On the Distribution of Traces of Frobenius of Rational Elliptic Curves

Brandon Tran, Minh-Tam Trinh, Phil Wertheimer
2012 Clemson University REU Report

15 August 2012

Contents

Chapter 1

Introduction

Alongside plane geometry, number theory is the oldest recorded branch of mathematics. Its history largely developed out of efforts to understand two questions, the former algebraic, the latter analytic:

1. What are the integer solutions of multivariable equations, in particular polynomials?

2. What are the distributions of subsets of the integers, in particular the primes?

Modern theory attacks these problems using tools from nearly every other branch of mathematics, bringing together algebraic, analytic, and geometric perspectives. It is common for problems in this field to have completely elementary formulations, yet require the most abstract machinery to receive an answer.

This report addresses topics at the intersection of the two motivating questions above. As one would expect, the source of our motivation has an elementary statement:

Problem. How many solutions exist to a cubic congruence in 2 variables, modulo a prime?

The technical, and more specific, side is: What the distribution of the traces of Frobenius of the reductions of an elliptic curve $E/\mathbb{Q}$? Here, $E/\mathbb{Q}$ is the set of $\mathbb{Q}$-rational points on a smooth projective curve of genus 1, which has a natural group structure $E(\mathbb{Q})$. The curve can be reduced modulo a prime p to $\overline{E}$, and the trace of Frobenius of $\overline{E}/\mathbb{F}_p$ is the quantity

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

All the background required to understand elliptic curves and the results we present in this report are covered in Chapter 2.

Our report falls into three parts. By a theorem of Hasse (Theorem V.1.1 of [18]), we know that $|a_p(E)| \leq 2\sqrt{p}$. We wish to understand, for a fixed elliptic curve $E/\mathbb{Q}$:

1. When $|a_p(E)|$ is maximized given the bound depending on p.
2. When $a_p(E)$ is prime.
3. How fast the $a_p(E)/2\sqrt{p}$ converge to their limiting distribution, which by work of Richard Taylor and others in [22] is semicircular.

We prove results that represent progress toward the first two questions, and give an exposition of what is known regarding the third. All new results are stated in their corresponding chapters, under the label "T-T-W."

1.1 Acknowledgments

The individuals here mentioned are all affiliated with Clemson University, unless otherwise noted. Firstly, it is a pleasure to thank our primary advisors: Professor Kevin James for his generous guidance and support, and Dania Zantout for her discussion and helpful criticism.

We thank Professor Jim Brown for his help, and for regulating many aspects of the REU where this work was conducted, and Professor Neil Calkin for a great deal of assistance with our work on prime traces of Frobenius, in particular the computation of difficult sums and other analytic techniques. We thank Professor Gang Yu of Kent State University for pointing us to the work of Kumchev and Ghosh. We thank Rodney Keaton for his kind advice and discussion. Finally, we wish to thank all of the individuals who participated in the 2012 Clemson University REU for their encouragement, insights, and for making the experience of research as fulfilling as it was; and Clemson University itself for hosting us.

This research was supported in part by NSF grant DMS-1156761.

Chapter 2

Background

2.1 Defining Elliptic Curves

In this report, we will work with elliptic curves over number fields and their reductions. Hence, instead of introducing elliptic curves from the viewpoint of algebraic geometry, we begin with a less general, but more intuitive, construction from lattices over $\mathbb{C}$, then pass to the generalization. Recall that a lattice is an additive subgroup $\Lambda \subseteq \mathbb{C}$ of rank 2, such as $\langle 1, i \rangle$.

2.1.1 Definition. Let Λ be a lattice. We define $g_2(\Lambda) = 60G_4(\Lambda)$ and $g_3(\Lambda) = 140G_6(\Lambda)$, where

$$G_k(\Lambda) = \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \frac{1}{\omega^k}$$

is the (absolutely convergent) kth Eisenstein series for all $k \geq 3$.

2.1.2 Definition. The Weierstrass $\wp$ function of Λ is

$$\wp(z; \Lambda) = \frac{1}{z^2} + \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left(\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2} \right)$$

How should we visualize the $\wp$ function? It is periodic in Λ, and its only singularities are double poles at each point of the lattice Λ. Thus, $\wp$ is analytic and well-defined on the torus $\mathbb{C}/\Lambda$, except at 0. It may surprise the reader that, for fixed Λ, $(\wp, \wp')$ satisfies a polynomial relation:

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$$

In fact, more is true: the map $\psi : z \mapsto (\wp(z), \wp'(z))$ is a homeomorphism between $\mathbb{C}/\Lambda$ and the surface E defined in $\mathbb{C}^2$ by the equation above, once we attach to E a "point at infinity" corresponding to $z = 0$. We have now arrived at the following preliminary definition: An elliptic curve over $\mathbb{C}$ is the image under $z \mapsto (\wp(z), \wp'(z))$ of a lattice Λ. Since $\mathbb{C}/\Lambda$ inherits its addition operation from $\mathbb{C}$, we can formally impose a group law on the points of E by defining $\psi(z_1) + \psi(z_2) = \psi(z_1 + z_2)$ for all $z_1, z_2 \in \mathbb{C}/\Lambda$.

2.1.1 Theorem (Uniformization)**.** *Let $g_2, g_3 \in \mathbb{C}$. Then the following are equivalent:*

1. $g_2^3 - 27g_3^2 \neq 0$.
2. *The surface in $\mathbb{C}^2$ defined by $Y^2 = 4X^3 - g_2X - g_3$ is smooth.*
3. *There exists a unique lattice Λ with $g_2(\Lambda) = g_2$ and $g_3(\Lambda) = g_3$.*

Proof. The equivalence of (1) and (2) follows from the discussion on pp. 6-7 of [14], after a change of variables. See Proposition 14.3 in [2] for the equivalence of (1) and (3). □

From 2.1.1, we deduce another characterization of elliptic curves over $\mathbb{C}$, that does not make the dependence on the lattice explicit: An elliptic curve over $\mathbb{C}$ is the surface formed by attaching a point at infinity O to a smooth surface in $\mathbb{C}^2$ defined by $Y^2 = 4X^3 - g_2X - g_3$ for some $g_2, g_3 \in \mathbb{C}$. From the perspective of algebraic geometry, O turns the surface from an affine variety into a projective variety; for further details, the reader should consult Chapter 1 of [18]. We can generalize this definition to elliptic curves over other fields:

2.1.3 Definition. Let K be a field of characteristic $\neq 2, 3$. An elliptic curve over K is the surface E formed by attaching a point at infinity O to a surface in K^2 defined by

$$Y^2 = 4X^3 - g_2X - g_3$$

for some $g_2, g_3 \in K$ such that $g_2^3 - 27g_3^2 \neq 0$.

