.2.1. In what follows, we assume that r, f, Q, v satisfy the non-vanishing conditions above.

Proof.

(1) Let n be an odd integer. Since the greatest common divisor is multiplicative, we have

an equivalence of conditions

$$(r^2 - af^2, 4n) = 4 \iff (r^2 - af^2, n) = 1,$$

because $r^2 - af^2$ is necessarily divisible by 4 as r and f are both odd and $a \equiv 1 \pmod 4$. A similar argument gives an equivalence of conditions

$$((r-2)^2 - af^2, 4n) = 4 \iff ((r-2)^2 - af^2, n) = 1.$$

Regarding the congruence condition coming from (4.3.2), since n is odd the Chinese Remainder Theorem allows us to write this congruence condition as equivalent to the simultaneous conditions

$$\begin{aligned} \frac{\Delta_{v,r}}{(Q,f^2)} &\equiv \frac{af^2}{(Q,f^2)} \pmod 4 \\ \frac{\Delta_{v,r}}{(Q,f^2)} &\equiv \frac{af^2}{(Q,f^2)} \left(\mathrm{mod}\ \left(\frac{Q}{(Q,f^2)}, n\right)\right) \end{aligned}$$

The first of these holds automatically because $r^2 - af^2$ is necessarily divisible by 4 for the reasons discussed earlier. Therefore, so far we have

$$c_{f,v}^r(n) = \sum_{\substack{a \pmod{4n} \\ a \equiv 1 \pmod 4 \\ (r^2 - af^2, f) = 1 \\ ((r-2)^2 - af^2, n) = 1 \\ \frac{\Delta_{v,r}}{(Q,f^2)} \equiv \frac{af^2}{(Q,f^2)} \left(\mathrm{mod}\ \frac{Q}{(Q,f^2)}, n\right)}} \left(\frac{a}{n}\right)$$

Finally we remark that there is a bijection using the Chinese Remainder Theorem between residues modulo $4n$ that are congruent to $1 \pmod 4$ and residues modulo n. Since the Kronecker character $(\cdot|n)$ is n-periodic for odd n, we immediately obtain the result that for odd n we have

$$c_{f,v}^r(n) = \sum_{\substack{a \pmod{n} \\ (r^2 - af^2, n) = 1 \\ ((r-2)^2 - af^2, n) = 1 \\ \frac{\Delta_{v,r}}{(Q,f^2)} \equiv \frac{af^2}{(Q,f^2)} \left(\mathrm{mod}\ \left(\frac{Q}{(Q,f^2)}, n\right)\right)}} \left(\frac{a}{n}\right). \tag{4.3.3}$$

(2) The fact that $c_{f,v}^r(1) = 1$ is verified by inspection of (4.3.3). Let m_1, m_2 be coprime

integers, and without losing generality, assume m_1 is odd. Using (4.3.2) and (4.3.3), we have

$$c_{f,v}^r(m_1)\cdot c_{f,v}^r(m_2)=\sum_{\substack{a \pmod{m_1}\\(r^2-af^2,m_1)=1\\((r-2)^2-af^2,m_1)=1\\\frac{\Delta_{v,r}}{(Q,f^2)}\equiv\frac{af^2}{(Q,f^2)}\left(\mathrm{mod}\ 4\left(\frac{Q}{(Q,f^2)},m_1\right)\right)}}\left(\frac{a}{m_1}\right)\cdot\sum_{\substack{a \pmod{4m_2}\\a\equiv 1 \pmod 4\\(r^2-af^2,4m_2)=4\\((r-2)^2-af^2,4m_2)=4\\\frac{\Delta_{v,r}}{(Q,f^2)}\equiv\frac{af^2}{(Q,f^2)}\left(\mathrm{mod}\left(\frac{Q}{(Q,f^2)},m_2\right)\right)}}\left(\frac{a}{m_2}\right).$$

Piecing together these two sums using the Chinese Remainder Theorem and then finally invoking the multiplicativity of the Kronecker symbol, we have

$$c_{f,v}^r(m_1)\cdot c_{f,v}^r(m_2)=\sum_{\substack{a \pmod{4m_1m_2}\\a\equiv 1 \pmod 4\\(r^2-af^2,4m_1m_2)=4\\((r-2)^2-af^2,4m_1m_2)=4\\\frac{\Delta_{v,r}}{(Q,f^2)}\equiv\frac{af^2}{(Q,f^2)}\left(\mathrm{mod}\left(\frac{Q}{(Q,k^2)},m_1m_2\right)\right)}}\left(\frac{a}{m_1}\right)\left(\frac{a}{m_2}\right)=c_{f,v}^r(m_1m_2).$$

(3) Let e be a positive integer, and consider the expression for $c_{f,v}^r(2^e)$ given in (4.3.2):

$$c_{f,v}^r(2^e)=\sum_{\substack{a \left(\mathrm{mod}\ 2^{e+2}\right)\\a\equiv 1 \pmod 4\\(r^2-af^2,2^{e+2})=4\\((r-2)^2-af^2,2^{e+2})=4\\\frac{\Delta_{v,r}}{(Q,f^2)}\equiv\frac{af^2}{(Q,f^2)}\left(\mathrm{mod}\left(\frac{Q}{(Q,f^2)},2^e\right)\right)}}\left(\frac{a}{2^e}\right)$$

Fix $a \left(\mathrm{mod}\ 2^{e+2}\right)$ satisfying $a\equiv 1 \pmod 4$. As we have seen, r^2-af^2 is necessarily divisible by 4. So the condition $(r^2-af^2,2^{e+2})=4$ holds if and only if $r^2-af^2\equiv 4 \pmod 8$. Write $r=2c+1$ and $f=2d+1$ for appropriate integers c and d. Working modulo 8, we have

$$r^2-af^2\equiv 4c(c+1)+1-4ad(d+1)-a\equiv 1-a.$$

So for $r^2-af^2\equiv 4 \pmod 8$ and $a\equiv 1 \pmod 4$, it is necessary and sufficient that $a\equiv 5 \pmod 8$. A similar argument as the one presented above applied to the condition $((r-2)^2-af^2,2^{e+2})=4$ also ends in the necessary and sufficient condition that $a\equiv 5 \pmod 8$. We note that for $a\equiv 5 \pmod 8$ we have $(a|2^e)=(a|2)^e=(-1)^e$ for all $e\geq 1$.

