Twin Prime Questions for Elliptic Curves

by

McKinley Meyer
B.Sc., University of Wisconsin-Madison, 2014

THESIS

Submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy in Mathematics
in the Graduate College of the
University of Illinois at Chicago, 2021

Chicago, Illinois

Defense Committee:
Alina Carmen Cojocaru, University of Illinois at Chicago, Chair and Advisor
Nathan Jones, University of Illinois at Chicago
Dhruv Mubayi, University of Illinois at Chicago
Paul Pollack, University of Georgia
Ramin Takloo-Bighash, University of Illinois at Chicago

For my dad, Steve Meyer, who has always been my biggest role model, both in academics and in life.

ACKNOWLEDGMENT

I'd first like to thank my advisor, Alina Carmen Cojocaru, for all your support and guidance over the years, especially in completing this thesis. Also, thank you for finding a problem well-suited to my interests and for always being patient with me despite my introversion, occasional mental health issues, and bouts of thick-headedness.

Further, I'd like to thank the rest of my thesis defense committee, Nathan Jones, Dhruv Mubayi, Paul Pollack, and Ramin Takloo-Bighash, for giving me their time as well as for their helpful criticism in editing this thesis. Additionally, I'd like to thank the Department of Mathematics, Statistics, and Computer Science for giving me the opportunity to study here and for supporting me financially during my time as a graduate student.

Lastly, thank you to my parents, Steve and Jeannine, for always supporting me in all my academic endeavors and for taking me in during a worldwide pandemic; to my brothers, Travis and Gage, for helping me enjoy life; and to our dog, d'Artagnan, for being a good source of stress relief during the past year.

MM

CONTRIBUTIONS OF AUTHORS

Section 2.4 of Chapter 2 and Sections 3.1-4.4 of Chapter 3 represent joint work with Alina Carmen Cojocaru.

TABLE OF CONTENTS

SUMMARY

For an elliptic curve E defined over $\mathbb{Q}$ and for a rational prime p of good reduction, one can define an integer a_p related to the number of $\mathbb{F}_p$-points lying on the reduction of E modulo p as $a_p = p + 1 - \#E(\mathbb{F}_p)$. The integer a_p, called the Frobenius trace of E modulo p, lies in the interval $(-2\sqrt{p}, 2\sqrt{p})$ and has several other remarkable properties. In this thesis, we study the arithmetic properties of a_p, specifically how often a_p is prime.

Using heuristical reasoning similar to that used in formulating the Hardy-Littlewood Conjecture regarding the number of twin primes up to a bound x, it is natural to formulate a conjecture for the asymptotic growth of the number of primes $p \leq x$ for which a_p is also prime. As evidence in support of this conjecture, we prove two main results, each in the case when E is without complex multiplication and under the θ-quasi Generalized Riemann Hypothesis. First, we establish an upper bound for the number of primes $p \leq x$ for which a_p is prime; this bound has the correct order of magnitude, as predicted by the aforementioned conjecture. Then we prove a lower bound, also with the correct order of magnitude, for the number of primes $p \leq x$ such that a_p is "almost" prime, in the sense of having at most a certain fixed number of prime factors, distinct or indistinct.

CHAPTER 1

INTRODUCTION

1.1 General notation

$\emptyset$ denotes the empty set.

$\mathbb{N}$ denotes the set of natural numbers, including 0.

$\mathbb{Z}$ denotes the set of integers.

$\mathbb{Q}$ denotes the set of rational numbers.

$\mathbb{R}$ denotes the set of real numbers.

$\mathbb{C}$ denotes the set of complex numbers. For $s \in \mathbb{C}$, we write $\mathrm{Re}(s)$ to denote the real part of s and $|s|$ to denote the absolute value of s.

For a finite set S, $\#S$ denotes the cardinality of S.

Unless stated otherwise, p and ℓ are rational primes, k, m, and n positive integers, and x and z positive real numbers.

$\mathbb{Z}/n\mathbb{Z}$ denotes the set of residue classes modulo n.

$\mathbb{Z}_p$ denotes the set of p-adic integers.

$\widehat{\mathbb{Z}}$ denotes the profinite completion of the integers.

$\mathbb{Z}[X]$ denotes the set of polynomials in X with coefficients in $\mathbb{Z}$.

$\mathbb{F}_p$ denotes the field of p elements.

For $a, b, c \in \mathbb{Z}$ with $c \neq 0$, we write $c \mid a$ to mean c divides a, and $c \mid a^{\infty}$ to mean c divides a^n for some n. We write $a \equiv b \pmod{c}$ to mean $c \mid (a-b)$, and $\gcd(a, b)$ to mean the greatest common divisor of a and b.

$\omega(n)$ denotes the function that counts the distinct prime factors of n, i.e. the prime factors of n without multiplicity. $\Omega(n)$ denotes the function that counts the prime factors of n with multiplicity. $\tau(n)$ denotes the function that counts the number of positive divisors of n.

$\mu(n)$ denotes the Möbius function, defined by

$$\mu(n) := \begin{cases} 1 & \text{if } \Omega(n) = \omega(n) = 2m \text{ for some } m \in \mathbb{N}, \\ -1 & \text{if } \Omega(n) = \omega(n) = 2m+1 \text{ for some } m \in \mathbb{N}, \\ 0 & \text{if } \Omega(n) > \omega(n). \end{cases}$$

Unless otherwise stated, $\phi(n)$ denotes Euler's totient function, defined by

$$\phi(n) := \sum_{\substack{1 \leq m \leq n \\ \gcd(m,n)=1}} 1 = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right).$$

$[x]$ denotes the integer part of x.

We write e^x to denote the exponential function, $\log x$ to denote the natural logarithm, and $\mathrm{li}(x)$ to denote the logarithmic integral, defined by $\mathrm{li}(x) := \int_2^x \frac{1}{\log t} dt$.

For real valued functions $f(x)$ and $g(x)$ with $g(x) \neq 0$ for all large enough x, we write

$$f(x) \sim g(x)$$

to mean $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$, and

$$f(x) = o(g(x))$$

to mean $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$. If $g(x)$ is positive valued, we write

$$f(x) = O_A(g(x))$$

to mean there exist positive constants $x_0 = x_0(A)$ and $c = c(A)$ depending on some quantity or object A such that, for all $x \geq x_0$, $|f(x)| \leq c(A)g(x)$. If $f(x)$ is also positive valued, we write

$$f(x) \ll_A g(x)$$

or

$$g(x) \gg_A f(x)$$

to mean $f(x) = O_A(g(x))$. We write

$$f(x) \asymp_A g(x)$$

to mean $f(x) \ll_A g(x) \ll_A f(x)$. If the constants $x_0(A)$ and $c(A)$ are both absolute, we simply omit the A from the above notation.

For a group G and a subset H of G, we write $H \leq G$ to mean H is a subgroup of G, and $H \trianglelefteq G$ to mean H is a normal subgroup of G. We denote by $[G : H]$ the index of H in G. If $H \trianglelefteq G$, we denote the quotient group of G modulo H by G/H or $\frac{G}{H}$.

For a unitary ring R, we denote the group of units of R by $R^\times$. We write $\mathcal{M}_{2\times 2}(R)$ to denote the the ring of 2×2 matrices with entries in R, and we write $\mathrm{GL}_2(R)$ to denote the general linear group of 2×2 invertible matrices with entries in R. We denote by I the identity matrix, and we write $\mathrm{PGL}_2(R)$ to denote the projective linear group, defined by

$$\mathrm{PGL}_2(R) := \frac{\mathrm{GL}_2(R)}{\{\alpha \mathrm{I} : \alpha \in R^\times\}}.$$

We recall

$$\# \,\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) = n^4 \prod_{p \mid n} \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{p^2}\right),$$

and

$$\# \,\mathrm{PGL}_2(\mathbb{Z}/n\mathbb{Z}) = n^3 \prod_{p \mid n} \left(1 - \frac{1}{p^2}\right).$$

For a field K, we write $\overline{K}$ to denote the algebraic closure of K.

For fields K and L, we write L/K to mean L is an extension of K. We denote the degree of L over K by $[L : K]$. If L is Galois over K, we denote its Galois group by $\mathrm{Gal}(L/K)$. For a subgroup H of $\mathrm{Gal}(L/K)$, we write L^H to denote the subextension of L fixed by H.

For a number field K, we denote by $\mathcal{O}_K$ the ring of integers of K, by n_K or $[K : \mathbb{Q}]$ the degree of K over $\mathbb{Q}$, by d_K the discriminant of K over $\mathbb{Q}$, and by $N_{K/\mathbb{Q}}$ the norm of K over $\mathbb{Q}$. For an extension of number fields L/K, we denote by $n_{L/K}$ or $[L : K]$ the degree of L over K, by $\mathrm{disc}(L/K) \trianglelefteq \mathcal{O}_K$ the discriminant ideal of L over K, and by $N_{L/K}$ the norm of L over K. For nonzero ideals I and J of $\mathcal{O}_K$ and a nonzero integer n, we write $I \mid J$ to mean $J \subseteq I$, and $I \mid n$ to mean $I \mid n\mathcal{O}_K$.

1.2 Primes

The study of rational primes dates back to the ancient Greeks, some of the earliest known mathematicians. Notably, the sieve of Eratosthenes, which we will talk about more later, gave us the first algorithm for finding primes; even more notably, Euclid's *Elements* provided a proof that there are infinitely many prime numbers.

This early study of primes led naturally to two questions:

1. How many primes are there up to a fixed bound?
2. Are there any patterns of primes that show up in infinite numbers?

To help answer the first question, we introduce the notation

$$\pi(x) := \#\{p \leq x : p \text{ is prime}\},$$

where x is an arbitrary positive real number. One can calculate a lower bound for $\pi(x)$ from Euclid's proof, deducing the growth $\pi(x) \gg \log\log x$, which is far from the truth. Carl Friedrich Gauss is believed to be the first person to suggest the correct answer in 1792, namely that, as $x \to \infty$,

$$\pi(x) \sim \frac{x}{\log x}.$$

Although this statement is true as written, Gauss would only later refine his guess for the growth of $\pi(x)$ to the better estimate

$$\pi(x) \sim \mathrm{li}(x) := \int_2^x \frac{dt}{\log t}, \tag{1.1}$$

which yields a better error than $x/\log x$ does. Called the Prime Number Theorem, (Equation 1.1) was first proved by Jacques Hadamard and Charles Jean de la Vallée Poussin independently in 1896, each using techniques from complex analysis based on the work of Bernhard Riemann from his celebrated 1859 paper, *Über die Anzahl der Primzahlen unter einer gegebenen Grösse*. Notably, in 1848, Chebychev proved, using elementary methods, a result almost as strong as (Equation 1.1): there exists positive constants c_1 and c_2 such that, for any $x > e$,

$$c_1 \frac{x}{\log x} < \pi(x) < c_2 \frac{x}{\log x}$$

(for example, we may take $c_1 = 0.92129...$ and $c_2 = 1.10555...$).

Our second question is expansively vague, but the general answer is yes, there are many patterns of primes that show up in infinite numbers. The pattern of primes we are interested in currently is called *twin primes*, i.e. primes p, for which $p + 2$ is also a prime. It has been conjectured for centuries, if not millennia, that there are infinitely many such primes. Similarly to $\pi(x)$, we consider

$$\pi_{\text{twin}}(x) := \#\{p \leq x : p, p+2 \text{ are both prime}\}.$$

Heuristically, one can argue based on the Prime Number Theorem, as G. H. Hardy and John Littlewood did in 1922, that the probabilities of p being prime and $p+2$ being prime are each approximately $1/\log p$, so that the probability of p being a twin prime is $1/(\log p)^2$. However, since the events of p and $p+2$ being prime are not independent, Hardy and Littlewood introduced a correction factor and formulated the following conjecture, which is a specific case of what is now referred to as *the Hardy-Littlewood Conjecture.*

Conjecture 1 *(Hardy-Littlewood Conjecture on Twin Primes (HaLi22), 1922)*

As $x \to \infty$,

$$\pi_{twin}(x) \sim C_{twin} \frac{x}{(\log x)^2},$$

where

$$C_{twin} := 2 \prod_{\substack{p \ prime \\ p \geq 3}} \left(1 - \frac{1}{(p-1)^2}\right).$$

Although Conjecture 1 is almost universally believed to be true, its proof currently remains an open question. However, much progress has been made since Hardy and Littlewood put forward their conjecture. An upper bound of the right order of magnitude $x/(\log x)^2$ is now known for $\pi_{\text{twin}}(x)$,

$$\pi_{\text{twin}}(x) \leq 7.8342 \cdot C_{\text{twin}} \frac{x}{(\log x)^2}, \tag{1.2}$$

while, concerning lower bounds, it is known that there are infinitely many primes p, such that $p+2$ is "almost" prime, in the following sense: as $x \to \infty$,

$$\#\{p \le x : p \text{ prime}, \Omega(p+2) \le 2\} \ge 0.899 \cdot C_{\mathrm{twin}} \frac{x}{(\log x)^2}, \tag{1.3}$$

where, for a positive integer n, $\Omega(n)$ denotes the number of prime factors of n, counted with multiplicity. Both results are derived from sieve methods and, as written, are due to Jie Wu ((Wu04) and (Wu08)); the former originates in the celebrated work on twin primes of Viggo Brun from 1919, and the latter is a variant of a celebrated result proven by J.R. Chen in 1966 (see (Ch73)). The next major breakthroughs on the study of twin primes came in 2009, when D.A. Goldston, J. Pintz and C. Y. Yildirim proved that there are infinitely many consecutive primes that have an arbitrarily small gap compared to the average gap (see (GoPiYi09)); in 2014, when Yitang Zhang proved that, for some positive integer $N \le 7 \times 10^7$, there are infinitely many primes p such that $p + N$ is also a prime (see (Zh14)); and in 2015, when J. Maynard proved that N above may be taken to satisfy $N \le 600$ (see (Ma15)). The polymath project has also contributed significant improvements on these techniques (see (Polymath14)).

In this thesis, while we are not interested in the ambitious goal of improving further upon the above results, we use them as motivation to investigate pairs of primes that occur in the setting of elliptic curves. For more background on questions about primes, we refer the reader to (Ap76), (Da00), (HaRi85), (HaWr08), (So07), and (Te15).

1.3 The Riemann Hypothesis

The two main new results to be proven in this thesis will depend on an important conjecture in mathematics, called the *Generalized Riemann Hypothesis*. As such, our goal in this section is to explain the statement of this conjecture.

Observant readers will recognize the name Riemann from the previous section, in which we explained that Hadamard and de la Vallée Poussin built upon the work of Riemann to prove the Prime Number Theorem. Indeed, Riemann's paper upon which they based their proofs was the same paper in which the Riemann Hypothesis was first stated. However, the story of the Riemann Hypothesis really begins a century prior with Leonhard Euler, who, in 1737, studied sums of the form

$$\sum_{n\geq 1} n^{-s}$$

for real numbers $s > 1$. Euler cleverly factored these sums into what are now called *Euler products*:

$$\prod_{p \text{ prime}} (1 + p^{-s} + p^{-2s} + \ldots) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}.$$

When one examines such a sum, it is very important that $s > 1$, since otherwise the series would diverge, and so any manipulations one might make to the sum would cease to have meaning. Undeterred by this fact, Euler made his manipulations with $s = 1$ anyway, and, despite the lack of rigor, came to the correct conclusion that

$$\sum_{p \text{ prime}} \frac{1}{p} = \log\log\infty, \tag{1.4}$$

or, as we would state it today,

$$\sum_{\substack{p \le x \\ p \text{ prime}}} \frac{1}{p} \sim \log\log x.$$

Although Euler ended up obtaining a correct statement, his proof of this result, of course, was not valid, and it would not be proven rigorously until 1874 by Franz Mertens. However, Euler's approach clearly influenced Riemann, as we will explain shortly.

Now, Riemann must have been inspired by the work of Euler, because he too chose to study sums of the form (1.3), but with the key alteration of allowing s to be a complex number rather than only a real number. With this in mind, one can define a complex-valued function

$$F(s) := \sum_{n \ge 1} n^{-s},$$

which is analytic on the half-plane $\mathrm{Re}(s) > 1$ but undefined for $\mathrm{Re}(s) \le 1$, since the series diverges in that region. However, one can use techniques from complex analysis to analytically continue $F(s)$ to a unique, meromorphic function, called *the Riemann zeta function*, $\zeta(s)$, which agrees with $F(s)$ on $\mathrm{Re}(s) > 1$, but is defined on the whole complex plane except for a simple pole at $s = 1$. Riemann was able to prove that this function satisfies the functional equation

$$\zeta(s) = 2^s \pi^{s-1} \sin\left(\frac{\pi s}{2}\right) \Gamma(1-s)\zeta(1-s). \tag{1.5}$$

Here,

$$\Gamma(s) := \int_0^\infty x^{s-1} e^{-s}\, dx$$

when $\mathrm{Re}(s) > 0$, and, starting from this half-plane, $\Gamma(s)$ can be continued to a function that is meromorphic on the whole complex plane.

Examining (Equation 1.5), it is fairly easy to see from the $\sin(\frac{\pi s}{2})$ factor that $\zeta(s)$ will have zeros at $s = -2n$ for each $n \in \mathbb{N} \setminus \{0\}$. These are known as the *trivial zeros* of the Riemann zeta function. It can be proven that there are no other zeros in the region $\mathrm{Re}(s) < 0$. Since $\zeta(s) = \sum_{n \geq 1} n^{-s}$ when $\mathrm{Re}(s) > 1$, we see from the Euler product formula that there are no zeros in the region $\mathrm{Re}(s) > 1$. Thus, the only area that remains a mystery in regards to the zeros of the Riemann zeta function is *the critical strip*, $\{s \in \mathbb{C} : 0 \leq \mathrm{Re}(s) \leq 1\}$. The Riemann Hypothesis predicts where these *nontrivial zeros* lie. What may be viewed as a more relaxed variation of this hypothesis is referred to as a *quasi Riemann Hypothesis.*

Conjecture 2 *(The θ-quasi Riemann Hypothesis)*
There exists $\theta \in \mathbb{R}$ with $\frac{1}{2} \leq \theta < 1$ such that each nontrivial zero of the Riemann zeta function (i.e., each zero in the critical strip) satisfies $\mathrm{Re}(s) \leq \theta$.