2.1.4 Definition. The discriminant of E is $\Delta(E) = g_2^3 - 27g_3^2$. The j-invariant of E is

$$j(E) = 1728\frac{g_2^3}{\Delta(E)}$$

We write E/K to indicate that E is defined over K. In particular, if the equation of E has coefficients in some subfield $F \subseteq K$, then E is also defined over F. More precisely, E/F is the subset of points of E/K with coordinates in F. In the other direction, the canonical field of definition of E is the algebraic closure $\overline{K}$ of K.

It is not obvious that, under our extended definition of elliptic curves, we still have a group law on the points. We find that a line in K^2 passing through two points $P_1, P_2 \in E$ always intersects E in a third point P_3, where we consider a line to intersect E twice at one point iff it is tangent to E there. Let $-P_3$ be the reflection of P_3 across the Y-axis, where $-O = O$. By defining $P_1 + P_2 = -P_3$, we obtain a group law on E. In the case $K = \mathbb{C}$, this group law is precisely the one induced by $\mathbb{C}/\Lambda$.

2.1.2 Theorem. *E/K forms an abelian group under the law described above, with identity O.*

Proof. See the discussion in III.2 of [18]. □

2.1.5 Definition. The Mordell-Weil group of E/K is the group $E(K)$ in 2.1.2. If $E(K)$ is finitely generated, then the rank of E/K is the unique r such that $E(K) = E(K)_{\text{tor}} \times \mathbb{Z}^r$.

2.2 Morphisms

2.2.1 Definition. Let $f \in K[X, Y]$ be the polynomial such that $f(X, Y) = 0$ defines E/K. The coordinate ring of E/K is

$$K[E] = \frac{K[X, Y]}{\langle f \rangle}$$

The function field of E/K is the field of fractions $K(E)$ of $K[E]$.

2.2.2 Definition. An (elliptic curve) morphism is a rational map $\phi : E_1/K \to E_2/K$ of the form $\phi(X, Y) \in K(E_1)$.

2.2.1 Theorem. *A morphism $\phi : E_1/K \to E_2/K$ is either constant or surjective.*

Proof. See II.6.8 of [5]. □

Intuitively, a morphism between elliptic curves is a change of variables between them that can be expressed in terms of rational functions. Suppose

that $\phi : E_1/K \to E_2/K$ is a nonconstant morphism. For all $f \in K(E_2)$, define

$$\phi^*(f) = f \circ \phi$$

Then ϕ^* is an injective map from $K(E_2)$ into $K(E_1)$. In fact, the map $\phi \mapsto \phi^*$ induces a contravariant functor from the category of elliptic curves to the category of their function fields, with a suitable class of morphisms. Intuitively, elliptic curves are dually symmetric to their function fields.

2.2.3 Definition. Let $\phi : E_1/K \to E_2/K$ be a morphism. The degree of ϕ is defined as $\deg \phi = 0$ if ϕ is constant and $\deg \phi = [K(E_1) : \phi^* K(E_2)]$ if otherwise. Also, ϕ is separable iff $K(E_1)$ is separable over $\phi^* K(E_2)$.

2.2.4 Definition. An isomorphism is a morphism of degree 1. If there exists an isomorphism between E_1/K and E_2/K, then E_1 and E_2 are called isomorphic over K.

We can also think of an elliptic curve isomorphism as a bijective morphism. For fixed K, it suffices to study representatives from the isomorphism classes of elliptic curves over K, because E_1, E_2 are isomorphic over K iff $K(E_1) = K(E_2)$. If K is of characteristic $\neq 2, 3$, then by substitution, every elliptic curve over K is isomorphic to a curve E/K of the form

$$Y^2 = X^3 + aX + b$$

for some $a, b \in K$. In some texts, this is called the Weierstrass form of the elliptic curve. Throughout the rest of this report, we prefer this form to the one arising from the $\wp$ function. We compute $\Delta(E) = -(4a^3 + 27b^2)$ and $j(E) = 1728(4a^3)/\Delta(E)$.

2.2.2 Theorem. *E_1/K, E_2/K are isomorphic over some finite extension of K if and only if $j(E_1) = j(E_2)$.*

Proof. This is Proposition 14.5 of [2]. □

2.3 Isogenies

Up to now, we have not discussed maps that preserve the group structure between elliptic curves. An isomorphism of elliptic curves is not always an isomorphism of their Mordell-Weil groups; as an example, we consider any isomorphism that does not fix O, such as the translation-by-P map $Q \mapsto Q + P$. This motivates the following definition:

2.3.1 Definition. An isogeny is a morphism $\phi : E_1/K \to E_2/K$ such that $\phi(O) = O$. If ϕ is surjective, then E_1 and E_2 are called isogenous over K.

2.3.1 Lemma. *An isogeny $\phi : E_1/K \to E_2/K$ induces a homomorphism from $E_1(K)$ into $E_2(K)$.*

Proof. See the discussion, "Isogenies," on pp. 49-50 of [14]. □

2.3.2 Corollary. *The set of isogenies from E_1/K to E_2/K forms a group under pointwise addition in $E_1(K)$, with identity the 0 map.*

2.3.2 Definition. We write $\mathrm{Hom}_K(E_1, E_2)$ for the group in 2.3.2. The endomorphism ring of E/K is the ring formed by $\mathrm{End}_K(E) = \mathrm{Hom}_K(E, E)$ under function composition. An endomorphism of E/K is an element of $\mathrm{End}_K(E)$.

To illustrate these new definitions, it may help to return to the case $K = \mathbb{C}$. Suppose $E_1/\mathbb{C}$ and $E_2/\mathbb{C}$ correspond to the lattices Λ_1 and Λ_2. Then E_1, E_2 are isogeneous over $\mathbb{C}$ if and only if Λ_2 is homothetic to a sublattice of Λ_1. In other words, there exists $z \in \mathbb{C}$ such that $z\Lambda_2 \subseteq \Lambda_1$; the lattices are related by a combination of rotation and dilation.

In the case $E = E_1 = E_2$ and $\Lambda = \Lambda_1 = \Lambda_2$, the set of endomorphisms of E is in bijective correspondence with the set of $z \in \mathbb{C}$ such that $z\Lambda \subseteq \Lambda$. Observe that $z \in \mathbb{Z}$ if and only if z transforms Λ by dilation alone. We recall that addition in $\mathbb{C}$ turns into the elliptic curve group law under the canonical homeomorphism $z \mapsto (\wp(z), \wp'(z))$; therefore, $\mathrm{End}_{\mathbb{C}}(E)$ contains an isomorphic copy of $\mathbb{Z}$. The "dilation" endomorphisms fit into a broader description:

2.3.3 Definition. Let $m \in \mathbb{Z}^+$. The multiplication-by-m endomorphism of E/K is the map $[m]$ such that

$$[m]P = \overbrace{P + \ldots + P}^{m \text{ terms}}$$

where the addition is that of $E(K)$.

