UNIVERSITY OF CALIFORNIA,
IRVINE

Average Cyclicity for Elliptic Curves in Torsion Families

DISSERTATION

submitted in partial satisfaction of the requirements
for the degree of

DOCTOR OF PHILOSOPHY

in Mathematics

by

Luke Fredericks

Dissertation Committee:
Associate Professor Nathan Kaplan, Chair
Assistant Professor Alexandra Florea
Professor Daqing Wan

2021

TABLE OF CONTENTS

Page

LIST OF TABLES

ACKNOWLEDGMENTS

First I would like to Nathan Kaplan for advising this thesis and for all of the support and guidance he has provided during my time at UC Irvine. Nathan's curiosity and enthusiasm is truly inspirational.

Thanks also to Alexandra Florea and Daqing Wan for serving on my thesis committee and for their helpful comments.

Thanks to all of the faculty, staff, and students at UC Irvine who have supported and challenged me along the way. Thanks especially to Alessandra Pantano and Joe Kramer-Miller and Dennis Eichhorn for helping me develop as an educator and helping me during my job search.

Thanks to my wife Rachel, friends and family for support and encouragement.

VITA

Luke Fredericks

EDUCATION

Doctor of Philosophy in Mathematics **2021**
University of California, Irvine *Irvine, CA*

Master of Arts in Mathematics **2015**
California State University, Sacramento *Sacramento, California*

Bachelor of Arts in French **2011**
California State University, Chico *Chico, CA*

Bachelor of Science in Mathematics **2011**
California State University, Chico *Chico, CA*

TEACHING EXPERIENCE

Teaching Assistant **2015–2021**
University of California, Irvine *Irvine, California*

ABSTRACT OF THE DISSERTATION

Average Cyclicity for Elliptic Curves in Torsion Families

By

Luke Fredericks

Doctor of Philosophy in Mathematics

University of California, Irvine, 2021

Associate Professor Nathan Kaplan, Chair

Let $E/\mathbb{Q}$ be an elliptic curve; for all but finitely many primes p, reduction modulo p yields an elliptic curve over the finite field $\mathbb{F}_p$, and it is natural to ask about the properties of these reductions for varying primes. The purpose of this dissertation is to study one such question, namely, how frequently the reductions result in an elliptic curve with cyclic group structure. To be precise, we let $\pi_E^{cyc}(x)$ denote the number of primes less than x for which the reduction of E modulo p is cyclic. The asymptotic behavior of this function has been established by Serre conditional on Generalized Riemann Hypothesis. Furthermore, Banks and Shparlinski showed that this asymptotic holds unconditionally on average over the family of elliptic curves given by short Weierstrass equations with coefficients taken in a 'box.' Inspired by the work of Battista, Bayless, Ivanov and James on the Lang-Trotter conjecture, we study the average asymptotic behavior of the functions π_E^{cyc} where the average is taken over certain thin families of elliptic curves: elliptic curves with a rational point of order m defined over $\mathbb{Q}$. The results we obtain are again in agreement with the conditional asymptotic. We also extend the study of cyclicity from elliptic curves defined over the rational numbers to elliptic curves defined over a quadratic extension of $\mathbb{Q}$ and obtain partial results in that case. As a key tool, we prove an analogue of a result of Vlăduţ that estimates the number of elliptic curves over a finite field which have some specified torsion and which have group structure that is as cyclic as possible.

Chapter 1

Introduction

In this chapter, we discuss the background and describe the results of this dissertation. In the second chapter, we recall necessary background on the topics of elliptic curves, and number fields. In the third chapter, we prove the necessary fixed field counting theorem, and in the fourth chapter, we obtain necessary estimates on the size of the set of rational numbers with given reduction modulo p. In chapter five, we prove the main result of this work, which we extend somewhat to elliptic curves defined over the field $\mathbb{Q}(\sqrt{-3})$ in the sixth chapter. Finally, we discuss several directions for future study.

Notation will be defined as needed, but here we set a few conventions that will hold throughout the dissertation. The symbols p and ℓ always represent prime numbers, and any summation over these symbols is taken over all the primes meeting the stated conditions. A sum over $d \mid n$ is taken over the positive divisors of n. Sums over $n \leq X$ are assumed to begin at $n = 1$. All logarithms are to the base e. Given a complex valued function f and a function g taking values in the positive real numbers, we write either $f = O(g)$ or $f \ll g$ to mean that there exists a positive constant C such that $|f| \leq Cg$ holds for every element of the domain. When f and g are functions of a real variable, we write $f = o(g)$ to mean that $\lim_{x\to\infty} f(x)/g(x) = 0$.

1.1 Background and motivation

Let E be an elliptic curve over $\mathbb{Q}$. For all but finitely many prime numbers p, we obtain an elliptic curve $E_p/\mathbb{F}_p$ by reduction modulo p. It is natural to ask how the properties of E_p vary with p. One might wonder how frequently $E_p(\mathbb{F}_p)$ is a prime number. One may ask how frequently the group $E_p(\mathbb{F}_p)$ is a cyclic group. One may ask how often the trace of Frobenius $a_p(E)$ is equal to a fixed number t, or how often the normalized trace $a_p(E)/\sqrt{p}$ lies in a particular interval. These questions lie behind the Koblitz conjecture, the cyclicity conjecture, the Lang-Trotter conjecture, and the Sato-Tate conjecture, respectively. To study cyclicity and Lang-Trotter, we introduce the following functions. Denote by

$$\pi_E^{cyc}(x) = \#\{p \le x : E_p(\mathbb{F}_p) \text{ is cyclic}\} \tag{1.1}$$

$$\pi_E^{t}(x) = \#\{p \le x : a_p(E) = t\}. \tag{1.2}$$

The asymptotic growth of these functions are the subjects of the Lang-Trotter conjecture and the cyclicity conjecture, respectively.

In the conjecture below, the symbols $\rho_{E,m}$ and m_E are as defined in Chapter 2, and for a set of matrices A, we denote by A_r those elements of A whose trace is equal to r.

Conjecture 1 (Lang-Trotter)**.** Let $E/\mathbb{Q}$ be an elliptic curve, and let $r \in \mathbb{Z}$ with $r \neq 0$ if E has complex multiplication. Then

$$\pi_E^r(x) \sim C_{E,r}\frac{\sqrt{x}}{\log x}, \tag{1.3}$$

where

$$C_{E,r} = \frac{2}{\pi} \cdot \frac{m_E \cdot \#(\rho_{E,m_E}(G_{\mathbb{Q}}))_r}{\#(\rho_{E,m_E}(G_{\mathbb{Q}}))} \prod_{\substack{\ell \nmid m_E \\ \ell \nmid r}} \frac{\ell(\ell^2-\ell-1)}{(\ell+1)(\ell-1)^2} \prod_{\substack{\ell \nmid m_E \\ \ell \mid r}} \frac{\ell^2}{\ell^2-1}.$$

Conjecture 2 (Cyclicity)**.** Let $E/\mathbb{Q}$ be a non-CM elliptic curve. Then

$$\pi_E^{cyc}(x) \sim C_E^{cyc}\pi(x). \tag{1.4}$$

where C_E^{cyc} is an explicit constant depending only on E.

The study of π_E^{cyc} goes back to the work of Borosh, Moreno and Porta [6] who suggested that for certain chosen examples of $E/\mathbb{Q}$, $E_p(\mathbb{F}_p)$ is cyclic for infinitely many p. Serre formulated and proved the cyclicity conjecture conditional on the Generalized Riemann Hypothesis for the division fields of E [32]. The best result to date is the following conditional theorem of Cojocaru and Murty.

Theorem 1. [9, Theorem 1.1] Let E be a non-CM elliptic curve defined over $\mathbb{Q}$ of conductor N. Assuming GRH for the Dedekind zeta functions of the division fields of E, we have that

$$\pi_E^{cyc}(x) = C_E^{cyc}\mathrm{li}(x) + O_N\left(x^{5/6}(\log x)^{2/3}\right) \tag{1.5}$$

where

$$C_E^{cyc} = \sum_{k \geq 1} \frac{\mu(k)}{[\mathbb{Q}(E[k]) : \mathbb{Q})]}. \tag{1.6}$$

Unconditionally, we cannot prove that the asymptotic in (1.3) or (1.4) holds for a single elliptic curve E. However, starting with the work of Fouvry and Murty [13], average versions of Conjectures 1.3 and 1.4 have been obtained. These average results provide strong unconditional evidence for the corresponding conjectures.

Let

$$\pi_{1/2}(X) = \int_2^X \frac{dt}{2\sqrt{t}\log t} \sim \frac{\sqrt{X}}{\log X}. \tag{1.7}$$

In the case of the Lang-Trotter conjecture we have the following Theorem due to David and Pappalardi.

Theorem 2. [11, Corollary 1.3] Let $E_{a,b} : y^2 = x^3 + ax + b$, and let $\epsilon > 0$. If $A, B > X^{1+\epsilon}$ then we have as $X \to \infty$

$$\frac{1}{4AB} \sum_{\substack{|a| \le A \\ |b| \le B}} \pi^r_{E(a,b)}(X) \sim D_r \pi_{1/2}(X) \tag{1.8}$$

where

$$D_r = \frac{2}{\pi} \prod_{\ell \nmid r} \frac{\ell(\ell^2 - \ell - 1)}{(\ell+1)(\ell-1)^2} \prod_{\ell \mid r} \frac{\ell^2}{\ell^2 - 1}. \tag{1.9}$$

In the case of the cyclicity conjecture, Banks and Shparlinski proved

Theorem 3. [4, Theorem 17] Let $\epsilon > 0$ and $K > 0$ be fixed. Then, for all integers A and B satisfying $AB \ge x^{1+\epsilon}, A, B \le x^{1-\epsilon}$, we have

$$\frac{1}{4AB} \sum_{|a| \le A} \sum_{|b| \le B} \pi^{cyc}_{E(a,b)}(x) = C_{cyc}\pi(x) + O(\pi(x)/(\log x)^K),$$

where

$$C_{cyc} = \prod_{\ell \text{ prime}} \left(1 - \frac{1}{\ell(\ell-1)(\ell^2-1)}\right),$$

and the constant implied by O depends only on ϵ and K.

The average asymptotic described above provide strong evidence for the conjectures in each case. In particular, the constants C_E^{cyc} and C_{cyc} and $C_{E,r}$ and D_r are clearly closely related. We view C_{cyc} and D_r as idealized constants where the variation of the constants from individual curves has been averaged out. Furthermore, Jones [21] proved that the average of the constants predicted by the respective conjectures is indeed the constant seen in the average results.

Jones' proof leveraged the fact (also due to Jones) that almost all elliptic curves are what are known as *Serre curves* [22]. However, there are interesting families which consist entirely of elliptic curves that are *not* Serre curves. These curves are essentially invisible in the prior average results cited above; it is therefore of interest to study the averages of the functions π_E^t and π_E^{cyc} as E varies over such a family.

One class of such families are the torsion families – the family of elliptic curves which possess some specified torsion structure. James [20] gave the first results in this direction when he obtained an asymptotic for the Lang-Trotter conjecture on average over the family of curves with a rational point of order 3. Battista, Bayless, Ivnaov, and James [5] extended this investigation to the family of elliptic curves which possess a rational point of order m for $m = 5, 7$ or 9. They prove

Theorem 4. [5, Theorem 3] Let $E_m(a)$ be the parameterization of elliptic curves which have a rational point of order $m \in \{5,7,9\}$. Then for any $c > 0$, we have

$$\frac{1}{\mathcal{C}(N)} \sideset{}{'}\sum_{|a| \le N} \pi^r_{E_m(a)}(X) = \frac{2}{\pi} C_{r,m} \pi_{1/2}(X) + O\left(\frac{X^{3/2}}{N} + \frac{\sqrt{X}}{\log^c X} \right),$$

where $\sum'$ represents the sum over non-singular curves, $\mathcal{C}(N)$ represents the number of curves in the sum, and

$$C_{r,m} = C_r(m) \prod_{\substack{\ell \nmid m \\ \ell \nmid r}} \frac{\ell(\ell^2 - \ell - 1)}{(\ell+1)(\ell-1)^2} \prod_{\substack{\ell \nmid m \\ \ell | r}} \frac{\ell^2}{\ell^2 - 1},$$

where

$$C_r(m) = \begin{cases} 5/4 & \text{if } m = 5 \text{ and } r \equiv 0,3,4 \pmod 5, \\ 7/6 & \text{if } m = 7 \text{ and } r \equiv 0,3,4,5,6 \pmod 7, \\ 3/2 & \text{if } m = 9 \text{ and } r \equiv 0,3,6 \pmod 9. \end{cases}$$

The main result of this thesis is to establish an average cyclicity result over torsion families of elliptic curves. For a rational number $a = r/s$ with $\gcd(r,s) = 1$, denote by $ht(a) = \max\{|r|, |s|\}$.

Theorem 5. Let $\epsilon > 0$, $A > x^{1+\epsilon}$, $B > 1$. Let $E_m(a)$ denote the parameterization of elliptic curves over $\mathbb{Q}$ which have a rational m-torsion point for $m \neq 2, 3$. Then

$$\frac{1}{\#\{a \in \mathbb{Q} : ht(a) \le A\}} \sideset{}{'}\sum_{ht(a) \le A} \pi^{cyc}_{E_m(a)}(x) = C_m \prod_{\ell \nmid m} \left(1 - \frac{1}{\ell(\ell-1)(\ell^2-1)}\right) \pi(x) + O\left(\frac{x}{\log^B x}\right)$$

where

$$C_m = \prod_{\ell \mid m} \left(1 - \frac{1}{\ell(\ell-1)}\right).$$

Remark 1. Every elliptic curve over $\mathbb{Q}$ with a rational m-torsion point is isomorphic to $E_m(a)$ for some $a \in \mathbb{Q}$; however, it is not true that every such curve is isomorphic to $E_m(a)$ where $a \in \mathbb{Z}$. Consider for example the curve $E_5(3/2)$ defined by the Weierstrass equation

$$E_5(3/2) : y^2 + \frac{1}{2}xy - \frac{3}{2}y = x^3 - \frac{3}{2}x^2.$$

As we explain in Section 3.2 this curve is only isomorphic to one other curve in the 5-torsion family, namely

$$E_5(-2/3) : y^2 + \frac{5}{3}xy + \frac{2}{3}y = x^3 + \frac{2}{3}x^2$$

given by parameter -2/3. In Theorem 5, we have taken the average over the entire torsion family, not just those given by integer parameters. We remark that the same asymptotic holds when the average is taken over curves given by integer parameters.