Lastly we investigate the congruence condition in the expression of $c_{f,v}^r(2^e)$. If Q is odd this congruence condition is modulo 1 and therefore holds automatically. On the other hand, if Q is even

then the congruence condition is modulo 2. Since r is odd, the left-hand side of $\Delta_{v,r} = r^2 - 4v$ is odd. If we assume $a \equiv 5 \pmod 8$ then the right-hand side of af^2 is also odd. Therefore assuming $a \equiv 5 \pmod 8$ implies the congruence condition holds automatically. So regardless of the parity of Q we have

$$c_{f,v}^r(2^e) = (-1)^e \sum_{\substack{a \pmod{2^{e+2}}^\times \\ a \equiv 5 \pmod 8}} 1 = (-1)^e \cdot 2^{e-1}.$$

(4) Let e be a positive integer, and let q be an odd prime dividing f. We use the expression from (4.3.3), that is

$$c_{f,v}^r(q^e) = \sum_{\substack{a \pmod{q^e} \\ (r^2 - af^2, q) = 1 \\ ((r-2)^2 - af^2, q) = 1 \\ \frac{\Delta_{v,r}}{(Q,f^2)} \equiv \frac{af^2}{(Q,f^2)} \left(\mathrm{mod}\ \left(\frac{Q}{(Q,f^2)}, q^e\right)\right)}} \left(\frac{a}{q^e}\right).$$

Since by assumption $(r, f) = (r-2, f) = 1$, we also have $(r, q) = (r-2, q) = 1$. Therefore since $q \mid f$ the conditions $(r^2 - af^2, q) = 1$ and $((r-2)^2 - af^2, q) = 1$ hold for all invertible $a \pmod{q^e}$.

Regardless of whether or not q divides Q, the modulus of the congruence condition in $c_{f,v}^r(q^e)$ is necessarily 1, and so the condition holds trivially by our assumptions. Therefore the orthogonality relations from Lemma 2.1.6 give us

$$c_{f,v}^r(q^e) = \sum_{a \pmod{q^e}} \left(\frac{a}{q}\right)^e = \begin{cases} \phi(q^e) & \text{if } e \text{ is even,} \\ 0 & \text{if } e \text{ is odd.} \end{cases}$$

(5) Let q be an odd prime, and let e be a positive integer. We assume $(q, f) = 1$, and use the expression from (4.3.3):

$$c_{f,v}^r(q^e) = \sum_{\substack{a \pmod{q^e} \\ (r^2 - af^2, q) = 1 \\ ((r-2)^2 - af^2, q) = 1 \\ \frac{\Delta_{v,r}}{(Q,f^2)} \equiv \frac{af^2}{(Q,f^2)} \left(\mathrm{mod}\ \left(\frac{Q}{(Q,f^2)}, q^e\right)\right)}} \left(\frac{a}{q^e}\right).$$

Note that the modulus of the congruence condition is q when $q \mid Q$ and 1 otherwise. Letting q^*

denote this function we have

$$c_{f,v}^{r}(q^e) = \sum_{\substack{a \pmod{q^e} \\ (r^2-af^2,q)=1 \\ ((r-2)^2-af^2,q)=1 \\ a\equiv\frac{\Delta_{v,r}}{f^2} \pmod{q^*}}} \left(\frac{a}{q^e}\right) = \sum_{\substack{a \pmod{q^e} \\ a\equiv\frac{\Delta_{v,r}}{f^2} \pmod{q^*}}} \left(\frac{a}{q}\right)^e - \sum_{\substack{a \pmod{q^e} \\ q\mid r^2-af^2 \text{ or } q\mid(r-2)^2-af^2 \\ a\equiv\frac{\Delta_{v,r}}{f^2} \pmod{q^*}}} \left(\frac{a}{q}\right)^e, \tag{4.3.4}$$

where we have used the fact that $(q, f) = 1$ implies that (Q, f^2) is invertible modulo q^*. The first sum on the right-hand side of (4.3.4) is

$$\sum_{\substack{a \pmod{q^e} \\ a\equiv\frac{\Delta_{v,r}}{f^2} \pmod{q^*}}} \left(\frac{a}{q}\right)^e = \begin{cases} \left(\frac{\Delta_{v,r}}{q}\right)^e \cdot q^{e-1} & \text{if } q \mid Q, \\ q^{e-1} & \text{if } q \nmid Q \text{ and } e \text{ is even}, \\ 0 & \text{if } q \nmid Q \text{ and } e \text{ is odd}, \end{cases} \tag{4.3.5}$$

where we have invoked the multiplicativity of the Kronecker symbol in the case that $q \mid Q$ and character orthogonality in the case that $q \nmid Q$.

The second sum in (4.3.4) will be evaluated using the principle of inclusion-exclusion. First we note that if $q \mid r^2 - af^2$ or $q \mid (r-2)^2 - af^2$ then a is a non-zero square modulo q. So the character value appearing in this sum is always $+1$. Therefore, the second sum in (4.3.4) can be written as

$$X + Y - Z := \sum_{\substack{a \pmod{q^e} \\ a\equiv r^2/f^2 \pmod{q} \\ a\equiv\Delta_{v,r}/f^2 \pmod{q^*}}} 1 + \sum_{\substack{a \pmod{q^e} \\ a\equiv(r-2)^2/f^2 \pmod{q} \\ a\equiv\Delta_{v,r}/f^2 \pmod{q^*}}} 1 - \sum_{\substack{a \pmod{q^e} \\ a\equiv r^2/f^2 \pmod{q} \\ a\equiv(r-2)^2/f^2 \pmod{q} \\ a\equiv\Delta_{v,r}/f^2 \pmod{q^*}}} 1. \tag{4.3.6}$$

First consider the X term of (4.3.6). If $q \mid Q$ then the two congruence conditions are compatible if and only if $r^2 \equiv \Delta_{v,r} \equiv r^2 - 4v \pmod{q}$. However q is odd and $(v, q) \leq (v, Q) = 1$ by assumption. Therefore when $q \mid Q$ these conditions are not compatible. When $q \nmid Q$ the final congruence condition has modulus 1, so it holds trivially. Therefore we have

$$X = \sum_{\substack{a \pmod{q^e} \\ a\equiv r^2/f^2 \pmod{q} \\ a\equiv\Delta_{v,r}/f^2 \pmod{q^*}}} 1 = \begin{cases} q^{e-1} & \text{if } q \nmid Qr, \\ 0 & \text{otherwise.} \end{cases} \tag{4.3.7}$$

An almost identical argument shows that

$$Y = \sum_{\substack{a \pmod{q^e} \\ a \equiv (r-2)^2/f^2 \pmod{q} \\ a \equiv \Delta_{v,r}/f^2 \pmod{q^*}}} 1 = \begin{cases} q^{e-1} & \text{if } q \nmid Q(r-2), \\ 0 & \text{otherwise.} \end{cases} \tag{4.3.8}$$

Finally we consider the Z term from (4.3.6). For the first two congruence conditions to be compatible, we require $r \equiv 1 \pmod{q}$. For the first and third conditions to be compatible the same argument as in the evaluation of the X term gives that $q \nmid Q$. So we compute

$$Z = \sum_{\substack{a \pmod{q^e} \\ a \equiv r^2/f^2 \pmod{q} \\ a \equiv (r-2)^2/f^2 \pmod{q} \\ a \equiv \Delta_{v,r}/f^2 \pmod{q^*}}} 1 = \begin{cases} q^{e-1} & \text{if } q \nmid Q \text{ and } q \mid r-1, \\ 0 & \text{otherwise.} \end{cases} \tag{4.3.9}$$

Taking (4.3.7), (4.3.8), and (4.3.9) and putting the results back into (4.3.6) gives

$$X + Y - Z = \begin{cases} q^{e-1} & \text{if } q \nmid Q \text{ and } q \mid r(r-1)(r-2), \\ 2q^{e-1} & \text{if } q \nmid Qr(r-1)(r-2), \\ 0 & \text{if } q \mid Q. \end{cases} \tag{4.3.10}$$

Putting (4.3.10) and (4.3.5) back into (4.3.4) completes the proof.