2.3.4 Definition. The m-torsion of E/K is the subgroup $E[m] \subseteq E(K)$ of points P such that $[m]P = O$.

2.3.3 Theorem. *Let $m \geq 2$ be coprime to the characteristic of K. Then $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.*

Proof. See III.6.4 in [18]. □

The structure of the isogenies between elliptic curves is very rich, and we cannot give a thorough description here without discussing algebraic geometry in far greater detail. We will return to the structure of $\mathrm{End}_K(E)$ in Section 2.6.

2.4 Galois Representations

Recall that a number field is a finite extension $K \supseteq \mathbb{Q}$, therefore an algebraic extension. We think of K as $\mathbb{Q}[X]/I$, where I is some ideal generated by a finite collection of polynomials. The ring of integers of K is the ring $\mathcal{O}_K$ formed by all $x \in K$ such that $f(x) = 0$ for some monic $f \in \mathbb{Z}[X]$. We generally refer to the prime ideals of $\mathcal{O}_K$ as the primes of K. The following properties of $\mathcal{O}_K$ are important:

2.4.1 Theorem. *Let K be a number field. Then:*

1. *$\mathcal{O}_K$ is a Dedekind domain, meaning every ideal of $\mathcal{O}_K$ has a unique factorization into prime ideals, up to order.*
2. *The map*
$$\mathbb{N}_K(\mathfrak{a}) = \#(\mathcal{O}_K/\mathfrak{a})$$
is a norm on the nonzero ideals $\mathfrak{a} \subseteq \mathcal{O}_K$; that is, a positive-valued totally multiplicative function.

Proof. These facts are covered in the discussion on Dedekind domains in standard references on algebraic number theory; see, for example, Chapter 4 of [17]. □

Suppose K is a number field. A major paradigm of the theory of elliptic curves is that we learn Galois-theoretic information about an elliptic curve E/K from how it interacts with the primes $\mathfrak{p}$ of K. To study this interaction, we form a new elliptic curve called the reduction of E at $\mathfrak{p}$.

2.4.1 Definition. Let K be a number field. Let $\mathfrak{p} \subseteq K$ be prime, and let $q = \mathbb{N}_K(\mathfrak{p})$. The reduction of E/K modulo $\mathfrak{p}$ is the curve $\overline{E}/\mathbb{F}_q$ formed by reducing the equation defining E modulo $\mathfrak{p}$.

When we reduce the coefficients g_2, g_3 modulo $\mathfrak{p}$ to $\overline{g}_2, \overline{g}_3$, it may be the case that $\overline{g}_2^3 + 27\overline{g}_3^2 = 0$ in $\mathbb{F}_q$, so that the reduction is no longer an elliptic curve. From an algebraic geometry perspective, the reduced curve is no longer smooth; it possesses a cusp or node point, which interferes the group law. Note that this occurs precisely when $\mathfrak{p} \mid \langle \Delta(E) \rangle$. We therefore make a distinction:

2.4.2 Definition. Let K be a number field. A prime $\mathfrak{p} \subseteq K$ is of good reduction for E/K iff $\mathfrak{p} \nmid \langle \Delta(E) \rangle$. Otherwise, $\mathfrak{p}$ is of bad reduction for E/K.

Intuitively, the trace of Frobenius describes the size of a reduced curve. In Section 1.1, we stated that the trace of Frobenius of the reduction of $E/\mathbb{Q}$ at p can be defined as $p + 1 - \#\overline{E}(\mathbb{F}_p)$. This section and the next, then, explain why this value is called a trace. First, we must give some background on Galois representations of elliptic curves.

2.4.3 Definition. An inverse system of groups is a family $\{G_i\}_{i \in \mathbb{Z}}$ of groups, together with homomorphisms $\phi_{i,j} : G_j \to G_i$ for all $i \leq j$, such that

1. $\phi_{i,i}$ is the identity map on G_i.
2. $\phi_{i,k} = \phi_{i,j} \circ \phi_{j,k}$ for all $i \leq j \leq k$.

The $\phi_{i,j}$ are called the transition homomorphisms. The inverse limit of this system is the group

$$\varprojlim_{i \in \mathbb{Z}} G_i = \left\langle (x_i)_{i \in \mathbb{Z}} \in \prod_{i \in \mathbb{Z}} G_i : x_i = \phi_{i,j}(x_j) \text{ for all } i \leq j \right\rangle$$

2.4.4 Definition. Recall that $\overline{K}$ is the algebraic closure of K. The absolute Galois group of the field K is

$$G_K = \mathrm{Gal}(\overline{K}/K)$$

interpreted as the inverse limit of the system of $\mathrm{Gal}(L/K)$, over all Galois extensions L/K, where the transitions are induced by inclusion.

2.4.5 Definition. Let ℓ be prime. The ℓ-adic Tate module of E is the inverse limit

$$T_\ell(E) = \varprojlim_{n} E[\ell^n]$$

where the transition homomorphisms are $[\ell^k] : E[\ell^{n+k}] \to E[\ell^n]$.

Observe that G_K acts on $E(K)$, since it preserves the equation of the curve; in fact, it distributes over the group law, since it preserves collinearity and commutes with reflection over the Y-axis. Hence, G_K acts on the m-torsion of E for all $m \in \mathbb{Z}^+$, and by commuting with the inverse limit, $T_\ell(E)$ for all prime ℓ. Now, suppose ℓ is not the characteristic of K. One way to define the ℓ-adic integers is to consider them as an inverse limit: $\mathbb{Z}_\ell \cong \varprojlim_n \mathbb{Z}/\ell^n\mathbb{Z}$. From 2.3.3, we deduce that $T_\ell(E) \cong \mathbb{Z}_\ell^2$, meaning

$$\mathrm{Aut}(T_\ell(E)) \cong \mathrm{GL}_2(\mathbb{Z}_\ell)$$

2.4.6 Definition. The ℓ-adic representation of G_K attached to E/K is the homomorphism $\overline{\rho}_{\ell,E/K} : G_K \to \mathrm{Aut}(T_\ell(E))$ defined by

$$\overline{\rho}_{\ell,E/K}(\sigma) = (P \mapsto \sigma P)$$

2.4.2 Lemma. *Let K be a number field. Let $m \geq 2$, and let $L = K(E[m])$, the field obtained by adjoining to K the coordinates of all the points of $E[m]$. Then L/K is a finite Galois extension.*

Proof. Recall that $E[m]$ is the image of $(\mathbb{C}/\Lambda)[m]$ under $z \mapsto (\wp(z), \wp'(z))$ and use the algebraic properties of the $\wp$ function. □

2.4.3 Corollary. *Let ℓ be prime. Then $K(T_\ell(E))/K$ is a finite Galois extension.*

2.4.4 Corollary. *Let $L = K(T_\ell(E))$. Then $\overline{\rho}_{\ell,E/K}$ factors through a Galois representation $\rho_{\ell,E/K} : \mathrm{Gal}(L/K) \to \mathrm{Aut}(T_\ell(E))$. That is, the following diagram commutes:*

$$\begin{array}{ccc} G_K & & \\ \downarrow & \searrow^{\overline{\rho}_{\ell,E/K}} & \\ \mathrm{Gal}(L/K) & \xrightarrow{\rho_{\ell,E/K}} & \mathrm{Aut}(T_\ell(E)) \end{array}$$

In particular, the image of G_K under $\overline{\rho}_{\ell,E/K}$ is finite.