Remark 2. The effect of the presence of m-torsion is apparent; we interpret the constant C_{cyc} as a product of local factors, each of which is the probability that E_p has cyclic ℓ-torsion. The presence of a point of order m should have some influence on these probabilities for $\ell \mid m$. Indeed, a curve with a point of order ℓ over $\mathbb{Q}$ need only acquire a single linearly independent point of order ℓ for cyclicity of the reduction to fail. Compared to the generic case of a curve without a point of order ℓ, we expect it to be much less likely that the reductions of these curves are cyclic. Our result quantifies this heuristic reasoning.

A key ingredient for the argument in [4] was the fixed-field count of Vlăduţ [36] which, for a finite field of q elements, estimates the number of $E/\mathbb{F}_q$ which have cyclic group structure. Our result requires an analogous fixed field count which takes into account the additional torsion data which we state below.

It is frequently convenient to express counts of elliptic curves over finite fields as weighted cardinalities where we weight each curve by the size of its automorphism group. We indicate weighted cardinalities by $\#'$.

For a prime number ℓ, denote by $v_\ell(n)$ the ℓ-adic valuation of n. Concretely, any positive integer n can be written $n = \ell^e m$ where $\ell \nmid m$ and $e \geq 0$. Then $v_\ell(n) = e$.

Theorem 6. Denote by

$$C_m(q) = \{E/\mathbb{F}_q : E(\mathbb{F}_q) \text{ is cyclic and contains a point of order } m\}/_{\cong_{\mathbb{F}_q}}.$$

Then

$$\#'C_m(q) = q \prod_{\substack{\ell \mid m \\ q \equiv 1 \ (\mathrm{mod}\ \ell)}} \frac{1}{\ell^{v_\ell(m)}} \prod_{\substack{\ell \mid m \\ q \not\equiv 1 \ (\mathrm{mod}\ \ell)}} \frac{1}{\varphi\left(\ell^{v_\ell(m)}\right)} \prod_{\substack{\ell \nmid m \\ q \equiv 1 \ (\mathrm{mod}\ \ell)}} \left(1 - \frac{1}{\ell(\ell^2 - 1)}\right) + O\left(q^{1/2}\right).$$

This Theorem is a special case of a more general theorem that counts the number of elliptic curves $E/\mathbb{F}_q$ which contain a subgroup isomorphic to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ but which have cyclic ℓ-torsion for all primes $\ell \nmid n$. We prove this result in Chapter Three.

Chapter 2

Preliminaries

In this chapter, we recall the necessary background from algebraic number theory and the theory of elliptic curves. Proofs of the assertions in this section may be found, for example, in [29].

2.1 Number fields

We are primarily concerned with quadratic extensions, but as it requires no extra effort, we recall the theory of number fields before specializing to degree 2. A number field K is a finite algebraic extension of the rational numbers. The *ring of integers* $\mathcal{O}_K$ is the subring of all elements of K which satisfy a monic polynomial with coefficients in $\mathbb{Z}$. The critical property of $\mathcal{O}_K$ is that it is a *Dedekind domain* which implies that every non-zero ideal $\mathfrak{a} \subset \mathcal{O}_K$ factors as a product of prime ideals which is unique up to reordering factors;

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}. \tag{2.1}$$

Let $p \in \mathbb{Z}$ be prime. Then the ideal $p\mathcal{O}_K$ has a factorization as in (2.1); we say that any prime ideal $\mathfrak{p}$ in this factorization *lies above* p, and we say that p *lies below* $\mathfrak{p}$. If any e_i is greater than 1, we say that p is ramified in $\mathcal{O}_K$ and that e_i is the *ramification index* of $\mathfrak{p}_i$ over p. If all e_i are equal to 1, we say that p is unramified in $\prime_K$.

One consequence of the fact that $\mathcal{O}_K$ is a Dedekind domain is that every prime ideal is maximal. Thus, for any prime ideal $\mathfrak{p} \subset \mathcal{O}_K$, we have that $\mathcal{O}_K/\mathfrak{p}$ is a field. In fact, this field is a finite degree extension of $\mathbb{Z}/p\mathbb{Z}$ where $p = \mathfrak{p} \cap \mathbb{Z}$ is the unique rational prime lying below $\mathfrak{p}$. The cardinality of $\mathcal{O}_K/\mathfrak{p}$ is the *norm* of $\mathfrak{p}$, and the degree $[\mathcal{O}_K : \mathfrak{p}/\mathbb{Z}/p\mathbb{Z}]$ of the extension is called the inertial degree of $\mathfrak{p}$. By *degree f primes*, we mean the set of all prime ideals of $\mathcal{O}_K$ whose inertial degree is exactly f.

For $p \in \mathbb{Z}$, the ramification indices and inertial degrees of the prime ideals appearing in the factorization (2.1) of $p\mathcal{O}_K$ satisfy the identity

$$[K : \mathbb{Q}] = \sum_{i=1}^{g} e_i f_i.$$

In the case where $K/\mathbb{Q}$ is Galois, it turns out that all ramification indices are equal and all inertial degrees are equal for the primes lying above p. Thus, the identity above becomes

$$[K : \mathbb{Q}] = efg.$$

For any number field $K/\mathbb{Q}$ there are only finitely many primes that ramify in K since a ramified prime must divide a numerical invariant associated to K called the *discriminant* of K. If $e = f = 1$, we say that the prime p *splits completely* in K, while if $e = g = 1$, we say that p is inert in K.

A quadratic field K is a number field with $[K : \mathbb{Q}] = 2$. All such fields arise by adjoining to $\mathbb{Q}$

the square root of a squarefree integer dj, i.e., $K = \mathbb{Q}(\sqrt{d})$. Since the conjugate root is also an element of the field, all quadratic fields are Galois extensions of $\mathbb{Q}$. Since the degree of the extension is prime, each rational prime p is either totally split, inert, or totally ramified. As mentioned above, there are finitely many ramified primes, but the sets of split primes and inert primes are both infinite. Indeed, $p \in \mathbb{Z}$ is split if and only if the Legendre symbol $\left(\frac{d}{p}\right)$ is equal to 1. By applying the law of Quadratic Reciprocity, this condition can be turned into congruence conditions modulo the discriminant of K. For example, in $K = \mathbb{Q}(\sqrt{-3})$, a prime p splits if and only if $\left(\frac{-3}{p}\right) = 1$. Since $-3 \equiv 1 \pmod 4$, this happens if and only if $\left(\frac{p}{-3}\right) = 1$. Since the squares modulo 3 are 0 and 1 we conclude that p splits in K if and only if $p \equiv 1 \pmod 3$.

In order to count elements the number field K, we define a (naïve) height function as follows. Fix a basis $\{e_1 \dots e_n\}$ for $K/\mathbb{Q}$. Then for each element $\alpha \in K$, we write

$$ht(\alpha) = ht(a_1e_1 + \ldots + a_ne_n) = \max\{ht(a_1), \ldots, ht(a_n)\}$$

where for a rational number q/r with $\gcd(q, r) = 1$, $ht(q/r) = \max\{\mid q \mid, \mid r \mid\}$.

2.2 Elliptic curves

We refer to [33] for the basic properties of elliptic curves.

Let K be a field; an elliptic curve defined over K is a smooth protective curve curve of genus 1 with a distinguished K-rational point O. For the purposes of this work, it will suffice to consider an elliptic curve as the zero locus of a Weierstrass equation, that is, an equation of the form

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

where the coefficients a_i belong to K, with the understanding that there is one extra point at infinity. As long as the characteristic of K is not equal to 2 or 3, we may, by a change of variables, consider E as the zero set of a short Weierstrass equation

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

for some $a, b \in K$ such that $\Delta_{a,b} = -16(4a^3 + 27b^2) \neq 0$. The quantity $\Delta_{a,b}$ is called the *discriminant* of $E_{a,b}$. The discriminant is a basic invariant of the Weierstrass equation (though not of elliptic curves).

Denote by $E(K)$ the set of K-rational points of E. It is well-known that $E(K)$ has the structure of an abelian group; determining its structure is a central problem in the study of elliptic curves. We are especially concerned with the case where $K = \mathbb{Q}$ and $K = \mathbb{F}_q$; next we recall general facts about $E(K)$ in these cases.

In the case where K is a number field, the Mordell-Weil Theorem states that E is a finitely generated abelian group, that is, $E(K) \cong \mathbb{Z}^r \oplus E(K)_{\text{tors}}$ where r is a non-negative integer, called the *rank* of E, and $E(K)_{\text{tors}}$ is a finite abelian group. We will be especially concerned with $E(K)_{\text{tors}}$ which is called the *torsion subgroup* of $E(K)$.

For any elliptic curve E, the multiplication-by-m map which acts by $P \mapsto m \cdot P$ is an endomorphism. Thus, we always have $\mathbb{Z} \hookrightarrow \operatorname{End} E$. For an elliptic curve E/K with $\operatorname{char}(K) = 0$, we say that E has *complex multiplication* if the endomorphism ring of E is strictly larger than $\mathbb{Z}$.

We denote by $E[m]$ the m-division points of E. These are the points of E defined over an algebraic closure of K which are annihilated by multiplication by m. We also denote by $E[m](K) = E[m] \cap E(K)$. It is well-known that $E[m] = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ as an abstract group when $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) \nmid m$, and when $\mathrm{char}(K) = p$, the p-power torsion is always cyclic, see [33, Corollary 6.4]. Since $E(K)_{\mathrm{tors}}$ can be written as the direct sum of the subgroups $E(K)[\ell]$, it follows from the Mordell-Weil theorem that when K is a number field, $E(K)_{\mathrm{tors}}$ is isomorphic to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ for some integers $m \mid n$.

In the case of $K = \mathbb{Q}$, Mazur's Torsion Theorem describes the possibilities for the group $E(K)_{\mathrm{tors}}$.

Theorem 7 (Mazur)**.** Let $E/\mathbb{Q}$ be an elliptic curve; then $E(\mathbb{Q})_{\mathrm{tors}}$ is isomorphic to one of $\mathbb{Z}/m\mathbb{Z}$ for $m = 1 - 10, 12$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ for $m = 1 - 4$.

It follows from Mazur's theorem that if $E/\mathbb{Q}$ has a rational point of order $m \geq 2$, then $m \in \{2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$. The elliptic curves $E/\mathbb{Q}$ that have a rational point of order $m \geq 4$ lie in a one-parameter family; these were described by Kubert [28] and are given in Table 2.1.

m	$E_m(a)$
4	$y^2 + xy - ay = x^3 - ax^2$
5	$y^2 + (1-a)\,xy - ay = x^3 - ax^2$
6	$y^2 + (1-a)\,xy - (a^2+a)\,y = x^3 - (a^2+a)\,x^2$
7	$y^2 + (1+a-a^2)\,xy + (a^2-a^3)\,y = x^3 + (a^2-a^3)\,x^2$
8	$y^2 + \left(\frac{-2a^2+4a-1}{a}\right) xy + \left(-2a^2+3a-1\right) y = x^3 + \left(-2a^2+3a-1\right) x^2$
9	$y^2 + (1+a^2-a^3)\,xy + (a^2-2a^3+2a^4-a^5)\,y = x^3 + (a^2-2a^3+2a^4-a^5)\,x^2$
10	$y^2 + \left(\dfrac{2a^3-2a^2-2a+1}{a^2-3a+1}\right) xy + \left(\dfrac{-2a^5+3a^4-a^3}{a^4-6a^3+11a^2-6a+1}\right) y$ $= x^3 + \left(\dfrac{-2a^5+3a^4-a^3}{a^4-6a^3+11a^2-6a+1}\right) x^2$
12	$y^2 + \left(\dfrac{6a^4-8a^3+2a^2+2a-1}{a^3-3a^2+3a-1}\right) xy + \left(\dfrac{-12a^6+30a^5-34a^4+21a^3-7a^2+a}{a^4-4a^3+6a^2-4a+1}\right) y$ $= x^3 + \left(\dfrac{-12a^6+30a^5-34a^4+21a^3-7a^2+a}{a^4-4a^3+6a^2-4a+1}\right) x^2$

Table 2.1: Parameterizations for elliptic curves with m-torsion.

The discriminant $\Delta_m(a)$ of the curve $E_m(a)$ given above is

$$\begin{aligned}
\Delta_4(a) &= (16a+1)a^4 \\
\Delta_5(a) &= a^5(a^2-11a-1) \\
\Delta_6(a) &= (9a+1)(a+1)^3a^6 \\
\Delta_7(a) &= (a-1)^7a^7(a^3-8a^2+5a+1) \\
\Delta_8(a) &= a^{-4}(2a-1)^4(a-1)^8(8a^2-8a+1) \\
\Delta_9(a) &= (a-1)^9a^9(a^2-a+1)^3(a^3-6a^2+3a+1) \\
\Delta_{10}(a) &= (2a-1)^5(a-1)^{10}a^{10}(a^2-3a+1)^{-10}(4a^2-2a-1) \\
\Delta_{12}(a) &= (a-1)^{-24}(2a-1)^6a^{12}(6a^2-6a+1)(2a^2-2a+1)^3(3a^2-3a+1)^4.
\end{aligned}$$

In the case where K is a finite field $\mathbb{F}_q$, we obviously have that $E(K)$ is a finite abelian group. Thus $E(K) \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ for positive integers $m \mid n$. Furthermore, the Hasse bound restricts the order mn of the group $E(K)$. Denote by $a_q(E) = q + 1 - \#E(K)$. Then $\mid a_q(E) \mid \leq 2\sqrt{q}$. The quantity $a_q(E)$ is called the *trace of Frobenius*; it is precisely the trace of the endomorphism of E defined by

$$(x, y) \mapsto (x^q, y^q).$$

Much more detail is known about the structure of the group $E(\mathbb{F}_q)$; we will end this section by mentioning the following property which is particularly relevant to our discussion; for a prime number ℓ, an elliptic curve $E/\mathbb{F}_q$ has $E[\ell] \subseteq E(\mathbb{F}_q)$ only if $\ell \mid q - 1$.