When $\theta = \frac{1}{2}$, the above conjecture is known as *the Riemann Hypothesis* and is denoted RH. Let us remark that, by virtue of symmetry, the Riemann Hypothesis claims that each nontrivial zero of the Riemann zeta function satisfies $\mathrm{Re}(s) = \frac{1}{2}$.

Although the Riemann Hypothesis is widely believed to be true, and there is a large amount of numerical evidence supporting it, this conjecture remains an open question, perhaps the most famous open question in all of mathematics. It was one of David Hilbert's 23 unsolved problems and is also one of the Clay Mathematics Institute's million dollar Millennium Prize problems.

To see one example of the powerful consequences of the Riemann Hypothesis, let us return to the Prime Number Theorem. In the previous section, we gave the growth of $\pi(x)$ as $\mathrm{li}(x)$, but neglected to say anything regarding the error in this estimate. We now see the growth of the difference between the two functions, with and without the Riemann Hypothesis, as follows.

Theorem 3

(i) Unconditionally, there exists a positive constant A *such that, for any sufficiently large positive real number* x*,*

$$|\pi(x) - \mathrm{li}(x)| \ll \frac{x}{\log x} e^{-A\sqrt{\log x}}.$$

(ii) Assuming the Riemann Hypothesis, for any sufficiently large positive real number x*,*

$$|\pi(x) - \mathrm{li}(x)| \ll x^{1/2} \log x.$$

The Riemann Hypothesis reduces the exponent of x occurring in the growth of the error term $|\pi(x) - \mathrm{li}(x)|$ by a full $\frac{1}{2}$. By itself, this is already a powerful consequence (and, in fact, is equivalent to the Riemann Hypothesis), but the Riemann Hypothesis has other wide-ranging consequences as well.

We stated at the beginning of this section that we will need the Generalized Riemann Hypothesis (GRH) rather than the Riemann Hypothesis itself to prove our new results, so we will now briefly explain exactly how we need the Riemann Hypothesis to be generalized. In short, we need the statement of the Riemann Hypothesis to hold not just for the Riemann zeta function, but also for generalizations of the Riemann zeta function, called Dedekind zeta functions.

For a number field K, *the Dedekind zeta function* is defined by

$$\zeta_{\mathsf{K}}(s) := \sum_{I \trianglelefteq \mathcal{O}_{\mathsf{K}}} |\mathcal{O}_{\mathsf{K}}/I|^{-s}$$

for $\mathrm{Re}(s) > 1$, where the sum ranges over all nonzero ideals, I, of the ring of integers, $\mathcal{O}_{\mathsf{K}}$, of K.

Besides being initially defined as a series which only converges for $\mathrm{Re}(s) > 1$, this function shares many other properties with the Riemann zeta function. It can be written as an Euler product,

$$\zeta_{\mathsf{K}}(s) = \prod_{\mathfrak{p} \trianglelefteq \mathcal{O}_{\mathsf{K}}} \frac{1}{1 - |\mathcal{O}_{\mathsf{K}}/\mathfrak{p}|^{-s}},$$

where the product ranges over all nonzero prime ideals $\mathfrak{p}$ of $\mathcal{O}_{\mathsf{K}}$; it satisfies a certain functional equation; it has an analytic continuation which is meromorphic on the whole complex plane with only a simple pole at $s = 1$; it has *trivial zeros* at each negative even integer (and each negative odd integer as well, unless K is a real extension).

Once again, the mystery is where the zeros lie within *the critical strip*, $\{s \in \mathbb{C} : 0 \leq \mathrm{Re}(s) \leq 1\}$. The *Generalized Riemann Hypothesis* predicts where these *nontrivial zeros* lie. In fact, the *quasi Generalized Riemann Hypothesis* makes the same assertion regarding the zeros of $\zeta_{\mathsf{K}}(s)$ as the quasi Riemann Hypothesis.

Conjecture 4 *(The θ-quasi Generalized Riemann Hypothesis)*

There exists $\theta \in \mathbb{R}$ *with* $\frac{1}{2} \leq \theta < 1$ *such that each zero of* $\zeta_K(s)$ *within the critical strip satisfies* $\mathrm{Re}(s) \leq \theta$.

As with the Riemann Hypothesis, the Generalized Riemann Hypothesis predicts that $\theta = \frac{1}{2}$. This is the statement we will need in order to prove the best versions of our main results.

1.4 Elliptic curves

The study of elliptic curves began motivated by interest in Diophantine equations. Over time, it distinguished itself as its own subject thanks to remarkable properties displayed by equations defining elliptic curves that other types of Diophantine equations did not display. Namely, one could impose a group structure on the points of an elliptic curve, as we will explain below.

There are many ways to define elliptic curves; we will follow the most naive and historical approach. We start with a field K and an equation called a *long Weierstrass equation*,

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

with each $a_i \in K$. If the characteristic of K is not 2 or 3, then through a little algebra and a change of variables, this equation can be rewritten into a form called the *short Weierstrass equation*,

$$y^2 = x^3 + Ax + B, \tag{1.6}$$

again with $A, B \in K$. This is the most common way to see the equation of an elliptic curve written. The elliptic curve, E, will consist of all points $P(x, y)$ with coordinates in an extension $L \supseteq K$ that satisfy the equation, along with one additional point that we will introduce shortly. We denote this set of points by $E(L)$. Additionally, we define *the discriminant of* E (rather, the discriminant of (Equation 1.6)) by

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

and make the assumption that

$$\Delta_E \neq 0.$$

If we were to have $\Delta_E = 0$, this would cause the right hand side of (Equation 1.6) to have a multiple root, which would lead to E having a point that we call a *singularity.* In this case, we call E a *singular curve.* Depending on whether the multiple root is a double or a triple root, we classify the singularity as either a *cusp* or a *node*, but in both cases, it cannot fit into any group structure on E. If we exclude the singularity, we can actually still impose a group structure on the rest of the points of E. However, we nevertheless omit singular curves from our definition of elliptic curves.

We will now discuss the method by which we can combine two points on E to obtain a third point also on E, which will soon help us define a group operation for the points of E. For this discussion, K can be any field with characteristic not 2 or 3, but it will be easiest to imagine that $K = \mathbb{R}$. This will allow us to visualize the way the third point is found as a geometric process called *the chord and tangent method*.

Let $P_1(x_1, y_1)$ and $P_2(x_2, y_2)$ be two points on E with coordinates in an extension $L \supseteq K$. Assume that $x_1 \neq x_2$. Then, since we also assume $\Delta_E \neq 0$, we know that the line through P_1 and P_2 intersects E at a distinct third point, $P_3(x_3, y_3)$. Since P_3 must satisfy both the equation of the line and the equation of the curve, we have that x_3 must be a solution of the equation

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B, \tag{1.7}$$

where

$$m := \frac{y_2 - y_1}{x_2 - x_1}.$$

After some rearranging, we see that

$$0 = x^3 - m^2x^2 + ...,$$

so then m^2 must be the sum of the roots of (Equation 1.7). We know one of the roots is x_3, but since P_1 and P_2 are also on the intersection of the line and the curve, the other two roots must be x_1 and x_2. Hence,

$$x_3 = m^2 - x_1 - x_2$$

and

$$y_3 = m(x_3 - x_1) + y_1.$$

Thus, given two points on E, we have found a third point also on E, and we can see from the formulas that since the coordinates of P_1 and P_2 are in L, the coordinates of P_3 will be in L as well. At this point, it might be tempting to define the group operation on $E(L)$ by $P_1+P_2 = P_3$. However, for reasons that will become clear shortly, we will actually need to define the group operation by

$$P_1 + P_2 = P_3',$$

where

$$P_3' = (x_3, -y_3),$$

i.e., we define the sum of P_1 and P_2 to be the reflection of the point we found above over the x-axis.

Adding a point to itself follows a similar process except, as one might expect, we use the tangent line to the point rather than a chord.

Now, in order to have a group structure on $E(L)$, we also need an identity element and inverses. It is not immediately clear what the identity element would be, and, in fact, there is no affine point P_0 on the curve that would satisfy $P + P_0 = P_0 + P = P$ for all points $P \in E(L)$. To remedy this, we define a new point to be on the curve that we call *the point at infinity* and denote by $\mathcal{O}$. For our purposes, this can be thought of as merely a formal symbol invented to make our calculations work out. However, it will be easier to accept and understand if we attach some physical intuition to it: one can think of the point at infinity as a terminal point that every vertical line eventually reaches as it goes both up and down, as if the real plane were a sheet of paper folded back on itself with the top and bottom ends glued together.

Although we simply define $P + \mathcal{O} = \mathcal{O} + P = P$ for any $P \in E(L)$, the aforementioned physical interpretation of the point at infinity $\mathcal{O}$ makes it intuitive why that would be the case. The line through P and $\mathcal{O}$ is simply the vertical line through P, the third point the line intersects the curve is P's reflection in the x-axis, and the reflection of that point is P itself. Similarly, if P and P' are reflections of each other over the x-axis, we can simply define $P + P' = \mathcal{O}$ (so $-P = P'$), but again our physical interpretation makes this choice intuitive. The line through P and P' is vertical, so the third point on the intersection of the line with the curve is $\mathcal{O}$, and the reflection of $\mathcal{O}$ in the x-axis is still $\mathcal{O}$.

We also remark that the group operation $+$ on $E(L)$ is clearly commutative, and it will turn out to be associative as well. Overall, we can summarize the above discussion succinctly in the following theorem.

Theorem 5

Let K be a field of characteristic not 2 or 3, and let $L \supseteq K$ be a field extension. Suppose an elliptic curve, E, is defined by the equation

$$y^2 = x^3 + Ax + B,$$

where $A, B \in K$ *are such that* $\Delta_E := -16(4A^3 + 27B^2) \neq 0$*. For any field extension* $L \supseteq K$*, define*

$$E(L) := \{\mathcal{O}\} \cup \{(x, y) \in L^2 : y^2 = x^3 + Ax + B\}.$$

Then, with the group operation defined above, $E(L)$ *is an abelian group.*

Since we now know that elliptic curves form groups, we might expect that there are group homomorphisms between elliptic curves, or, as we will focus on currently, endomorphisms from an elliptic curve to itself. More specifically, for an elliptic curve E defined over $\mathbb{Q}$, we are interested in the structure of its *endomorphism ring*, $\mathrm{End}_{\overline{\mathbb{Q}}}(E)$.

For $n \in \mathbb{Z}$ and for $P \in E(\overline{\mathbb{Q}})$, we use nP to denote adding P to itself n times if n is positive, adding $-P$ to itself $|n|$ times if n is negative, and $\mathcal{O}$ if n is 0. We see immediately that, for any $n \in \mathbb{Z}$, $\phi_n : E(\overline{\mathbb{Q}}) \to E(\overline{\mathbb{Q}})$ defined by $\phi_n(P) := nP$ for each P is an endomorphism of E. Thus, $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \supseteq \mathbb{Z}$.

If $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \neq \mathbb{Z}$, i.e., if E has an endomorphism that is not simply multiplication by an integer, we say that E *has complex multiplication* or that E is *with complex multiplication.* Otherwise, it will be the case that $\mathrm{End}_{\overline{\mathbb{Q}}}(E) = \mathbb{Z}$, and we say that E *does not have complex multiplication* or that E is *without complex multiplication.* The results presented in this thesis will focus entirely on elliptic curves without complex multiplication. For a thorough introduction to the theory of elliptic curves, we refer the reader to (Si00) and (Wa03).

1.5 Reductions modulo primes of an elliptic curve

In this section, our main goals are to explain some of the nuances of reducing an elliptic curve over $\mathbb{Q}$ modulo a rational prime p and to define the associated Frobenius trace a_p, which our new results will be about.

Fix a prime $p \in \mathbb{N}$ and an elliptic curve $E/\mathbb{Q}$, defined by the Weierstrass equation

$$y^2 = x^3 + Ax + B \tag{1.8}$$

for some $A, B \in \mathbb{Q}$. First, note that we may actually assume $A, B \in \mathbb{Z}$, since otherwise the change of variables $x = u^{-2}\hat{x}$ and $y = u^{-3}\hat{y}$, where u is the least common multiple of the denominators of A and B, would yield the new Weierstrass equation

$$\hat{y}^2 = \hat{x}^3 + u^4 A\hat{x} + u^6 B,$$

which does have integral coefficients. At this point, we can obtain a Weierstrass equation for a curve, E_p defined over $\mathbb{F}_p$, by simply reducing the coefficients of (Equation 1.8) modulo p. Similarly, one can define a homomorphism, $E(\mathbb{Q}) \to E_p(\mathbb{F}_p)$, by reducing the coordinates of each point $P \in E(\mathbb{Q})$ modulo p, provided both coordinates do not contain p in their denominators. If one or both of the coordinates of P do contain p in the denominator, then such a reduction is impossible; in this case, these points are sent to the point at infinity.

Note that in the above discussion, we called E_p merely a curve defined over $\mathbb{F}_p$, not an *elliptic* curve over $\mathbb{F}_p$. Indeed, it will sometimes occur that the reduction of an elliptic curve modulo

p turns out to be a singular curve. If E_p is an elliptic curve, then we say p is *a prime of good reduction* for (Equation 1.8); otherwise, we say p is *a prime of bad reduction* for (Equation 1.8).

Since we assumed the coefficients A and B were integers, we will have that the discriminant, Δ_E, is an integer as well, and so we can find the discriminant of E_p by reducing Δ_E mod p. Thus, from our discussion in Section 1.3, we know that if $\Delta_E \not\equiv 0 \pmod{p}$, then p will have good reduction for (Equation 1.8). Counterintuitively, the converse is not true. This is because the discriminant is not an invariant of the curve. It depends on the Weierstrass equation, but the same curve can be described by many different Weierstrass equations. One can imagine that with the right change of variables, we may find an equation for which $\Delta_E \not\equiv 0 \pmod{p}$ even though $\Delta_E \equiv 0 \pmod{p}$ for some initial equation. Fortunately, there is a quantity called *the conductor of* E, denoted N_E, which is an invariant of E and encodes whether each prime is of good or bad reduction, as well as the extent of badness, in a certain sense, for those of bad reduction. For our purposes, we only need the following result.

Proposition 6

Let $E/\mathbb{Q}$ be an elliptic curve with conductor N_E, and let p be a rational prime. Then, p has good reduction for any Weierstrass equation of E if and only if $p \nmid N_E$.

Next, we will examine the order of the group $E_p(\mathbb{F}_p)$, which we will see is intimately connected to a_p, the quantity our new results are concerned with.

For an odd prime p of good reduction (for any Weierstrass equation of E), denote by $\tilde{A}$ and $\tilde{B}$ the reductions of A and B modulo p. Then, the Weierstrass equation of E_p can be given by

$$y^2 = x^3 + \tilde{A}x + \tilde{B}. \tag{1.9}$$

From this equation, it is easy to see that, for any $x_0 \in \mathbb{F}_p$, the number of $y_0 \in \mathbb{F}_p$ such that (x_0, y_0) satisfies the equation will be determined by the value of the Legendre symbol $\left(\frac{x_0^3+\tilde{A}x_0+\tilde{B}}{p}\right)$. If $x_0^3 + \tilde{A}x_0 + \tilde{B}$ is a quadratic residue modulo p, then there will be two such y_0. If $x_0^3 + \tilde{A}x_0 + \tilde{B}$ is zero modulo p, then there will be one such y_0. If $x_0^3 + \tilde{A}x_0 + \tilde{B}$ is a quadratic non-residue modulo p, then there will be no such y_0. Remembering that $\mathcal{O}$ is included in $E_p(\mathbb{F}_p)$, we then see that the size of $E_p(\mathbb{F}_p)$ is given by

$$\begin{aligned} \#E_p(\mathbb{F}_p) &= 1 + \sum_{x_0 \in \mathbb{F}_p} \left(1 + \left(\frac{x_0^3 + \tilde{A}x_0 + \tilde{B}}{p}\right)\right) \\ &= 1 + p - a_p, \end{aligned}$$

where

$$a_p := -\sum_{x_0 \in \mathbb{F}_p} \left(\frac{x_0^3 + \tilde{A}x_0 + \tilde{B}}{p}\right).$$

Now, in principle, we could have $|a_p|$ as large as p, but one would probably expect there to be some cancellation in the sum above. The question is, how much? In 1933, Helmut Hasse proved the best bound as follows, and this result was later generalized by André Weil.

Theorem 7

For an elliptic curve $E/\mathbb{Q}$ *and a prime* p *of good reduction, with* a_p *defined as above, we have*

$$|a_p| \leq 2\sqrt{p}. \tag{1.10}$$

There are many other questions about a_p that might spark curiosity (and, indeed, have sparked curiosity), such as the famous Sato-Tate Conjecture from 1960 on the distribution of the angles $\arccos\left(\frac{a_p}{2\sqrt{p}}\right)$ (see (Ca08) and (Cl06)), and the Lang-Trotter Conjecture from 1976 on the asymptotic behavior of the counting function $\#\{p \leq x : p \nmid N_E, a_p = \alpha\}$ (see (LaTr76)). In the next section, we will discuss yet another question about the integers a_p and present the main results of this thesis.