2.5 The Trace of Frobenius

Retain the notation from the previous section. For simplicity, this section focuses on the case $K = \mathbb{Q}$. Let $p \neq \ell$ be prime. We will find the trace of Frobenius $a_p(E)$ is the trace held in common by a conjugacy class of matrices in $\mathrm{GL}_2(\mathbb{Z}_\ell)$, these being the images of conjugate elements of $G_\mathbb{Q}$, and that $a_p(E)$ is independent of ℓ. Throughout this section, we assume $L/\mathbb{Q}$ is finite.

2.5.1 Definition. The prime $\mathfrak{P} \subseteq L$ lies over a rational prime p iff $\mathfrak{P} \mid p\mathcal{O}_L$, in which case we write $\mathfrak{P} \mid p$. The decomposition group $D_{\mathfrak{P},L/\mathbb{Q}}$ is the subgroup of $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ such that $\sigma\mathfrak{P} = \mathfrak{P}$.

2.5.2 Definition. Let p be prime such that $p\mathcal{O}_L$ has the prime factorization $\mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_g^{e_g}$ in $\mathcal{O}_L$.

1. p ramifies in L iff $e_i \geq 2$ for some $1 \leq i \leq g$.
2. p splits in L iff $g \geq 2$. In this case, p splits completely iff $g = [L : \mathbb{Q}]$.
3. p is inert in L iff $g = e_1 = \ldots = e_g = 1$.

2.5.1 Theorem. *Let $L/\mathbb{Q}$ be Galois, and let p be prime with the prime factorization $p\mathcal{O}_L = \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_g^{e_g}$ in $\mathcal{O}_L$. Then $\mathrm{Gal}(L/\mathbb{Q})$ acts transitively on the $\mathfrak{P}_i$.*

Proof. See Proposition 1 in §6.2 of [17]. □

What 2.5.1 says is that the "splitting" of primes in Galois extensions is well-behaved in several senses. First of all, if p splits into g primes in L, then $e_1 = \ldots = e_g$. Moreover, the decomposition groups $D_{\mathfrak{P}_i, L/\mathbb{Q}}$ are all conjugate with $\#D_{\mathfrak{P}_i, L/\mathbb{Q}} = [L : \mathbb{Q}]/g$. Most importantly, we obtain the following corollary:

2.5.2 Corollary. *Let $L/\mathbb{Q}$ be Galois, and let $\mathfrak{P} \mid p$ in L. Then there exists a canonical homomorphism*

$$\phi_{\mathfrak{P}|p} : D_{\mathfrak{P}, L/\mathbb{Q}} \to \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$$

where $q = p^n = \mathbb{N}_L(\mathfrak{P})$, given by the action of $D_{\mathfrak{P}}$ on $\mathcal{O}_L/\mathfrak{P} \cong \mathbb{F}_q$.

2.5.3 Corollary. *The map $\phi_{\mathfrak{P}|p}$ in 2.5.2 is surjective. It is an isomorphism if p is unramified in L.*

Proof. See Theorem 14.1.5 and Corollary 14.1.7 in [20]. □

2.5.3 Definition. Let $L/\mathbb{Q}$ be Galois. Let p be unramified in L, and let $\mathfrak{P} \mid p$. The Frobenius element of $D_{\mathfrak{P}, L/\mathbb{Q}}$ is the unique automorphism

$$\mathrm{Frob}_{\mathfrak{P}, L/\mathbb{Q}} = \phi_{\mathfrak{P}|p}^{-1}(x \mapsto x^q)$$

where $q = p^n = \mathbb{N}_L(\mathfrak{P})$ and $x \mapsto x^q$ is the Frobenius endomorphism of $\mathbb{F}_q$, the canonical generator of $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$.

Not only is $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ cyclic for all $q = p^n$, but the group $G_{\mathbb{F}_p} = \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) = \varprojlim_{\mathbb{F}_q} \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ is also "cyclic" in a topological sense. To be precise, $G_{\mathbb{F}_p}$ consists of limits of sequences of elements taking the form ϕ_p^n for some $n \in \mathbb{Z}$, where

$$\phi_p = (x \mapsto x^p, x \mapsto x^{p^2}, \ldots)$$

is the lift to $G_{\mathbb{F}_p}$ of $(x \mapsto x^q) \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$.

2.5.4 Definition. The absolute Frobenius element $\mathrm{Frob}_p \in G_{\mathbb{Q}}$ is the preimage, defined up to conjugation, of ϕ_p under the homomorphism $G_{\mathbb{Q}} \to G_{\mathbb{F}_p}$ having image $\langle \phi_p \rangle$, induced by reducing polynomials modulo p.

Another way of interpreting Frob_p is as the lift to $G_{\mathbb{Q}}$ of $\mathrm{Frob}_{\mathfrak{P},L/\mathbb{Q}} \in \mathrm{Gal}(L/\mathbb{Q})$ for all $(\mathfrak{P}, L)$ such that $L/\mathbb{Q}$ is (finite) Galois and $\mathfrak{P} \mid p$ with p unramified in L.

We are now almost ready to draw the connection between our *ad hoc* definition of $a_p(E)$ and our knowledge about Galois representations and Frobenius elements. We use the following lemma about isogenies, which will also help us prove Hasse's Theorem.

2.5.4 Lemma. *Let $\phi : E_1/K \to E_2/K$ be a nonzero isogeny. Then:*

1. $\ker \phi = \phi^{-1}(O)$ *is finite and isomorphic to* $\mathrm{Aut}(E_1(K)/\phi^* E_2(K))$.
2. *If ϕ is separable, then* $\#\ker \phi = \deg \phi$.

Proof. See III.4.10 in [18]. □

2.5.5 Definition. Write $\mu_m \subseteq \mathbb{C}^\times$ for the group of mth roots of unity. The Prüfer ℓ-group is

$$T_\ell(\mu) = \varprojlim_n \mu_{\ell^n}$$

2.5.6 Definition. Let (P_1, P_2) be a basis for $E[m] \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. The Weil pairing on $E[m]$ is the map $e_m : E[m]^2 \to \mu_m$ defined by

$$e_m(P, Q) = \zeta_m^{\det((P_1,P_2)\mapsto(P,Q))}$$

which, by linear algebra, is independent of (P_1, P_2). The Weil pairing $\overline{e}_\ell : T_\ell(E)^2 \to T_\ell(\mu)$ is constructed by letting $\overline{e}_\ell$ commute with the inverse limits of the $E[\ell^n]$ and μ_{ℓ^n}.