2.2.1 Galois representations

Throughout this section, let E be an elliptic curve over $\mathbb{Q}$, and let m be a positive integer. We denote by $\mathbb{Q}(E[m])$ the field extension obtained by adjoining to $\mathbb{Q}$ the x and y-coordinates of all points of $E[m]$, and we denote by $G_m(E)$ the Galois group of $\mathbb{Q}(E[m])/\mathbb{Q}$. Note that by fixing a basis for $E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, we may view $G_m(E)$ as a subgroup of $\mathrm{GL}_2\left(\mathbb{Z}/n\mathbb{Z}\right)$.

Let $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ be the absolute Galois group. Then $G_{\mathbb{Q}}$ acts on $E[m]$. Fixing a basis, this yields a Galois representation

$$\rho_{E,m} : G_{\mathbb{Q}} \to \mathrm{GL}_2\left(\mathbb{Z}/m\mathbb{Z}\right).$$

By taking the inverse limit over all positive integers, we obtain a continuous homomorphism

$$\rho_E : G_{\mathbb{Q}} \to \mathrm{GL}_2\left(\hat{\mathbb{Z}}\right).$$

Serre proved that the image of this Galois representation is an open subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$.

Theorem 8 (Serre's Open Image Theorem)**.** Suppose that E is a non-CM elliptic curve defined over $\mathbb{Q}$. Then the index $[\mathrm{GL}_2(\hat{\mathbb{Z}}) : \rho_E(G_{\mathbb{Q}})]$ is finite.

In fact, Serre proved that the image of the absolute Galois group always sits in an index two subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ which leads to the following definition. A *Serre curve* is an elliptic curve where the image of Galois is as large as possible, i.e., an elliptic curve such that the index $[\mathrm{GL}_2(\hat{\mathbb{Z}}) : \rho_E(G_{\mathbb{Q}})]$ is equal to 2. Serre curves are in a certain sense typical elliptic curves; Jones [22] proved that Serre curves form a density one subfamily of all elliptic curves.

A consequence of Serre's open image theorem is that there exists a positive integer m such that $\rho_E(G_{\mathbb{Q}}) = \pi^{-1}(G_m(E))$ where π denotes the natural projection map

$$\pi : GL_2(\hat{\mathbb{Z}}) \to GL_2(\mathbb{Z}/m\mathbb{Z}).$$

For a non-CM curve E, denote by m_E the smallest such integer m. We will call m_E Serre's constant (corresponding to the curve E). This constant has the property that for any integers m_1 and m_2 where $m_1 \mid m_E$ and $\gcd(m_1, m_E) = 1$, we have

$$G_{m_1 m_2} \cong G_{m_1} \times \mathrm{GL}_2(\mathbb{Z}/m_2\mathbb{Z}) \tag{2.2}$$

That is, the Galois representation obtained by letting the absolute Galois group act on $E[m]$ is surjective for m relatively prime to m_E.

2.2.2 The cyclicity constant

The existence of Serre's constant along with the identity (2.2) are critical because the constants corresponding to cyclicity and Lang-Trotter are phrased in terms of the corresponding

Galois representations. In the case of cyclicity we have

$$C_E^{cyc} = \sum_{n \geq 1} \frac{\mu(n)}{[\mathbb{Q}(E[n]) : \mathbb{Q}]}.$$

This constant is derived from the fact that for a prime p of good reduction for E and a prime $\ell \neq p$, the group of $\mathbb{F}_p$-rational points of E_p contains $E_p[\ell]$ if and only if p splits completely in $\mathbb{Q}(E[\ell])$; the inclusion-exclusion principle, together with the Chebotarev Density Theorem yield this expression for C_E^{cyc}, see [9, Section 2].

When E does not have complex multiplication, we apply (2.2) to write

$$\begin{aligned} C_E^{cyc} &= \left(\sum_{n \mid m_E} \frac{\mu(n)}{[\mathbb{Q}(E[n]) : \mathbb{Q}]} \right) \cdot \prod_{\ell \nmid m_E} \left(1 - \frac{1}{\# \operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})} \right) \\ &= \left(\sum_{n \mid m_E} \frac{\mu(n)}{[\mathbb{Q}(E[n]) : \mathbb{Q}]} \right) \cdot \prod_{\ell \nmid m_E} \left(1 - \frac{1}{\ell(\ell-1)^2(\ell+1)} \right). \end{aligned}$$

Jones proved that the average of the constants C_E^{cyc} for elliptic curves E taken over the family of Serre curves is

$$C^{cyc} = \prod_{\ell \text{prime}} \left(1 - \frac{1}{\ell(\ell-1)^2(\ell+1)} \right).$$

This is the same constant that appears in the average of the prime counting functions π_E^{cyc} obtained by Banks and Shparlinski in Theorem 3. This constant may be viewed as a product of local factors, each one being the probability that the Frobenius endomorphism of the reduction of E modulo p lies in a given conjugacy class. Indeed, when $\ell \nmid m_E$, $\varphi_{E,\ell}$ is surjective. In this case, the only way that E_p can fail to have cyclic ℓ-torsion is that $E_p[\ell] \subseteq E_p(\mathbb{F}_p$. Thus, the there is but one possibility for the matrix of Frobenius; since Frobenius fixes the points of E_p, it fixes the ℓ torsion points of E_p, so the matrix representation of Frobenius obtained by fixing a basis for $E_p[\ell]$ is the identity. Therefore, the probability that E_p has cyclic ℓ-torsion is $1 - 1/(\ell(\ell-1)^2(\ell+1))$.

In this thesis, we study the functions π_E^{cyc} for elliptic curves $E/\mathbb{Q}$ which have a point of order m. Suppose that E is such a curve; it seems natural to expect that the presence of a point of order m on E should reduce the likelihood that $E_p(\mathbb{F}_p)$ is cyclic. Indeed, for a prime $p \geq 3$ that does not divide the discriminant of E, we have that $E(\mathbb{Q})_{\text{tors}}$ injects into $E_p(\mathbb{F}_p)$, [27] Theorem 5.1]. Thus, for any prime factor $\ell \mid m$, in order that $E_p[\ell] \subset E_p(\mathbb{F}_p)$, our curve need only acquire one linearly independent point of order ℓ after reduction modulo p instead of the two points that would be required if we had started with an elliptic curve without a point of order ℓ.

The vague heuristic of the preceding paragraph is made more precise by considering the image of the homomorphism $\rho_{E,\ell}$. Fix a basis for the ℓ torsion of E_p where the first point is defined over $\mathbb{F}_p$. Then the image of $\rho_{E,\ell}$ lies inside the subgroup $H \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ described below:

$$H = \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} : b \neq 0 \right\}.$$

The subgroup H has order $\ell^2 - \ell$, and again, the only way that E_p can fail to be cyclic if the matrix of Frobenius is the identity. Thus, the probability that E_p has cyclic ℓ torsion is

$$1 - \frac{1}{\ell(\ell-1)}.$$

A quick calculation shows that the difference between the probability that E_p has cyclic ℓ torsion and the probability that E_p has cyclic ℓ torsion given that $E(\mathbb{Q})$ has a point of order

ℓ is

$$\begin{aligned} 1 - \frac{1}{\ell(\ell-1)^2(\ell+1)} - \left(1 - \frac{1}{\ell(\ell-1)}\right) &= \frac{\ell^2-1}{\ell(\ell-1)^2(\ell+1)} - \frac{1}{\ell(\ell-1)^2(\ell+1)} \\ &= \frac{\ell^2-2}{\ell(\ell-1)^2(\ell+1)}. \end{aligned}$$

Viewing the factors of C^{cyc} as a product of local probabilities allows us to make a prediction for the constant that will appear when we average over curves in torsion families. Namely, we expect that the average over curves with a rational point of order m defined over $\mathbb{Q}$ will be

$$C^{cyc}(m) = \prod_{\ell | m} \left(1 - \frac{1}{\ell(\ell-1)}\right) \prod_{\ell \nmid m} \left(1 - \frac{1}{\ell(\ell-1)^2(\ell+1)}\right).$$

We prove that this is, indeed, the correct average constant for curves in this family.

Remark 3. One would expect that, as in the case of the family of all elliptic curves, the average constant for the family of m-torsion curves will be the average of the constants C_E^{cyc} as E varies through curves with a point of order m. Jones' proof that C^{cyc} is the average of the constants C_E^{cyc} relied on the fact that most elliptic curves are Serre curves. However, a Serre curve has trivial torsion, so Jones' technique of reducing the study to the case of Serre curves does not directly apply to torsion families. We would require a generalization of the notion of Serre curve to these families. That is, a 'Serre curve in the m-torsion family' should be a curve whose image of Galois is as large as possible given the constraint imposed by having a point of order m. It would be of interest to show that the image of Galois for elliptic curves in torsion families is "*aussi gros que possible.*"

Chapter 3

Fixed field counts and isomorphism counts

In this chapter, we obtain estimates for the number of elliptic curves $E/\mathbb{F}_q$ which have a given subgroup but which are 'as cyclic as possible.' We also count the number of parameters $b \in \mathbb{F}_q$ such that $E_m(b)$ is isomorphic to $E_m(a)$.

3.1 Fixed field count

There has been significant recent interest in counting problems for elliptic curves over a fixed finite field $\mathbb{F}_q$ with specified conditions on their group of $\mathbb{F}_q$-rational points. See for example Howe, [17], Vlăduţ [36], Castryck and Hubrechts [7] and Kaplan and Petrow [25].

Our goal is to generalize Vlăduţ's result giving the number of elliptic curves $E/\mathbb{F}_q$ such that $E(\mathbb{F}_q)$ is cyclic to obtain a count of the number of $E/\mathbb{F}_q$ such that for some fixed $m, n \in \mathbb{Z}$,

$E(\mathbb{F}_q)$ contains a subgroup isomorphic to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, and for all $\ell \nmid n$, $E(\mathbb{F}_q$ has cyclic ℓ-torsion. Following Vlăduţ, our proof is based on the inclusion-exclusion principle and relies on estimates provided by Howe. We begin by recalling the required notation and results.

Denote by φ the Euler totient function, and define $\psi(n) = n\prod_{l|n}(1+1/l)$. For $a \mid b$, denote by $W(a,b) = \{E/\mathbb{F}_q : E[b](\mathbb{F}_q) \cong (\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z})\}/_{\cong \mathbb{F}_q}$. Estimates for the size of $W(a,b)$ are given by Howe [17]. Howe shows that

$$\mid \#' W(a,b) - \hat{w}(a,b) \mid < Cq^{1/2}$$

for an explicit constant C where

$$\hat{w}(a,b) = \frac{q\psi(b/a)}{a\varphi(b)\psi(b)} \prod_{\ell | \gcd(b,q-1)/b} \left(1 - \frac{1}{\ell}\right).$$

It will also be convenient to define $\tilde{w}(a,b) = \hat{w}(a,b)/q$. Howe notes that $\tilde{w}(a,b)$ is a multiplicative function of both arguments simultaneously.

Vlăduţ observes the following 'obvious' cyclicity condition: $E(\mathbb{F}_q)$ is cyclic if and only if for any prime $\ell \mid q-1$, $E \notin W(\ell,\ell)$. Now let us assume that $E/\mathbb{F}_q$ is an elliptic curve such that the n-torsion subgroup of E is isomorphic to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. We observe that $E(\mathbb{F}_q)$ is as cyclic as possible given this condition if and only if for all $\ell \mid q-1$, with $\ell \nmid n$, we have $E \notin W(\ell m, \ell n)$. Denote by

$$\mathcal{E}_{m,n}(q) = \{E/\mathbb{F}_q : E[n](\mathbb{F}_q) \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \text{ and } \ell \nmid n \Rightarrow E[\ell] \not\subseteq E(\mathbb{F}_q)\}/_{\cong \mathbb{F}_q};$$

We are now ready to state and prove our theorem.

Theorem 9. The weighted cardinality of $\mathcal{E}_{m,n}(q)$ is

$$q\frac{\psi(n/m)}{m\varphi(n)\psi(n)}\prod_{\ell|\gcd(n,q-1)/m}\left(1-\frac{1}{\ell}\right)\prod_{\substack{\ell|q-1\\ \ell\nmid n}}\left(1-\frac{1}{\ell(\ell^2-1)}\right)+O\left(q^{1/2}\right)$$

if $m \mid q-1$, and it is 0 otherwise.

Proof. We have already observed in the previous chapter that $m \mid q-1$ is a necessary condition for there to exist an elliptic curve over $\mathbb{F}_q$ with full m-torsion, so assume this to be the case.

We proceed by inclusion-exclusion, following [36]. We have

$$\begin{aligned}
\#'\mathcal{E}_{m,n}(q) &= \#'W(m,n)+\sum_{\substack{d|q-1\\ \gcd(n,d)=1}}\mu(d)\#'W(md,nd)\\
&= \hat{w}(m,n)+\sum_{\substack{d|q-1\\ \gcd(n,d)=1}}\mu(d)\hat{w}(md,md)+O\left(q^{1/2}\right)\\
&= q\tilde{w}(m,n)\left(1+\sum_{\substack{d|q-1\\ \gcd(n,d)=1}}\mu(d)\tilde{w}(d,d)\right)+O\left(q^{1/2}\right)\\
&= q\tilde{w}(m,n)\prod_{\substack{\ell|q-1\\ \ell\nmid n}}\left(1-\frac{1}{\ell(\ell^2-1)}\right)+O\left(q^{1/2}\right)\\
&= q\frac{\psi(n/m)}{m\varphi(n)\psi(n)}\prod_{\ell|\gcd(n,q-1)/m}\left(1-\frac{1}{\ell}\right)\prod_{\substack{\ell|q-1\\ \ell\nmid n}}\left(1-\frac{1}{\ell(\ell^2-1)}\right)+O\left(q^{1/2}\right).
\end{aligned}$$

□

Example 3.1. Taking $m = n = 1$, we recover Vlăduţ's result.