□

4.4 Exploiting the Multiplicative Structure of D_v^r

For a fixed odd integer r and a fixed $v \in \mathcal{V}$ satisfying $(Q, v+1-r) = 1$, the object of interest in this section is

$$D_v^r := \sum_{\substack{n \geq 1 \\ f \geq 1 \\ f \text{ odd} \\ (f,r)=(f,r-2)=1 \\ (Q,f^2) \mid \Delta_{v,r}}} \frac{c_{f,v}^r(n)}{\phi([Q, nf^2])nf} \left(\prod_{\substack{\ell \mid (r-1)[Q,nf^2] \\ \ell \neq 2}} \frac{\ell - 1}{\ell - 2} \right).$$

We begin by noticing that a prime $\ell \mid (r-1)[Q, nf^2]$ if and only if $\ell \mid (r-1)Qnf^2$. We can group such primes into divisors of $(r-1)Qf$ and divisors of n and then remove the double-counted primes that divide $((r-1)Qf, n)$. Set

$$P(w) := \prod_{\substack{\ell \neq 2 \\ \ell \mid w}} \frac{\ell - 1}{\ell - 2},$$

which we note is multiplicative in w so that

$$P(\ (r-1)[Q, nf^2]\ ) = \frac{P((r-1)Qf^2)P(n)}{P(\ (\ (r-1)Qf^2\ ,\ n\ )\ )}.$$

With the notation and identities in (2.1.1) and (2.1.4), we have

$$\frac{1}{\phi([Q, nf^2])} = \frac{(Q, f^2)\phi((Qf^2, n))}{\phi(Qf^2)\phi(n)(Qf^2, n)} \prod_{\ell \mid n} \frac{(Q, nf^2)_\ell}{(Q, f^2)_\ell}.$$

So with these observations we can rewrite D_v^r to obtain

$$D_v^r = \sum_{\substack{f \geq 1 \\ f \text{ odd} \\ (f,r)=(f,r-2)=1 \\ (Q,f^2) \mid \Delta_{v,r}}} \frac{(Q, f^2)}{f\phi(Qf^2)} \cdot P((r-1)Qf^2) \sum_{n \geq 1} E_{f,v}^r(n), \tag{4.4.1}$$

where

$$E_{f,v}^r(n) := \frac{\phi((Qf^2, n))c_{f,v}^r(n)}{n\phi(n)(Qf^2, n)} \cdot \frac{P(n)}{P(\ (\ (r-1)Qf^2\ ,\ n\ )\ )} \cdot \prod_{\ell \mid n} \frac{(Q, nf^2)_\ell}{(Q, f^2)_\ell}.$$

The function $E_{f,v}^r(n)$ is a product of multiplicative functions in n and therefore is multiplicative in n itself. The evaluation of this function at prime powers ℓ^e depends on certain divisibility conditions involving r, f, Q, and v. We write

$$\sum_{n \geq 1} E_{f,v}^r(n) =: \prod_{\ell \mid f} \sum_{e \geq 0} b_{f,v}^r(\ell^e)\ \cdot\ \prod_{\ell \mid f} \sum_{e \geq 0} d_{f,v}^r(\ell^e) = \left(\prod_{\ell} \sum_{e \geq 0} b_{f,v}^r(\ell^e) \right) \left(\prod_{\ell \mid f} \frac{\sum_{e \geq 0} d_{f,v}^r(\ell^e)}{\sum_{e \geq 0} b_{f,v}^r(\ell^e)} \right),$$

where $d_{f,v}^r(1) = b_{f,v}^r(1) = 1$, and where we use Lemma 4.2.1 and the definition of $E_{f,v}^r(n)$ above to

explicitly compute for odd primes ℓ and integers $e \geq 1$:

$$d^r_{f,v}(\ell^e) = \begin{cases} (\ell-1)/\ell^{e+1} & \text{if } e \text{ is even,} \\ 0 & \text{if } e \text{ is odd;} \end{cases} \tag{4.4.2}$$

$$b^r_{f,v}(\ell^e) = \begin{cases} \dfrac{1}{\ell^e} & \text{if } \ell \nmid Q,\ \ell \mid r(r-2), \text{ and } e \text{ even;} \\ \dfrac{\ell-2}{\ell^e(\ell-1)} & \text{if } \ell \nmid Q,\ \ell \mid r-1, \text{ and } e \text{ even;} \\ \dfrac{\ell-3}{\ell^e(\ell-2)} & \text{if } \ell \nmid Q,\ \ell \nmid r(r-1)(r-2), \text{ and } e \text{ even;} \\ -\dfrac{1}{\ell^e(\ell-2)} & \text{if } \ell \nmid Q,\ \ell \mid r(r-2), \text{ and } e \text{ odd;} \\ -\dfrac{1}{\ell^e(\ell-1)} & \text{if } \ell \nmid Q,\ \ell \mid r-1, \text{ and } e \text{ odd;} \\ -\dfrac{2}{\ell^e(\ell-2)} & \text{if } \ell \nmid Q,\ \ell \nmid r(r-1)(r-2), \text{ and } e \text{ odd;} \\ \dfrac{\left(\frac{\Delta_{v,r}}{\ell}\right)^e}{\ell^e} & \text{if } \ell \mid Q. \end{cases} \tag{4.4.3}$$

It is also worth noting that $b^r_{f,v}(2^e) = (-1)^e/2^e$.

Note that the evaluation of $b^r_{f,v}(\ell^e)$ has no dependence on f, and as such we change notation to $b^r_v(n) := b^r_{f,v}(n)$. Similarly the evaluation of $d^r_{f,v}(n)$ does not depend on any of the parameters r, f or v, and so we set $d(n) := d^r_{f,v}(n)$. Keeping these calculations in mind, returning to (4.4.1) yields

$$D^r_v = \frac{1}{\phi(Q)} \left(\prod_{\ell} \sum_{e \geq 0} b^r_v(\ell^e) \right) \sum_{\substack{f \geq 1 \\ f \text{ odd} \\ (f,r)=(f,r-2)=1 \\ (Q,f^2) \mid \Delta_{v,r}}} \frac{\phi((Q,f^2))}{f\phi(f^2)} \cdot P((r-1)Qf^2) \left(\prod_{\ell \mid f} \frac{\sum_{e \geq 0} d(\ell^e)}{\sum_{e \geq 0} b^r_v(\ell^e)} \right),$$

where we've used the fact that $\phi(Qf^2) = \phi(Q) \cdot \phi(f^2) \cdot (Q, f^2)/\phi((Q, f^2))$ from (2.1.3). Using the same prime-counting technique as earlier, we can use the similar identity