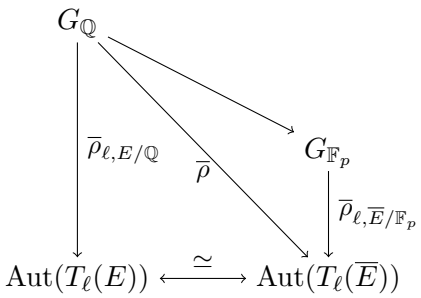
2.5.5 Theorem. *Let p be a prime of good reduction for $E/\mathbb{Q}$, and let $\overline{E}$ be the reduction of E modulo p. Let $\ell \neq p$ be prime. Let*

$$\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{Aut}(T_\ell(\overline{E})) \cong \mathrm{GL}_2(\mathbb{Z}_\ell)$$

be the representation formed by composing $\overline{\rho}_{\ell,E/\mathbb{Q}}$ with the isomorphism $\mathrm{Aut}(T_\ell(E)) \to \mathrm{Aut}(T_\ell(\overline{E}))$ induced by reducing a basis modulo p. Then

$$\begin{aligned} \det(\overline{\rho}(\mathrm{Frob}_p)) &= p \\ \mathrm{tr}(\overline{\rho}(\mathrm{Frob}_p)) &= p + 1 - \#\overline{E}(\mathbb{F}_p) \end{aligned}$$

Proof. From chasing around the diagram



we discover that, up to conjugation on either side, $\overline{\rho}$ maps Frob_p to $\phi_{p,\ell} = \overline{\rho}_{\ell,\overline{E}/\mathbb{F}_p}(\phi_p) \in \mathrm{Aut}(T_\ell(\overline{E}))$, where we also consider ϕ_p an element of $\mathrm{End}_{\overline{\mathbb{F}}_p}(E)$ via

$$\phi_p(X, Y) = (X^p, Y^p)$$

By the definition of isogeny degree, $\deg \phi_p = p$. Pick a basis (P_1, P_2) for $T_\ell(\overline{E})$. Note that the Weil pairing $\overline{e}_\ell : T_\ell(\overline{E})^2 \to T_\ell(\mu)$ is a nondegenerate, Galois-invariant, bilinear alternating map. We therefore have the chain of equalities

$$\begin{aligned}\overline{e}_\ell(P_1, P_2)^{\deg \phi_p} = \overline{e}_\ell(P_1, P_2)^p &= \overline{e}_\ell([p]P_1, P_2) \\ &= \overline{e}_\ell(\phi_{p,\ell}P_1, \phi_{p,\ell}P_2) \\ &= \overline{e}_\ell(P_1, P_2)^{\det \phi_{p,\ell}}\end{aligned}$$

(In Proposition III.8.6 of [18], this step uses the properties of the dual isogeny $\widehat{\phi}_{p,\ell}$, which for our purposes is the unique map such that $\widehat{\phi}_{p,\ell} \circ \phi_{p,\ell} = [p]$.) So $\det(\phi_{p,\ell}) = \deg \phi_p = p$. By linear algebra, we also arrive at $\mathrm{tr}(\phi_{p,\ell}) = \deg \phi_p + 1 - \deg([1] - \phi_p)$.

Observe that $\det(\phi_{p,\ell})$ and $\mathrm{tr}(\phi_{p,\ell})$ are independent of ℓ. Since $[1] - \phi_p$ is separable, we get $\deg([1] - \phi_p) = \#\ker([1] - \phi_q) = \#\overline{E}(\mathbb{F}_p)$ by 2.5.5, as needed. As a check, note that conjugate matrices have the same determinant and trace, so we are justified in defining a single determinant and trace for a full conjugacy class in $\mathrm{GL}_2(\mathbb{Z}_\ell)$. □

2.5.7 Definition. Let p be a prime of good reduction for $E/\mathbb{Q}$, and let $\overline{E}$ be the reduction of E modulo p. Let $\overline{\rho}$ be defined as in 2.5.5. The trace of Frobenius of $\overline{E}/\mathbb{F}_p$ is

$$\begin{aligned}a_p(E) &= \mathrm{tr}(\overline{\rho}(\mathrm{Frob}_p)) = \mathrm{tr}(\overline{\rho}_{\ell,\overline{E}/\mathbb{F}_p}(\phi_p)) \\ &= p + 1 - \#\overline{E}(\mathbb{F}_p)\end{aligned}$$

2.5.6 Theorem (Hasse)**.** *Let p be a prime of good reduction for $E/\mathbb{Q}$. Then $|a_p(E)| \leq 2\sqrt{p}$.*

Proof in [18]. The degree map defines a positive-define quadratic form on $\mathrm{End}_{\overline{\mathbb{F}}_p}(\overline{E})$. Let

$$f(\phi_1, \phi_2) = \deg(\phi_2 - \phi_1) - \deg\phi_1 - \deg\phi_2$$

for all $\phi_1, \phi_2 \in \mathrm{End}_{\overline{\mathbb{F}}_p}(\overline{E})$, the corresponding bilinear form. Then the inequality

$$0 \leq 4(\deg\phi_1)(\deg\phi_2) - f(\phi_1, \phi_2)^2$$

follows from the positive-definiteness. In turn, this yields

$$|f(\phi_1, \phi_2)| \leq 2\sqrt{(\deg\phi_1)(\deg\phi_2)}$$

Set $\phi_1 = \mathrm{Frob}_q$ and $\phi_2 = [1]$. Since Frob_p generates $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$, we know that $\mathbb{F}_p = \ker([1] - \mathrm{Frob}_p)$. As in the previous proof, 2.5.5 implies $\#\overline{E}(\mathbb{F}_p) = \deg([1] - \mathrm{Frob}_p)$, and the result follows. □

Later, we find that Hasse's Theorem actually provides an effective bound in a sense to be made precise. Investigating the conditions under which the extreme of $a_p(E) = \lfloor 2\sqrt{p} \rfloor$ is reached for prime p is one of our research interests.

2.6 Complex Multiplication

In this section, we assume some familiarity with the statements of global class field theory. Our goal is to study the endomorphism ring $\mathrm{End}_{\overline{K}}(E)$, where $\overline{K}$ is either $\mathbb{C}$ or $\overline{\mathbb{F}}_q$.