Example 3.2. Let n'_q be the prime to $q-1$ part of n, and let $n_q = n/n'_q$. Then in the case where $m = 1$, we have

$$\#'\mathcal{E}_{1,n} = \frac{1}{n_q \varphi(n'_q)} \prod_{\substack{\ell \mid q-1 \\ \ell \nmid n}} \left(1 - \frac{1}{\ell(\ell^2 - 1)}\right) + O\left(q^{1/2}\right).$$

This estimate will be used in Chapter 5.

Example 3.3. Now suppose that $n = m$. Then we have

$$\#'\mathcal{E}_{n,n} = \frac{1}{n\varphi(n)\psi(n)} \prod_{\substack{\ell \mid q-1 \\ \ell \nmid n}} \left(1 - \frac{1}{\ell(\ell^2 - 1)}\right) + O\left(q^{1/2}\right).$$

This estimate will be used in Chapter 6.

3.2 Parameters yielding isomorphic curves

The parameterizations given in Table 2.1 were derived by Kubert by studying the modular curve $X_1(m)$. A point of $X_1(m)$ corresponds to an elliptic curve E together with a point of order m up to action by automorphisms of E. For example, if (E, P) represents a point of $X_1(m)$ and $\#\mathrm{Aut}_{\mathbb{F}_q}(E) = 2$, then $(E, -P)$ represents the same point. We will be concerned with which parameter values yield isomorphic curves over $\mathbb{F}_q$ where $q = p^n$ and $p > 3$. With at most 10 exceptions, an isomorphism class of elliptic curves over $\mathbb{F}_q$ consists of curves whose automorphism group has cardinality 2. If $\#\mathrm{Aut}_{\mathbb{F}_q}(E_m(a)) = 2$, there are $\varphi(m)/2$ values $b \in \mathbb{F}_q$ such that $E_m(b) \cong E_m(a)$. These correspond to the $\varphi(m)$ points of order m on $E_m(a)$, up to the action of of $\mathrm{Aut}_{\mathbb{F}_q}(E_m(a))$.

If $\#\mathrm{Aut}_{\mathbb{F}_q}(E) > 2$, the number of parameters yielding an isomorphic curve will vary depending on the size of the automorphism group and the number of m-torsion points of E; in general, the number of parameters which yield an isomorphic curve will not be $\varphi(m)/2$. However, these $O(1)$ isomorphism classes can be absorbed into the 'unweighted' version of Theorem 6.

Corollary 1 (to Theorem 6)**.**

$$C_m(q) = 2q \prod_{\substack{\ell \mid m \\ q \equiv 1 \ (\mathrm{mod}\ \ell)}} \frac{1}{\ell^{v_\ell(m)}} \prod_{\substack{\ell \mid m \\ q \not\equiv 1 \ (\mathrm{mod}\ \ell)}} \frac{1}{\varphi(\ell^{v_\ell(m)})} \prod_{\substack{\ell \nmid m \\ q \equiv 1 \ (\mathrm{mod}\ \ell)}} \left(1 - \frac{1}{\ell(\ell^2-1)}\right) + O\left(q^{1/2}\right).$$

Proof. Denote by $C_m(q,n) = \{E \in C_m(q) \colon \#\mathrm{Aut}(E) = n\}$. Then

$$C_m(q) = C_m(q,2) + C_m(q,4) + C_m(q,6) + C_m(q,12) + C_m(q,24).$$

We then have

$$\frac{\#C_m(q,2)}{2} = \#' C_m(q) - \frac{\#C_m(q,4)}{4} - \frac{\#C_m(q,6)}{6} - \frac{\#C_m(q,12)}{12} - \frac{\#C_m(q,24)}{24}.$$

Multiplying by 2 and applying Theorem 6 and the fact that $\#C_m(q,4)/2 - \#C_m(q,6)/3 - \#C_m(q,12)/6 - \#C_m(q,24)/12 = O(1)$, we have

$$\#C_m(q,2) = 2q \prod_{\substack{\ell \mid m \\ q \equiv 1 \ (\mathrm{mod}\ \ell)}} \frac{1}{\ell^{v_\ell(m)}} \prod_{\substack{\ell \mid m \\ q \not\equiv 1 \ (\mathrm{mod}\ \ell)}} \frac{1}{\varphi(\ell^{v_\ell(m)})} \prod_{\substack{\ell \nmid m \\ q \equiv 1 \ (\mathrm{mod}\ \ell)}} \left(1 - \frac{1}{\ell(\ell^2-1)}\right) + O\left(q^{1/2}\right),$$

which completes the proof. □

Given an m-torsion curve $E_m(a)$, we can (outside of characteristic 2 or 3) perform a change of variables to obtain a short Weierstrass equation $y^2 = x^3 + Ax + B$. In order for $E_m(a)$ to have more than two automorphisms, the j-invariant must be 0 or 1728. In terms of the short Weierstass equation, this means that $A = 0$ or $B = 0$, respectively. The coefficients A and B will be polynomials or rational functions in the parameter a. Since such functions have finitely many zeros, we deduce the following

Lemma 1. For any field K, there are finitely many parameters a such that $j((E_m(a)) = 0$ or 1728. The parameters which yield curves with these j-invariants are the roots of a polynomial that depends only on m.

Using explicit change of variables, it is possible to specify precisely which parameter values yield isomorphic curves. If $\#\mathrm{Aut}_{\mathbb{F}_q}(E_m(a)) = 2$, then $E_m(a) \cong E_m(b)$ for precisely the b appearing in Table 3.1.

m	Parameters		
4	a		
5	a		$-a^{-1}$
6	a		
7	a	$(1-a)a^{-1}$	$-(1-a)^{-1}$
8	a	$-a+1$	
9	a	$(a-1)a^{-1}$	$-(a-1)^{-1}$
10	a	$(a-1)(2a-1)^{-1}$	
12	a	$-a+1$	

Table 3.1: Parameters yielding isomorphic curves.

Chapter 4

Reductions of rational numbers modulo p

The elliptic curves we wish to study lie in one-parameter family. The authors of [5] took averages over the curves in torsion families given by integer parameters. However, not all curves in these families are isomorphic to one given by integer parameters, so it is natural to allow for non-integer parameters. In this chapter, we obtain estimates for the number of rational numbers up to height x which reduce modulo p to a given value. We begin with some lemmas.

4.1 Summing the normalized totient function

Consider the normalized totient function $\varphi(n)/n$; it is well-known (see, for example, [30]) that

$$\sum_{n\leq x}\frac{\varphi(n)}{n}=\frac{6}{\pi^2}x+O(\log(x)). \tag{4.1}$$

The proof exploits the identity

$$\frac{\varphi(n)}{n}=\sum_{d|n}\frac{\mu(d)}{d}$$

to deduce the exact formula

$$\sum_{n\leq x}\frac{\varphi(n)}{n}=\sum_{d\leq x}\frac{\mu(d)}{d}\sum_{\substack{n\leq x\\ d|n}}1.$$

In this section, we will prove three lemmas related to summing the normalized totient function over different subsets of the positive integers. Though elementary, these results are not easily found in the literature.

Lemma 2. Let p be prime. Then

$$\sum_{\substack{n\leq x\\ \gcd(n,p)=1}}\frac{\varphi(n)}{n}=\frac{p}{p+1}\frac{6}{\pi^2}x+O(\log(x)).$$

Remark 4. Neither here nor in the following lemmas have we tried to write the most general result; a similar result holds with composite modulus, due to Suryanarayana [34]. Nor have we tried to prove the best possible result since an error term of the form $O\left(\log(x)\right)$ is sufficient for our intended application.

Lemma 3. Let p be prime. Then

$$\sum_{\substack{n\leq x\\ p|n}} \frac{\varphi(n)}{n} = \frac{1}{p+1}\frac{6}{\pi^2}x + O(\log(x)).$$

Lemma 4. Let p be prime, and let r be relatively prime to p. Then

$$\sum_{\substack{n\leq x\\ n\equiv r \pmod p}} \frac{\varphi(n)}{n} = \frac{p}{p^2-1}\frac{6}{\pi^2}x + O(\log(x)).$$

Remark 5. The topic of estimating the sum of a multiplicative function over residue classes has seen extensive study, see for example [12], [16], [3]. Comparing the results of Lemmas 2 and 4 shows that a much better error term than that predicted by Theorem 1 of [12] holds for this function.

Below we use the notation $[x]$ to denote the floor of the real number x.

Proof of Lemma 2. We have

$$\begin{aligned}\sum_{\substack{n\leq x\\ \gcd(n,p)=1}} \frac{\varphi(n)}{n} = \sum_{\substack{n\leq x\\ \gcd(n,p)=1}} \sum_{d|n} \frac{\mu(d)}{d} &= \sum_{\substack{d\leq x\\ p\nmid d}} \frac{\mu(d)}{d} \sum_{\substack{n\leq x\\ d|n\\ p\nmid n}} 1 \\ &= \sum_{\substack{d\leq x\\ p\nmid d}} \frac{\mu(d)}{d} \left[\frac{x}{d}\right] \frac{p-1}{p} \\ &= x\frac{p-1}{p} \sum_{\substack{d\leq x\\ p\nmid d}} \frac{\mu(d)}{d^2} + O(\log x). \qquad (4.2)\end{aligned}$$

Now write

$$\sum_{\substack{d\leq x\\ p\nmid d}} \frac{\mu(d)}{d^2} = \sum_{\substack{d=1\\ p\nmid d}}^{\infty} \frac{\mu(d)}{d^2} - \sum_{\substack{d>x\\ p\nmid d}} \frac{\mu(d)}{d^2} = \sum_{\substack{d=1\\ p\nmid d}}^{\infty} \frac{\mu(d)}{d^2} + O\left(\frac{1}{x}\right).$$

From the Euler product expansion of $1/\zeta(s)$, we have that

$$\sum_{\substack{d=1\\ p\nmid d}}^{\infty} \frac{\mu(d)}{d^2} = \frac{6}{\pi^2}\frac{p^2}{p^2-1}.$$

Inserting this into (4.2) completes the proof. □

Proof of Lemma 3. We have

$$\sum_{\substack{n\leq x\\ p|n}} \frac{\varphi(n)}{n} = \sum_{\substack{n\leq x\\ p|n}}\sum_{d|n} \frac{\mu(d)}{d} = \sum_{d\leq x} \frac{\mu(d)}{d} \sum_{\substack{n\leq x\\ d|n\\ p|n}} 1 \tag{4.3}$$

$$= \sum_{\substack{d\leq x\\ p|d}} \frac{\mu(d)}{d}\left[\frac{x}{d}\right] + \sum_{\substack{d\leq x\\ p\nmid d}} \frac{\mu(d)}{d}\left[\frac{x}{pd}\right]. \tag{4.4}$$

We estimate these sums separately. For the first, we have

$$\sum_{\substack{d\leq x\\ p|d}} \frac{\mu(d)}{d}\left[\frac{x}{d}\right] = x\sum_{\substack{d\leq x\\ p|d}} \frac{\mu(d)}{d^2} + O(\log x) = x\left(\sum_{d\leq x} \frac{\mu(d)}{d^2} - \sum_{\substack{d\leq x\\ p\nmid d}} \frac{\mu(d)}{d^2}\right) + O(\log x).$$

Using (4.1) and the proof of Lemma 2, this becomes

$$\frac{6}{\pi^2}x - \frac{p^2}{p^2-1}\frac{6}{\pi^2}x + O(\log x) = \frac{-1}{p^2-1}\frac{6}{\pi^2}x + O(\log x).$$

For the second sum in (4.4), we have

$$\sum_{\substack{d\le x\\ p\nmid d}} \frac{\mu(d)}{d}\left[\frac{x}{pd}\right] = \frac{x}{p}\sum_{\substack{d\le x\\ p\nmid d}} \frac{\mu(d)}{d^2} + O(\log x). \tag{4.5}$$

Again appealing to the proof of Lemma 2, this is equal to

$$\frac{6x}{\pi^2}\frac{p}{p^2-1} + O(\log x) \tag{4.6}$$

and the lemma is proved.

$\square$

Proof of Lemma 4. We have

$$\begin{aligned}\sum_{\substack{n\le x\\ n\equiv r \pmod p}} \frac{\varphi(n)}{n} = \sum_{\substack{n\le x\\ n\equiv r \pmod p}} \sum_{d\mid n} \frac{\mu(d)}{d} &= \sum_{\substack{d\le x\\ p\nmid d}} \frac{\mu(d)}{d} \sum_{\substack{n\le x\\ d\mid n\\ n\equiv r \pmod p}} 1 &(4.7)\\ &= \sum_{\substack{d\le x\\ p\nmid d}} \frac{\mu(d)}{d}\left[\frac{x}{pd}\right] &(4.8)\\ &= \frac{x}{p}\sum_{\substack{d\le x\\ p\nmid d}} \frac{\mu(d)}{d^2} + O(\log x). &(4.9)\end{aligned}$$

Using the same steps as in Lemma 2, this becomes

$$\frac{x}{p}\left(\frac{6}{\pi^2}\right)\left(\frac{p^2}{p^2-1}\right) + O(\log x) = \left(\frac{p}{p^2-1}\right)\frac{6}{\pi^2}x + O(\log x),$$

as required. $\square$

4.2 Rational numbers reducing to a unit of $\mathbb{F}_p$

In order to study average problems for curves in torsion families, we need an estimate for the number of parameters that reduce modulo p to a given element of $\mathbb{F}_p$. In the case of integer parameters, this is straightforward since we get precisely one integer reducing to a given value modulo p inside each interval of length p.

When we consider reduction of *rational* numbers, the count is more subtle since out of the $4x^2$ possible pairs of integers that combine to give a positive rational number of height less than x, many pairs will yield the same number. We have two problems to keep track of; first, we must keep track of which pairs of integers (m, n) give distinct rational numbers, and second, we must ensure that we take pairs that reduce to a chosen value.

First, consider the case of reducing to a unit in $\mathbb{F}_p$. Let $t \in \mathbb{F}_p^\times$. There are $p-1$ ways of expressing t as a 'fraction,' namely, $t \equiv ab^{-1} \pmod{p}$ where b runs through the units of $\mathbb{F}_p$ and a is uniquely determined by b.