1.6 Main results of the thesis

For an elliptic curve E defined over $\mathbb{Q}$, of conductor N_E, and without complex multiplication, we are interested in counting primes $p \leq x$ such that a_p is prime. Inspired by a heuristical reasoning similar to the one used for twin primes, we investigate:

Main Conjecture

Let E *be an elliptic curve defined over* $\mathbb{Q}$, *of conductor* N_E, *and without complex multiplication. Then, as* $x \to \infty$,

$$\#\{p \leq x : p \nmid N_E, a_p \text{ is prime}\} \sim C(E)\frac{x}{(\log x)^2}, \tag{1.11}$$

where $C(E)$ *is a non-negative constant defined in terms of* E*. More precisely, the constant is explicitly defined as*

$$C(E) := 2 \cdot \frac{m_E}{\phi(m_E)} \cdot \frac{\#\{M \in \mathrm{Gal}(\mathbb{Q}(E[m_E])/\mathbb{Q}) : \gcd(\mathrm{tr}\, M, m_E) = 1\}}{\#\, \mathrm{Gal}(\mathbb{Q}(E[m_E])/\mathbb{Q})} \cdot \prod_{\substack{\ell \nmid m_E \\ \ell \ \mathit{prime}}} \left(1 - \frac{1}{\ell^3 - \ell^2 - \ell + 1}\right), \tag{1.12}$$

where m_E *is the torsion conductor of* $E/\mathbb{Q}$ *and* $\mathrm{Gal}(\mathbb{Q}(E[m_E])/\mathbb{Q})$ *is the Galois group of the* m_E*-division field of* E*, whose elements are viewed in the matrix group* $\mathrm{GL}_2(\mathbb{Z}/m_E\mathbb{Z})$ *(see Section 2.3).*

Related to this conjecture, we will prove the following results, which are the main theorems of this thesis.

Our first result is reminiscent of the upper bound (Equation 1.2) on twin primes.

Main Theorem A

Let E *be an elliptic curve defined over* $\mathbb{Q}$*, of conductor* N_E*, and without complex multiplication. Assume that there exists some* $\frac{1}{2} \leq \theta < 1$ *such that the* θ*-quasi Generalized Riemann Hypothesis holds for Dedekind zeta functions. Then, for all sufficiently large* x*,*

$$\#\{p \leq x : p \nmid N_E, a_p \ \mathit{is\ prime}\} \leq \left(\frac{3}{1-\theta} + o(1)\right) C(E) \frac{x}{(\log x)^2}, \tag{1.13}$$

where $C(E)$ *is the explicit constant introduced in (Equation 1.12). In particular, when* $\theta = \frac{1}{2}$, *(Equation 1.13) becomes*

$$\#\{p \le x : p \nmid N_E, a_p \textit{ is prime}\} \le (6 + o(1))\, C(E) \frac{x}{(\log x)^2}. \tag{1.14}$$

As a corollary to this theorem we obtain the convergence of the sum of reciprocal primes p for which a_p is a prime, a result reminiscent of the famous theorem of Viggo Brun (Br19) on twin primes that $\displaystyle\sum_{\substack{p \text{ prime} \\ p+2 \text{ prime}}} \frac{1}{p} < \infty$, but drastically different from Euler's result (Equation 1.4) on the divergence of the sum of reciprocal primes.

Corollary A'

Let E *be an elliptic curve defined over* $\mathbb{Q}$, *of conductor* N_E, *and without complex multiplication. Assume that there exists some* $\frac{1}{2} \le \theta < 1$ *such that the* θ*-quasi Generalized Riemann Hypothesis holds for Dedekind zeta functions. Then*

$$\sum_{\substack{p \nmid N_E \\ a_p \textit{ prime}}} \frac{1}{p} < \infty.$$

More precisely, for each $\varepsilon > 0$, *there exists* $x_0 = x_0(E, \theta, \varepsilon)$ *such that*

$$\sum_{\substack{p \ge x_0 \\ a_p \textit{ prime}}} \frac{1}{p} \le \left(\frac{3}{1 - \theta} + \varepsilon \right) C(E) \frac{1}{\log x_0},$$

where $C(E)$ *is the explicit constant introduced in (Equation 1.12).*

Our second result is reminiscent of the lower bound (Equation 1.3) related to twin primes.

Main Theorem B

Let E be an elliptic curve defined over $\mathbb{Q}$, of conductor N_E, and without complex multiplication. Assume that there exists some $\frac{1}{2} \leq \theta < 1$ such that the θ-quasi Generalized Riemann Hypothesis holds for Dedekind zeta functions. Then, for all sufficiently large x,

$$\#\{p \leq x : p \nmid N_E, a_p \neq \pm 1, \omega(a_p) \leq r_1\} \geq \frac{3}{1-\theta}(0.00692... + o(1))C(E)\frac{x}{(\log x)^2}, \tag{1.15}$$

and

$$\#\{p \leq x : p \nmid N_E, a_p \neq \pm 1, \Omega(a_p) \leq r_2\} \geq \frac{3}{1-\theta}(0.3162... + o(1))C(E)\frac{x}{(\log x)^2}, \tag{1.16}$$

where $C(E)$ is the explicit constant introduced in conjectural (Equation 1.11), and where

$$\begin{aligned} r_1 = r_1(\theta) &:= 1 + \left[\frac{1}{0.83}\left(\frac{3}{2(1-\theta)} - \frac{1}{6}\right)\right], \\ r_2 = r_2(\theta) &:= 1 + \left[\frac{5}{2(1-\theta)} - \frac{5}{12}\right]. \end{aligned}$$

In particular, when $\theta = \frac{1}{2}$, (Equation 1.15) and (Equation 1.16) become

$$\#\{p \leq x : p \nmid N_E, a_p \neq \pm 1, \omega(a_p) \leq 4\} \geq (0.0415... + o(1))C(E)\frac{x}{(\log x)^2},$$

and

$$\#\{p \leq x : p \nmid N_E, a_p \neq \pm 1, \Omega(a_p) \leq 5\} \geq (1.8972... + o(1))C(E)\frac{x}{(\log x)^2}.$$

1.7 Further motivation for our main results

As we mentioned in Section 1.4, the properties of the integers a_p defined by the reductions modulo primes p of an elliptic curve E defined over $\mathbb{Q}$ have attracted the interest of several prominent mathematicians and have been the main objects of study in now-famous problems in arithmetic geometry, such as the Sato-Tate Conjecture and the Lang-Trotter Conjecture.

In addition to the above two problems, the study of the arithmetic properties of the sequence a_p, e.g., understanding the asymptotic behavior of the functions $\omega(a_p)$, $\Omega(a_p)$, and $\tau(a_p)$ as p varies, has been of increasing interest to number theorists. For example, in (MuMu84), the authors proved that, under GRH, the sequence $\omega(a_p)$ defined by an elliptic curve $E/\mathbb{Q}$ without complex multiplication has normal order $\log \log p$, while in (CoDaSiSt16), the authors showed that the aforementioned normal order result is a particular instance of a much more general phenomenon in the theory of abelian varieties.

The study of the prime factors of a_p naturally leads to the study of the primality of a_p pursued in this thesis. Under the guidance of A.C. Cojocaru, the primality of a_p was priorly pursued by Matthew Lane in (La05). While in Lane's thesis only a weak version of the conjectural asymptotic formula (Equation 1.11) was stated (that is, no constant was predicted, nor discussed, there), in (La05) an investigation of the primality of a_p, based on sieve methods, was pursued in analogy with classical investigations of the primality of $p+2$. In particular, it was shown that, under GRH and for any elliptic curve $E/\mathbb{Q}$ without complex multiplication,

$$\#\{p \leq x : p \nmid N_E, a_p \text{ is prime}\} \ll_E \frac{x}{(\log x)^2},$$

$$\#\{p \leq x : p \nmid N_E, \omega(a_p) \leq 5\} \gg_E \frac{x}{(\log x)^2}, \tag{1.17}$$

$$\#\{p \leq x : p \nmid N_E, \Omega(a_p) \leq 7\} \gg_E \frac{x}{(\log x)^2}. \tag{1.18}$$

Our results, Main Theorem A and Main Theorem B, improve upon the above in several aspects, such as the following: the bounds exhibit an explicit relation between the $\ll$ and $\gg$ constants and the conjectural constant $C(E)$ predicted in (Equation 1.12); the bounds refine the lower bounds (Equation 1.17) and (Equation 1.18) from $\omega(a_p) \leq 5$ and $\Omega(a_p) \leq 7$ to $\omega(a_p) \leq 4$ and $\Omega(a_p) \leq 5$, respectively; finally, each of our results is accompanied by a version that assumes only a quasi-GRH instead of the full GRH.

To achieve the above improvements, our techniques differ from those in (La05) through the employment of more powerful sieves, and, most importantly, through a more refined treatment of the divisibility condition $m \mid a_p$ for an arbitrary positive integer m.

CHAPTER 2

PRELIMINARIES

2.1 Sieve basics

The first basic notion of a sieve as used in number theory dates all the way back to the ancient Greeks with the sieve of Eratosthenes. In its simplest application, one starts with a set of positive integers, each at most x for some positive real number x, then successively removes from this set all multiples of p for each prime $p \leq \sqrt{x}$. The remaining numbers are then all guaranteed to be prime. Thus, this process gives us a slightly easier way to find all the primes in a given set than checking whether each number in the set is prime one by one.

The sieve of Eratosthenes was not rigorously formalized and generalized until the early twentieth century, starting with the work of Viggo Brun. Since then, through the use of some clever ideas and tricks, several mathematicians created improved sieves and used them to prove results about primes and irreducibles in a variety of settings. In particular, sieves have been used to prove results relating to the Twin Prime Conjecture, such as those we mentioned in Chapter 1.

The general setup for most sieves is the same, although the definitions are usually left vague intentionally in order to maintain flexibility. We have a multiset $\mathcal{A} \subset \mathbb{Z}$ (i.e., a set of integers which can contain multiple instances of the same element), usually defined to depend in some way on a real number $x > 0$ that is thought to grow to infinity. Additionally, we have a set of primes, $\mathcal{P}$. Ideally, the goal of a sieve would be to find all elements of $\mathcal{A}$ that are coprime to each "small" prime in $\mathcal{P}$. However, that goal is too difficult in practice, so instead the goal is merely to estimate the number of such elements in $\mathcal{A}$, i.e., to estimate the cardinality

$$\mathcal{S}(\mathcal{A}, \mathcal{P}, z) := \#\{a \in \mathcal{A} : \gcd(a, P(z)) = 1\},$$

where $z > 0$ is a parameter and

$$P(z) := \prod_{\substack{\ell \in \mathcal{P} \\ \ell < z}} \ell.$$

To that end, we define, for each prime power, ℓ^r, with $\ell \in \mathcal{P}$,

$$\mathcal{A}_{\ell^r} := \{a \in \mathcal{A} : a \equiv 0 \pmod{\ell^r}\}$$

and, for each square-free $d \in \mathbb{N} \setminus \{0\}$ consisting only of products of primes in $\mathcal{P}$,

$$\mathcal{A}_d := \bigcap_{\ell | d} \mathcal{A}_\ell = \{a \in \mathcal{A} : a \equiv 0 \pmod{d}\}.$$

Having defined $\mathcal{A}_d$ as an intersection in the above, it is easy to see that we can use the inclusion-exclusion principle to calculate $\mathcal{S}(\mathcal{A},\mathcal{P},z)$. We have that

$$\begin{aligned}\mathcal{S}(\mathcal{A},\mathcal{P},z) &= \#\Big(\mathcal{A} \setminus \bigcup_{\ell \mid P(z)} \mathcal{A}_\ell\Big) \\ &= \#\mathcal{A} - \sum_{\ell \mid P(z)} \#\mathcal{A}_\ell + \sum_{\substack{\ell_1 \ell_2 \mid P(z) \\ \ell_1 \neq \ell_2}} \#\mathcal{A}_{\ell_1 \ell_2} - \dots \\ &= \sum_{d \mid P(z)} \mu(d) \#\mathcal{A}_d,\end{aligned}$$

where

$$\mathcal{A}_1 := \mathcal{A}.$$

This observation forms the starting point for all of sieve theory. It should come as no surprise, then, that sieves require accurate estimates for the sizes of the subsets $\mathcal{A}_d$.

While the exact assumptions about the $\#\mathcal{A}_d$'s vary, nearly always we write

$$\#\mathcal{A}_d = \frac{w(d)}{d} X + R_d, \tag{2.1}$$

where $w : \mathbb{N} \setminus \{0\} \to \mathbb{R}$ is a multiplicative function, $X > 0$ is defined in terms of x and is thought to approximate $\#\mathcal{A}$, and R_d is some remainder term.

In order to prove the upper and lower bounds stated in our two main results, we will use the *Selberg sieve* and the *weighted Greaves' sieve*, which we will recall at the time of their use. These sieves have very similar setups and assumptions. For Greaves' sieve, in addition to (Equation 2.1), we will need the similar assumption that, for each $\ell \in \mathcal{P}$,

$$\#\mathcal{A}_{\ell^2} = \frac{w\left(\ell^2\right)}{\ell^2}X + R_{\ell^2}. \tag{2.2}$$

Both sieves will also require the somewhat less common assumptions that:

1. for each $\ell \in \mathcal{P}$ and some fixed $\varepsilon > 0$,

$$0 \leq \frac{w(\ell)}{\ell} \leq 1 - \varepsilon; \tag{2.3}$$

2. there exist $L, A \geq 1$ such that, for all z_1, z_2 with $2 \leq z_1 \leq z_2$,

$$-L \leq \sum_{z_1 \leq \ell < z_2} \frac{w(\ell)}{\ell} \log \ell - \log \frac{z_2}{z_1} \leq A. \tag{2.4}$$

As well as sharing these assumptions, both sieves will estimate the size of the sifted set in terms of the product

$$V(z) := \prod_{\substack{\ell \in \mathcal{P} \\ \ell < z}} \left(1 - \frac{w(\ell)}{\ell}\right). \tag{2.5}$$

For more on sieve theory, we refer the reader to (Gr00) and (HaRi85).

2.2 Classical analytic estimates

In many sieves, including the ones we will be using, there are some assumptions on the function $w(\cdot)$ mentioned in the previous section. To help us verify one such assumption, we will need the following theorem due to Mertens.

Theorem 8 *(Mertens' First Theorem, 1874)*

For all $x > e$*,*

$$\left| \sum_{p \le x} \frac{\log p}{p} - \log x \right| \le 2.$$

Now, remaining in the general sieve setting of the previous section, we note that, intuitively we might expect the proportion of $\mathcal{A}$ that is not divisible by a prime, ℓ, to be approximately $1 - \frac{1}{\ell}$, and thus the proportion of $\mathcal{A}$ without small prime factors to be something akin to $\prod_{\ell < z}(1 - \frac{1}{\ell})$. This naive line of reasoning will turn out to come fairly close to the truth. In both of the sieves we will use, the main term will consist of a product similar to this times X. In order to estimate this product, we employ another of Mertens' theorems.

Theorem 9 *(Mertens' Third Theorem, 1874)*

$$\lim_{x \to \infty} (\log x) \cdot \prod_{p \le x} \left(1 - \frac{1}{p}\right) = e^{-\gamma},$$

where γ *is Euler's constant.*

There is, of course, a Mertens' Second Theorem, but we will not need to make use of it. However, the following property of convergent products will also be helpful in dealing with the product we mentioned above.

Lemma 10

Suppose a series $\sum_{n\geq 1} a_n$ *converges absolutely. Define* $F(x) := \sum_{n\geq x} |a_n|$*. Then, for large enough* x*,*

$$\prod_{n\geq x}(1+a_n) = 1 + O(F(x)).$$

Proof. We start by taking the log of the product. Then, provided x is large enough, we will be guaranteed to have $|a_n| < 1$, so that we can rewrite $\log(1+a_n)$ as a power series. We obtain

$$\begin{aligned}
\left|\log \prod_{n\geq x}(1+a_n)\right| &= \left|\sum_{n\geq x}\log(1+a_n)\right| \\
&= \left|\sum_{n\geq x}\sum_{k\geq 1}\left(-\frac{(-a_n)^k}{k}\right)\right| \\
&\leq \sum_{n\geq x}\sum_{k\geq 1}|a_n|^k \\
&\ll F(x).
\end{aligned}$$

This then tells us that $\prod_{n\geq x}(1+a_n) = e^{O(F(x))} = 1 + O(F(x))$. Note that we know $F(x) = o(1)$ since we assumed that $\sum_{n\geq 1} a_n$ converges absolutely, so we are able to rewrite $e^{O(F(x))}$ in this way.

□

Finally, the following computational lemma will also be helpful in calculating the error terms in the sieves we will use.

Lemma 11

Let $r \in \mathbb{R}$ *with* $r > -1$ *and let* $s \in \mathbb{N} \setminus \{0\}$*. For each* $y > e$*, we have*

$$\sum_{n \leq y} n^r s^{\omega(n)} \ll_{r,s} y^{r+1} (\log y)^{s-1}. \tag{2.6}$$

Proof. We will first prove the formula when $r = 0$ by inducting on s. The base case, $s = 1$, is clear. Note that, for any $s \in \mathbb{N} \setminus \{0\}$,

$$s^{\omega(n)} \leq \sum_{d_1 d_2 \ldots d_s = n} 1. \tag{2.7}$$

Now, assume that (Equation 2.6) holds for $r = 0$ and some fixed s. Then we see from (Equation 2.7) above that

$$\begin{aligned}
\sum_{n\le y}(s+1)^{\omega(n)} &\le \sum_{n\le y}\sum_{d_1\ldots d_{s+1}=n} 1\\
&= \sum_{d_{s+1}\le y}\sum_{\substack{n\le y\\ d_{s+1}|n}}\sum_{d_1\ldots d_s=n/d_{s+1}} 1\\
&= \sum_{d_{s+1}\le y}\sum_{k\le y/d_{s+1}}\sum_{d_1\ldots d_s=k} 1\\
&\ll_s \sum_{d_{s+1}\le y}\frac{y}{d_{s+1}}\left(\log\frac{y}{d_{s+1}}\right)^{s-1}\\
&\ll_s y(\log y)^s.
\end{aligned}$$

This completes the induction, so we have verified the formula for $r = 0$. To prove it for $r \neq 0$, we start by fixing an $r > -1$ and $s \in \mathbb{N}\setminus\{0\}$. Then, using partial summation we obtain

$$\begin{aligned}
\sum_{n\le y} n^r s^{\omega(n)} &= y^r\sum_{n\le y}s^{\omega(n)} - r\int_1^y t^{r-1}\sum_{n\le t}s^{\omega(n)}dt\\
&\ll_r y^{r+1}(\log y)^{s-1} + \int_1^y t^r(\log t)^{s-1}dt.
\end{aligned}$$

The integral above can be evaluated through repeated uses of integration by parts and will also turn out to be $\ll_{r,s} y^{r+1}(\log y)^{s-1}$, which gives us the overall statement. □

2.3 Division fields of elliptic curves

Let E be an elliptic curve defined over $\mathbb{Q}$, of conductor N_E, and let m be a positive integer m. We denote by $\mathsf{E}[m]$ the group of $\overline{\mathbb{Q}}$-rational points of E of order dividing m and by $\mathbb{Q}(\mathsf{E}[m])$ the field obtained by adjoining to $\mathbb{Q}$ the x and y coordinates of the points of $\mathsf{E}[m]$. We recall from the theory of elliptic curves that the group $\mathsf{E}[m]$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^2$, that the field extension $\mathbb{Q}(\mathsf{E}[m])/\mathbb{Q}$ is finite and Galois, and that the rational primes that ramify in $\mathbb{Q}(\mathsf{E}[m])$ are among the prime factors of $m\mathsf{N}_\mathsf{E}$.