$$P((r-1)Qf^2) = \frac{P(Q(r-1)) \cdot P(f^2)}{P(\ (Q(r-1)\ ,\ f^2)\ )},$$

and obtain

$$D^r_v = \frac{P(Q(r-1))}{\phi(Q)} \left(\prod_{\ell} \sum_{e \geq 0} b^r_v(\ell^e) \right) \sum_{\substack{f \geq 1 \\ f \text{ odd} \\ (f,r)=(f,r-2)=1 \\ (Q,f^2) \mid \Delta_{v,r}}} g^r_v(f), \tag{4.4.4}$$

where

$$g_v^r(f) := \frac{\phi((Q,f^2))}{f\phi(f^2)} \cdot \frac{P(f^2)}{P(\ (Q(r-1)\ ,\ f^2)\ )} \left(\prod_{\ell \mid f} \frac{\sum_{e\geq 0} d(\ell^e)}{\sum_{e\geq 0} b_v^r(\ell^e)} \right).$$

From its expression above we see that the function $g_v^r(k)$ is a product of multiplicative functions in f and therefore itself is multiplicative in f. In summing over integers $f \geq 1$ subject to the conditions in (4.4.4) we only see primes $\ell \nmid 2r(r-2)$ and prime powers ℓ^e such that $(Q,\ell^{2e}) \mid \Delta_{v,r}$, and so we can write

$$\sum_{\substack{f\geq 1 \\ f \text{ odd} \\ (f,r)=(f,r-2)=1 \\ (Q,f^2)\mid \Delta_{v,r}}} g_v^r(f) = \prod_{\ell \nmid 2r(r-2)} \left(1 + \sum_{\substack{e\geq 1 \\ (Q,\ell^{2e})\mid \Delta_{v,r}}} g_v^r(\ell^e) \right),$$

where for $\ell \nmid 2r(r-2)$, $e \geq 1$, and $(Q,\ell^{2e}) \mid \Delta_{v,r}$ we calculate

$$g_v^r(\ell^e) = \left\{ \begin{array}{ll} \frac{1}{\ell^{3e-1}(\ell-2)} & \text{if } \ell \nmid Q \text{ and } \ell \nmid r-1, \\ \frac{1}{\ell^{3e-1}(\ell-1)} & \text{if } \ell \nmid Q \text{ and } \ell \mid r-1, \\ \frac{1}{\ell^{3e-1}} & \text{if } \ell \mid Q. \end{array} \right\} \cdot \left(\frac{\sum_{a\geq 0} d(\ell^a)}{\sum_{a\geq 0} b_v^r(\ell^a)} \right). \tag{4.4.5}$$

Having identified the multiplicativity in the sum over integers $f \geq 1$ we return to (4.4.4) to express

$$D_v^r = \frac{P(Q(r-1))}{\phi(Q)} \left(\prod_{\ell} \sum_{e\geq 0} b_v^r(\ell^e) \right) \prod_{\ell \nmid 2r(r-2)} \left(1 + \sum_{\substack{e\geq 1 \\ (Q,\ell^{2e})\mid \Delta_{v,r}}} g_v^r(\ell^e) \right). \tag{4.4.6}$$

We now make explicit calculations of the sums appearing above, which are immediate upon

using (4.4.2), (4.4.3), (4.4.5) and geometric series arguments. For ℓ an odd prime, we have

$$\sum_{a\geq 0} b_v^r(\ell^a) = \begin{cases} \dfrac{\ell(\ell^2-2\ell-1)}{(\ell-2)(\ell^2-1)} & \text{if } \ell \nmid Q \text{ and } \ell \mid r(r-2), \\ \dfrac{\ell^3-\ell^2-\ell-1}{(\ell+1)(\ell-1)^2} & \text{if } \ell \nmid Q \text{ and } \ell \mid r-1, \\ \dfrac{\ell^3-2\ell^2-2\ell-1}{(\ell-2)(\ell^2-1)} & \text{if } \ell \nmid Q \text{ and } \ell \nmid r(r-1)(r-2), \\ \dfrac{\ell\left[\ell+\left(\frac{\Delta_\gamma^r}{\ell}\right)\right]}{\ell^2-1} & \text{if } \ell \mid Q \text{ and } \ell \nmid \Delta_\gamma^r, \\ 1 & \text{if } \ell \mid Q \text{ and } \ell \mid \Delta_\gamma^r. \end{cases} \tag{4.4.7}$$

$$\sum_{a\geq 0} d(\ell^a) = \frac{\ell^2+\ell+1}{\ell(\ell+1)} \tag{4.4.8}$$

It is also worth noting that $\sum_{a\geq 0} b_v^r(2^a) = 2/3$. For $\ell \nmid 2r(r-2)$, we use the results above and (4.4.5) to compute

$$1 + \sum_{\substack{e\geq 1 \\ (Q,\ell^{2e})\mid \Delta_{v,r}}} g_v^r(\ell^e) = \begin{cases} \dfrac{\ell(\ell^2-2\ell-2)}{\ell^3-2\ell^2-2\ell-1} & \text{if } \ell \nmid Q \text{ and } \ell \nmid r-1, \\ \dfrac{\ell(\ell^2-\ell-1)}{\ell^3-\ell^2-\ell-1} & \text{if } \ell \nmid Q \text{ and } \ell \mid r-1, \\ 1 & \text{if } \ell \mid Q \text{ and } \ell \nmid \Delta_{v,r}, \\ \dfrac{\ell^2}{\ell^2-1} & \text{if } \ell \mid Q \text{ and } \ell \mid \Delta_{v,r}. \end{cases} \tag{4.4.9}$$

Set $B_v^r(\ell) := \sum_{e\geq 0} b_v^r(\ell^e)$ and $G_v^r(\ell) := 1 + \sum_{e\geq 1} g_v^r(\ell)$. Returning to (4.4.6), we will partition the primes according to the conditions established in the above computations. Recalling the definition of $P(Q(r-1))$ and noting that $B_v^r(2) = 2/3$, we have

$$D_v^r = \frac{2P(Q)}{3\phi(Q)} \cdot \left(\prod_{\substack{\ell \nmid 2Q \\ \ell \mid r-1}} \frac{\ell-1}{\ell-2} \right) \cdot \left(\prod_{\ell \neq 2} B_v^r(\ell) \right) \cdot \left(\prod_{\ell \nmid 2r(r-2)} G_v^r(\ell) \right). \tag{4.4.10}$$

For convenience, set

$$\begin{aligned} B(\ell) &:= \frac{\ell^3-2\ell^2-2\ell-1}{(\ell-2)(\ell^2-1)}, \\ G(\ell) &:= \frac{\ell^3-2\ell^2-2\ell}{\ell^3-2\ell^3-2\ell-1}, \end{aligned}$$

which correspond to the functions that $B_v^r(\ell)$ and $G_v^r(\ell)$ take for all but finitely many primes ℓ.