Recall that if $\overline{K}$ is an algebraic closure, then $\mathrm{End}_{\overline{K}}(E)$ is the set of isogenies $\phi : E \to E$, where addition is defined pointwise and multiplication is function composition. In particular, $\mathrm{End}_{\overline{K}}(E)$ contains the multiplication-by-m map $[m]$ for all $m \in \mathbb{Z}$, such that $[m] \neq [0]$ for all nonzero $[m]$. Using this fact, we can classify the possibilities for $\mathrm{End}_{\overline{K}}(E)$:

2.6.1 Definition. Let R be a finitely generated $\mathbb{Q}$-algebra. An R-subring $\mathcal{O}$ is an order of R iff it is a finitely generated $\mathbb{Z}$-module such that $R = \mathcal{O} \otimes \mathbb{Q}$. (Intuitively, taking a tensor product with $\mathbb{Q}$ means allowing the coefficients of elements of $\mathcal{O}$ to live in $\mathbb{Q}$ rather than in $\mathbb{Z}$.)

2.6.1 Theorem. $\mathrm{End}_{\overline{K}}(E)$ *is a $\mathbb{Z}$-module of rank ≤ 4. Moreover, one of the following holds:*

1. $\mathrm{End}_{\overline{K}}(E) \cong \mathbb{Z}$.
2. $\mathrm{End}_{\overline{K}}(E)$ *is isomorphic to an order in an imaginary quadratic field.*
3. $\mathrm{End}_{\overline{K}}(E)$ *is isomorphic to an order in a quaternion algebra.*

Proof. This is Theorem III.9.3 in [18]. □

For now, consider the case that $\overline{K} = \mathbb{C}$ and $\mathrm{End}_{\mathbb{C}}(E)$ is an order in an imaginary quadratic field $K = \mathbb{Q}(\sqrt{d})$, where $d < 0$ is square-free. The discriminant Δ_K of K is d if $d \equiv 1 \pmod 4$ and $4d$ if $d \equiv 2, 3 \pmod 4$. Note that Δ_K is square-free and uniquely determines K. The ring of integers of K is the subring $\mathcal{O}_K \subseteq K$ of roots of monic polynomials with coefficients in $\mathbb{Z}$. We compute $\mathcal{O}_K = \mathbb{Z}[\omega_K]$, where $\omega_K = (1 + \sqrt{|d|})/2$ if $d \equiv 1 \pmod 4$ and $\sqrt{|d|}$ if $d \equiv 2, 3 \pmod 4$.

2.6.2 Theorem. *Let $\mathcal{O}$ be an order in K. Then $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ for some unique $f \in \mathbb{Z}^+$.*

Proof. See the discussion, "Orders in Quadratic Fields," on p. 133 in [2], especially Lemma 7.2. □

2.6.2 Definition. The conductor of $\mathcal{O}$ is the integer f defined in 2.6.2. The discriminant of $\mathcal{O}$ is $\Delta_{\mathcal{O}} = f^2\Delta_K$.

Thus, $\mathcal{O}$ is unique to its discriminant. We write $\mathcal{O}_{K,f}$ for the order of conductor f in K. Henceforth, the term "order" means an order in an imaginary quadratic field, unless otherwise stated.

The following discussion is condensed from [2], pp. 134-136, 143-150. The ideal theory of $\mathcal{O}$ is more complicated than that of $\mathcal{O}_K$. Like with $\mathcal{O}_K$, we can speak of fractional ideals, and similarly to $\mathcal{O}_K$, we find that the fractional $\mathcal{O}$-ideals are precisely the $\mathcal{O}$-modules of the form $\mathfrak{a} = x\mathfrak{b}$, where $x \in K^\times$ and $\mathfrak{b}$ is an integral $\mathcal{O}$-ideal. We know that if $x \in \mathcal{O}$, then $x\mathfrak{a} \subseteq \mathfrak{a}$. However, the converse does not necessarily hold. If $\mathcal{O} = \mathcal{O}_{\mathbb{Q}(\sqrt{-3}),2} = \mathbb{Z}[\sqrt{-3}]$ and $\mathfrak{a} = \langle 2, 1 + \sqrt{-3}\rangle$, then $x\mathfrak{a} \subseteq \mathfrak{a}$ for all $x \in \mathcal{O}_K$, whether or not $x \in \mathcal{O}$.

2.6.3 Definition. A fractional $\mathcal{O}$-ideal $\mathfrak{a}$ is faithful iff $x\mathfrak{a} \subseteq \mathfrak{a}$ implies $x \in \mathcal{O}$, for all $x \in K$. (Note that [2] uses the term "proper.")

2.6.3 Theorem. *Let $\mathfrak{a}$ be a fractional $\mathcal{O}$-ideal. Then $\mathfrak{a}$ is faithful if and only if $\mathfrak{a}$ is invertible in $\mathcal{O}$.*

Proof. This is Proposition 7.4 in [2]. □

2.6.4 Definition. Let $I_{\mathcal{O}}$ be the group of faithful fractional $\mathcal{O}$-ideals. Let $P_{\mathcal{O}}$ be the group of principal fractional $\mathcal{O}$-ideals, so that $P_{\mathcal{O}} \subseteq I_{\mathcal{O}}$. The ideal class group of $\mathcal{O}$ is

$$\mathcal{C}_{\mathcal{O}} = \frac{I_{\mathcal{O}}}{P_{\mathcal{O}}}$$

The class number of $\mathcal{O}$ is $h(\mathcal{O}) = \#\mathcal{C}_{\mathcal{O}}$.

We would like to relate $\mathcal{C}_{\mathcal{O}}$ to the ray class groups of K, to understand $\mathcal{O}$ in terms of class field theory. Let f be the conductor of $\mathcal{O}$. We check that every (integral) $\mathcal{O}$-ideal coprime to $f\mathcal{O}$ in $\mathcal{O}$ is faithful. Let $I_{\mathcal{O}}^f$ be the group of fractional $\mathcal{O}$-ideals generated by the integral $\mathcal{O}$-ideals coprime to $f\mathcal{O}$, and let $P_{\mathcal{O}}^f$ be defined similarly. Let $P_{K,\mathbb{Z}}^f = P_{\mathcal{O}}^f \mathcal{O}_K$.

2.6.4 Theorem. *The following is a diagram of homomorphisms:*

$$\begin{array}{ccccc} & & I_{\mathcal{O}}^f & \xhookrightarrow{\simeq} & I_K^f \\ & & \downarrow & & \downarrow \\ \mathcal{C}_{\mathcal{O}} & \xhookrightarrow{\simeq} & I_{\mathcal{O}}^f/P_{\mathcal{O}}^f & \xhookrightarrow{\simeq} & I_K^f/P_{K,\mathbb{Z}}^f \\ & & & & \downarrow \\ & & & & \mathcal{C}_K^f \end{array}$$

where $\mathcal{C}_K^f = I_K^f/P_{K,1}^f$.