Fix such a pair $a, b \in \mathbb{F}_p^\times$; for each $r \in \mathbb{Z}$ that reduces to a, we want to compute the number of admissible denominators. That is, we wish to estimate the cardinality of the set

$$B(x; r, p) = \{s \leq x : s \equiv b \,(\mathrm{mod}\ p), \gcd(s, r) = 1\}.$$

This is easily accomplished by applying the inclusion-exclusion principle; denote by

$$A_d(x; r, p) = \{s \in B(x; r, p) : d \mid s\} = \{s \leq x : s \equiv b \,(\mathrm{mod}\ pd)\}.$$

Then we have

$$\#B(x;r,p)=\sum_{d|r}\mu(d)\#A_d(x;r,p).$$

Since $\#A_d(x;r,p)=\frac{x}{pd}+O(1)$, our estimate becomes

$$\#B(x;r,p)=\frac{x}{p}\sum_{d|r}\frac{\mu(d)}{d}+O(1)=\frac{x}{p}\frac{\varphi(r)}{r}+O(1). \tag{4.10}$$

According to Lemma 4, we conclude that the number of rationals of height bounded by x which reduce to r modulo p is

$$\frac{12x^2}{(p^2-1)\pi^2}+O(x\log x). \tag{4.11}$$

Applying this result for the $p-1$ possible values of a,b such that $ab^{-1}\equiv r \pmod{p}$, we obtain the desired estimate, which we record as a lemma.

Lemma 5. There are

$$\frac{12x^2}{(p+1)\pi^2}+O(x\log x) \tag{4.12}$$

rational numbers of height less than x which reduce modulo p to r.

4.3 Rational numbers reducing to zero

For the sake of completeness, we now we estimate the number of $a\in\mathbb{Q}$ of height less than x which reduce to 0 modulo p. Note that this result would be necessary if one wanted to study the reductions of an elliptic curve defined over a quadratic number field modulo a prime ideal of norm p^2.

Obviously the numerator of any such rational number is a multiple of p; if r is any admissible numerator (i.e., a multiple of p that is less than x), our task is to estimate the number of denominators. Similar to the previous case, we denote this set by

$$B(x; r, p) = \{s \leq x : \gcd(r, s) = 1\}.$$

As before, we use inclusion-exclusion to estimate the size of $B(x; r, p)$. Set

$$A_d(x; r, p) = \{s \in B(x; r, p) : d \mid s\}.$$

Then

$$\begin{aligned}
\#B(x; r, p) &= \sum_{d|r} \mu(d) \#A(x, r, p) \\
&= \sum_{d|r} \mu(d) \left(\frac{x}{d} + O(1) \right) \\
&= x \sum_{d|r} \frac{\mu(d)}{d} + O(1) \\
&= x \frac{\varphi(r)}{r} + O(1).
\end{aligned}$$

Summing over the multiples of p up to x and applying Lemma 3, we find the the number of positive and negative rational numbers of height less than x which reduce to zero modulo p is

$$\frac{12}{(p+1)\pi^2} x^2 + O(x \log x).$$

Chapter 5

Proof of main result

In this section we will prove Theorem 5; we begin with an overview. The key step is to turn a sum over elliptic curves of prime-counting functions into a sum over primes of elliptic curves counts; we have

$$\sum_{ht(a)\le A} \pi^{cyc}_{E_m(a)}(x) = \sum_{p\le x} \sum_{\substack{b\in\mathbb{F}_p \\ \Delta_m(b)\neq 0 \\ E_m(b)(\mathbb{F}_p)\text{ cyclic}}} \#\{a\in\mathbb{Q} : ht(a)\le A, E_m(a)_p \cong E_m(b)\}. \tag{5.1}$$

After applying the estimates of the preceding sections and some manipulation, we find that the expression for the main term is obtained by estimating the expressions

$$\sum_{\substack{p\le x \\ p\equiv 1 \ (\mathrm{mod}\ \ell_0)}} \prod_{\substack{\ell\mid p-1 \\ \gcd(\ell,m)=1}} \left(1-\frac{1}{\ell(\ell^2-1)}\right) \text{ and } \sum_{\substack{p\le x \\ p\not\equiv 1 \ (\mathrm{mod}\ \ell_0)}} \prod_{\ell\mid p-1} \left(1-\frac{1}{\ell(\ell^2-1)}\right).$$

We recognize the summands as a multiplicative function $F(n)$ evaluated on the sequence of shifted primes by setting

$$F(n) = \prod_{\substack{\ell | n \\ \gcd(\ell, m)=1}} \left(1 - \frac{1}{\ell(\ell^2-1)}\right)$$

Thus, we are left to evaluate the mean value of these multiplicative functions along the shifted primes which satisfy some congruence condition. This is accomplished by appealing to a technical result of Indlekofer, Weimeier, and Lucht.

The fixed field counts of $E/\mathbb{F}_p$ which have an m-torsion point and cyclic group of $\mathbb{F}_p$-points depends on the value of p modulo the prime divisors of m. For one-parameter torsion families over $\mathbb{Q}$, we are concerned with $m \in \{4, 5, 6, 7, 8, 9, 10, 12\}$. In this case, m has at most two prime divisors, and if m is not a prime power, then one of its prime factors is 2. Since all odd primes are $1 \pmod 2$, the number of curves we are counting varies according to the value of $p \pmod \ell$ where ℓ is the unique odd prime divisor of m.

Let $m \in \{4, 5, 6, 7, 8, 9, 10, 12\}$, and denote by

$$\mathcal{E}_m(A) = \{E_m(a) : ht(a) \leq A\}$$

the family of elliptic curves over $\mathbb{Q}$ with an m-torsion point given above. Write the prime factorization of m as $m = 2^k \ell_0^n$ where we take $n = \ell_0 = 1$ if m is a power of 2. Let $A \geq x^{1+\epsilon}$ for $x, \epsilon > 0$.

For convenience of notation, set

$$\mathcal{A}(p, m, n) = \{b \in \mathbb{F}_p \colon \Delta_m(b) \neq 0, E_m(b)(\mathbb{F}_p) \text{ cyclic}, \#\mathrm{Aut}(E_m(b)) = n)\}.$$

Continuing on from Equation (5.1) above, by Lemma 5, there are $\frac{12A^2}{(p+1)\pi^2} + O\left(A \log A\right)$ values of a up to height A which yield a particular Weierstrass model modulo p. Thus the expression above becomes

$$\begin{aligned}&\sum_{p\le x}\left(\frac{12A^2}{(p+1)\pi^2}+O\left(A\log A\right)\right)\left(\sum_{b\in\mathcal{A}(p,m,2)}1+\sum_{b\in\mathcal{A}(p,m,4)}1+\sum_{b\in\mathcal{A}(p,m,6)}1\right)\\ =&\sum_{p\le x}\left(\frac{12A^2}{(p+1)\pi^2}+O\left(A\log A\right)\right)\left(\frac{\varphi(m)}{2}\#C_m(p,2)+\frac{\varphi(m)}{4}\#C_m(p,4)+\frac{\varphi(m)}{6}\#C_m(p,6)\right).\end{aligned}$$

Applying the estimate obtained in Corollary 1 and Lemma 1, this is equal to

$$\begin{aligned}&\sum_{\substack{p\le x\\ p\equiv 1 \pmod{\ell_0}}}\left(\frac{12A^2}{(p+1)\pi^2}+O\left(A\log A\right)\right)\left(\frac{\varphi(m)}{2}\frac{2p}{m}\prod_{\substack{\ell\mid p-1\\ \gcd(\ell,m)=1}}\left(1-\frac{1}{\ell(\ell^2-1)}\right)+O\left(p^{1/2}\right)\right)\\ &+\sum_{\substack{p\le x\\ p\not\equiv 1 \pmod{\ell_0}}}\left(\frac{12A^2}{(p+1)\pi^2}+O\left(A\log A\right)\right)\left(\frac{\varphi(m)}{2}\frac{2p}{2^k\varphi(\ell_0^n)}\prod_{\substack{\ell\mid p-1\\ \gcd(\ell,m)=1}}\left(1-\frac{1}{\ell(\ell^2-1)}\right)+O\left(p^{1/2}\right)\right).\end{aligned}$$

Note that if m is a power of 2, then the second sum is empty. Simplifying and applying the trivial estimate

$$\frac{\varphi(m)p}{2^k\varphi(\ell_0^n)}\prod_{\substack{\ell\mid p-1\\ \gcd(\ell,m)=1}}\left(1-\frac{1}{\ell(\ell^2-1)}\right)<p,$$

this becomes

$$\begin{aligned}&\sum_{\substack{p\le x\\ p\equiv 1 \pmod{\ell_0}}}\frac{12A^2\varphi(m)p}{(p+1)\pi^2 m}\prod_{\substack{\ell\mid p-1\\ \gcd(\ell,m)=1}}\left(1-\frac{1}{\ell(\ell^2-1)}\right)\\ &+\sum_{\substack{p\le x\\ p\not\equiv 1 \pmod{\ell_0}}}\frac{12A^2\varphi(m)p}{\pi^2(p-1)2^k\varphi(\ell_0^n)}\prod_{\ell\mid p-1}\left(1-\frac{1}{\ell(\ell^2-1)}\right)\end{aligned}\tag{5.2}$$

$$+ O\left(A \log A \sum_{p\le x} p + \frac{12A^2}{\pi^2}\sum_{p\le x}\frac{\sqrt{p}}{p+1}\right). \tag{5.3}$$

Note that according to Lemma 3.4 of [35], we have

$$\sum_{p\le x} p = O\left(\frac{x^2}{2\log x}\right).$$

For the other part of the error term, the estimate,

$$\sum_{p\le x}\frac{\sqrt{p}}{p+1} \ll \int_2^x \frac{1}{\sqrt{t}} = O(\sqrt{x})$$

will suffice. Substituting these estimates, the error term becomes

$$\frac{Ax^2\log A}{2\log x} + \frac{12A^2\sqrt{x}}{\pi^2}. \tag{5.4}$$

We now turn our attention to the main term. First, note that

$$\begin{aligned}
&\sum_{\substack{p\le x\\ p\equiv 1 \ (\mathrm{mod}\ \ell_0)}} \frac{12A^2\varphi(m)p}{(p+1)\pi^2 m}\prod_{\substack{\ell\mid p-1\\ \gcd(\ell,m)=1}}\left(1-\frac{1}{\ell(\ell^2-1)}\right)\\
&+\sum_{\substack{p\le x\\ p\not\equiv 1 \ (\mathrm{mod}\ \ell_0)}} \frac{12A^2\varphi(m)p}{\pi^2(p-1)2^k\varphi(\ell_0^n)}\prod_{\ell\mid p-1}\left(1-\frac{1}{\ell(\ell^2-1)}\right)\\
&=\sum_{\substack{p\le x\\ p\equiv 1 \ (\mathrm{mod}\ \ell_0)}} \frac{12A^2\varphi(m)}{\pi^2 m}\prod_{\substack{\ell\mid p-1\\ \gcd(\ell,m)=1}}\left(1-\frac{1}{\ell(\ell^2-1)}\right)\\
&\quad+\sum_{\substack{p\le x\\ p\not\equiv 1 \ (\mathrm{mod}\ \ell_0)}} \frac{12A^2\varphi(m)}{\pi^2 2^k\varphi(\ell_0^n)}\prod_{\ell\mid p-1}\left(1-\frac{1}{\ell(\ell^2-1)}\right)\\
&\qquad+O\left(\frac{12A^2}{\pi^2}\sum_{p\le x}\frac{1}{p+1}\right).
\end{aligned}$$

Note that the error term in the above equation is dominated by our previous error term (5.4).

We analyze these two sums individually following [4]. A main input to this analysis is a theorem on averages of multiplicative functions due to [19, Theorem 3] which we record below for convenience. We denote by $f * g$ the Dirichlet convolution of the multiplicative functions f and g.

Theorem 10. Let f and g be multiplicative functions such that $g = 1 * f$. Suppose that there exists a constant $\vartheta \geq 0$ such that

$$| g(p) |\leq \frac{\vartheta}{p} + r(p) \tag{5.5}$$

for all primes p and

$$\sum_{p} | r(p) |< \infty, \quad \sum_{p} \sum k = 2^{\infty} | g(p^k) |< \infty. \tag{5.6}$$

Then for any $B > 0$,

$$\frac{1}{\pi(x)} \sum_{p \leq x} f(p-1) = \sum_{d=1}^{\infty} \frac{g(d)}{\varphi(d)} + O\left(\log(^{-B} x\right).$$

Assume first that m is not a power of 2, so that $\ell_0 > 1$. For any integer n, define the functions

$$\chi_{\ell_0}(n) = \begin{cases} 1 \text{ if } \ell_0 \nmid n \\ 0 \text{ if } \ell_0 | n, \end{cases}$$

$$F(n) = \prod_{\substack{\ell \mid n \\ \ell \nmid m}} \left(1 - \frac{1}{\ell(\ell^2-1)}\right),$$

and

$$F'(n) = \prod_{\substack{\ell \mid n \\ \ell \nmid m}} \left(1 - \frac{1}{\ell(\ell^2-1)}\right) \chi_{\ell_0 h}(n).$$

Note that χ_{ℓ_0} and F are multiplicative (whence F' is multiplicative as well). We compute

$$\begin{aligned}
&\sum_{\substack{p \le x \\ p \equiv 1 \pmod{\ell_0}}} \prod_{\substack{\ell \mid p-1 \\ \gcd(\ell,m)=1}} \left(1 - \frac{1}{\ell(\ell^2-1)}\right) \\
&= \sum_{p \le x} \prod_{\substack{\ell \mid p-1 \\ \gcd(\ell,m)=1}} \left(1 - \frac{1}{\ell(\ell^2-1)}\right) - \sum_{\substack{p \le x \\ p \not\equiv 1 \pmod{\ell_0}}} \prod_{\substack{\ell \mid p-1 \\ \gcd(\ell,m)=1}} \left(1 - \frac{1}{\ell(\ell^2-1)}\right) \\
&= \sum_{p \le x} \prod_{\substack{\ell \mid p-1 \\ \gcd(\ell,m)=1}} \left(1 - \frac{1}{\ell(\ell^2-1)}\right) - \sum_{p \le x} \prod_{\substack{\ell \mid p-1 \\ \gcd(\ell,m)=1}} \left(1 - \frac{1}{\ell(\ell^2-1)}\right) \chi_{\ell_0}(p-1) \\
&= \sum_{p \le x} F(p-1) + \sum_{p \le x} F'(p-1).
\end{aligned}$$