We first write

$$\prod_{\ell \neq 2} B_v^r(\ell) = \prod_{\substack{\ell \neq 2 \\ \ell | Q}} B_v^r(\ell) \cdot \prod_{\ell \nmid 2Q} B_v^r(\ell) \tag{4.4.11}$$

$$\prod_{\ell \nmid 2r(r-2)} G_v^r(\ell) = \prod_{\substack{\ell \nmid 2r(r-2) \\ \ell | Q}} G_v^r(\ell) \cdot \prod_{\ell \nmid 2Qr(r-2)} G_v^r(\ell). \tag{4.4.12}$$

Since the function $B(\ell)$ and $G(\ell)$ are the values that $B_v^r(\ell)$ and $G_v^r(\ell)$ take (respectively) when ℓ does not divide $2Qr(r-1)(r-2)$, we can express the second factors of (4.4.11) and (4.4.12) as

$$\prod_{\ell \nmid 2Q} B_v^r(\ell) = \prod_{\ell \nmid 2Q} B(\ell) \cdot \prod_{\substack{\ell \nmid 2Q \\ \ell | r-1}} \frac{B_v^r(\ell)}{B(\ell)} \cdot \prod_{\substack{\ell \nmid 2Q \\ \ell | r(r-2)}} \frac{B_v^r(\ell)}{B(\ell)} \tag{4.4.13}$$

$$\prod_{\ell \nmid 2Qr(r-2)} G_v^r(\ell) = \prod_{\ell \nmid 2Q} G(\ell) \cdot \prod_{\substack{\ell \nmid 2Q \\ \ell | r-1}} \frac{G_v^r(\ell)}{G(\ell)} \cdot \prod_{\substack{\ell \nmid 2Q \\ \ell | r(r-2)}} \frac{1}{G(\ell)}. \tag{4.4.14}$$

Multiplying (4.4.13) and (4.4.14) together and applying the calculations from the cases where $l \nmid Q$ in (4.4.7) and (4.4.9), we get

$$\begin{aligned}
&\left(\prod_{\ell \nmid 2Q} B_v^r(\ell)) \right) \left(\prod_{\ell \nmid 2Qr(r-2)} G_v^r(\ell) \right) \\
&= \prod_{\ell \nmid 2Q} B(\ell)G(\ell) \cdot \prod_{\substack{\ell \nmid 2Q \\ \ell | r-1}} \frac{B_v^r(\ell)G_v^r(\ell)}{B(\ell)G(\ell)} \cdot \prod_{\substack{\ell \nmid 2Q \\ \ell | r(r-2)}} \frac{B_v^r(\ell)}{B(\ell)G(\ell)} \\
&= \prod_{\ell \nmid 2Q} \frac{\ell(\ell^2 - 2\ell - 2)}{(\ell-2)(\ell^2-1)} \prod_{\substack{\ell \nmid 2Q \\ \ell | r-1}} \left(1 + \frac{\ell+1}{\ell^2 - 2\ell - 2} \right) \cdot \frac{\ell - 2}{\ell - 1} \prod_{\substack{\ell \nmid 2Q \\ \ell | r(r-2)}} \left(1 + \frac{1}{\ell^2 - 2\ell - 2} \right).
\end{aligned}$$

Putting this work back into (4.4.10), we obtain

$$D_v^r = C_v^r \cdot \frac{2P(Q)}{3\phi(Q)} \prod_{\ell \nmid 2Q} \frac{\ell(\ell^2 - 2\ell - 2)}{(\ell-2)(\ell^2-1)} \prod_{\substack{\ell \nmid 2Q \\ \ell | r-1}} \left(1 + \frac{\ell+1}{\ell^2 - 2\ell - 2} \right) \prod_{\substack{\ell \nmid 2Q \\ \ell | r(r-2)}} \left(1 + \frac{1}{\ell^2 - 2\ell - 2} \right),$$

where we use the calculations in (4.4.7) and (4.4.9) to express

$$C_v^r := \left(\prod_{\substack{\ell\neq 2\\ l\mid Q}} B_v^r(\ell)\right)\cdot\left(\prod_{\substack{\ell\nmid 2r(r-2)\\ \ell\mid Q}} G_v^r(\ell)\right) = \prod_{\substack{\ell\neq 2\\ \ell\mid Q}}\left(1+\frac{\ell\left(\frac{\Delta_{v,r}}{\ell}\right)+1}{\ell^2-1}\right).$$

This completes the proof of Lemma 4.2.2.

4.5 Summing Euler Products

In this section we assume $(Q,v)=1$ and study the quantity

$$J_v(R) := \sum_{\substack{|r|<R\\ r \text{ odd; } r\neq 1\\ (v+1-r,Q)=1}} \prod_{\ell\neq 2}\left(1+e_v^r(\ell)\right), \tag{4.5.1}$$

where

$$e_v^r(\ell) = \begin{cases} \bar{e}_v^r(\ell) := \dfrac{\ell\left(\frac{\Delta_{v,r}}{\ell}\right)+1}{\ell^2-1} & \text{if } \ell\mid Q,\\ e^{(1)}(\ell) := \dfrac{\ell+1}{\ell^2-2\ell-2} & \text{if } \ell\nmid Q \text{ and } \ell\mid r-1,\\ e^{(2)}(\ell) := \dfrac{1}{\ell^2-2\ell-2} & \text{if } \ell\nmid Q \text{ and } \ell\mid r(r-2).\end{cases}$$

We begin by noting that as r runs through the integers $|r|<R$, we see each primitive residue class $v+1-r$ modulo Q several times. Grouping these contributions together and observing that $\bar{e}_v^r(\ell)=\bar{e}_v^s(\ell)$ for $r\equiv s \pmod{Q}$, we obtain

$$J_v(R) = \sum_{a \pmod{Q}^\times}\left[\prod_{\substack{\ell\neq 2\\ \ell\mid Q}}\left(1+\bar{e}_v^{v+1-a}(\ell)\right)\right]K_{v,a}(R), \tag{4.5.2}$$

where

$$K_{v,a}(R) := \sum_{\substack{|r|<R\\ r \text{ odd; } r\neq 1\\ r\equiv v+1-a \pmod{Q}}}\left[\prod_{\substack{\ell\nmid 2Q\\ \ell\mid r-1}}\left(1+e^{(1)}(\ell)\right)\cdot\prod_{\substack{\ell\nmid 2Q\\ \ell\mid r(r-2)}}\left(1+e^{(2)}(\ell)\right)\right]. \tag{4.5.3}$$

The quantity $K_{v,a}(R)$ is almost identical to a quantity studied in [BCD11, Lemma 18]; the difference is that in this work we are summing over an additional congruence condition. As such we

will follow the same technique and notation established in that paper.