2.6.1 Remark. The notation $I_K^f, P_{K,1}^f, \mathcal{C}_K^f$ is from class field theory. Here, I_K^f is the group of fractional $\mathcal{O}_K$-ideals generated by the $\mathcal{O}_K$-ideals coprime to $f\mathcal{O}_K$, and $P_{K,1}^f$ is the subgroup of I_K^f generated by the principal ideals $x\mathcal{O}_K$ such that $x \equiv 1 \pmod{f\mathcal{O}_K}$. We call $\mathcal{C}_K^f$ the ray class group modulo f of K.

Proof. See the discussion, "Ideals Prime to the Conductor," on pp. 143-146 in [2], in particular Propositions 7.20 and 7.22. □

Since $I_K^f/P_{K,\mathbb{Z}}^f$ is a congruence subgroup of $\mathcal{C}_K^f$, class field theory predicts a unique abelian extension $K_{\mathcal{O}}$ of K, such that every prime of K that ramifies in L must divide $f\mathcal{O}_K$, and

$$\mathcal{C}_{\mathcal{O}} \cong I_K^f/P_{K,\mathbb{Z}}^f \cong \mathrm{Gal}(K_{\mathcal{O}}/K)$$

2.6.5 Definition. Let $\mathcal{O}$ be an order in K. The ring class field of $\mathcal{O}$ is $K_{\mathcal{O}}$ defined above.

For example, the ring class field of $\mathcal{O}_K$ is the Hilbert class field of K, the maximal unramified abelian extension of K, since in this case $f = 1$. The significance of this definition will become apparent in the next section, when we find that an "ordinary" elliptic curve over $\mathbb{F}_p$ "lifts" to an elliptic curve over the ring class field of its endomorphism ring.

We now connect this new theory with our previous exposition: Every order is a lattice in $\mathbb{C}$, so every fractional ideal of an order is a lattice as well.

2.6.6 Definition. The lattices Λ_1, Λ_2 are homothetic iff there exists $z \in \mathbb{C}$ such that $z\Lambda_2 = \Lambda_1$. In this case, we write $\Lambda_1 \sim \Lambda_2$.

Observe that homothety is an equivalence relation on the lattices in $\mathbb{C}$. We wish to describe the homothety classes of the faithful fractional ideals of a fixed order $\mathcal{O}$. To do this, recall that the j-invariant is a function on elliptic curves over $\mathbb{C}$, hence a function on lattices.

2.6.5 Lemma. *Let Λ_1, Λ_2 be lattices. Then $j(\Lambda_1) = j(\Lambda_2)$ if and only if $\Lambda_1 \sim \Lambda_2$.*

Proof. Since homothety corresponds to the $\mathbb{C}$-isomorphism of elliptic curves, this lemma is a corollary of 2.2.2. □

2.6.6 Theorem. *Let Λ be a lattice, $z \in \mathbb{C} - \mathbb{Z}$. Then $z\Lambda \subseteq \Lambda$ if and only if there exists an order $\mathcal{O}$ such that $z \in \mathcal{O}$ and L is homothetic to a faithful fractional $\mathcal{O}$-ideal.*

Proof. This is Theorem 10.14 in [2]. □

2.6.7 Definition. The ring of complex multiplication of Λ is the order $\mathcal{O}$ defined in 2.6.6.

Let Λ_1, Λ_2 be lattices with the same ring of complex multiplication $\mathcal{O}$. Then $\Lambda_1 \sim \Lambda_2$ if and only if Λ_1 and Λ_2 are respectively homothetic to faithful fractional $\mathcal{O}$-ideals that belong to the same class in $\mathcal{C}_\mathcal{O}$. Therefore, each element of $\mathcal{C}_\mathcal{O}$ corresponds to a well-defined j-invariant, which in turn corresponds to a homothety class of faithful fractional $\mathcal{O}$-ideals. In fact:

2.6.7 Theorem. *Let $j_1, \ldots, j_h$ be the j-invariants corresponding to the $h = h(\mathcal{O})$ classes in $\mathcal{C}_\mathcal{O}$. Then:*

1. *The $j_1, \ldots, j_h$ are conjugate algebraic integers.*
2. *$K_\mathcal{O} = K(j_k)$ for all $1 \leq k \leq h$. That is, the ring class field of $\mathcal{O}$ is obtained by adjoining the j-invariant of any faithful fractional $\mathcal{O}$-ideal to K.*

2.7 The Theorems of Deuring

Let $E/\mathbb{C}$ be an elliptic curve with lattice Λ. The Uniformization Theorem tells us $\mathrm{End}_{\mathbb{C}}(E)$, the endomorphism ring of its $\mathbb{C}$-rational points, is isomorphic to the ring of $z \in \mathbb{C}$ such that $z\Lambda \subseteq \Lambda$. Using 2.6.6, we deduce that $\mathrm{End}_{\mathbb{C}}(\mathcal{O})$ strictly contains $\mathbb{Z}$ if and only if Λ has a ring $\mathcal{O}$ of complex multiplication, and in this case, $\mathrm{End}_{\mathbb{C}}(\mathcal{O}) \cong \mathcal{O}$.

However, the situation for the endomorphism rings of elliptic curves over finite fields is more complicated. There are two kinds of elliptic curves over $\mathbb{F}_p$ with p prime:

2.7.1 Definition. We say $E/\mathbb{F}_p$ is ordinary if $a_p(E) \neq 0$ and supersingular if otherwise.

It turns out that if $E/\mathbb{F}_p$ is supersingular, then $\mathrm{End}_{\overline{\mathbb{F}}_p}(E)$ is an order in an quaternion algebra; we will not deal with this case. Nonetheless, we note that in both cases, $\mathrm{End}_{\overline{\mathbb{F}}_p}(E)$ is strictly larger than $\mathbb{Z}$. Hence, we say that elliptic curves over finite fields always have "complex multiplication."

The crucial observation is: If $E/\mathbb{F}_p$ is ordinary, then $\mathrm{End}_{\overline{\mathbb{F}}_p}(E)$ takes the same form as $\mathrm{End}_{\mathbb{C}}(E')$ for some $E'/\mathbb{C}$. Our goal is to understand the precise correspondence. In what follows, it will be important to keep track of the subscript F in the notation $\mathrm{End}_F(E)$ for the various endomorphism rings of E.

The following statements of theorems of Max Deuring from the mid-20th century are adapted from theorems proven in [13], Ch. 13, and [2], Section 14. In what follows, we assume $p \neq 2, 3$ is a rational prime. Recall that a prime $\mathfrak{p}$ of a number field lies over p iff $N(\mathfrak{p}) = p$. We write $\mathfrak{p} \mid p$ to mean $\mathfrak{p}$ lies over p.