Let $G = F * \mu$ and $G' = F' * \mu$. Then G and G' are multiplicative functions defined on prime powers by

$$G(\ell^k) = \begin{cases} \frac{-1}{\ell(\ell^2-1)} & \text{if } \ell \nmid m, k = 1 \\ 0 & \text{if } \ell \mid m, k = 1 \\ 0 & \text{if } k > 1, \end{cases}$$

and

$$G'(\ell^k) = \begin{cases} \frac{-1}{\ell(\ell^2-1)} & \text{if } \ell \nmid m, k=1 \\ -1 & \text{if } \ell = \ell_0, k=1 \\ 0 & \text{if } \ell = 2 \mid m, k=1 \\ 0 & \text{if } k > 1. \end{cases}$$

Both pairs of functions F, G and F', G' satisfy the hypotheses of [19, Theorem 3]. It follows that

$$\frac{1}{\pi(x)} \sum_{p \le x} F(p-1) = \sum_{d=1}^{\infty} \frac{G(d)}{\varphi(d)} + O_B(\log^{-B} x)$$

holds for any $B > 0$, and similarly for F', G'. Now we have

$$\sum_{d=1}^{\infty} \frac{G(d)}{\varphi(d)} = \prod_{\ell \nmid m} \left(1 - \frac{1}{\ell(\ell^2-1)(\ell-1)}\right),$$

and

$$\sum_{d=1}^{\infty} \frac{G'(d)}{\varphi(d)} = \frac{\ell_0 - 2}{\ell_0 - 1} \prod_{\ell \nmid m} \left(1 - \frac{1}{\ell(\ell^2-1)(\ell-1)}\right).$$

Thus,

$$\sum_{\substack{p \le x \\ p \equiv 1 \pmod{\ell_0}}} \frac{12A^2\varphi(m)}{\pi^2 m} \prod_{\substack{\ell \mid p-1 \\ \gcd(\ell,m)=1}} \left(1 - \frac{1}{\ell(\ell^2-1)}\right)$$

$$= \frac{12A^2\varphi(m)}{\pi^2 m} \frac{1}{\ell_0 - 1} \prod_{\ell \nmid m} \left(1 - \frac{1}{\ell(\ell-1)(\ell^2-1)}\right) \pi(x) + O\left(A^2 \frac{x}{\log^{B+1} x}\right). \quad (5.7)$$

Similarly, we write

$$\sum_{\substack{p\le x\\ p\not\equiv 1 \pmod{\ell_0}}} \prod_{\ell\mid p-1}\left(1-\frac{1}{\ell(\ell^2-1)}\right)=\sum_{p\le x}\prod_{\ell\mid p-1}\left(1-\frac{1}{\ell(\ell^2-1)}\right)\chi_{\ell_0}(p-1)=\sum_{p\le x}F'(p-1)$$

so that, again by [19, Theorem 3], we have

$$\begin{aligned}\frac{1}{\pi(x)}\sum_{p\le x}F'(p-1)&=\sum_{d=1}^{\infty}\frac{G'(d)}{\varphi(d)}+O_B(\log^{-B}x)\\ =\frac{\ell_0-2}{\ell_0-1}&\prod_{\ell\nmid 2\ell_0}\left(1-\frac{1}{\ell(\ell-1)(\ell^2-1)}\right)+O_B(\log^{-B}x)\end{aligned}$$

holds for any $B>0$. Thus,

$$\begin{aligned}&\sum_{\substack{p\le x\\ p\not\equiv 1 \pmod{\ell_0}}}\frac{12A^2\varphi(m)}{\pi^2 2^k\varphi(\ell_0^n)}\prod_{\ell\mid p-1}\left(1-\frac{1}{\ell(\ell^2-1)}\right)\\ &=\frac{12A^2\varphi(m)}{\pi^2 2^k\varphi(\ell_0^n)}\frac{(\ell_0-2)}{(\ell_0-1)}\prod_{\ell\nmid m}\left(1-\frac{1}{\ell(\ell-1)(\ell^2-1)}\right)\pi(x)+O\left(A^2\frac{x}{\log^{B+1}x}\right).\end{aligned}\tag{5.8}$$

Combining (5.2), (5.4), (5.7), and (5.8), we have

$$\begin{aligned}\sum_{ht(a)\le A}\pi_{E(a)}^{cyc}(x)=\frac{12A^2}{\pi^2}\left(\frac{\varphi(m)}{2^k\varphi(\ell_0^n)}\frac{(\ell_0-2)}{(\ell_0-1)}+\frac{\varphi(m)}{m}\frac{1}{\ell_0-1}\right)\prod_{\ell\nmid m}\left(1-\frac{1}{\ell(\ell-1)(\ell^2-1)}\right)\pi(x)\\ +O\left(A^2\frac{x}{\log^{B+1}x}\right)+O\left(\frac{Ax^2\log A}{2\log x}+\frac{12A^2\sqrt{x}}{\pi^2}\right).\end{aligned}$$

In the case where m is a power of 2, we have that $\varphi(m)/m=1/2$, and we are left to evaluate

$$\frac{1}{2}\sum_{p\le x}\prod_{\substack{\ell\mid p-1\\ \gcd(\ell,m)=1}}\left(1-\frac{1}{\ell(\ell^2-1)}\right).$$

An argument analogous to the above shows

$$\sum_{ht(a)\leq A} \pi_{E(a)}^{cyc}(x) = \frac{6A^2}{\pi^2} \prod_{\ell\neq 2} \left(1 - \frac{1}{\ell(\ell-1)(\ell^2-1)}\right) \pi(x) + O\left(A^2 \frac{x}{\log^{B+1} x}\right)$$
$$+O\left(\frac{Ax^2 \log A}{2\log x} + \frac{12A^2\sqrt{x}}{\pi^2}\right).$$

Computing

$$C_m = \begin{cases} \left(\frac{\varphi(m)}{2^k\varphi(\ell_0^n)}\frac{\ell_0-2}{\ell_0-1} + \frac{\varphi(m)}{m}\frac{1}{\ell_0-1}\right) & \text{if } m \text{ is not a power of 2} \\ 1/2 & \text{if } m \text{ is a power of 2} \end{cases}$$

for $m \in \{4, 5, 6, 7, 8, 9, 10, 12\}$, we complete the proof.

Chapter 6

A torsion family defined over a quadratic field

Mazur's Torsion Theorem describes the possibilities for $E(\mathbb{Q})_{tors}$ where E is an elliptic curve defined over $\mathbb{Q}$. There has been substantial effort to determine which torsion structures occur over number fields of larger degree. Kamienny [23] and Kenku and Momose [26] determined which torsion structures may occur over a quadratic field. Najman gave the analog to Mazur's theorem for the two quadratic cyclotomic fields $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$ [31]. Obtaining the list of torsion structures that occur over cubic and quartic fields has been the focus of many recent papers, but the complete list is not yet known. Moreover, obtaining the analog of Mazur's theorem for a particular field is still quite hard, though Kamienny and Najman describe a general technique to obtain such results in the case of quadratic fields [24].

Given a torsion structure that occurs over a number field K, we would like to study the prime counting functions analogous to those we studied in the preceding chapter. However, when

$K \neq \mathbb{Q}$, not all of the torsion families are parameterizable since the corresponding modular curve need not have genus zero. In the case where the corresponding modular curve has genus greater than 1, there are finitely many elliptic curves with that torsion structure by Faltings' Theorem. In the case in which the modular curve has genus 1, there are infinitely many elliptic curves with that torsion structure, but those curves are not parameterizable.

6.1 Elliptic curves with full three-torsion

In order to apply the techniques we have already developed, we will focus our attention on the field $K = \mathbb{Q}(\sqrt{-3})$. According to Najman's analog of Mazur's Theorem for K, the torsion structures occurring over this field are those which occur over $\mathbb{Q}$ along with $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, and both of the new torsion structures occur infinitely often. We will focus our attention on the family of curves with full three-torsion. Husemöller [18] described a procedure for parameterizing these curves. Let K be a field containing a primitive cube root of unity ρ. Then a curve with full three torsion is isomorphic to the curve given by

$$E(a) : y^2 + (3a-1)xy + a(\rho-1)(a-(\rho+1)/3)y = x^3 \tag{6.1}$$

for some $a \in K$ satisfying $((3a-1)^3 - 27a(\rho-1)(a-(\rho+1)/3))(a(\rho-1)(a-(\rho+1)/3))^3$. The points $(0,0)$ and $(a, a(1-\rho)/3)$ form a basis for the subgroup $E(a)[3]$.

The smallest field extension of $\mathbb{Q}$ in which the study of reduction of such curves makes sense is the quadratic field $K = \mathbb{Q}(\sqrt{-3})$; furthermore, according to Najman [31], K is the only quadratic field over which there exists an elliptic curve with fully rational three torsion.

Clearly the reduction of curves in this family will never be cyclic; however, it makes sense to ask a question analogous to cyclicity for curves in this family. That is, we could ask how often the reduction of a curve $E(a)$ is "as cyclic as possible" given that it has full three-torsion which injects into its reduction modulo $\mathfrak{p}$. We will say that a curve $E(a)$ in this family has reduction that is as cyclic as possible if its group of $\mathbb{F}_q$ rational points is isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3N\mathbb{Z}$. Clearly, this condition is equivalent to imposing that for each $\ell \neq 3$, the reduction of $E(a)$ has cyclic ℓ-torsion. For each curve in this family, we define the prime counting function

$$\pi_E^{cyc}(x) = \#\{\mathfrak{p} \subset \mathcal{O}_K : N(\mathfrak{p}) \leq x, \ell \neq 3 \Rightarrow E_{\mathfrak{p}}(\mathcal{O}/\mathfrak{p})[\ell] \text{ is cyclic }\}. \tag{6.2}$$

We study these prime counting functions on average, using the same approach as we employed in the study of average cyclicity. As before, we will need an estimate of the number of $E/\mathbb{F}_q$ whose group of $\mathbb{F}_q$-rational points satisfies the conditions imposed by the family of curves and our problem. We will also require an understanding of how many parameters in a given finite field correspond to a given isomorphism class.

There is a new feature that appears in the case of elliptic curves defined over a number field larger that $\mathbb{Q}$, namely that our primes are now prime ideals instead of prime numbers, and prime ideals come in three types according to the splitting behavior of the unique rational prime lying below. They can split, remain prime (i.e., be inert), or they can ramify. Since only finitely many rational primes ramify in a given number field and we are studying a question of asymptotics of prime counting functions, we will from this point on ignore ramified primes by making the convention that our prime counting functions do not count these finitely many ramified primes.

The degree of a prime ideal of $\mathcal{O}_K$ dictates the size of the finite field $\mathcal{O}_K/\mathfrak{p}$ over which the reductions of our elliptic curves will be defined. Thus, it will be convenient to modify our prime counting functions to count primes of degree one and degree two separately. Define

$$\pi_{E,d}^{cyc}(x) = \#\{\mathfrak{p} \subset \mathcal{O}_K : \ \deg(\mathfrak{p}) = d, \ N(\mathfrak{p}) \leq x, \ell \neq 3 \Rightarrow E_{\mathfrak{p}}(\mathcal{O}_K/\mathfrak{p})[\ell] \text{ is cyclic } \}. \quad (6.3)$$

We will see that it is easy to obtain an average asymptotic for these functions when $d = 1$, but that a new input from analytic number theory will be required in the case where $d = 2$.

6.2 Isomorphisms of curves with full three-torsion

In this section we determine the number of parameters a which yield isomorphic curves in the family of curves with full three-torsion. Recall that curves $E(a)$ in this family are equipped with a basis for their three torsion which is $(0, 0)$ and $(a, a(1 - \rho)/3)$ where ρ is a primitive cube root of unity. Let $E = E(a)$ be a curve in the form (6.1), and let P and Q be linearly independent points in $E[3]$ (so that $Q \neq -P$). Denote by P_x and P_y the affine coordinates of P, and similarly for Q. We will count the isomorphisms (u, r, s, t) which send P to $(0, 0)$ and Q to $(b, b(1 - \rho)/3)$ for some $b \in K$ which (we will see) depends on (u, r, s, t).

Since (u, r, s, t) acts by the change of variables

$$x = u^2x' + r$$
$$y = u^3y' + u^2sx' + t,$$

we have $P \mapsto (0, 0)$ if and only if $r = P_x$ and $t = P_y$. Then s is determined by this choice of r and t and the fact that the coefficient on x in (6.1) is zero. We find that

$$s = \frac{3P_x^2 - (3a - 1)P_y}{a(\rho - 1)(a - (\rho + 1)/3) + (3a - 1)P_x + 2P_y}.$$

Next, in order that $Q \mapsto (b, b(1-\rho)/3)$, we must have

$$\begin{aligned} u^2 b + r &= Q_x \\ u^3 b(1-\rho)/3 + u^2 s b + t &= Q_y. \end{aligned}$$

Solving each equation for b, we have

$$\begin{aligned} b &= \frac{Q_x - P_x}{u^2}, \\ b &= \frac{Q_y - P_y}{u^3(1-\rho)/3 + u^2 s}. \end{aligned}$$

Equating these expressions for b and clearing denominators, we obtain the equation

$$(u(1-\rho)/3 + s)(Q_x - P_x) = Q_y - P_y.$$

Solving, we find that

$$u = \left(\frac{Q_y - P_y}{Q_x - P_x} - s\right)\left(\frac{3}{1-\rho}\right).$$

We have shown that the isomorphism (u, r, s, t) is completely determined by the choice of a basis (P, Q) for $E[3]$. Since there are 8 choices for P and 6 choices for Q, we conclude that there are 48 isomorphisms that preserve the equation (6.1). Furthermore, a straightforward but tedious calculation shows that the value of u which arises from taking $(-P, -Q)$ as a basis is the opposite of the u obtained by taking (P, Q) as a basis. From the relation

$$b = \frac{Q_x - P_x}{u^2},$$

we see that the parameters b which yield isomorphic curves are determined by the x-

coordinates of the chosen basis points, together with u. Thus, from the 48 isomorphisms which preserve the family, half of them yield a curve given by the same parameter.