For a fixed r the internal product in (4.5.3) is a product over the odd primes in the number $r(r-1)(r-2)$, discounting those primes in Q. Expanding the product leads to the motivation for the following definitions.

$$\begin{aligned}
\mathcal{P}(r) &:= \{\ell \text{ odd prime} : \ell \nmid Q,\ \ell \mid r(r-1)(r-2)\} \\
\mathcal{F}(r) &:= \{q \text{ odd, positive and square-free integer} : \ell \mid q \Rightarrow \ell \in \mathcal{P}(r)\} \\
\mathcal{D}(R) &:= \bigcup_{\substack{|r|<R \\ r \text{ odd; } r\neq 1 \\ r\equiv v+1-a \pmod{Q}}} \mathcal{F}(r), \\
e_v^r(q) &:= \prod_{\ell \mid q} e_v^r(\ell), \text{ and also } e_v^r(1) := 1.
\end{aligned}$$

Expanding the product in (4.5.3) and using the notation above gives

$$K_{v,a}(R) = \sum_{\substack{|r|<R \\ r \text{ odd; } r\neq 1 \\ r\equiv v+1-a \pmod{Q}}} \sum_{q\in\mathcal{F}(r)} e_v^r(q),$$

For a fixed $q \in \mathcal{F}(r)$, the function $e_v^r(q) = \prod_{\ell|q} e^{(w_\ell)}(\ell)$ for some map of sets $w : \{\ell \mid q\} \to \{1,2\}$. Upon grouping the contributions of all such $q \in \mathcal{F}(r)$ with the same value of $e_v^r(q)$, we obtain

$$K_{v,a}(R) = \sum_{q\in\mathcal{D}(R)} \sum_{\substack{\text{maps } w \\ \{\ell|q\}\to\{1,2\}}} \left(\prod_{\ell|q} e^{(w_\ell)}(\ell)\right) N_{v,a}^{q,w}(R), \tag{4.5.4}$$

where

$$\begin{aligned}
N_{v,a}^{q,w}(R) &:= \#\left\{ |r| < R : \begin{array}{l} r \text{ odd, } r \neq 1 \\ r \equiv v+1-a \pmod{Q} \\ e_v^r(\ell) = e^{(w_\ell)}(\ell) \text{ for all } \ell \mid q \end{array} \right\} \\
&= \#\left\{ |r| < R : \begin{array}{l} r \equiv 1 \pmod{2} \\ r \equiv v+1-a \pmod{Q} \\ r \equiv 1 \pmod{\ell} \text{ for all } \ell \mid q \text{ with } w_\ell = 1 \\ r \equiv 0,2 \pmod{\ell} \text{ for all } \ell \mid q \text{ with } w_\ell = 2 \end{array} \right\} + \mathrm{O}(1).
\end{aligned}$$

This system of congruences is well-suited for the Chinese Remainder Theorem. Recall that q is comprised of odd primes distinct from the primes in Q, so the only potential obstruction to this system is if Q is even. When Q is even, we require both r and $v+1-a$ to odd, however this holds automatically based on the assumption that $(v,Q)=1$ and a is invertible modulo Q. As a result there is no obstruction to the system of congruences above – we can study its solutions modulo $2qQ/(2,Q)$. In particular there are $\prod_{\ell|q} 2^{w_\ell-1}$ unique solutions modulo $2qQ/(2,Q)$. Therefore we have

$$N_{v,a}^{q,w}(R) = \left(\frac{2R(2,Q)}{2Qq} + \mathrm{O}(1)\right)\cdot \prod_{\ell|q} 2^{w_\ell-1} = \frac{R(2,Q)}{Qq}\prod_{\ell|q} 2^{w_\ell-1} + \mathrm{O}(2^{\nu(q)}),$$

where $\nu(q)$ is the multiplicative function that counts the number of distinct prime factors of q. Using this estimate we can write $K_{v,a}(R)$ as

$$\frac{R(2,Q)}{Q}\sum_{q\in\mathcal{D}(R)}\left[\frac{1}{q}\sum_{\substack{\text{maps } w\\ \{\ell|q\}\to\{1,2\}}}\prod_{\ell|q} e^{(w_\ell)}(\ell)\cdot 2^{w_\ell-1}\right] + \mathrm{O}\left(\sum_{q\in\mathcal{D}(R)}\left[2^{\nu(q)}\sum_{\substack{\text{maps } w\\ \{\ell|q\}\to\{1,2\}}}\prod_{\ell|q} e^{(w_\ell)}(\ell)\right]\right). \quad (4.5.5)$$

Both quantities in square brackets above are multiplicative functions in the variable q. Furthermore, since the $q\in\mathcal{D}(R)$ are square-free it suffices to only evaluate these functions at the prime power $p^1=p$. Doing so to both simultaneously gives

$$\begin{aligned}\frac{1}{p}\sum_{\substack{\text{maps } w\\ \{\ell|p\}\to\{1,2\}}}\prod_{\ell|p} e^{(w_\ell)}(\ell)\cdot 2^{w_\ell-1} &= \frac{e^{(1)}(p)+2e^{(1)}(p)}{p},\\ 2^{\nu(p)}\sum_{\substack{\text{maps } w\\ \{\ell|p\}\to\{1,2\}}}\prod_{\ell|p} e^{(w_\ell)}(\ell) &= 2[e^{(1)}(p)+e^{(2)}(p)].\end{aligned}$$

Recalling that $q\in\mathcal{D}(R)$ is built from the odd primes distinct from those in Q but dividing $r(r-1)(r-2)$ for some $|r|<R$, we conclude that we see no primes that are larger than R in the expression of $K_{v,a}(R)$ in (4.5.5). Exploiting the multiplicativity in q therefore gives

$$K_{v,a}(R) = \frac{R(2,Q)}{Q}\prod_{\substack{\ell\nmid 2Q\\ \ell<R}}\left(1+\frac{e^{(1)}(\ell)+2e^{(2)}(\ell)}{\ell}\right) + \mathrm{O}\left(\prod_{\substack{\ell\nmid 2Q\\ \ell<R}}\left(1+2e^{(1)}(\ell)+2e^{(2)}(\ell)\right)\right).$$

Using Mertens' second theorem and a Taylor expansion for $\log(1+t)$, the error term is

asymptotically bounded above by

$$\prod_{\ell<R}\left(1+\frac{2(\ell^2+\ell-1)}{\ell(\ell^2-2\ell-2)}\right)\ll\exp\left(\sum_{\ell<R}\log\left(1+\frac{2}{\ell}\right)\right)\ll\log^2 R.$$

A similar estimate gives the product in the main term as

$$\prod_{\substack{\ell\nmid 2Q\\ \ell<R}}\left(1+\frac{\ell+3}{\ell(\ell^2-2\ell-2)}\right)=\prod_{\ell\nmid 2Q}\left(1+\frac{\ell+3}{\ell(\ell^2-2\ell-2)}\right)+\mathrm{O}(1).$$

Therefore upon rewriting the factor occurring in the product we have shown

$$K_{v,a}(R)=\frac{R(2,Q)}{Q}\prod_{\ell\nmid 2Q}\frac{\ell^3-2\ell^2-\ell+3}{\ell(\ell^2-2\ell-2)}+\mathrm{O}(\log^2 R).$$