By fixing a $\mathbb{Z}/m\mathbb{Z}$-basis of $\mathsf{E}[m]$, we obtain a Galois representation

$$\overline{\rho}_{\mathsf{E},m} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$$

having the property that

$$\mathbb{Q}(\mathsf{E}[m]) = \overline{\mathbb{Q}}^{\mathrm{Ker}\,\overline{\rho}_{\mathsf{E},m}}. \tag{2.8}$$

The representation $\overline{\rho}_{\mathsf{E},m}$ is referred to as *the residual modulo* m *Galois representation of* $\mathsf{E}/\mathbb{Q}$. Taking the inverse limit over m of the representations $\overline{\rho}_{\mathsf{E},m}$, we obtain a continuous Galois representation

$$\rho_\mathsf{E} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2\left(\hat{\mathbb{Z}}\right),$$

referred to as *the absolute Galois representation of* $E/\mathbb{Q}$. Setting m to be powers ℓ^k of a fixed prime ℓ and taking the inverse limit over k of the representations $\overline{\rho}_{E,\ell^k}$, we obtain a continuous representation

$$\rho_{E,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2\left(\mathbb{Z}_\ell\right),$$

referred to as *the ℓ-adic Galois representation of* $E/\mathbb{Q}$.

We recall that, for each prime $p \nmid mN_E$, the p-Weil polynomial

$$P_{E,p}(X) := X^2 - a_p X + p \in \mathbb{Z}[X]$$

satisfies the congruence

$$P_{E,p}(X) \equiv \det\left(XI_2 - \overline{\rho}_{E,m}\left(\left(\frac{\mathbb{Q}(E[m]/\mathbb{Q}}{p}\right)\right)\right) \pmod{m},$$

where $\left(\frac{\mathbb{Q}(E[m]/\mathbb{Q}}{p}\right)$ denotes the Artin symbol at p in $\mathbb{Q}(E[m])/\mathbb{Q}$. Thus, we always have the congruences

$$\operatorname{tr} \overline{\rho}_{E,m}\left(\left(\frac{\mathbb{Q}(E[m]/\mathbb{Q}}{p}\right)\right) \equiv a_p \pmod{m} \tag{2.9}$$

and

$$\det \overline{\rho}_{E,m}\left(\left(\frac{\mathbb{Q}(E[m]/\mathbb{Q}}{p}\right)\right) \equiv p \pmod{m}.$$

Congruence (Equation 2.9) suggests that the field extension $\mathbb{Q}(E[m])/\mathbb{Q}$ plays a crucial role in the study of the arithmetic properties of a_p. In what follows, we record additional properties of this extension.

Thanks to (Equation 2.8), the Galois group $\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$, which we will denote by

$$G_E(m) := \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}),$$

may be identified with a subgroup of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$:

$$G_E(m) \simeq \overline{\rho}_{E,m}\left(G_E(m)\right) \leq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

As a consequence, the degree of the extension $\mathbb{Q}(E[m])/\mathbb{Q}$ has the natural upper bound

$$[\mathbb{Q}(E[m]) : \mathbb{Q}] \leq \#\,\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) = m^4 \prod_{\ell \mid m} \left(1 - \frac{1}{\ell}\right)\left(1 - \frac{1}{\ell^2}\right) \leq m^4. \tag{2.10}$$

If $E/\mathbb{Q}$ is without complex multiplication, then Serre's Open Image Theorem for elliptic curves (Se72) implies the existence of a smallest positive integer m_E having the property that, upon writing the fixed arbitrary integer m uniquely as

$$m = m_1 m_2 \tag{2.11}$$

for some positive integers m_1, m_2 such that

$$m_1 \mid m_E^\infty \quad \text{and} \quad \gcd(m_2, m_E) = 1,$$

there exists a subgroup $H_{E,m_1} \leq \mathrm{GL}_2(\mathbb{Z}/m_1\mathbb{Z})$ such that

$$G_E(m) \simeq H_{E,m_1} \times \mathrm{GL}_2(\mathbb{Z}/m_2\mathbb{Z}). \tag{2.12}$$

Following (Jo10), we will refer to m_E as *the torsion conductor of* $E/\mathbb{Q}$. For future purposes, let us note that m_E is an even positive integer (see (Jo10)).

As a consequence of (Equation 2.12), if $E/\mathbb{Q}$ is without complex multiplication, then the degree of $\mathbb{Q}(E[m])/\mathbb{Q}$ is the product of the function of m_1 defined by $[H_{E,m_1} : \mathbb{Q}]$ and the function of m_2 defined by $\#\,\mathrm{GL}_2(\mathbb{Z}/m_2\mathbb{Z})$. In particular, the degree of $\mathbb{Q}(E[m])/\mathbb{Q}$ obeys the lower bound

$$m_2^4 \prod_{\ell \mid m_2} \left(1 - \frac{1}{\ell}\right)\left(1 - \frac{1}{\ell^2}\right) = \#\,\mathrm{GL}_2(\mathbb{Z}/m_2\mathbb{Z}) \leq [\mathbb{Q}(E[m]) : \mathbb{Q}]\,.$$

Our approach to studying the prime factors of a_p will rely mostly on the properties of a particular subfield of the division field $\mathbb{Q}(E[m])$, defined as follows. Upon identifying $G_E(m)$

with its image under $\overline{\rho}_{E,m}$ in $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, we set J_m to be the subfield of $\mathbb{Q}(E[m])$ fixed by the scalar subgroup $\mathrm{Scal}_{G_E(m)}$ of $G_E(m)$, that is,

$$J_m := \mathbb{Q}(E[m])^{\mathrm{Scal}_{G_E(m)}},$$

where

$$\mathrm{Scal}_{G_E(m)} := G_E(m) \cap \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) : a \in (\mathbb{Z}/m\mathbb{Z})^\times \right\}.$$

We observe that

$$\mathrm{Scal}_{G_E(m)} \trianglelefteq G_E(m)$$

and deduce that $J_m/\mathbb{Q}$ is a finite Galois extension. We will call its Galois group

$$\widehat{G}_E(m) := \mathrm{Gal}(J_m/\mathbb{Q}).$$

Moreover, we observe that

$$J_m = \overline{\mathbb{Q}}^{\mathrm{Ker}\, \widehat{\rho}_{E,m}},$$

where

$$\widehat{\rho}_{E,m} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{PGL}_2(\mathbb{Z}/m\mathbb{Z})$$

is the Galois representation obtained by composing the natural projection $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \to \mathrm{PGL}_2(\mathbb{Z}/m\mathbb{Z})$ with $\overline{\rho}_{E,m}$. As a consequence, we obtain that the degree of $J_m/\mathbb{Q}$ satisfies the upper bounds

$$[J_m : \mathbb{Q}] \leq \# \mathrm{PGL}_2(\mathbb{Z}/m\mathbb{Z}) = m^3 \prod_{\ell \mid m} \left(1 - \frac{1}{\ell^2}\right) \leq m^3. \tag{2.13}$$

If $E/\mathbb{Q}$ is without complex multiplication, then, using factorization (Equation 2.11) of m and invoking Serre's Open Image Theorem as before, we deduce that

$$\widehat{G}_E(m) \simeq \frac{G_E(m)}{\mathrm{Scal}_{G_E(m)}} \simeq \frac{H_{E,m_1}}{\mathrm{Scal}_{H_{E,m_1}}} \times \mathrm{PGL}_2(\mathbb{Z}/m_2\mathbb{Z}). \tag{2.14}$$

Consequently, the degree of $J_m/\mathbb{Q}$ is the product of the function of m_1 defined by $\frac{\# H_{E,m_1}}{\# \mathrm{Scal}_{H_{E,m_1}}}$ and the function of m_2 defined by $\# \mathrm{PGL}_2(\mathbb{Z}/m_2\mathbb{Z})$. With additional work, by starting from the group isomorphism(Equation 2.14), it can be shown (see (CoJo21)) that the degree of $J_m/\mathbb{Q}$ obeys the lower bound $m^3 \ll_E [J_m : \mathbb{Q}]$.

2.4 Applications of the Chebotarev Density Theorem for division fields of elliptic curves

As in Section 2.3, let E be an elliptic curve defined over $\mathbb{Q}$, of conductor N_E, and let m be an arbitrary positive integer. Throughout this section, we always assume that E is without complex multiplication and we use the notation m_E for its torsion conductor, that is, the integer whose existence is ensured by Serre's Open Image Theorem for elliptic curves, as mentioned in Section 2.3. Similarly to the previous section, we use factorization (Equation 2.11) for m and we appeal to the group isomorphism (Equation 2.12), whenever needed.

Crucial to our analytic study of the primality of the Frobenius traces a_p of E are applications in the setting $\mathbb{Q}(E[m])/\mathbb{Q}$ and $J_m/\mathbb{Q}$ of an effective version of the Chebotarev Density Theorem, which we now recall.

Let L/K be a Galois extension of number fields, with $G := \mathrm{Gal}(L/K)$, and let $\emptyset \neq \mathcal{C} \subseteq G$ be a union of conjugacy classes of G. We denote by $[L:K]$ the degree of L over K, by $\mathrm{disc}(L/K) \trianglelefteq \mathcal{O}_K$ the discriminant ideal of L/K, and by $d_L \in \mathbb{Z}$ and $d_K \in \mathbb{Z}$ the discriminant of an integral basis of the ring of integers $\mathcal{O}_L$ of L, respectively of the ring of integers $\mathcal{O}_K$ of K. We set

$$\pi_{\mathcal{C}}(x, L/K) := \sum_{\substack{\mathfrak{p} \trianglelefteq \mathcal{O}_K \\ \mathfrak{p} \nmid \mathrm{disc}(L/K) \\ N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x}} \delta_{\mathcal{C}}\left(\left(\frac{L/K}{\mathfrak{p}}\right)\right),$$

where $\delta_{\mathcal{C}}(\cdot)$ is the characteristic function of $\mathcal{C}$, the sum is over non-zero prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ which are unramified in L/K and have norm $N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x$, and $\left(\frac{L/K}{\mathfrak{p}}\right) \subseteq G$ is the Artin symbol at $\mathfrak{p}$ in L/K.

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

$$\pi_{\mathcal{C}}(x, L/K) \sim \frac{\#\mathcal{C}}{\#G}\pi(x) \sim \frac{\#\mathcal{C}}{\#G}\,\mathrm{li}(x). \tag{2.15}$$

In studies such as ours, the above asymptotic formula is needed in a formulation that highlights the dependence of the growth of the error term $\left|\pi_{\mathcal{C}}(x, L/K) - \frac{\#\mathcal{C}}{\#G}\pi(x)\right|$ on the extension L/K and on the set $\mathcal{C}$. For this purpose, we introduce

$$\mathcal{P}(L/K) := \{p : \ \exists\, \mathfrak{p} \text{ non-zero prime ideal of } \mathcal{O}_K \text{ such that } \mathfrak{p} \mid p \text{ and } \mathfrak{p} \mid \mathrm{disc}(L/K)\}$$

and

$$M(L/K) := 2[L:K]|d_K|^{\frac{1}{[K:\mathbb{Q}]}} \prod_{p \in \mathcal{P}(L/K)} p,$$

and we recall that

$$\log \left| N_{K/\mathbb{Q}}(\operatorname{disc}(L/K)) \right| \leq ([L:\mathbb{Q}] - [K:\mathbb{Q}]) \left(\sum_{p \in \mathcal{P}(L/K)} \log p \right) + [L:\mathbb{Q}] \log[L:K] \tag{2.16}$$

(see (Se81, Proposition 5, p. 129)).

With this notation, we are now ready to state the effective version of (Equation 2.15) that we will be using in the proofs of our main results.

Theorem 12 *(Lagarias - Odlyzko; Serre)*
Let L/K be a Galois extension of number fields, with $G := \mathrm{Gal}(L/K)$, and let $\emptyset \neq \mathcal{C} \subseteq G$ be a union of conjugacy classes of G. Assume that, for some $\frac{1}{2} \leq \theta < 1$, the θ-quasi-GRH holds for the number field L. Then there exists an absolute constant $c > 0$ such that, for any $x > e$,

$$\left| \pi_{\mathcal{C}}(x, L/K) - \frac{\#\mathcal{C}}{\#G} \pi(x) \right| \leq c \frac{\#\mathcal{C}}{\#G} x^{\theta} \left(\log |d_L| + [L:\mathbb{Q}] \log x \right).$$

Proof. The original reference is (LaOd77). For this variation, see (Se81, Théorème 4, p. 133). □

The particular elliptic curve settings of Theorem 12 of relevance to our study are

$$L = \mathbb{Q}(E[m])), \ K = \mathbb{Q}, \ \mathcal{C} = \mathcal{C}_E(m, \alpha)$$

for a fixed $\alpha \in \mathbb{Z}$, and

$$L = J_m,\ K = \mathbb{Q},\ \mathcal{C} = \widehat{\mathcal{C}}_E(m, 0),$$

where

$$\mathcal{C}_E(m, \alpha) := \{M \in G_E(m) : \operatorname{tr} M \equiv \alpha \pmod{m}\}$$

and

$$\widehat{\mathcal{C}}_E(m, 0) := \left\{\widehat{M} \in \widehat{G}_E(m) : \operatorname{tr} M \equiv 0 \pmod{m}\right\},$$

with $M \in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ denoting an arbitrary representative of a given coset $\widehat{M} \in \mathrm{PGL}_2(\mathbb{Z}/m\mathbb{Z})$.

Observe that the group isomorphism (Equation 2.12) gives rise to the bijection

$$\begin{aligned} \mathcal{C}_E(m, \alpha) &\rightarrow \mathcal{C}_E(m_1, \alpha) \times \mathcal{C}(m_2, \alpha) \\ M &\mapsto (M_1, M_2), \end{aligned} \tag{2.17}$$

where

$$\mathcal{C}_E(m_1, \alpha) := \{M_1 \in H_{E,m_1} : \operatorname{tr} M_1 \equiv \alpha \pmod{m_1}\},$$

$$\mathcal{C}(m_2, \alpha) := \{M_2 \in \mathrm{GL}_2(\mathbb{Z}/m_2\mathbb{Z}) : \operatorname{tr} M_2 \equiv \alpha \pmod{m_2}\},$$

and that the group isomorphism (Equation 2.14) gives rise to the bijection

$$\begin{aligned} \widehat{\mathcal{C}}_E(m, 0) &\rightarrow \widehat{\mathcal{C}}_E(m_1, 0) \times \widehat{\mathcal{C}}(m_2, 0) \\ \widehat{M} &\mapsto \left(\widehat{M}_1, \widehat{M}_2\right), \end{aligned} \tag{2.18}$$

where

$$\widehat{\mathcal{C}}_E(m_1, 0) := \left\{ \widehat{M_1} \in H_{E,m_1} / \operatorname{Scal}_{H_{E,m_1}} : \operatorname{tr} M_1 \equiv 0 \pmod{m_1} \right\},$$

$$\widehat{\mathcal{C}}(m_2, 0) := \left\{ \widehat{M_2} \in \operatorname{PGL}_2(\mathbb{Z}/m_2\mathbb{Z}) : \operatorname{tr} M_2 \equiv 0 \pmod{m_2} \right\},$$

with $M_1 \in H_{E,m_1}$ an arbitrary representative of a given coset $\widehat{M_1} \in H_{E,m_1} / \operatorname{Scal}_{H_{E,m_1}}$ and with $M_2 \in \operatorname{GL}_2(\mathbb{Z}/m_2\mathbb{Z})$ an arbitrary representative of a given coset $\widehat{M_2} \in \operatorname{PGL}_2(\mathbb{Z}/m_2\mathbb{Z})$.

With this notation, we are ready to write two particular cases of Theorem 12.

Theorem 13

Let E be an elliptic curve defined over $\mathbb{Q}$, of conductor N_E, without complex multiplication, and of torsion conductor m_E. Let $m = m_1 m_2$ be a positive integer such that $m_1 \mid m_E^\infty$ and $\gcd(m_2, m_E) = 1$.