As in the case of the curves $E_m(a)$ from Table 2.1, remark that the parameters which yield a curve with j-invariant equal to 0 or 1728 are the roots of a polynomial that does not depend on the field of definition. As in the previous calculation, these finitely many parameters are irrelevant to our asymptotic considerations. We remark for completeness that there are 8 parameters corresponding to $j = 0$ and 12 parameters corresponding to $j = 1728$.

6.3 Reduction of elements of K modulo $\mathfrak{p}$

In this section we use the estimates obtained in Chapter 4 to estimate the number of $\alpha = a + b\sqrt{-3} \in K$ whose height is bounded by $A > 0$ which reduce modulo $\mathfrak{p}$ to a given value. We will prove the following.

Lemma 6.

Let $r \in \mathcal{O}_K/\mathfrak{p}$. Then

$$\#\{\alpha \in K : ht(\alpha) \leq A, \alpha \equiv r \pmod{\mathfrak{p}}\} = \begin{cases} \frac{144}{\pi^4(p+1)}x^4 + O\left(x^3\log(x)\right) & \text{if } \deg(\mathfrak{p}) = 1, \\ \frac{144}{\pi^4(p+1)^2}x^4 + O\left(x^3\log(x)\right) & \text{if } \deg(\mathfrak{p}) = 2. \end{cases}$$

Proof. Assume first that $\mathfrak{p}$ is a degree 1 prime. For any $r \in \mathbb{Z}$ and for any choice of b, we have $\alpha \equiv r \pmod{\mathfrak{p}}$ if and only if $a \equiv r - b\sqrt{-3} \pmod{\mathfrak{p}}$. Applying the estimates of Chapter 4, we conclude that

$$\begin{aligned}
&\#\{\alpha \in K : ht(\alpha) \leq A, \alpha \equiv r \pmod{\mathfrak{p}}\}\\
&= \left(\frac{12}{\pi^2(p+1)}x^2 + O\left(x\log(x)\right)\right)\left(\frac{12}{\pi^2}x^2 + O\left(x\log(x)\right)\right)\\
&= \frac{144}{\pi^4(p+1)}x^4 + O\left(x^3\log(x)\right).
\end{aligned}$$

If, on the other hand, $\mathfrak{p}$ is a degree 2 prime then the image of 1 and $\sqrt{-3}$ under the reduction mod $\mathfrak{p}$ form a basis for $\mathcal{O}_K/\mathfrak{p}$ over $\mathbb{Z}/p\mathbb{Z}$. Writing $r = a_0 + b_0\sqrt{-3}$, we have that $\alpha \equiv r \pmod{\mathfrak{p}}$ if and only if $a \equiv a_0 \pmod{\mathfrak{p}}$ and $b \equiv b_0 \pmod{\mathfrak{p}}$. Thus, we have

$$\begin{aligned}
&\#\{\alpha \in K : ht(\alpha) \leq A, \alpha \equiv r \pmod{\mathfrak{p}}\}\\
&= \left(\frac{12}{\pi^2(p+1)}x^2 + O\left(x\log(x)\right)\right)^2\\
&= \frac{144}{\pi^4(p+1)^2}x^4 + O\left(x^3\log(x)\right),
\end{aligned}$$

which completes the proof. □

6.4 Average cyclicity for curves with full three-torsion

We now study the averages of the functions (6.3) for $d = 1$. Each prime of degree 1 must lie above a prime number p which splits in K, and we know that p splits in K if and only if the discriminant of K, which in this case is 3, is a quadratic residue modulo p. By the law of quadratic reciprocity, simply means that p is congruent to 1 modulo 3. Thus,

$$\sum_{ht(a)\leq A} \pi^{cyc}_{E(a),1}(x) = 2 \sum_{\substack{p\leq x\\ p\equiv 1 \pmod 3}} \sum_{\substack{E/\mathbb{F}_p\\ (\mathbb{Z}/3\mathbb{Z})^2\hookrightarrow E(\mathbb{F}_p)\\ (\mathbb{Z}/\ell\mathbb{Z})^2\not\hookrightarrow E(\mathbb{F}_p)}} \#\{a : ht(a) \leq A,\ E(a)_{\mathfrak{p}}(\mathcal{O}_K/\mathfrak{p}) \cong E\},$$

the 2 appearing because each prime under consideration lies below two prime ideals in $\mathcal{O}_K$. Each isomorphism class is represented by 24 parameter values modulo p except for the finitely many isomorphism classes of j-invariant 0 or 1728 which are represented by 8 and 12 parameters, respectively. Applying the estimate from section 6.3, this is equal to

$$2\sum_{\substack{p\leq x\\ p\equiv 1 \ (\mathrm{mod}\ 3)}}\left(\frac{144A^4}{\pi^4(p-1)}+O\left(A^3\log(A)\right)\right)\left(24\sum_{\substack{E/\mathbb{F}_p\\ \#\mathrm{Aut}(E)=2\\ (\mathbb{Z}/3\mathbb{Z})^2\hookrightarrow E(\mathbb{F}_p)\\ (\mathbb{Z}/\ell\mathbb{Z})^2\not\hookrightarrow E(\mathbb{F}_p)}}1+12\sum_{\substack{E/\mathbb{F}_p\\ \#\mathrm{Aut}(E)=4\\ (\mathbb{Z}/3\mathbb{Z})^2\hookrightarrow E(\mathbb{F}_p)\\ (\mathbb{Z}/\ell\mathbb{Z})^2\not\hookrightarrow E(\mathbb{F}_p)}}1+8\sum_{\substack{E/\mathbb{F}_p\\ \#\mathrm{Aut}(E)=6\\ (\mathbb{Z}/3\mathbb{Z})^2\hookrightarrow E(\mathbb{F}_p)\\ (\mathbb{Z}/\ell\mathbb{Z})^2\not\hookrightarrow E(\mathbb{F}_p)}}1\right).$$

Absorbing the sums over E with $\#\mathrm{Aut}(E)>2$ into the error term and applying the estimate from Corollary 1, this becomes

$$\begin{aligned}&2\sum_{\substack{p\leq x\\ p\equiv 1 \ (\mathrm{mod}\ 3)}}\left(\frac{144A^4}{\pi^4(p+1)}+O\left(A^3\log(A)\right)\right)\left(2p\prod_{\substack{\ell\mid p-1\\ \ell\neq 3}}\left(1-\frac{1}{\ell(\ell^2-1)}\right)+O(p^{1/2})\right)\\ &=4\sum_{\substack{p\leq x\\ p\equiv 1 \ (\mathrm{mod}\ 3)}}\frac{144A^4}{\pi^4}\frac{p}{p+1}\prod_{\substack{\ell\mid p-1\\ \ell\neq 3}}\left(1-\frac{1}{\ell(\ell^2-1)}\right)\\ &+O\left(A^4\sum_{p\leq x}\frac{\sqrt{p}}{p+1}\right)+O\left(A^3\log(A)\sum_{p\leq x}p\right).\end{aligned}$$

The main term was analyzed in Chapter 5 using Theorem 3 of Indlekofer, Wehmeier, and Lucht. Applying that result, we obtain

$$\begin{aligned}&4\frac{144A^4}{\pi^4}\sum_{\substack{p\leq x\\ p\equiv 1 \ (\mathrm{mod}\ 3)}}\prod_{\substack{\ell\mid p-1\\ \ell\neq 3}}\left(1-\frac{1}{\ell(\ell^2-1)}\right)+O\left(A^4\sum_{p\leq x}\frac{\sqrt{p}}{p+1}\right)+O\left(A^3\log(A)\sum_{p\leq x}p\right)\\ &=2\frac{144A^4}{\pi^4}\left(\prod_{\ell\neq 3}\left(1-\frac{1}{\ell(\ell-1)(\ell^2-1)}\right)\pi(x)+O\left(\frac{x}{\log^{B+1}x}\right)\right)\end{aligned}$$

$$+O\left(A^4\sum_{p\leq x}\frac{\sqrt{p}}{p+1}\right)+O\left(A^3\log(A)\sum_{p\leq x}p\right).$$

Dividing by $144A^4/\pi^4$, we obtain the average asymptotic for the functions $\pi^{cyc}_{E(a),1}$:

Proposition 1.

$$\frac{1}{\#\{a\in K : ht(a)\leq A\}}\sum_{ht(a)\leq A}\pi^{cyc}_{E(a),1}(x)=2\prod_{\ell\neq 3}\left(1-\frac{1}{\ell(\ell-1)(\ell^2-1)}\right)\pi(x)$$
$$+O\left(\frac{A}{\log^B(A)}\right).$$

Remark 6. The factor 2 in the Proposition above appears because for each finite field $\mathbb{F}_p$ for $p\equiv 1 \pmod 3$, there are two prime ideals of $\mathbb{O}_K$ such that the residue field is isomorphic to $\mathbb{F}_p$. The constant is what we should expect; the definition of $\pi^{cyc}_{E(a),d}$ imposes the same condition for $\ell\neq 3$ as π^{cyc}_E and imposes no condition at all for $\ell=3$. Thus, it is unsurprising that we get the same constant with the factor corresponding to 3 removed.

6.5 Degree two primes

We would also like to study the average over primes of degree 2. It is easy to see that the argument will proceed upon much the same lines, except that now the reductions of the E_a will be elliptic curves over the finite field $\mathcal{O}_K/\mathfrak{p}\cong\mathbb{F}_{p^2}$. Consequently, we need to compute the mean value of the multiplicative function $f(n)=\prod_{3\neq\ell|n}\left(1-\frac{1}{\ell(\ell^2-1)}\right)$ evaluated on the sequence of shifted *squares of primes* instead of the sequence of shifted squares. More generally, studying average cyclicity for elliptic curves defined over a degree n number field will likely require generalizing Indlekofer, Wehmeier, and Lucht's result to mean value of multiplicative functions over the sequence $\{p^n-1 : p \text{ is prime}\}$.

In the rest of this section, we will describe two approaches to resolving the technical obstacle caused by primes of degree 2.

Studying the average cyclicity of the family (6.1) over degree two primes will require evaluating

$$\sum_{\substack{p\leq x\\ p\equiv 2 \pmod 3}} \prod_{\ell\mid p^2-1}\left(1-\frac{1}{\ell(\ell^2-1)}\right). \tag{6.4}$$

For an odd prime p, the only prime number that divides both $p+1$ and $p-1$ is 2. Thus, we can write

$$\prod_{\ell\mid p^2-1}\left(1-\frac{1}{\ell(\ell^2-1)}\right)=\prod_{\ell\mid p-1}\left(1-\frac{1}{\ell(\ell^2-1)}\right)\cdot\prod_{\substack{\ell\mid p+1\\ \ell\neq 2}}\left(1-\frac{1}{\ell(\ell^2-1)}\right).$$

Denote by

$$\begin{aligned}
f(n)&=\prod_{\ell\mid n}\left(1-\frac{1}{\ell(\ell^2-1)}\right),\\
f_1(n)&=\prod_{\ell\mid n}\left(1-\frac{1}{\ell(\ell^2-1)}\right),\\
f_2(n)&=\prod_{\substack{\ell\mid n\\ \ell\neq 2}}\left(1-\frac{1}{\ell(\ell^2-1)}\right).
\end{aligned}$$

Then we have

$$\sum_{\substack{p\leq x\\ p\equiv 2 \pmod 3}} \prod_{\ell\mid n}\left(1-\frac{1}{\ell(\ell^2-1)}\right)=\sum_{\substack{p\leq x\\ p\equiv 2 \pmod 3}} f(p^2-1)=\sum_{\substack{p\leq x\\ p\equiv 2 \pmod 3}} f_1(p-1)f_2(p+1).$$

We can turn this into a sum over all primes by multiplying by the indicator function for integers relatively prime to 3. The topic of mean values of products of multiplicative functions over various sequences has seen substantial study in recent years; however, we are unaware of a result in the literature with the exact set of features we require.

Proving such a mean value theorem would be one way to complete the study of average cyclicity of reductions of elliptic curves at degree two primes. However, we note that should we eventually wish to the study of reductions of curves defined over fields of degree greater than 2, such a result will be of no help whatsoever in the study of reductions at primes of higher degree since it is particular to the factorization of $p^2 - 1$ as a product of linear polynomials in p.

A second potential approach would be to directly generalize the result of Indlekofer, Wehmeier, and Lucht. This theorem gives the mean value of multiplicative functions evaluated on the sequence of shifted primes $p - 1 : p$ prime; to study reductions of elliptic curves modulo degree d primes, we would require a theorem that gives the mean value of multiplicative functions along the sequence $p^d - 1 : p$ prime. Whether or not it is reasonable to expect such a theorem is unclear at this point since, for example, the sequence of squares of primes is much thinner than the sequence of primes.

The main technical tool in the proof of Theorem 10 is the Bombieri-Vinogradov theorem which describes the average error of the prime counting functions

$$\pi(x, d, a) = \#\{p \leq x : p \equiv a \pmod{d}\} \tag{6.5}$$

that counts the primes in the arithmetic progression

$$\{a, d + a, 2d + a, 3d + a, \ldots\} \tag{6.6}$$

Generalizing the result in the same way would likely require an analog of Bombieri-Vinogradov for the prime counting functions

$$\pi^n(x, d, a) = \#\{p \leq x : p^n \equiv a \pmod{d}\} \tag{6.7}$$

which count prime n^{th} powers in the arithmetic progression (6.6).

Question 1. Can we prove an analog to the Bombieri-Vinogradov theorem for the functions $\pi^n(x, d, a)$?

The functions $\pi^n(x, d, a)$ do not appear to have seen much study. Below we focus on the case of $\pi^2(x, d, a)$ and show how to relate $\pi^2(x, d, a)$ to $\pi(x, d', a')$ which are already well-understood. Again, we rely on the fact that $p^2 - 1$ factors as $(p+1)(p-1)$.