Substituting this expression for $K_{v,a}(R)$ back into (4.5.2) gives

$$J_v(R)=\frac{R(2,Q)}{Q}\prod_{\ell\nmid 2Q}\frac{\ell^3-2\ell^2-\ell+3}{\ell(\ell^2-2\ell-2)}\cdot\overline{K}_v(Q)+\mathrm{O}\left(\log^2 R\cdot\overline{K}_v(Q)\right),\tag{4.5.6}$$

where

$$\overline{K}_v(Q):=\sum_{a\pmod{Q}^\times}\left[\prod_{\substack{\ell\neq 2\\ \ell\mid Q}}\left(1+\bar{e}_v^{\,v+1-a}(\ell)\right)\right].$$

The term $\overline{K}_v(Q)$ is multiplicative in Q. To see this, let q_1 and q_2 be coprime integers and consider the product

$$\overline{K}_v(q_1)\overline{K}_v(q_2)=\sum_{a_1\pmod{q_1}^\times}\prod_{\substack{\ell_1\neq 2\\ \ell_1\mid q_1}}\left(1+\bar{e}_v^{\,v+1-a_1}(\ell_1)\right)\sum_{a_2\pmod{q_2}^\times}\prod_{\substack{\ell_2\neq 2\\ \ell_2\mid q_2}}\left(1+\bar{e}_v^{\,v+1-a_2}(\ell_2)\right).$$

By the Chinese Remainder Theorem there is a unique invertible residue c modulo q_1q_2 such that $c\equiv a_1 \pmod{q_1}$ and $c\equiv a_2 \pmod{q_2}$. For both $j=1$ and $j=2$ we have

$$\Delta_{v,v+1-c}=(v+1-c)^2-4v\equiv(v+1-a_j)^2-4v\pmod{q_j}\equiv\Delta_{v,v+1-a_j}.$$

and so in particular

$$\left(\frac{\Delta_{v,v+1-c}}{\ell}\right) = \begin{cases} \left(\frac{\Delta_{v,v+1-a_1}}{\ell_1}\right) & \text{if } \ell_1 \mid q_1, \\ \left(\frac{\Delta_{v,v+1-a_2}}{\ell_2}\right) & \text{if } \ell_2 \mid q_2. \end{cases}$$

As the characters agree on the appropriate primes, we also have $\bar{e}_v^{v+1-c}(\ell_j) = \bar{e}_v^{v+1-a_j}(\ell_j)$ for both $j = 1$ and $j = 2$. Therefore we conclude

$$\overline{K}_v(q_1)\overline{K}_v(q_2) = \sum_{\substack{a_1 \pmod{q_1}^\times \\ a_2 \pmod{q_2}^\times}} \prod_{\substack{\ell \neq 2 \\ \ell \mid q_1 q_2}} \left(1 + \bar{e}_v^{v+1-c}(\ell)\right),$$

after which the bijection $(\mathbb{Z}/q_1\mathbb{Z})^\times \times (\mathbb{Z}/q_2\mathbb{Z})^\times \leftrightarrow (\mathbb{Z}/q_1q_2\mathbb{Z})^\times$ completes the proof of multiplicativity.

Since $\overline{K}_v(Q)$ is multiplicative in Q, it suffices to evaluate it at prime powers dividing Q. As Q is square-free we simply obtain

$$\overline{K}_v(Q) = \prod_{\substack{\ell \neq 2 \\ \ell \mid Q}} \left(\sum_{a \pmod{\ell}^\times} (1 + \bar{e}_v^{v+1-a}(\ell)) \right) = \prod_{\substack{\ell \neq 2 \\ \ell \mid Q}} \left(\phi(\ell) + \sum_{a \pmod{\ell}^\times} \frac{\ell\left(\frac{\Delta_{v,v+a-1}}{\ell}\right) + 1}{\ell^2 - 1} \right).$$

As $\Delta_{v,v+a-1} = a^2 - 2(v+1)a + (v-1)^2$ and $(Q, v) = 1$, we may use Lemma 2.1.7 to conclude

$$\sum_{a \pmod{\ell}^\times} \left(\frac{\Delta_{v,v+a-1}}{\ell}\right) = -\left(\frac{(v-1)^2}{\ell}\right) + \sum_{a \pmod{\ell}} \left(\frac{\Delta_{v,v+a-1}}{\ell}\right) = -\left(\frac{(v-1)^2}{\ell}\right) - 1.$$

Therefore

$$\overline{K}_v(Q) = \prod_{\substack{\ell \neq 2 \\ \ell \mid Q}} \left(\phi(\ell) - \frac{\ell\left[\left(\frac{(v-1)^2}{\ell}\right) + 1\right]}{\ell^2 - 1} + \frac{\phi(\ell)}{\ell^2 - 1} \right) = \frac{Q}{(2, Q)} \prod_{\substack{\ell \neq 2 \\ \ell \mid Q}} \frac{\ell^2 - \ell - \left[1 + \left(\frac{(v-1)^2}{\ell}\right)\right]}{\ell^2 - 1}.$$

Putting this result back into (4.5.6) gives the main result of this section:

$$J_v(R) = R \prod_{\ell \nmid 2Q} \frac{\ell^3 - 2\ell^2 - \ell + 3}{\ell(\ell^2 - 2\ell - 2)} \cdot \prod_{\substack{\ell \neq 2 \\ \ell \mid Q}} \frac{\ell^2 - \ell - \left[1 + \left(\frac{(v-1)^2}{\ell}\right)\right]}{\ell^2 - 1} + \mathrm{O}\left(\log^2 R\right).$$

Bibliography

[Apo76] Tom Apostol. *Introduction to Analytic Number Theory*. Springer, 1976.

[Bai07] Stephan Baier. The Lang-Trotter conjecture on average. *Journal of the Ramanujan Mathematical Society*, 22:299–314, 2007.

[BBIJ05] Johnathan Battista, Jonathan Bayless, Dmitriy Ivanov, and Kevin James. Average Frobenius distributions for elliptic curves with nontrivial rational torsion. *Acta Arithmetica*, 119(1):81–91, 2005.

[BCD11] Antal Balog, Alina-Carmen Cojocaru, and Chantal David. Average twin prime conjecture for elliptic curves. *American Journal of Mathematics*, 133(5):1179–1229, 2011.

[BLGHT11] Tom Barnet-Lamb, David Geraghty, Michael Harris, and Richard Taylor. A family of Calabi–Yau varieties and potential automorphy II. *Publications of the Research Institute for Mathematical Sciences*, 47(1):29–98, 2011.

[CDKS16] Vorrapan Chandee, Chantal David, Dimitris Koukoulopoulos, and Ethan Smith. Frequency of elliptic curve groups over prime finite fields. *Canadian Journal of Mathematics*, 68(4):721–761, 2016.

[CHT08] Laurent Clozel, Michael Harris, and Richard Taylor. Automorphy for some ℓ-adic lifts of automorphic mod ℓ Galois representations. *Publications mathématiques*, 108(1):1, 2008.