(i) Let $\alpha \in \mathbb{Z}$. Assume that, for some $\frac{1}{2} \leq \theta < 1$, the θ-quasi-GRH holds for $\mathbb{Q}(E[m])/\mathbb{Q}$. Then

$$\begin{aligned} &\#\{p \leq x : p \nmid mN_E, a_p \equiv \alpha \pmod{m}\} \\ = &\frac{\#\mathcal{C}_E(m_1, \alpha) \cdot \#\mathcal{C}(m_2, \alpha)}{\#H_{E,m_1} \cdot \# \operatorname{GL}_2(\mathbb{Z}/m_2\mathbb{Z})} \pi(x) + O_E\left(\#\mathcal{C}(m_2, \alpha)\ x^\theta \log(mN_E x)\right). \end{aligned}$$

(ii) Assume that, for some $\frac{1}{2} \leq \theta < 1$, the θ-quasi-GRH holds for $J_m/\mathbb{Q}$. Then

$$\begin{aligned} &\#\{p \leq x : p \nmid mN_E, a_p \equiv 0 \pmod{m}\} \\ = &\frac{\#\widehat{\mathcal{C}}_E(m_1, 0) \cdot \# \operatorname{Scal}_{H_{E,m_1}} \cdot \#\widehat{\mathcal{C}}(m_2, 0)}{\#H_{E,m_1} \cdot \# \operatorname{PGL}_2(\mathbb{Z}/m_2\mathbb{Z})} \pi(x) + O_E\left(\#\widehat{\mathcal{C}}(m_2, 0)\ x^\theta \log(mN_E x)\right). \end{aligned}$$

Proof. Recalling (Equation 2.13) and that the ramified primes of $\mathbb{Q}(E[m])/\mathbb{Q}$, hence of $J_m/\mathbb{Q}$, are among the prime factors of mN_E, by applying (Equation 2.10), respectively (Equation 2.16), we deduce that

$$\frac{\log|d_{\mathbb{Q}(E[m])}|}{[\mathbb{Q}(E[m]):\mathbb{Q}]} \leq \sum_{p\in\mathcal{P}(\mathbb{Q}(E[m])/\mathbb{Q})} \log p + \log[\mathbb{Q}(E[m]):\mathbb{Q}] \ll \log(mN_E)$$

and

$$\frac{\log|d_{J_m}|}{[J_m:\mathbb{Q}]} \leq \sum_{p\in\mathcal{P}(J_m/\mathbb{Q})} \log p + \log[J_m:\mathbb{Q}] \ll \log(mN_E).$$

The asymptotic formulae claimed in the statement of the theorem now follow from Theorem 12 by using these estimates, along with (Equation 2.17) and (Equation 2.18). □

It is clear that any application of the above theorem will require a better understanding of the matrix counts that occur in both the main term and the error term of each of the two asympotic formulae. We record such counts below.

Lemma 14

Let ℓ be an odd prime and let $\alpha \in \mathbb{Z}$. Then

$$\#\mathcal{C}(\ell,\alpha) = \begin{cases} \ell^3-\ell^2-\ell & \text{if } \alpha \not\equiv 0 \pmod{\ell}, \\ \ell^3-\ell^2 & \text{if } \alpha \equiv 0 \pmod{\ell}; \end{cases} \tag{2.19}$$

$$\#\mathcal{C}\left(\ell^2,\alpha\right) = \ell^6-\ell^5 \quad \text{if } \alpha \equiv 0 \pmod{\ell}; \tag{2.20}$$

$$\#\widehat{\mathcal{C}}(\ell,0) = \ell^2; \tag{2.21}$$

$$\#\widehat{\mathcal{C}}\left(\ell^2, 0\right) = \ell^4. \tag{2.22}$$

Proof. Let us focus on proving formula (Equation 2.19) for $\#\mathcal{C}(\ell, \alpha)$ in the case $\alpha \equiv 0 \pmod{\ell}$. First, we see easily that there are ℓ^3 matrices with trace 0 in $\mathcal{M}_{2\times 2}(\mathbb{Z}/\ell\mathbb{Z})$; but how many have determinant 0 (mod ℓ)? Any matrix $M \in \mathcal{M}_{2\times 2}(\mathbb{Z}/\ell\mathbb{Z})$ with trace 0 can be written in the form

$$M = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$$

for some $a, b, c \in \mathbb{Z}/\ell\mathbb{Z}$. For a fixed pair $b, c \in \mathbb{Z}/\ell\mathbb{Z}$, there will be $1 + (\frac{-bc}{\ell})$ possible a such that $\det M \equiv 0 \pmod{\ell}$, where $(\frac{\cdot}{\ell})$ is the Legendre symbol. Thus, the number of matrices $M \in \mathcal{M}_{2\times 2}(\mathbb{Z}/\ell\mathbb{Z})$ with $\operatorname{tr} M \equiv \det M \equiv 0 \pmod{\ell}$ will be given by

$$\sum_{b,c \in \mathbb{Z}/\ell\mathbb{Z}} \left(1 + \left(\frac{-bc}{\ell}\right)\right) = \ell^2 + \sum_{b \in (\mathbb{Z}/\ell\mathbb{Z})^\times} \sum_{c \in (\mathbb{Z}/\ell\mathbb{Z})^\times} \left(\frac{-bc}{\ell}\right) = \ell^2.$$

We deduce that

$$\#\{M \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \operatorname{tr} M \equiv 0 \pmod{\ell}\} = \ell^3 - \ell^2 = \ell^2\phi(\ell), \tag{2.23}$$

establishing formula (Equation 2.19) for $\#\mathcal{C}(\ell, \alpha)$ in the case $\alpha \equiv 0 \pmod{\ell}$.

Now, let us focus on proving formula (Equation 2.19) for $\#\mathcal{C}(\ell,\alpha)$ in the case $\alpha \not\equiv 0 \,(\mathrm{mod}\, \ell)$. Note that, for any $\alpha_1, \alpha_2 \in (\mathbb{Z}/\ell\mathbb{Z})^\times$, by setting $\beta := \alpha_2\alpha_1^{-1}$, the map

$$\begin{array}{ccc} \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) & \longrightarrow & \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \\ M & \mapsto & \beta M \end{array}$$

induces a bijection

$$\{M \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \operatorname{tr} M = \alpha_1\} \longrightarrow \{M \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \operatorname{tr} M = \alpha_2\}.$$

This observation leads to formula (Equation 2.19) for $\#\mathcal{C}(\ell,\alpha)$ in the case $\alpha \not\equiv 0 \; (\mathrm{mod}\, \ell)$.

Next, observe that we can write any $M \in \mathcal{M}_{2\times 2}(\mathbb{Z}/\ell^2\mathbb{Z})$ with $\operatorname{tr} M \equiv 0 \; (\mathrm{mod}\, \ell)$ uniquely in the form

$$M = \begin{pmatrix} a_0 + a_1\ell & b_0 + b_1\ell \\ c_0 + c_1\ell & -a_0 - a_1\ell \end{pmatrix}$$

for some $a_0, a_1, b_0, b_1, c_0, c_1 \in \mathbb{Z}/\ell\mathbb{Z}$. From here, the calculation is identical to the one for formula (Equation 2.19) for $\#\mathcal{C}(\ell, 0)$, except for taking into account that we have three completely free variables in a_1, b_1, c_1, so both the number of matrices with trace 0 and the number of matrices with trace and determinant 0 increase by a factor of ℓ^3. We deduce that

$$\#\left\{M \in \mathrm{GL}_2\left(\mathbb{Z}/\ell^2\mathbb{Z}\right) : \operatorname{tr} M \equiv 0 \left(\mathrm{mod}\, \ell^2\right)\right\} = \ell^6 - \ell^5 = \ell^4\phi\left(\ell^2\right). \tag{2.24}$$

From (Equation 2.23) and (Equation 2.24), respectively, we conclude that

$$\#\widehat{\mathcal{C}}(\ell, 0) = \frac{\#\mathcal{C}(\ell, 0)}{\phi(\ell)} = \ell^2$$

and

$$\#\widehat{\mathcal{C}}(\ell^2, 0) = \frac{\#\mathcal{C}(\ell^2, 0)}{\phi(\ell^2)} = \ell^4.$$

□

Of primary interest to us is the following application of part (ii) of Theorem 13.

Theorem 15

Let E be an elliptic curve defined over $\mathbb{Q}$, of conductor N_E, without complex multiplication, and of torsion conductor m_E.

(i) Let d be a squarefree positive integer such that $\gcd(d, m_E) = 1$. Assume that there exists some $\frac{1}{2} \leq \theta < 1$ such that the θ-quasi-GRH holds for $J_{dk}/\mathbb{Q}$ for all positive squarefree integers k with $k \mid m_E$. Then

$$\begin{aligned}&\#\{a_p : p \leq x, p \nmid N_E, \gcd(a_p, m_E) = 1, a_p \equiv 0 \pmod{d}\} \\ &= \frac{1}{d}\left(\prod_{\ell \mid d}\left(1 - \frac{1}{\ell^2}\right)^{-1}\right) C_1(E)\pi(x) + O_E\left(d^2 x^\theta \log(dx)\right),\end{aligned}$$

where

$$C_1(E) := \frac{\#\{M \in G_E(m_E) : \gcd(\operatorname{tr} M, m_E) = 1\}}{\#G_E(m_E)}. \tag{2.25}$$

(ii) Let ℓ be a prime such that $\ell \nmid m_E$. Assume that there exists some $\frac{1}{2} \leq \theta < 1$ such that the θ-quasi-GRH holds for $J_{\ell^2}/\mathbb{Q}$. Then

$$\begin{aligned}\#\left\{a_p : p \leq x, p \nmid N_E, \gcd(a_p, m_E) = 1, a_p \equiv 0 \left(\bmod \ell^2\right)\right\}\\ = \frac{1}{\ell^2 - 1} \cdot C_1(E)\pi(x) + O_E\left(\ell^4 x^\theta \log(\ell x)\right),\end{aligned}$$

with $C_1(E)$ defined as in (Equation 2.25).

Proof. Let m be a positive integer with $\gcd(m, m_E) = 1$, so that, in the notation $m = m_1 m_2$ of Theorem 13, $m_1 = 1$ and $m_2 = m$. We want to estimate the cardinality of the set

$$\mathcal{A}_m := \{a_p : p \leq x, p \nmid N_E, \gcd(a_p, m_E) = 1, a_p \equiv 0 \,(\bmod\, m)\} \tag{2.26}$$

when m is an odd squarefree positive integer such that, for some $\frac{1}{2} \leq \theta < 1$, the θ-quasi-GRH holds for $J_{mk}/\mathbb{Q}$ for all positive squarefree integers k with $k \mid m_E$, and when $m = \ell^2$ for some odd prime ℓ such that, for some $\frac{1}{2} \leq \theta < 1$, the θ-quasi-GRH holds for $J_{\ell^2}/\mathbb{Q}$.

Before making these particular choices of m, let us observe that

$$
\begin{aligned}
\#\mathcal{A}_m &= \#\{a_p : p \le x, p \nmid N_E, \gcd(a_p, m_E) = 1, a_p \equiv 0 \pmod m\} \\
&= \#\{a_p : p \le x, p \nmid mN_E, \gcd(a_p, m_E) = 1, a_p \equiv 0 \pmod m\} + O(\log m) \\
&= \left(\sum_{\substack{p \le x \\ p \nmid mN_E \\ a_p \equiv 0 \ (\mathrm{mod}\ m)}} \ \sum_{\substack{k \ge 1 \\ k \mid \gcd(a_p, m_E)}} \mu(k) \right) + O(\log m) \\
&= \left(\sum_{\substack{k \ge 1 \\ k \mid m_E}} \mu(k) \#\{p \le x : p \nmid mN_E, a_p \equiv 0 \pmod m, a_p \equiv 0 \pmod k\} \right) + O(\log m) \\
&= \left(\sum_{\substack{k \ge 1 \\ k \mid m_E}} \left(\mu(k) \#\{p \le x : p \nmid mkN_E, a_p \equiv 0 \pmod{mk}\} + O(\log k)\right) \right) + O(\log m) \\
&= \left(\sum_{\substack{k \ge 1 \\ k \mid m_E}} \mu(k) \#\{p \le x : p \nmid mkN_E, a_p \equiv 0 \pmod{mk}\} \right) + O(\log x),
\end{aligned}
$$

where, to pass to the second and fifth lines, we used that for any positive integer n, $\omega(n) \le 2 \log n$; and to pass to the fifth line, we used that $\gcd(m, k) = 1$ since $k \mid m_E$ and $\gcd(m, m_E) = 1$.

By invoking part (ii) of Theorem 13 under the assumption of a θ-quasi-GRH for $J_{mk}/\mathbb{Q}$ for all positive squarefree integers k with $k \mid m_E$, we obtain that

$$
\#\mathcal{A}_m = \frac{\#\widehat{\mathcal{C}}(m, 0)}{\#\,\mathrm{PGL}_2(\mathbb{Z}/m\mathbb{Z})} \left(\sum_{\substack{k \ge 1 \\ k \mid m_E}} \mu(k) \frac{\#\widehat{\mathcal{C}}_E(k, 0) \cdot \#\,\mathrm{Scal}_{H_{E,k}}}{\#H_{E,k}} \right) \pi(x) + O_E\left(\#\widehat{\mathcal{C}}(m, 0)\ x^{\theta} \log(mN_E x)\right). \tag{2.27}
$$

Now, let us analyze the summation over $k \mid m_E$. Observe that, for each such k, we have

$$\#\widehat{\mathcal{C}}_E(k,0)\cdot \#\,\mathrm{Scal}_{H_{E,k}} = \#\{M \in G_E(k) : \operatorname{tr} M \equiv 0 \pmod{k}\}.$$

Furthermore,

$$\begin{aligned}\frac{\#\{M \in G_E(k) : \operatorname{tr} M \equiv 0 \pmod{k}\}}{\#H_{E,k}} &= \frac{\#\{M \in G_E(k) : \operatorname{tr} M \equiv 0 \pmod{k}\}}{\#G_E(k)} \\ &= \frac{\#\{M \in G_E(m_E) : \operatorname{tr} M \equiv 0 \pmod{k}\}}{\#G_E(m_E)}.\end{aligned}$$

Then

$$\begin{aligned}\sum_{\substack{k\geq 1\\ k\mid m_E}} \mu(k)\frac{\#\widehat{\mathcal{C}}_E(k,0)\cdot \#\,\mathrm{Scal}_{H_{E,k}}}{\#H_{E,k}} &= \frac{1}{\#G_E(m_E)}\sum_{\substack{k\geq 1\\ k\mid m_E}} \mu(k)\#\{M \in G_E(m_E) : \operatorname{tr} M \equiv 0 \pmod{k}\} \\ &= \frac{\#\{M \in G_E(m_E) : \operatorname{tr} M \not\equiv 0 \pmod{\ell}\ \forall \ell \mid m_E\}}{\#G_E(m_E)} \\ &= C_1(E).\end{aligned}$$

Plugging this in (Equation 2.27), we obtain that, under the assumption of a θ-quasi-GRH for $J_{mk}/\mathbb{Q}$ for all positive squarefree integers k with $k \mid m_E$,

$$\#\mathcal{A}_m = \frac{\#\widehat{\mathcal{C}}(m,0)}{\#\,\mathrm{PGL}_2(\mathbb{Z}/m\mathbb{Z})}\cdot C_1(E)\pi(x) + O_E\left(\#\widehat{\mathcal{C}}(m,0)\ x^{\theta}\log(mN_E x)\right).$$

Next, let us specialize (Equation 2.27) to our two desired types of m.

(i) In (Equation 2.27), take $m = d$ for some odd squarefree positive integer d coprime to m_E. The claimed estimate for $\#\mathcal{A}_d$ follows by invoking the Chinese Remainder Theorem and by recalling that, from Lemma 14, for any odd prime ℓ we have $\#\widehat{\mathcal{C}}(\ell, 0) = \ell^2$.

(ii) In (Equation 2.27), take $m = \ell^2$ for some odd prime $\ell \nmid m_E$. The claimed estimate for $\#\mathcal{A}_{\ell^2}$ follows by recalling that, from Lemma 14, $\#\widehat{\mathcal{C}}\left(\ell^2, 0\right) = \ell^4$. □

We end this section with an application of part (i) of Theorem 12, which we will need in the proof of our two main theorems:

Proposition 16

Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication, of conductor N_E, and of torsion conductor m_E. Assume that there exists some $\frac{1}{2} \le \theta < 1$ such that the θ-quasi-GRH holds for the division fields of E. Then, for any $\alpha \in \mathbb{Z}$ with $\alpha \neq 0$,

$$\#\{p \le x : p \nmid N_E, a_p = \alpha\} \ll_E \frac{x^{1-\frac{1-\theta}{4}}}{(\log x)^{\frac{1}{2}}}, \tag{2.28}$$

and

$$\#\{p \le x : p \nmid N_E, a_p = 0\} \ll_E \frac{x^{1-\frac{1-\theta}{3}}}{(\log x)^{\frac{1}{3}}}. \tag{2.29}$$

Proof. Let ℓ be a prime such that $\ell \nmid m_E$. Then

$$\#\{p \le x : p \nmid N_E, a_p = \alpha\} \le \#\{p \le x : p \nmid N_E, a_p \equiv \alpha \,(\mathrm{mod}\, \ell)\}$$

and, for the latter, we invoke part (i) of Theorem 13. By also using (Equation 2.19) of Lemma 14, we obtain that

$$\#\{p \leq x : p \nmid N_E, a_p \equiv \alpha \pmod{\ell}\} \ll_E \frac{x}{\ell \log x} + \ell^3 x^\theta \log(\ell x).$$

Choosing $\ell \asymp \frac{x^{\frac{1-\theta}{4}}}{(\log x)^{\frac{1}{2}}}$ gives us the desired upper bound for $\#\{p \leq x : p \nmid N_E, a_p = \alpha\}$.

When $\alpha = 0$, the result can be strengthened by invoking part (ii) of Theorem 13 and (Equation 2.21) of Lemma 14, leading to the upper bounds

$$\#\{p \leq x : p \nmid N_E, a_p = 0\} \leq \#\{p \leq x : p \nmid N_E, a_p \equiv 0 \pmod{\ell}\} \ll_E \frac{x}{\ell \log x} + \ell^2 x^\theta \log(\ell x).$$

Choosing $\ell \asymp \frac{x^{\frac{1-\theta}{3}}}{(\log x)^{\frac{2}{3}}}$ gives us the desired upper bound for $\#\{p \leq x : p \nmid N_E, a_p = 0\}$. $\square$

Note that much better conditional results are known regarding upper bounds for

$$\#\{p \leq x : p \nmid N_E, a_p = \alpha\}$$

(e.g., see (MuMuSa88) for better conditional bounds, and (CoWa21, Section 1) for a recent account of the best such bounds as of the writing of this thesis). For the purpose of our two main theorems, the weaker upper bound (Equation 2.28) of Lemma 16, under the assumption of a θ-quasi-GRH and not of the full GRH, suffices. Note also that a stronger unconditional result is known only for $\alpha = 0$, and in that case the weaker conditional upper bound (Equation 2.29) of Lemma 16 is superfluous (see (El91)).