Factor $d = \ell_1^{e_1} \cdots \ell_r^{e_r}$, and let a be a quadratic residue modulo d that is relatively prime to d. Then $d \mid p^2 - a$ if and only if $\ell_i^{e_i} \mid (p+b)(p-b)$ holds for $1 \leq i \leq r$ where b is a square root of a modulo p. Let $\ell = \ell_i$, and assume that $\ell \nmid 2b$. Since ℓ_i divides $(p+b)(p-b)$, it must divide one or the other factor. But since ℓ^i does not divide $2b$, we conclude that $\ell_i^{e_i}$ divides precisely one of $p - b$ or $p + b$. Thus, the $p \leq x$ which satisfy $p^2 \equiv a \pmod{d}$ must satisfy one of two congruence conditions modulo $\ell_i^{e_i}$. Using the Chinese Remainder Theorem, we obtain a congruence condition modulo d' that p must satisfy, where d' is the product of the prime divisors of d that do not divide $2b$.

Next we must address those prime factors of d which also divide $2b$. In fact, we only need concern ourselves with the prime 2. Indeed, since we are assuming that the GCD of a and d is 1, the square root of a modulo d must be a unit in $\mathbb{Z}/d\mathbb{Z}$. Since any factor of d is automatically a zero divisor in this ring, we will never encounter this case.

As for the prime 2, there are several cases to go through. We assume that p is an odd prime since the exception does not contribute to asymptotic concerns. If b is even, then 2 does not divide $p^2 - 1$. If b is odd, then 2 divides both $p+1$ and $p-1$. Assume that 2^e is the exact power of 2 that divides d. Thus, the primes we are trying to count satisfy $2^e \mid p^2 - 1$.

If $e = 1$, then $2^e \mid p+1$, and $2^e \mid p-1$ holds for all odd primes. If $e = 2$, then since precisely one of $p+1$ or $p-1$ is divisible by 4, we will again have $2^e \mid p^2-1$ for all odd primes. Finally, suppose that $e \geq 3$. Using again the fact that precisely one of $p+1$ or $p-1$ is divisible by 4, we see that precisely one of $p+1$ or $p-1$ must be divisible by 2^{e-1}. In this case, the primes we are counting must satisfy the congruence condition modulo 2^{e-1}, the other factor of 2 being automatically supplied. In summary we have

$$\pi^2(x, 2^e, a) = \begin{cases} \pi(x, 2, 1) & \text{if } e = 1 \\ \pi(x, 4, 1) + \pi(x, 4, -1) & \text{if } e = 2 \\ \pi(x, 2^{e-1}, a) + \pi(x, 2^{e-1}, -a) & \text{if } e \geq 3. \end{cases}$$

Assembling all of the above discussion, we have shown the following.

Theorem 11. Let a be a quadratic residue modulo d that is relatively prime to d. Let k denote the number of odd prime factors of d, and let v be the 2-adic valuation of d. Then

$$\pi^2(x, d, a) \sim \frac{2^{k+\epsilon}}{\varphi(d)} \pi(x)$$

where $\epsilon = \begin{cases} 0 & \text{if } v = 0 \text{ or } 1 \\ 1 & \text{if } v = 2 \\ 2 & \text{if } v \geq 3. \end{cases}$

This theorem and its proof show that to a large extent, the study of prime squares in arithmetic progressions can be reduced to the study of primes in closely related arithmetic progressions. However, the fact that we must include data on quadratic residues means that it is not obvious that we can get a Bombieri-Vinogradov type theorem for these functions. We remark further that it is possible to estimate the error term

$$|\pi^2(x, d, a) - \frac{2^{k+\epsilon}}{\varphi(d)}\pi(x)|$$

by repeatedly using the error term for primes in arithmetic progressions for each of the prime power factor of d. The error term arising from this approach will depend on the number of distinct prime factors of d.

Chapter 7

Future research

In this chapter, we describe future directions of study.

7.1 Cyclicity

We have studied average cyclicity by ordering elliptic curves with a point of order m according to the parameterizations in Table 2.1, while Banks and Shparlinski ordered their curves by naive height, that is, by size of coefficients of short Weierstrass equations in absolute value. For an abelian group G appearing in allowed by Mazur's Torsion Theorem, Harron and Snowden [15] gave an estimate for the number of isomorphism classes of elliptic curves $E/\mathbb{Q}$ up to height x such that $E(\mathbb{Q})_{\mathrm{tors}} \cong G$. It is reasonable to expect that the average of the functions π_E^{cyc} over elliptic curves E in a torsion family ordered by height should be the same as the average of the same functions ordered according to Kubert's parameterizations. Determining if this is, indeed the case will be the subject of future work.

There are some cases of torsion families defined over $\mathbb{Q}$ that we have not addressed. Namely, we have not studied the family of elliptic curves with a point of order 2 or 3, nor have we studied average cyclicity for the family of curves with non-cyclic 2-torsion. However, we have made a prediction of what C_E^{cyc} should be for these curves, and the details of the argument will be similar. Working out the details of these cases would provide an opportunity for undergraduate research.

As described above, there is still some work to do in order to study average cyclicity over degree 2 prime ideals of $\mathcal{O}_K$, K quadratic. There are several approaches one could take to resolve this problem, all of which require a new input from analytic number theory. The most general question that we could pose would be "can we obtain the mean value of multiplicative functions along shifted prime powers in the style of Indlekofer Wehmeier, and Lucht?" An affirmative answer would enable us to study averages of the functions π_E^{cyc} for E defined over higher degree number fields.

7.2 Primality

We have focused on the case where E_p has cyclic group structure. If $\#E_p(\mathbb{F}_p)$is prime, then $E_p(\mathbb{F}_p)$ is certainly cyclic; thus, a related problem would be to study the prime counting functions

$$\pi_E^{twin}(x) = \#\{p \leq x : \#E_p(\mathbb{F}_p) \text{ is a prime number}\}.$$

The study of these functions was initiated by Koblitz, who was motivated by applications to cryptography. He conjectured that π_E^{twin} is asymptotic to $C_E^{twin}\frac{x}{(\log x)^2}$ for an explicit constant C_E^{twin}. Koblitz' conjecture was refined by Zywina [37], and this refined conjecture has been established on average over the family of all elliptic curves given by a short Weierstrass equation of bounded height by Balog, Cojocaru, and David [2]. As in the case of average Lang-Trotter and average cyclicity, the average results agree with the conjecture for individual curves, and in this case too, Jones [21] has proven that the average of the constants (as refined by Zywina [37]) is the constant appearing in the average result.

It would be of interest to study the average of the functions π_E^{twin} over thinner families of curves, for example, over torsion families. Obviously, when $E/\mathbb{Q}$ has a point of order m, there are only finitely many p for which $\#E_p(\mathbb{F}_p)$ is a prime number since for all sufficiently large p, we have $m \mid \#E_p(\mathbb{F}_p)$. Instead, we ask how frequently the ratio $\#E_p(\mathbb{F}_p)/m$ is a prime number.

Studying this question on average is less straightforward than in the case of cyclicity or Lang-Trotter; in these cases, we have good estimates for the number of elliptic curves over $\mathbb{F}_p$ with either cyclic group structure or fixed trace of Frobenius. In the case of primality, we would like to know how many $E/\mathbb{F}_p$ have a prime number of points. In 2000 Galbraith and McKee [14] gave a conjecture, but this remains open. However, David, Koukoulopoulos, and Smith [10] established the conjecture of Galbraith and McKee on average over primes $p \leq x$.

7.3 Squarefreeness

We conclude by mentioning a similar problem that has seen some study in recent years but for which less is known. Given an elliptic curve $E/\mathbb{Q}$ and a prime p of good reduction, if $\#E_p(\mathbb{F}_p)$ is a squarefree number, then $E_p(\mathbb{F}_p)$ is certainly a cyclic group. Thus, we would like to understand the behavior of the prime counting function

$$\pi_E^{SF}(x) = \#\{p \leq x : \#E_p(\mathbb{F}_p) \text{ is a squarefree number}\}.$$

Cojocaru [8] obtained an asymptotic for π_E^{SF} in the case where E has complex multiplication by the full ring of integers of an imaginary quadratic number field. More recently, the authors of [1] made a conjecture for the asymptotic of π_E^{SF} in the non-CM case and proved that it holds on average over the family of elliptic curves given by short Weierstrass equations of small height. So far, it does not appear that anyone has considered the average of π_E^{SF} over thin families such as torsion families, nor has the study of these functions been extended to elliptic curves defined over number fields. These are natural projects to pursue.

We would also like to study the corresponding fixed field count. That is, given a prime power q, how many isomorphism classes of elliptic curves over $\mathbb{F}_q$ have squarefree number of points? This is likely to be difficult to answer since it is, in part, asking about the number of squarefree integers in a short interval. However, even if we cannot obtain a fixed field count, obtaining a reasonable conjecture that holds on average, as was done for Galbraith–McKee in the case of primality, may be enough to study the functions π_E^{SF} on average.

Bibliography

[1] S. Akhtari, C. David, H. Hahn, and L. Thompson. Distribution of squarefree values of sequences associated with elliptic curves. In *Women in numbers 2: research directions in number theory*, volume 606 of *Contemp. Math.*, pages 171–188. Amer. Math. Soc., Providence, RI, 2013.

[2] A. Balog, A.-C. Cojocaru, and C. David. Average twin prime conjecture for elliptic curves. *Amer. J. Math.*, 133(5):1179–1229, 2011.

[3] A. Balog, A. Granville, and K. Soundararajan. Multiplicative functions in arithmetic progressions. *Ann. Math. Qué.*, 37(1):3–30, 2013.

[4] W. D. Banks and I. E. Shparlinski. Sato-Tate, cyclicity, and divisibility statistics on average for elliptic curves of small height. *Israel J. Math.*, 173:253–277, 2009.

[5] J. Battista, J. Bayless, D. Ivanov, and K. James. Average Frobenius distributions for elliptic curves with nontrivial rational torsion. *Acta Arith.*, 119(1):81–91, 2005.

[6] I. Borosh, C. J. Moreno, and H. Porta. Elliptic curves over finite fields. II. *Math. Comput.*, 29:951–964, 1975.

[7] W. Castryck and H. Hubrechts. The distribution of the number of points modulo an integer on elliptic curves over finite fields. *Ramanujan J.*, 30(2):223–242, 2013.

[8] A. C. Cojocaru. Square-free orders for CM elliptic curves modulo p. *Math. Ann.*, 342(3):587–615, 2008.

[9] A. C. Cojocaru and M. R. Murty. Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linnik's problem. *Math. Ann.*, 330(3):601–625, 2004.

[10] C. David, D. Koukoulopoulos, and E. Smith. Sums of Euler products and statistics of elliptic curves. *Math. Ann.*, 368(1-2):685–752, 2017.

[11] C. David and F. Pappalardi. Average Frobenius distributions of elliptic curves. *Internat. Math. Res. Notices*, (4):165–183, 1999.

[12] P. D. T. A. Elliott. Multiplicative functions on arithmetic progressions. *Mathematika*, 34(2):199–206, 1987.

[13] E. Fouvry and M. R. Murty. On the distribution of supersingular primes. *Canad. J. Math.*, 48(1):81–104, 1996.

[14] S. D. Galbraith and J. McKee. The probability that the number of points on an elliptic curve over a finite field is prime. *J. London Math. Soc. (2)*, 62(3):671–684, 2000.

[15] R. Harron and A. Snowden. Counting elliptic curves with prescribed torsion. *J. Reine Angew. Math.*, 729:151–170, 2017.

[16] A. Hildebrand. Multiplicative functions on arithmetic progressions. *Proc. Amer. Math. Soc.*, 108(2):307–318, 1990.

[17] E. W. Howe. On the group orders of elliptic curves over finite fields. *Compositio Math.*, 85(2):229–247, 1993.

[18] D. Husemöller. *Elliptic curves*, volume 111 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2004. With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen.

[19] K.-H. Indlekofer, S. Wehmeier, and L. G. Lucht. Mean behaviour and distribution properties of multiplicative functions. *Comput. Math. Appl.*, 48(12):1947–1971, 2004.

[20] K. James. Average Frobenius distributions for elliptic curves with 3-torsion. *J. Number Theory*, 109(2):278–298, 2004.

[21] N. Jones. Averages of elliptic curve constants. *Math. Ann.*, 345(3):685–710, 2009.

[22] N. Jones. Almost all elliptic curves are Serre curves. *Trans. Amer. Math. Soc.*, 362(3):1547–1570, 2010.

[23] S. Kamienny. Torsion points on elliptic curves and q-coefficients of modular forms. *Invent. Math.*, 109(2):221–229, 1992.

[24] S. Kamienny and F. Najman. Torsion groups of elliptic curves over quadratic fields. *Acta Arith.*, 152(3):291–305, 2012.

[25] N. Kaplan and I. Petrow. Elliptic curves over a finite field and the trace formula. *Proc. Lond. Math. Soc. (3)*, 115(6):1317–1372, 2017.

[26] M. A. Kenku and F. Momose. Torsion points on elliptic curves defined over quadratic fields. *Nagoya Math. J.*, 109:125–149, 1988.

[27] A. W. Knapp. *Elliptic curves*, volume 40 of *Mathematical Notes*. Princeton University Press, Princeton, NJ, 1992.

[28] D. S. Kubert. Universal bounds on the torsion of elliptic curves. *Proc. London Math. Soc. (3)*, 33(2):193–237, 1976.

[29] D. A. Marcus. *Number fields.* Universitext. Springer, Cham, 2018. Second edition of [MR0457396], With a foreword by Barry Mazur.

[30] M. R. Murty. *Problems in analytic number theory*, volume 206 of *Graduate Texts in Mathematics.* Springer, New York, second edition, 2008. Readings in Mathematics.

[31] F. Najman. Torsion of elliptic curves over quadratic cyclotomic fields. *Math. J. Okayama Univ.*, 53:75–82, 2011.

[32] J. P. Serre. Résumé des cours de 1977-1978. *Annuiaire du Collège de France*, 67-70, 1978.

[33] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics.* Springer, Dordrecht, second edition, 2009.

[34] D. Suryanarayana. The greatest divisor of n which is prime to k. *Math. Student*, 37:147–157, 1969.

[35] E. Treviño. The least inert prime in a real quadratic field. *Math. Comp.*, 81(279):1777–1797, 2012.

[36] S. G. Vlăduţ. Cyclicity statistics for elliptic curves over finite fields. *Finite Fields Appl.*, 5(1):13–25, 1999.

[37] D. Zywina. A refinement of Koblitz's conjecture. *Int. J. Number Theory*, 7(3):739–769, 2011.