[Coh08] Henri Cohen. *Number Theory: Tools and Diophantine Equations*, volume 239. Springer, 2008.

[Coj05] Alina Carmen Cojocaru. Reductions of an elliptic curve with almost prime orders. *Acta Arithmetica*, 119(3):265, 2005.

[Cox89] David Cox. *Primes of the form $x^2 + ny^2$*. John Wiley & Sons, 1989.

[Dav00] Harold Davenport. *Multiplicative Number Theory*, volume 74. Springer, 2000.

[Deu41] Max Deuring. Die typen der multiplikatorenringe elliptischer funktionenkörper. In *Abhandlungen aus dem mathematischen Seminar der Universität Hamburg*, volume 14, pages 197–272, 1941.

[DP99] Chantal David and Francesco Pappalardi. Average Frobenius distributions of elliptic curves. *International Math Research Notices*, (4):165 – 183, 1999.

[DP04] Chantal David and Francesco Pappalardi. Average Frobenius distribution for inerts in $\mathbb{Q}(i)$. *Journal of the Ramanujan Mathematical Society*, 19(3):181–201, 2004.

[DW12] Chantal David and Jie Wu. Almost prime values of the order of elliptic curves over finite fields. In *Forum Mathematicum*, volume 24, pages 99–119, 2012.

[FJKP11] Bryan Faulkner, Kevin James, Matthew King, and David Penniston. Average Frobenius distributions for elliptic curves over abelian extensions. *Acta Arithimetica*, 149(3):215–244, 2011.

[FM96] Etienne Fouvry and M Ram Murty. On the distribution of supersingular primes. *Canadian Journal of Mathematics*, 48(1):81–104, 1996.

[GS03] Andrew Granville and Kannan Soundararajan. The distribution of values of $L(1, \chi_d)$. *Geometric and Functional Analysis*, 13(5):992–1028, 2003.

[HJX14] Jason Hedetniemi, Kevin James, and Hui Xue. Champion primes for elliptic curves over fields of prime order. *INTEGERS*, 14, 2014.

[HL23] G.H Hardy and John Littlewood. Some problems of Partitio numerorum; III: On the expression of a number as a sum of primes. *Acta Mathematica*, 44(1):1–70, 1923.

[HSBT10] Michael Harris, Nick Shepherd-Barron, and Richard Taylor. A family of Calabi-Yau varieties and potential automorphy. *Annals of Mathematics*, pages 779–813, 2010.

[IJU10] Henryk Iwaniec and Jorge Jiménez Urroz. Orders of CM elliptic curves modulo p with at most two primes. *Annali della Scuola Normale Superiore di Pisa. Classe di scienze*, 9(4):815–832, 2010.

[IK04] Henryk Iwaniec and Emmanuel Kowalski. *Analytic Number Theory*, volume 53. American Mathematical Society, 2004.

[IR90] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*, volume 84. Springer, 1990.

[Jam04] Kevin James. Average Frobenius distributions for elliptic curves with 3-torsion. *Journal of Number Theory*, 109(2):278–298, 2004.

[Jam05] Kevin James. Averaging special values of Dirichlet L-series. *The Ramanujan Journal*, 10(1):75–87, 2005.

[Jon09] Nathan Jones. Averages of elliptic curve constants. *Mathematische Annalen*, 345(3):685–710, 2009.

[JP17] Kevin James and Paul Pollack. Extremal primes for elliptic curves with complex multiplication. *Journal of Number Theory*, 172:383–391, 2017.

[JS11] Kevin James and Ethan Smith. Average Frobenius distribution for elliptic curves defined over finite Galois extensions of the rationals. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 150, pages 439–458. Cambridge Univ Press, 2011.

[JS13] Kevin James and Ethan Smith. Average Frobenius distribution for the degree two primes of a number field. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 154, pages 499–525. Cambridge Univ Press, 2013.

[JTT+16] Kevin James, Brandon Tran, Minh-Tam Trinh, Phil Wertheimer, and Dania Zantout. Extremal primes for elliptic curves. *Journal of Number Theory*, 164:282–298, 2016.

[Kna92] Anthony W Knapp. *Elliptic Curves*, volume 40. Princeton University Press, 1992.

[Kob88] Neal Koblitz. Primality of the number of points on an elliptic curve over a finite field. *Pacific Journal of Mathematics*, 131(1):157–165, 1988.

[Kob12] Neal Koblitz. *Introduction to Elliptic Curves and Modular Forms*, volume 97. Springer, 2012.

[Kou15] Dimitris Koukoulopoulos. Primes in short arithmetic progressions. *International Journal of Number Theory*, 11(05):1499–1521, 2015.

[LT76] Serge Lang and Hale Trotter. *Frobenius Distributions in GL_2-Extensions: Distribution of Frobenius Automorphisms in GL_2-Extensions of the Rational Numbers*, volume 504. Springer, 1976.

[May15] James Maynard. Small gaps between primes. *Annals of mathematics*, 181(1):383–413, 2015.

[ME06] M.R. Murty and Jody Esmonde. *Problems in Algebraic Number Theory*, volume 190. Springer New York, 2006.

[Mer74] Franz Mertens. Ein beitrag zur analytischen zahlentheorie. *Journal für die reine und angewandte Mathematik*, 78:46–62, 1874.

[MM01] S Ali Miri and V Kumar Murty. An application of sieve methods to elliptic curves. In *International Conference on Cryptology in India*, pages 91–98. Springer, 2001.

[Mur01] M. Ram Murty. *Problems in Analytic Number Theory*, volume 206. Springer, 2001.

[Pol14] DHJ Polymath8B. Variants of the Selberg sieve, and bounded intervals containing many primes. *Research in the Mathematical sciences*, 1(1):12, 2014.

[Rib01] Paulo Ribenboim. *Classical Theory of Algebraic Numbers*. Springer, 2001.

[Sil86] Joseph Silverman. *The Arithmetic of Elliptic Curves*, volume 106. 1986.

[ST94] Joseph. Silverman and John Tate. *Rational Points on Elliptic Curves*. Springer, 1994.

[SW05] Jörn Steuding and Annegret Weng. On the number of prime divisors of the order of elliptic curves modulo p. *Acta Arithmetica*, 117(4):341–352, 2005.

[Tay08] Richard Taylor. Automorphy for some ℓ-adic lifts of automorphic mod ℓ Galois representations. II. *Publications mathématiques*, 108(1):183–239, 2008.

[Was97] Lawrence C Washington. *Introduction to Cyclotomic Fields*, volume 83. Springer, 1997.

[Wat69] William Waterhouse. Abelian varieties over finite fields. In *Annales Scientifiques de l'École Normale Supérieure*, volume 2, pages 521–560, 1969.

[Zha14] Yitang Zhang. Bounded gaps between primes. *Annals of Mathematics*, 179(3):1121–1174, 2014.

[Zyw11] David Zywina. A refinement of Koblitz's conjecture. *International Journal of Number Theory*, 7(03):739–769, 2011.

Symbolic Index