CHAPTER 3

MAIN THEOREMS

3.1 Heuristical reasoning for the conjectural asymptotic formula

Let E be an elliptic curve over $\mathbb{Q}$, of conductor N_E, without complex multiplication, and of torsion conductor m_E. To count the number of primes $p \nmid N_E$ such that a_p is prime, we outline the heuristical approach of (Co21).

Recalling that, for each prime $p \nmid N_E$, we have $|a_p| < 2\sqrt{p}$, we consider a naive probabilistic model in which the integer a_p is replaced with a random integer r_p in the interval $(-2\sqrt{p}, 2\sqrt{p})$. Observing that, for any $\varepsilon > 0$,

$$\lim_{p\to\infty} \frac{\#\left\{r_p \in (-2\sqrt{p}, 2\sqrt{p}) \cap \mathbb{Z} : |r_p| \leq p^{\frac{1}{2}-\varepsilon}\right\}}{\#\left\{r_p \in (-2\sqrt{p}, 2\sqrt{p}) \cap \mathbb{Z}\right\}} = 0,$$

we deduce that for all but a zero density set of primes p (within the set of primes) we have that, as $p \to \infty$,

$$\text{Prob}\ (r_p \text{ is prime}) \sim \frac{1}{\log\sqrt{p}} = \frac{2}{\log p}.$$

As such, it is natural to predict that, as $x \to \infty$,

$$\begin{aligned}\#\{p \leq x : p \nmid N_E, r_p \text{ is prime}\} &\sim \int_2^x \frac{1}{\log t} \cdot \frac{2}{\log t} dt \\ &= 2\int_2^x \frac{1}{(\log t)^2} dt \\ &\sim \frac{2x}{(\log x)^2}.\end{aligned}$$

Let us note that in the above discussion we replaced the Frobenius trace a_p with a *random* integer r_p in the interval $(-2\sqrt{p}, 2\sqrt{p})$. However, according to (Equation 2.9), for any positive integer m, the probability that a_p is coprime to m equals

$$\frac{\#\{M \in G_E(m) : \gcd(\operatorname{tr} M, m) = 1\}}{\# G_E(m)},$$

while, from elementary number theory, the probability that r_p is coprime to m equals

$$\frac{\phi(m)}{m}.$$

Thus, in our previous naive probabilistic model, for each m we should introduce the correction factor

$$f(m) := \frac{m}{\phi(m)} \cdot \frac{\#\{M \in G_E(m) : \gcd(\operatorname{tr} M, m) = 1\}}{\# G_E(m)}.$$

As a consequence of Serre's Open Image Theorem for $E/\mathbb{Q}$ and on matrix counting arguments in $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, upon taking $m_n := \prod_{\substack{\ell \leq n \\ \ell \text{ prime}}} \ell$, the limit $\lim_{n\to\infty} f(m_n)$ exists and equals $\frac{C(E)}{2}$, where

$$C(E) := 2 \cdot \frac{m_E}{\phi(m_E)} \cdot \frac{\#\{M \in G_E(m_E) : \gcd(\operatorname{tr} M, m_E) = 1\}}{\# G_E(m_E)} \cdot \prod_{\substack{\ell \nmid m_E \\ \ell \text{ prime}}} \left(1 - \frac{1}{\ell^3 - \ell^2 - \ell + 1}\right),$$

as introduced in (Equation 1.12). Therefore, it is now natural to predict that, as $x \to \infty$,

$$\#\{p \leq x : p \nmid N_E, a_p \text{ is prime}\} \sim \frac{C(E)}{2} \cdot \#\{p \leq x : p \nmid N_E, r_p \text{ is prime}\} \sim C(E) \frac{x}{(\log x)^2},$$

as claimed in (Equation 1.11).

Remark. We tested the above prediction using the elliptic curve

$$E/\mathbb{Q} : y^2 = x^3 + 6x - 2,$$

for which $N_E = 2^6 \cdot 3^3$. This is an elliptic curve without complex multiplication for which $m_E = 6$. We obtained that

$$C(E) = 2 \cdot \frac{6}{2} \cdot \frac{36}{144} \cdot \prod_{\substack{\ell \geq 5 \\ \ell \text{ prime}}} \left(1 - \frac{1}{\ell^3 - \ell^2 - \ell + 1}\right) = 1.476318...$$

and that

$$\frac{\#\left\{5 \leq p \leq 10^8 : a_p \text{ is prime}\right\}}{C(E) \sum_{p \leq 10^8} \frac{1}{\log p}} = 1.070829...$$

In future work, we plan to test our prediction on a wider sample of elliptic curves and on a wider sequence of primes.

3.2 Sieve commonalities for elliptic curve setting

In the proofs of our two main theorems, we apply the Selberg sieve and the weighted Greaves' sieve, respectively, in the following setting. We fix an elliptic curve $E/\mathbb{Q}$, of conductor N_E, without complex multiplication, and of torsion conductor m_E, and we assume that there exists some $\frac{1}{2} \leq \theta < 1$ such that the θ-quasi-GRH holds for $\mathbb{Q}(E[m])/\mathbb{Q}$ and $J_m/\mathbb{Q}$ for all positive integers m. We fix $x > 0$, to be thought of as going to infinity, and we take

$$\begin{aligned}
\mathcal{A} &:= \{a_p : p \leq x, p \nmid N_E, \gcd(a_p, m_E) = 1\}, \\
\mathcal{P} &:= \{\ell : \ \ell \nmid m_E\}.
\end{aligned}$$

With these definitions, we see that, for each positive squarefree d with $\gcd(d, m_E) = 1$,

$$\mathcal{A}_d = \{a_p : p \leq x, p \nmid N_E, \gcd(a_p, m_E) = 1, a_p \equiv 0 \ (\mathrm{mod}\ d)\},$$

and that, for each prime $\ell \nmid m_E$,

$$\mathcal{A}_{\ell^2} = \{a_p : p \leq x, p \nmid N_E, \gcd(a_p, m_E) = 1, a_p \equiv 0 \ (\mathrm{mod}\ \ell^2)\}.$$

In this sieve setting, it remains to identify X, $w(\cdot)$, and the growth of $|R_d|$ and $|R_{\ell^2}|$, which is what we do next.

Recalling that these were the sets introduced in (Equation 2.26) of Subsection 2.4, from Theorem 15 we deduce that

$$\#\mathcal{A}_d = \frac{1}{d}\left(\prod_{\ell \mid d}\left(1-\frac{1}{\ell^2}\right)^{-1}\right) C_1(E)\pi(x) + O_E\left(d^2 x^\theta \log(dx)\right) \tag{3.1}$$

and

$$\#\mathcal{A}_{\ell^2} = \frac{1}{\ell^2-1}\cdot C_1(E)\pi(x) + O_E\left(\ell^4 x^\theta \log(\ell x)\right).$$

From the above observations, we conclude that, in our particular sieve setting, we may take

$$X := C_1(E)\pi(x) \tag{3.2}$$

and

$$w(d) := \prod_{\ell \mid d}\left(1-\frac{1}{\ell^2}\right)^{-1}, \tag{3.3}$$

in which case

$$|R_d| \ll_E d^2 x^\theta \log(dx) \tag{3.4}$$

and

$$|R_{\ell^2}| \ll_E \ell^4 x^\theta \log(\ell x). \tag{3.5}$$

We emphasize that the exponent θ reflects the assumption of the θ-quasi-GRH.

Using (Equation 3.3), for $z > m_E$ the function $V(z)$ defined in (Equation 2.5) of Section 2.1 becomes

$$
\begin{aligned}
V(z) &:= \prod_{\substack{\ell<z \\ \ell\nmid m_E}} \left(1 - \ell^{-1}\left(1-\frac{1}{\ell^2}\right)^{-1}\right) \\
&= \left(\prod_{\substack{\ell<z \\ \ell\nmid m_E}} \left(1-\frac{1}{\ell}\right)\right) \cdot \left(\prod_{\substack{\ell<z \\ \ell\nmid m_E}} \left(1-\frac{1}{\ell^3-\ell^2-\ell+1}\right)\right) \\
&= \left(\prod_{\substack{\ell<z \\ \ell\mid m_E}} \left(1-\frac{1}{\ell}\right)^{-1}\right) \cdot \left(\prod_{\ell<z} \left(1-\frac{1}{\ell}\right)\right) \cdot \left(\prod_{\ell\nmid m_E} \left(1-\frac{1}{\ell^3-\ell^2-\ell+1}\right)\right) \cdot \left(\prod_{\ell\geq z} \left(1-\frac{1}{\ell^3-\ell^2-\ell+1}\right)\right)^{-1} \\
&= \frac{m_E}{\phi(m_E)} \cdot \left(\prod_{\ell<z} \left(1-\frac{1}{\ell}\right)\right) \cdot \left(\prod_{\ell\nmid m_E} \left(1-\frac{1}{\ell^3-\ell^2-\ell+1}\right)\right) \cdot \left(\prod_{\ell\geq z} \left(1+\frac{1}{\ell^3-\ell^2-\ell}\right)\right) \\
&= \frac{m_E}{\phi(m_E)} \cdot \left(\prod_{\ell\nmid m_E} \left(1-\frac{1}{\ell^3-\ell^2-\ell+1}\right)\right) \cdot \left(\prod_{\ell<z} \left(1-\frac{1}{\ell}\right)\right) \cdot \left(1 + O\left(\frac{1}{z^2}\right)\right) \\
&= \frac{m_E}{\phi(m_E)} \cdot \left(\prod_{\ell\nmid m_E} \left(1-\frac{1}{\ell^3-\ell^2-\ell+1}\right)\right) \cdot \left(\frac{e^{-\gamma}}{\log z} + o\left(\frac{1}{\log z}\right)\right).
\end{aligned}
$$

Here, we have used Lemma 10 to pass from the fourth line to the fifth, and Mertens' Third Theorem 9 to pass from the fifth line to the sixth.

For later purposes, let us record the above calculation as

$$V(z) = C_2(E) \cdot \left(\frac{e^{-\gamma}}{\log z} + o\left(\frac{1}{\log z}\right)\right), \tag{3.6}$$

where

$$C_2(E) := \frac{m_E}{\phi(m_E)} \cdot \prod_{\ell\nmid m_E} \left(1-\frac{1}{\ell^3-\ell^2-\ell+1}\right). \tag{3.7}$$

We can now verify that the sieve assumptions mentioned previously, (Equation 2.3) and (Equation 2.4), which will be required for both the Selberg sieve and the Greaves sieve, are satisfied. Firstly, $w(\cdot)$ is easily seen to be decreasing on prime values, so that for any prime, ℓ,

$$0 \leq \frac{w(\ell)}{\ell} \leq \frac{2}{3}.$$

Therefore, the first assumption is satisfied. Now, for the second assumption, fix z_1 and z_2 with $2 \leq z_1 \leq z_2$. Then

$$\begin{aligned}
\sum_{z_1 \leq \ell < z_2} \frac{w(\ell)}{\ell} \log \ell &= \sum_{z_1 \leq \ell < z_2} \frac{\left(1 - \frac{1}{\ell^2}\right)^{-1}}{\ell} \log \ell \\
&= \sum_{z_1 \leq \ell < z_2} \frac{\ell}{\ell^2 - 1} \log \ell \\
&= \sum_{z_1 \leq \ell < z_2} \frac{\log \ell}{\ell} + \sum_{z_1 \leq \ell < z_2} \frac{\log \ell}{\ell(\ell^2 - 1)}. \qquad (3.8)
\end{aligned}$$

Using Mertens' First Theorem 8, we see that the first sum in line (Equation 3.8) differs from $\log \frac{z_2}{z_1}$ by at most 4. Extending the range of the second sum to all primes $\ell \geq 2$ yields a series that converges to a value less than 1, so that

$$\left| \sum_{z_1 \leq \ell < z_2} \frac{w(\ell)}{\ell} \log \ell - \log \frac{z_2}{z_1} \right| < 5. \qquad (3.9)$$

Thus, the second assumption, (Equation 2.4), holds in this setting as well.

3.3 Proof of Main Theorem A

To prove Main Theorem A, we will use a simplified version of the Selberg sieve as presented in (HaRi74, Thm. 8.3, p. 231).

Theorem 17 *(Selberg Sieve)*

Assume the setting described at the beginning of Section 2.1. In particular, with notation as described in that section, assume that for any squarefree d *composed of primes in* $\mathcal{P}$*,* $\#\mathcal{A}_d$ *can be written in the form*

$$\#\mathcal{A}_d = \frac{w(d)}{d} X + R_d$$

for some $X > 0$*, some remainders* R_d*, and some multiplicative function* $w(\cdot)$ *which satisfies the assumptions (Equation 2.3) and (Equation 2.4) from Section 2.1. Then*

$$\mathcal{S}(\mathcal{A}, \mathcal{P}, z) \leq XV(z)\left(e^{\gamma} + \frac{BL}{(\log z)^{1/14}}\right) + \sum_{\substack{d \leq z^2 \\ d | P(z)}} 3^{\omega(d)} |R_d|, \tag{3.10}$$

where γ *is Euler's constant,* $B > 0$ *is some absolute constant,* $L \geq 1$ *is the constant appearing in assumption (Equation 2.4), and* $V : \mathbb{N} \setminus \{0\} \to \mathbb{R}$ *is, as before, given by* $V(z) = \prod_{\substack{\ell \in \mathcal{P} \\ \ell < z}} \left(1 - \frac{w(\ell)}{\ell}\right)$.

Proof. See (HaRi74). □

Before we begin proving Main Theorem A, it is worth remarking on an interesting wrinkle that arises from the set of a_p's being a true multiset, i.e. that certain values of a_p can and do repeat for different values of p. The Selberg sieve, as well as sieves in general, are designed to detect each $a \in \mathcal{A}$ whose only prime factors are large, and so the sieve only bounds the number of large primes appearing in $\mathcal{A}$. In particular, it gives us no information about the small primes appearing in $\mathcal{A}$. When $\mathcal{A}$ is a set (that is, has no repeated elements), this is not a problem since, in that case, we can write

$$\begin{aligned}\#\{a \in \mathcal{A} : a \text{ prime}\} &= \#\{a \in \mathcal{A} : a \text{ prime}, |a| < z\} + \#\{a \in \mathcal{A} : a \text{ prime}, |a| \geq z\} \\ &\leq 2z + \mathcal{S}(\mathcal{A}, \mathcal{P}, z).\end{aligned}$$

Thus, since z is chosen to be of negligible size, the sieve on its own is enough to obtain an upper bound for the number of primes appearing in $\mathcal{A}$. However, when $\mathcal{A}$ is a multiset, we cannot bound $\#\{a \in \mathcal{A} : a \text{ prime}, |a| < z\}$ by $2z$ since $\mathcal{A}$ could contain 2, or any other small prime, infinitely many times. In this way, the sieve itself is not enough to bound the number of primes in $\mathcal{A}$. We need more information about $\mathcal{A}$ to bound the number of small primes appearing in it (and so the number of primes overall). In our case, this means that we need a partial Lang-Trotter result under θ-quasi GRH, such as Proposition 16 of Section 2.3, to bound the number of p such that a_p is a small prime.

Proof of Main Theorem A. As in Section 3.1, we define

$$\mathcal{A} := \{a_p : p \leq x, p \nmid N_E, \gcd(a_p, m_E) = 1\},$$

where N_E is the conductor of E, and we define

$$\mathcal{P} := \{\ell \text{ prime} : \ell \nmid m_E\},$$

where m_E is the torsion conductor of E. With these choices, we showed in (Equation 3.1), (Equation 3.2), (Equation 3.3), (Equation 3.4), and (Equation 3.6) of Section 3.2 that

$$\#\mathcal{A}_d = \frac{1}{d}\left(\prod_{\ell \mid d}\left(1-\frac{1}{\ell^2}\right)^{-1}\right) C_1(E)\pi(x) + O_E\left(d^2 x^\theta \log(dx)\right),$$

$$X = C_1(E)\pi(x),$$

$$w(d) = \prod_{\ell \mid d}\left(1-\frac{1}{\ell^2}\right)^{-1},$$

$$|R_d| \ll_E d^2 x^\theta \log(dx),$$

and, for $z > m_E$,

$$V(z) = C_2(E)\cdot\left(\frac{e^{-\gamma}}{\log z} + o\left(\frac{1}{\log z}\right)\right).$$

Furthermore, we showed that $w(\cdot)$ satisfies the assumptions (Equation 2.3) and (Equation 2.4), so that we fulfill all the requirements to use Theorem 17.

Let $z = z(x) > m_E$ be a parameter to be chosen optimally later. At this point, using the shorthand

$$\pi_{\mathrm{twin},E}(x) := \#\{a_p : p \le x, p \nmid N_E, a_p \text{ prime}\},$$

we can apply the definition of $\mathcal{S}(\mathcal{A},\mathcal{P},z)$, Proposition 16, and Theorem 17 to write

$$\begin{aligned}
\pi_{\mathrm{twin},E}(x) &= \#\{a_p : p \le x, p \nmid N_E, a_p \text{ prime}, |a_p| \ge z\} + \#\{a_p : p \le x, p \nmid N_E, a_p \text{ prime}, |a_p| < z\} \\
&\le \mathcal{S}(\mathcal{A},\mathcal{P},z) + O_E\left(\frac{x^{1-\frac{1-\theta}{4}}z}{(\log x)^{\frac{1}{2}}}\right) \\
&\le XV(z)\left(e^{\gamma} + \frac{5B}{(\log z)^{1/14}}\right) + \sum_{\substack{d \le z^2 \\ \gcd(d,m_E)=1}} 3^{\omega(d)}|R_d| + O_E\left(\frac{x^{1-\frac{1-\theta}{4}}z}{(\log x)^{\frac{1}{2}}}\right). \qquad (3.11)
\end{aligned}$$

Now, in order for the last inequality to be meaningful, we will need both of the error terms to be $o\left(\frac{x}{(\log x)^2}\right)$. We claim this will be the case if we choose

$$z := \frac{x^{\frac{1-\theta}{6}}}{(\log x)^2}, \qquad (3.12)$$

For the first error term, using our aforementioned bound (Equation 3.4) for R_d and Lemma 11 from Section 2.2, we obtain

$$\begin{aligned}
\sum_{\substack{d \le z^2 \\ \gcd(d,m_E)=1}} 3^{\omega(d)}|R_d| &\ll_E \sum_{d \le z^2} d^2 3^{\omega(d)} x^{\theta} \log x \\
&\ll x^{\theta} z^6 \log x (\log z)^2 \\
&\ll \frac{x}{(\log x)^9},
\end{aligned}$$

so the first error term is negligible in comparison to the main term. For the second error term, we see immediately that

$$\frac{x^{1-\frac{1-\theta}{4}}z}{(\log x)^{\frac{1}{2}}} \ll \frac{x^{1-\frac{1-\theta}{12}}}{(\log x)^{5/2}}.$$

Thus, choice (Equation 3.12) of z makes the last two terms on the right hand side of inequality (Equation 3.11) be $o\left(\frac{x}{(\log x)^2}\right)$.

Finally, we examine the first term on the right hand side of inequality (Equation 3.11). Recalling the aforementioned expressions (Equation 3.2) and (Equation 3.6) for X and $V(z)$, we see that

$$\begin{aligned} XV(z)e^{\gamma} &= C_1(E)C_2(E)\pi(x)\left(\frac{1}{\log z} + o\left(\frac{1}{\log z}\right)\right) \\ &= \left(\frac{3}{1-\theta} + o(1)\right)C(E)\frac{x}{(\log x)^2}, \end{aligned} \tag{3.13}$$

where $C(E)$ is as in the conjectural (Equation 1.11).

Overall then, we can substitute (Equation 3.13) into our initial inequality (Equation 3.11) and gather all the error terms into the little o-notation to obtain

$$\pi_{\mathrm{twin},E}(x) \le \left(\frac{3}{1-\theta} + o(1)\right)C(E)\frac{x}{(\log x)^2}.$$

This completes the proof of Main Theorem A. □

Lastly, we can now prove our analogue to Brun's Theorem about the convergence of the sum of the reciprocal primes p having the property that the Frobenius trace a_p is also a prime.

Proof of Corollary A'. Fix $\varepsilon > 0$. Then, by Main Theorem A, there exists $x_0 = x_0(E, \theta, \varepsilon)$ such that for all $x \geq x_0$,

$$\pi_{\mathrm{twin},E}(x) \leq \left(\frac{3}{1-\theta} + \varepsilon\right) C(E) \frac{x}{(\log x)^2}.$$

By using partial summation and the above inequality, we deduce that

$$\begin{aligned}
\sum_{\substack{p \geq x_0 \\ a_p \text{ prime}}} \frac{1}{p} &= \left.\frac{\pi_{\mathrm{twin},E}(t)}{t}\right|_{x_0}^{\infty} + \int_{x_0}^{\infty} \frac{\pi_{\mathrm{twin},E}(t)}{t^2} dt \\
&\leq \left(\frac{3}{1-\theta} + \varepsilon\right) C(E) \frac{1}{\log x_0} - \frac{\pi_{\mathrm{twin},E}(x_0)}{x_0} \\
&\leq \left(\frac{3}{1-\theta} + \varepsilon\right) C(E) \frac{1}{\log x_0}.
\end{aligned}$$

□

3.4 Proof of Main Theorem B

In order to prove Main Theorem B, we will largely follow the approach of David and Wu in (DaWu12), including using the version of the weighted Greaves' sieve presented as in (HaRi85, Theorem A) with the simplifications $E = V$ and $T = U$. Once again recalling the setting outlined at the beginning of Section 2.1, we state the sieve theorem in the proceeding discussion. We note that, rather than estimating the size of the sieve $\mathcal{S}(\mathcal{A}, \mathcal{P}, z)$ directly, the Greaves' sieve theorem provides a lower bound for a weighted sifted function, defined as follows.

For real parameters $z > 0$ and u, v satisfying

$$0.074368... =: v_0 < v \leq \frac{1}{4}, \quad \frac{1}{2} \leq u < 1, \quad u + 3v \geq 1, \tag{3.14}$$

we define

$$\mathcal{H}(\mathcal{A}, \mathcal{P}, z^v, z^u) := \sum_{a \in \mathcal{A}} \mathcal{G}(\gcd(a, P(z^u))),$$

where

$$\mathcal{G}(n) := \left\{ 1 - \sum_{\substack{\ell | n \\ \ell \in \mathcal{P}}} (1 - \mathcal{W}(\ell)) \right\}^+ \tag{3.15}$$

with

$$\{x\}^+ := \max\{0, x\}$$

and

$$\mathcal{W}(\ell) := \begin{cases} \frac{1}{u-v}\left(\frac{\log \ell}{\log z} - v\right) & \text{if } z^v \leq \ell \leq z^u \\ 0 & \text{otherwise.} \end{cases} \tag{3.16}$$

It is this function, $\mathcal{H}(\mathcal{A}, \mathcal{P}, z^v, z^u)$, that the theorem will estimate.

We need some more notation, as follows. We set

$$h_{2r}(t) := \int \cdots \int_{\substack{t < t_{2r} < \ldots < t_1 \\ 3t_{2i} + \ldots + t_1 \geq 1 \; \forall 1 \leq i \leq r-1 \\ 3t_{2r} + \ldots + t_1 \geq 1 \\ t_{2r} < 1 - t - t_1 - \ldots - t_{2r}}} \frac{1}{1 - t - t_1 - \ldots - t_{2r}} \cdot \frac{dt_1 \ldots dt_{2r}}{t_1 \ldots t_{2r}},$$

$$h(t) := \sum_{r \geq 1} h_{2r}(t),$$

$$\psi(t) := \frac{1}{1-t} - h(t) \quad \text{for } 0 < t \leq \frac{1}{4}.$$

Note that, for $t \geq v_0$,

$$\psi(t) \geq 0$$

(see (HaRi85, p. 205)). Following Greaves, Halberstam, and Richert, we also set

$$\alpha(v) := \int_v^{\frac{1}{4}} \psi(t)\ dt$$

and

$$\beta(v) := \int_v^{\frac{1}{4}} \psi(t)\ \frac{dt}{t}.$$

As pointed out in (DaWu12, p. 115), we have that, for $\frac{1}{6} \leq v \leq \frac{1}{4}$,

$$\alpha(v) = \log \frac{4(1-v)}{3} - \int_4^{\frac{1}{v}} \left(\frac{2}{t} \log(2-tv) + \log \frac{1-\frac{1}{t}}{1-v} \right) \frac{\log(t-3)}{t-2}\ dt, \tag{3.17}$$

$$\beta(v) = \log \frac{1-v}{3v} - \int_4^{\frac{1}{v}} \left(\log(2-tv) + \log \frac{1-\frac{1}{t}}{1-v} \right) \frac{\log(t-3)}{t-2}\ dt. \tag{3.18}$$

Now, we can state the sieve theorem.

Theorem 18 *(Weighted Greaves' sieve)*

Assume the setting described at the beginning of Section 2.1. In particular, with notation as *described in that section, assume that for any squarefree* d *composed of primes in* $\mathcal{P}$, $\#\mathcal{A}_d$ *can be written in the form*

$$\#\mathcal{A}_d = \frac{w(d)}{d}X + R_d$$

for some $X > 0$*, some remainders* R_d*, and some multiplicative function* $w(\cdot)$ *which satisfies the assumptions (Equation 2.3) and (Equation 2.4). Then*

$$\mathcal{H}(\mathcal{A}, \mathcal{P}, z^v, z^u) \geq 2e^{\gamma} X V(z) \left(J(u,v) + O\left(\frac{\log\log\log z}{(\log\log z)^{1/5}} \right) \right) - (\log z)^{1/3} \left| \sum_{m<M} \sum_{\substack{n<N \\ mn | P(z^u)}} \alpha_m \beta_n R_{mn} \right|, \tag{3.19}$$

where γ *is Euler's constant;* M, N *are any real numbers satisfying* $M > z^u$, $N > 1$*, and* $MN = z$*;* α_m, β_n *are certain real numbers satisfying* $|\alpha_m|, |\beta_n| \leq 1$*;* $V : \mathbb{N} \setminus \{0\} \to \mathbb{R}$ *is, as before, given by* $V(z) = \prod_{\substack{\ell \in \mathcal{P} \\ \ell < z}} \left(1 - \frac{w(\ell)}{\ell}\right)$*; additionally,*

$$J(u,v) := \frac{1}{u-v} \left(u \log \frac{1}{u} + (1-u) \log \frac{1}{1-u} - \log \frac{4}{3} + \alpha(v) - v \log 3 - v\beta(v) \right).$$

It is not immediately clear that the inequality in the above theorem will give us the desired result. In light of this, we will prove the following lemma that shows how the sieve leads to a lower bound on almost primes. The lemma is similar to Lemma 4.1 in (DaWu12), except that it is stated in a more general setting.

Lemma 19

In the setting of Theorem 18, suppose that, for each $a \in \mathcal{A}$*, if* $\ell \mid a$*, then* $\ell \in \mathcal{P}$*. Also, suppose that there exists* $x_0 > 0$ *and* $r \in \mathbb{N}$ *such that for all* $x \geq x_0$*,*

$$\max_{a \in \mathcal{A}} |a| \leq z^{ru+v}, \tag{3.20}$$

and

$$\mathcal{H}(\mathcal{A}, \mathcal{P}, z^v, z^u) \geq f(x) \tag{3.21}$$

for some $f : \mathbb{R}_{>0} \to \mathbb{R}$*. Then*

$$\#\{a \in \mathcal{A} : \omega(a) \leq r\} \geq f(x). \tag{3.22}$$

Moreover, if

$$\sum_{\substack{z^v \leq \ell < z^u \\ \ell \in \mathcal{P}}} \#\mathcal{A}_{\ell^2} = o(f(x)), \tag{3.23}$$

then

$$\#\{a \in \mathcal{A} : \Omega(a) \leq r\} \geq f(x) + o(f(x)). \tag{3.24}$$

Proof. We start by establishing two properties of $\mathcal{G}(n)$, first that $0 \leq \mathcal{G}(n) \leq 1$ for all $n \in \mathbb{N}$. First, note that if n is not divisible by any $\ell \in \mathcal{P}$, then we clearly see from (Equation 3.15) that

$\mathcal{G}(n) = 1$. Additionally, if n is divisible by some $\ell \in \mathcal{P}$ outside of the range $z^v \leq \ell \leq z^u$, we see that $\mathcal{G}(n) = 0$. Now, fix $\ell \in \mathcal{P}$ with $z^v \leq \ell < z^u$. Then

$$v \leq \frac{\log \ell}{\log z} < u,$$

so that

$$0 \leq \frac{1}{u - v}\left(\frac{\log \ell}{\log z} - v\right) < 1.$$

Since the middle expression in the above inequality is the definition of $\mathcal{W}(\ell)$, we have

$$0 < 1 - \mathcal{W}(\ell) \leq 1,$$

which implies for any $n \in \mathbb{N}$ such that $\ell \mid n$,

$$1 - \sum_{\substack{\ell \mid n \\ \ell \in \mathcal{P}}} \Big(1 - \mathcal{W}(\ell)\Big) < 1.$$

Thus,

$$0 \leq \mathcal{G}(n) < 1.$$

The second property that we will need is that if $\gcd(n, P(z^v)) > 1$, then $\mathcal{G}(n) = 0$. We will prove this claim directly, so assume that, for some fixed $n \in \mathbb{N}$, $\gcd(n, P(z^v)) > 1$. Then, we can fix $\ell \in \mathcal{P}$ such that $\ell \mid n$ and $\ell < z^v$. By definition, that means $\mathcal{W}(\ell) = 0$, so that

$$\sum_{\substack{\ell \mid n \\ \ell \in \mathcal{P}}} \Big(1 - \mathcal{W}(\ell)\Big) \geq 1$$

since we have shown that each summand is nonnegative. We see immediately that

$$1 - \sum_{\substack{\ell \mid n \\ \ell \in \mathcal{P}}} \Big(1 - \mathcal{W}(\ell)\Big) \leq 0,$$

so then $\mathcal{G}(n) = 0$.

Next, putting together the first property we proved above with the assumption (Equation 3.21), we have

$$\begin{aligned} \sum_{\substack{a \in \mathcal{A} \\ \mathcal{G}(\gcd(a, P(z^u)))>0}} 1 &\geq \sum_{a \in \mathcal{A}} \mathcal{G}(\gcd(a, P(z^u))) \qquad (3.25) \\ &= \mathcal{H}(\mathcal{A}, \mathcal{P}, z^v, z^u) \\ &\geq f(x). \end{aligned}$$

However, we claim that each a counted in the left hand sum above satisfies that $\omega(a) \leq r$ and, further, if assumption (Equation 3.23) holds as well, that the number of a in that sum such that $\Omega(a) > r$ is $o(f(x))$. We first introduce new notation that will be useful in verifying this claim.

$$\omega(n;y) := \sum_{\ell|n} 1 + \sum_{\substack{\ell^k|n \\ \ell\geq y \\ k\geq 2}} 1$$

Now, assume for a fixed $a \in \mathcal{A}$, $\mathcal{G}(\gcd(a, P(z^u))) > 0$, so that from our discussion above, we know $\gcd(a, P(z^v)) = 1$. We will show $\omega(a) \leq r$. From the definitions (Equation 3.15) and (Equation 3.16), we have

$$\begin{aligned}
0 &< 1 - \sum_{\substack{\ell|a \\ \ell\leq z^u}} \left(1 - \frac{1}{u-v}\left(\frac{\log \ell}{\log z} - v\right)\right) \\
&= 1 - \frac{1}{u-v} \sum_{\substack{\ell|a \\ \ell\leq z^u}} \left(u - \frac{\log \ell}{\log z}\right) \\
&\leq 1 - \frac{1}{u-v} \sum_{\substack{\ell|a \\ \ell\leq z^u}} \left(u - \frac{\log \ell}{\log z}\right) - \frac{1}{u-v} \sum_{\substack{\ell^k|a \\ \ell\geq z^u \\ k\geq 2}} \left(u - \frac{\log \ell}{\log z}\right) \\
&\leq 1 - \frac{u}{u-v} \cdot \omega(a; z^u) + \frac{1}{u-v} \cdot \frac{\log a}{\log z}.
\end{aligned}$$

Following some algebraic manipulations, we then obtain

$$u \cdot \omega(a; z^u) < u - v + \frac{\log a}{\log z}.$$

Recalling assumption (Equation 3.20), we then see

$$\begin{aligned} u \cdot \omega(a; z^u) &< u - v + (ru - v) \\ &= u(r+1). \end{aligned}$$

Dividing by u gives us $\omega(a; z^u) < r+1$, so that $\omega(a; z^u) \leq r$, and since clearly $\omega(a) \leq \omega(a; z^u)$, this yields $\omega(a) \leq r$, as desired. Overall then, we see that

$$\begin{aligned} \#\{a \in \mathcal{A} : \omega(a) \leq r\} &\geq \sum_{\substack{a \in \mathcal{A} \\ \mathcal{G}(\gcd(a, P(z^u))) > 0}} 1 \\ &\geq f(x), \end{aligned}$$

completing the first part of the lemma.

For the second part of the lemma, we start by rewriting the left hand sum of (Equation 3.25) as follows,

$$\sum_{\substack{a \in \mathcal{A} \\ \mathcal{G}(\gcd(a, P(z^u))) > 0}} 1 = \sum_{\substack{a \in \mathcal{A} \\ \mathcal{G}(\gcd(a, P(z^u))) > 0 \\ \Omega(a) = \omega(a; z^u)}} 1 \; + \sum_{\substack{a \in \mathcal{A} \\ \mathcal{G}(\gcd(a, P(z^u))) > 0 \\ \Omega(a) > \omega(a; z^u)}} 1.$$

Now, since we showed that each a in the left hand sum above must have $\omega(a; z^u) \leq r$, we see that the first sum on the right is clearly smaller than $\#\{a \in \mathcal{A} : \Omega(a) \leq r\}$. On the other hand, for an a to be counted in the second sum, there must be an $\ell < z^u$ such that

$\ell^2 \mid a$ since $\Omega(a) > \omega(a; z^u)$. However, such an ℓ must also have $\ell \geq z^v$ since we showed that $\mathcal{G}(\gcd(a, P(z^u)))$ would be 0 otherwise. Therefore,

$$\begin{aligned}
\sum_{\substack{a \in \mathcal{A} \\ \mathcal{G}(\gcd(a, P(z^u)))>0 \\ \Omega(a)>\omega(a,z^u)}} 1 &\leq \#\{a \in \mathcal{A} : \exists \ell \in \mathcal{P} \text{ with } z^v \leq \ell < z^u \text{ and } \ell^2 \mid a\} \\
&\leq \sum_{\substack{z^v \leq \ell < z^u \\ \ell \in \mathcal{P}}} \#\mathcal{A}_{\ell^2} \\
&= o(f(x)), \qquad (3.26)
\end{aligned}$$

provided the assumption (Equation 3.23) holds. Thus, (Equation 3.26) combined with (Equation 3.25) yields

$$\begin{aligned}
\#\{a \in \mathcal{A} : \Omega(a) \leq r\} &\geq \sum_{\substack{a \in \mathcal{A} \\ \mathcal{G}(\gcd(a, P(z^u)))>0}} 1 + o(f(x)) \\
&\geq f(x) + o(f(x)),
\end{aligned}$$

completing the second part of the lemma as well. $\square$

Having proved the lemma, we now move to proving the main result.

Proof of Main Theorem B. Again, just as in the proof of Main Theorem A, we will use the setup described in Section 3.2. Namely, we take

$$\mathcal{A} := \{a_p : p \leq x, p \nmid N_E, \gcd(a_p, m_E) = 1\},$$

$$\mathcal{P} := \{\ell \text{ prime} : \ell \nmid m_E\},$$

and, for each $\ell \in \mathcal{P}$,

$$\mathcal{A}_\ell := \{a_p \in \mathcal{A} : a_p \equiv 0 \pmod{\ell}\},$$

$$\mathcal{A}_{\ell^2} := \left\{a_p \in \mathcal{A} : a_p \equiv 0 \left(\bmod\ \ell^2\right)\right\}.$$

Recall once again that, with these choices, we showed in (Equation 3.1), (Equation 3.2), (Equation 3.3), (Equation 3.4), and (Equation 3.6) of Section 3.2 that

$$\#\mathcal{A}_d = \frac{1}{d}\left(\prod_{\ell \mid d}\left(1 - \frac{1}{\ell^2}\right)^{-1}\right) C_1(E) + O_E\left(d^2 x^\theta \log(dx)\right),$$

$$X = C_1(E)\pi(x),$$

$$w(d) = \prod_{\ell \mid d}\left(1 - \frac{1}{\ell^2}\right)^{-1},$$

$$|R_d| \ll_E d^2 x^\theta \log(dx),$$

and, for $z > m_E$,

$$V(z) = C_2(E) \cdot \left(\frac{e^{-\gamma}}{\log z} + o\left(\frac{1}{\log z}\right)\right).$$

Furthermore, we showed that $w(\cdot)$ satisfies the assumptions (Equation 2.3) and (Equation 2.4), so that we fulfill all the requirements to use Theorem 18. Thus, Theorem 18 yields

$$\mathcal{H}(\mathcal{A}, \mathcal{P}, z^v, z^u) \geq 2C_1(E)C_2(E) \cdot \frac{\pi(x)}{\log z}(J(u,v) + o(1)) - (\log z)^{1/3}\left|\sum_{m<M}\ \sum_{\substack{n<N \\ mn \mid P(z^u)}} \alpha_m \beta_n R_{mn}\right|.$$

Recalling that the constant $C(E)$ of conjectural (Equation 1.11) is

$$C(E) = 2C_1(E)C_2(E),$$

we rewrite the above inequality as

$$\mathcal{H}(\mathcal{A}, \mathcal{P}, z^v, z^u) \geq C(E) \cdot \frac{\pi(x)}{\log z}(J(u,v) + o(1)) - (\log z)^{1/3} \left| \sum_{m<M} \sum_{\substack{n<N \\ mn|P(z^u)}} \alpha_m \beta_n R_{mn} \right|. \tag{3.27}$$

We can now turn our attention to applying Lemma 19. Note that since we have defined $\mathcal{A}$ to include only those a_p coprime to m_E and, similarly, defined $\mathcal{P}$ to include only those ℓ coprime to m_E, we know if $\ell \mid a_p$, then $\ell \in \mathcal{P}$, as required by the lemma. We set

$$z := \frac{x^{\xi}}{(\log x)^2}$$

and we wish to find values for the parameters u, v, ξ, and r that minimize r while still satisfying the assumptions of the lemma and guaranteeing that the error in (Equation 3.27) is negligible in comparison to the main term. Remembering that $MN = z$ and $|\alpha_m|, |\beta_n| \le 1$, we see that

$$\begin{aligned}
\left| \sum_{m<M} \sum_{\substack{n<N \\ mn|P(z^u)}} \alpha_m \beta_n R_{mn} \right| &\le \sum_{\substack{d \le z \\ d|P(z^u)}} 2^{\omega(d)} |R_d| \\
&\le \sum_{d \le z} 2^{\omega(d)} d^2 x^\theta \log x \\
&\le x^\theta z^3 \log x \log z \\
&\ll \frac{x^{3\xi+\theta}}{(\log x)^4},
\end{aligned}$$

so that the error term will be negligible provided

$$\xi \le \frac{1-\theta}{3}.$$

Next, from the Hasse bound, we have that $|a_p| \le 2\sqrt{p} \le 2\sqrt{x}$. Hence, the assumption (Equation 3.20) will be satisfied if

$$2\sqrt{x} \le \left(\frac{x^\xi}{(\log x)^2} \right)^{ru+v}.$$

Examining the exponents of x on each side, we see that this inequality will hold if

$$\frac{1}{2} < \xi(ru+v),$$

i.e., if

$$r > \frac{1}{u}\left(\frac{1}{2\xi} - v\right). \tag{3.28}$$

From this last relation, we see that if any two of the three parameters, u, v, and ξ are held constant, then r will be minimized when the third parameter takes its largest possible value.

For the case of minimizing the distinct prime factors of a_p, there are no other restrictions on u and v beyond (Equation 3.14) stated at the beginning of this section and the fact that, in order to have a meaningful result, we will need $J(u, v) > 0$. In the region $\frac{1}{6} \le v \le \frac{1}{4}$, $J(u, v)$ can be numerically approximated via the simplified integral formulae (Equation 3.17) and (Equation 3.18) that are valid for v in that range. The numerical data suggests that for u, v satisfying $J(u, v) = 0$ in this region, $|1 - u - v| < 0.0005$, so that the curve $J(u, v) = 0$ can be closely approximated by $u = 1 - v$. Under this constraint, with ξ held constant, we find that the right hand side of (Equation 3.28) is minimized when $u = \frac{5}{6}$ and $v = \frac{1}{6}$. However, this choice of u and v would result in $J\left(\frac{5}{6}, \frac{1}{6}\right) = -0.00109... < 0$, so we make the adjustment

$$u := 0.83 \text{ and } v := \frac{1}{6},$$

which results in

$$J\left(0.83, \frac{1}{6}\right) = 0.00692... > 0.$$

Then, we can set

$$\xi := \frac{1 - \theta}{3}$$

and

$$r_1 := 1 + \left[\frac{1}{0.83} \left(\frac{3}{2(1-\theta)} - \frac{1}{6} \right) \right].$$

With the above choices, the error term in (Equation 3.27) is negligible, $J\left(0.83, \frac{1}{6}\right) > 0$, and the assumption (Equation 3.20) in Lemma 19 is satisfied. As a result, Lemma 19 gives us

$$\#\{a_p : p \leq x, p \nmid N_E, \gcd(a_p, m_E) = 1, \omega(a_p) \leq r_1\} \geq \frac{3}{1-\theta}(0.00692... + o(1))C(E)\frac{x}{(\log x)^2}. \tag{3.29}$$

Since removing the gcd condition will only make the set larger, we achieve the first part of the desired result.

The choices of parameters above will be approximately optimal within the region $\frac{1}{6} \leq \nu \leq \frac{1}{4}$. For $\nu_0 < \nu < \frac{1}{6}$, the simplified integral formulae (Equation 3.17) and (Equation 3.18) are not valid, so a more careful analysis of $J(u, \nu)$ will be required in order to find the optimal choice of parameters in that range of ν.

Now, when we move toward proving the result with multiplicity, the situation regarding the parameters u and ν becomes clearer since we also need to satisfy the additional assumption, (Equation 3.23), in Lemma 19. Using part (ii) of Theorem 15 of Section 2.4, we deduce that

$$\begin{aligned} \sum_{\substack{z^\nu \leq \ell < z^u \\ \ell \in \mathcal{P}}} \#\mathcal{A}_{\ell^2} &\ll_E \sum_{z^\nu \leq \ell \leq z^u} \left(\frac{\pi(x)}{\ell^2} + \ell^4 x^\theta \log x \right) \\ &\ll \frac{x^{1-\xi\nu}}{(\log x)^{1-2\nu}} + \frac{x^{5\xi u + \theta}}{(\log x)^{10u-1}}. \end{aligned}$$

Since ξ and ν are both positive, clearly the first term in the above will be $o(x/(\log x)^2)$. In order for the second term to also be $o(x/(\log x)^2)$, we will need

$$5\xi u + \theta \leq 1,$$

i.e.

$$u \leq \frac{1-\theta}{5\xi}.$$

Thus, if we take

$$\xi := \frac{1-\theta}{3},$$

we can set

$$u := \frac{3}{5}.$$

Since we have now fixed u and ξ, we know the right hand side of (Equation 3.28) will be minimized when we choose the largest possible ν, i.e.

$$\nu := \frac{1}{4}.$$

Then the assumption (Equation 3.20) from Lemma 19 will be satisfied for

$$r_2 := 1 + \left[\frac{5}{2(1-\theta)} - \frac{5}{12}\right].$$

Once again, with these choices, we also have that the error term in (Equation 3.27) is negligible, and that

$$J\left(\frac{3}{5},\frac{1}{4}\right) = 0.3162... > 0.$$

Overall then, the second part of Lemma 19 now yields

$$\#\{a_p : p \le x, p \nmid N_E, \gcd(a_p, m_E) = 1, \Omega(a_p) \le r_2\} \ge \frac{3}{1-\theta}(0.3162... + o(1))C(E)\frac{x}{(\log x)^2}. \tag{3.30}$$

Again, removing the gcd condition only makes the set larger, so we have now essentially proven the second desired result as well.

We now make one final remark. While we have demonstrated that the bounds are true as written, one may worry that the statements are misleading since they seem to offer lower bounds for the number of p such that the integer a_p is almost prime, but the p being counted would include those for which $a_p = \pm 1$ as well. This inclusion has a negligible affect on the final result, however, since we know from our partial Lang-Trotter result, Proposition 16, that the number of $p \le x$ such that $a_p = \pm 1$ is $\ll_E x^{1-\frac{1-\theta}{4}} = o(x/(\log x)^2)$. Thus, (Equation 3.29) and (Equation 3.30) give

$$\#\{a_p : p \le x, p \nmid N_E, \gcd(a_p, m_E) = 1, a_p \ne \pm 1, \omega(a_p) \le r_1\} \ge \frac{3}{1-\theta}(0.00692...+o(1))C(E)\frac{x}{(\log x)^2}$$

and

$$\#\{a_p : p \leq x, p \nmid N_E, \gcd(a_p, m_E) = 1, a_p \neq \pm 1, \Omega(a_p) \leq r_2\} \geq \frac{3}{1-\theta}(0.3162...+o(1))C(E)\frac{x}{(\log x)^2}.$$

This completes the proof of Main Theorem B. $\square$

CITED LITERATURE

[Ap76] T. M. Apostol, *Introduction to analytic number theory,* Undergraduate Texts in Mathematics, Springer-Verlag, New York-Heidelberg, 1976.

[Br19] V. Brun, *La serie* $1/5+1/7+1/11+1/13+1/17+1/19+1/29+1/31+1/41+1/43+1/59+1/61...$ *les dénominateurs sont nombres premiers jumeaux est convergente où finie,* Bull. Sci. Math. 43, 1919, pp. 124–128.

[Ca08] H. Carayol, *La conjecture de Sato-Tate (d'après Clozel, Harris, Shepherd-Barron, Taylor),* Séminaire Bourbaki. Vol. 2006/2007, Astérisque No. 317, 2008, Exp. No. 977, ix, pp. 345–391.

[Ch73] J. Chen, *On the representation of a larger even integer as the sum of a prime and the product of at most two primes,* Sci. Sinica 16, 1973, pp. 157–176.

[Cl06] L. Clozel, *The Sato-Tate conjecture,* Current developments in mathematics, 2006, pp. 1–34, Int. Press, Somerville, MA, 2008.

[CoDaSiSt16] A.C. Cojocaru, R. Davis, A. Silverberg, and K.E. Stange, *Arithmetic properties of the Frobenius traces defined by a rational abelian variety (with two appendices by J-P. Serre),* International Mathematics Research Notices 12, 2017, pp. 3557–3602.

[Co21] A.C. Cojocaru, *Abelian varieties with prime Frobenius traces,* in preparation.

[CoJo21] A.C. Cojocaru and N. Jones, *Degree bounds for projective division fields associated to elliptic modules with a trivial endomorphism ring,* to appear in Journal de Théorie des Nombres de Bordeaux.

[CoMe21] A.C. Cojocaru and M. Meyer, *Prime Frobenius traces for non-CM elliptic curves over* $\mathbb{Q}$, in preparation.

[CoWa21] A.C. Cojocaru and T. Wang, *Bounds for the distribution of the Frobenius traces associated to products of non-CM elliptic curves,* preprint 2021.

[Da00] H. Davenport, *Multiplicative number theory,* Graduate Texts in Mathematics 74, Springer Verlag 2000.

[DaWu12] C. David and J. Wu, *Almost prime values of the order of elliptic curves over finite fields,* Forum Math. 24, 2012, no. 1, pp. 99–119.

[El91] N.D. Elkies, *Distribution of supersingular primes,* Journées Arithmétiques (1989): Luminy, Astérisque No. 198-200, 1991, pp. 127–132.

[GoPiYi09] D.A. Goldston, J. Pintz, and C.Y. Yildirim, *Primes in tuples. I*, Annals of Math. 170 (2), 2009 No. 2, pp. 819–862.

[Gr00] G. Greaves, *Sieves in number theory,* Springer, A Series of Modern Surveys in Mathematics, 43, 2000.

[HaRi74] H. H. Halberstam and H.-E. Richert, *Sieve methods,* London Academic Press, 1974.

[HaRi85] H. H. Halberstam and H.-E. Richert, *A weighted sieve of Greaves' type, II,* Elementary and Analytic Theory of Numbers, pp. 183-215, Banach Center Publication 171, 1985.

[HaLi22] G.H. Hardy and J.E. Littlewood, *Some problems of "Partitio Numerorum", III: on the expression of a number as a sum of two primes,* Acta Math. 44, 1922, pp. 1–70.

[HaWr08] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers,* 6th edition, revised by D. R. Heath-Brown and J. H. Silverman, with a foreword by A. Wiles, Oxford University Press, Oxford, 2008.

[Jo10] N. Jones, *Almost all elliptic curves are Serre curves,* Trans. Amer. Math. Soc. vol. 362, no. 3, 2010, pp. 1547–1570.

[LaOd77] J. Lagarias and A. Odlyzko, *Effective versions of the Chebotarev density theorem,* in: A. Fröhlich (Ed.), Algebraic Number Fields, Academic Press, New York, 1977, pp. 409–464.

[LaTr76] S. Lang and H. Trotter, *Frobenius distributions in* GL_2*-extensions,* Lecture Notes in Mathematics, Vol. 504, Springer-Verlag, Berlin-New York, 1976.

[La05] M. Lane, *Elliptic curve analogues of the twin prime conjecture,* Bachelor's Thesis, Princeton University, 2005, 115 pages.

[Ma15] J. Maynard, *Small gaps between primes,* Annals of Math. 181 (2), 2015, No. 1, pp. 383–413.

[MuMu84] M. R. Murty and V. K. Murty, *Prime divisors of Fourier coefficients of modular forms,* Duke Math. Journal Vol. 51, No. 1, 1984, pp. 57–76.

[MuMuSa88] M. R. Murty, V. K. Murty and N. Saradha, *Modular forms and the Chebotarev density theorem,* Amer. J. Math. 110, 1988, No. 2, pp. 253–281.

[Polymath14] D.H.J. Polymath, *Variants of the Selberg sieve and bounded intervals containing many primes,* Res. Math. Sci, 2014 (1), Art. 12, 83 pages.

[Se72] J-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques,* Inventiones Mathematicae 15, 1972, pp. 259–331.

[Se81] J-P. Serre, *Quelques applications du théorème de densité de Chebotarev,* Publ. Math. I. H. E. S., no. 54, 1981, pp. 123–201.

[Si00] J.H. Silverman, *The arithmetic of elliptic curves,* Graduate Texts in Mathematics 106, Springer Verlag 2000.

[So07] K. Soundararajan, *The distribution of prime numbers,* in "Equidistribution in number theory, an introduction," NATO Sci. Ser. II Math. Phys. Chem., 237, Springer, Dordrecht, 2007, pp. 59–83.

[Te15] G. Tenenbaum, *Introduction to analytic and probabilistic number theory,* 3rd edition, Graduate Texts in Mathematics Vol. 163, American Mathematical Society, 2015.

[Wa03] L.C. Washington, *Elliptic Curves: Number Theory and Cryptology,* Chapman & Hall/CRC, Boca Raton, Florida, 2003.

[Wu04] J. Wu, *Chen's double sieve, Goldbach's conjecture and the twin prime problem,* Acta Arithmetica 114, 2004, No. 3, pp. 215–273.

[Wu08] J. Wu, *Chen's double sieve, Goldbach's conjecture and the twin prime problem. II,* Acta Arithmetica 131, 2008, No. 4, pp. 367–387.

[Zh14] Y. Zhang, *Bounded gaps between primes,* Annals of Math. 179 (2), 2014, No. 3, pp. 1121–1174.

VITA

NAME McKinley Meyer

EDUCATION

- **PhD in Mathematics**,
  University of Illinois at Chicago, August 2021
- **MS in Mathematics**,
  University of Illinois at Chicago, May 2017
- **BS in Mathematics, Physics, Astronomy-Physics**,
  University of Wisconsin-Madison, May 2014

RESEARCH INTERESTS Analytic Number Theory and Arithmetic Geometry

PUBLICATIONS

- Cojocaru, A. C. and Meyer, M. *Prime Frobenius traces for non-CM elliptic curves over* $\mathbb{Q}$, in preparation
- Hoffman, J., Meyer, M., Sardarli, M., and Sherman, A. *Maximization of the size of monic orthogonal polynomials on the unit circle corresponding to measures in the Steklov class.* Involve: A Journal of Mathematics. 8-4 (2015), 571–592. DOI 10.2140/involve.2015.8.571
- Terry, P., Dolan, D., Maccoux, M., and Meyer, M. *Removal of phosphates and chromates in a multi-ion solution.* Global Journal of Researches in Engineering-C. June 2014, v. 14.

PRESENTATIONS

- *The* $\mathfrak{j}$*-function*, University of Illinois at Chicago, August 2018
- *Binary, positive definite, quadratic forms: genus theory*, University of Illinois at Chicago, June 2018
- *Gaps between primes*, University of Illinois at Chicago, January - February 2018

TEACHING

- Fall 2015 - Spring 2021
  Teaching Assistant, University of Illinois-Chicago
  Courses taught include: Intermediate Algebra, College Algebra, Pre-calculus, Calculus I, II, and III, Differential Equations
- Fall 2014 - Spring 2015
  Associate Lecturer, University of Wisconsin-Green Bay
  Courses taught include: Intermediate Algebra and Pre-calculus

- Fall 2011 - Spring 2014
  Math Tutor, University of Wisconsin-Madison Housing

MEMBERSHPS

- American Mathematical Society
- Phi Beta Kappa Honor Society

LANGUAGES

Proficient in reading German