2.7.1 Theorem (Deuring Reduction)**.** *Let F be a number field. Let E/F be an elliptic curve with $\mathrm{End}_{\mathbb{C}}(E) \cong \mathcal{O}_{K,f}$, and let $\mathfrak{p} \mid p$ be a prime of F of good reduction for E. Then:*

1. *The reduction $\overline{E}$ of E modulo $\mathfrak{p}$ is ordinary if and only if p splits completely in K.*
2. *If $\overline{E}$ is ordinary, then $\mathrm{End}_{\overline{\mathbb{F}}_p}(\overline{E}) \cong \mathcal{O}_{K,f_0}$, where $f = p^e f_0$ and $p \nmid f_0$.*

Proof. This is Theorem 12 in Ch. 13 of [13]. □

2.7.2 Theorem (Deuring Lifting)**.** *Let $E/\mathbb{F}_p$ be an ordinary elliptic curve with $\mathcal{O} \cong \mathrm{End}_{\overline{\mathbb{F}}_p}(E)$. Then there exist an elliptic curve $E'/K_{\mathcal{O}}$ and a prime $\mathfrak{p} \mid p$ of $K_{\mathcal{O}}$ of good reduction for E' such that $E = E' \pmod{\mathfrak{p}}$.*

Proof. We assemble this statement from Theorem 14.16 in [2] and 2.7.1. □

2.7.3 Theorem. *Let $\mathcal{O}$ be an order. Let $E/K_{\mathcal{O}}$ be an elliptic curve with $\mathrm{End}_{\mathbb{C}}(E) \cong \mathcal{O}$, and let $\mathfrak{p} \mid p$ be a prime of $K_{\mathcal{O}}$ of good reduction for E. Let $\overline{E} = E \pmod{\mathfrak{p}}$. Then:*

1. $\mathrm{End}_{\overline{\mathbb{F}}_p}(\overline{E}) \cong \mathcal{O}$.
2. *There exists $\pi \in \mathcal{O}$ such that $N(\pi) = p$ and $a_p(\overline{E}) = \pi + \overline{\pi}$. Here, π corresponds to the Frobenius endomorphism $x \mapsto x^p$ of $\overline{\mathbb{F}}_p$.*

Proof. This is Theorem 14.16 in [2]. □

Together, the three results above completely characterize the relationship between curves over ring class fields and ordinary elliptic curves over $\mathbb{F}_p$ via their endomorphism rings. We sketch the proof of the final theorem in this section, which enumerates the ordinary curves over $\mathbb{F}_p$ of a given order.

2.7.2 Definition. The Hurwitz class number of $\mathcal{O} = \mathcal{O}_{K,f}$ is

$$H(\mathcal{O}) = \sum_{f_0 \mid f} 2\,\frac{h(\mathcal{O}_{K,f_0})}{\#\mathcal{O}_{K,f_0}^{\times}}$$

We also write $H(D)$ for the Hurwitz class number of the order of discriminant D.

2.7.4 Theorem (Deuring Counting)**.** *Let $p \neq 2, 3$ be prime, and let $a \neq 0$ be an integer with $|a| \leq 2\sqrt{p}$. Then the number of elliptic curves $E/\mathbb{F}_p$ with $\#E(\mathbb{F}_p) = p + 1 - a$ is*

$$\frac{p-1}{2}\,H(a^2 - 4p)$$

2.7.5 Lemma (Tate)**.** *Let E_1, E_2 be elliptic curves over $\mathbb{F}_p$, at least one of which is ordinary. Then E_1 and E_2 are isomorphic over $\mathbb{F}_p$ if and only if $\#E_1(\mathbb{F}_p) = \#E_2(\mathbb{F}_p)$ and $j(E_1) = j(E_2)$.*

Proof in [2]. Suppose E_1 and E_2 are isomorphic over $\mathbb{F}_p$. The groups $E_1(\mathbb{F}_p)$ and $E_2(\mathbb{F}_p)$ are isomorphic, so have the same number of points. Moreover, E_1 and E_2 are isomorphic over $\overline{\mathbb{F}}_p$ via the natural embedding $\mathbb{F}_p \hookrightarrow \overline{\mathbb{F}}_p$, so have the same j-invariant, by 2.2.2.

Now suppose $\#E_1(\mathbb{F}_p) = \#E_2(\mathbb{F}_p)$ and $j(E_1) = j(E_2)$. Without loss of generality, assume E_1 is ordinary. A theorem of Tate says $\#E_1(\mathbb{F}_p) = \#E_2(\mathbb{F}_p)$ implies that E_1 and E_2 are at least isogenous. Let $\phi : E_1/\mathbb{F}_p \to$

$E_2/\mathbb{F}_p$ be an isogeny. Without loss of generality, assume ϕ is separable, since we can replace ϕ with $[1]-\phi$. At the same time, 2.2.2 says $j(E_1)=j(E_2)$ implies that E_1 and E_2 are isomorphic over some finite extension $\mathbb{F}_{p^e}$ of $\mathbb{F}_p$. Let $\psi : E_2/F \to E_1/F$ be an isomorphism.

Note $\psi\circ\phi \in \mathrm{End}_{\overline{\mathbb{F}}_p}(E_1)$. Since E_1 is ordinary, we know $\mathrm{End}_{\overline{\mathbb{F}}_p}(E_1)\cong\mathcal{O}$, where $\mathcal{O}$ is an order in some imaginary quadratic field. So $\mathbb{Z}[\pi]$ has finite index m in $\mathrm{End}_{\overline{\mathbb{F}}_p}(E_1)$, where π is the element of $\mathcal{O}$ corresponding to Frob_p. We check that p does not divide the conductor of $\mathbb{Z}[\pi]$, so does not divide m. Thus, $m\psi\circ\phi = \psi\circ m\phi \in \mathbb{Z}[\mathrm{Frob}_p]$, which implies $\psi\circ m\phi \in \mathrm{End}_{\mathbb{F}_p}(E_1)$. But $m\phi$ is separable, so ψ is defined over $\mathbb{F}_p$, as needed. □

Proof of 2.7.4. We enumerate the possibilities for the order $\mathcal{O}\cong\mathrm{End}_{\overline{\mathbb{F}}_p}(E)$, then count how many elliptic curves are associated with each order.

By 2.7.2 and 2.7.3, it is necessary and sufficient that $\mathcal{O}$ contains an element π such that $N(\pi)=p$ and $a=\pi+\overline{\pi}$, corresponding to the Frobenius map. Hence, the minimal polynomial of π is $(x-\pi)(x-\overline{\pi})=x^2-ax+p$, from which

$$\pi=\frac{a\pm\sqrt{a^2-4p}}{2}$$

(The solutions differ by $a\in\mathbb{Z}$, so we can treat them interchangeably.) The orders that contain π are precisely the orders that contain $\mathbb{Z}[\pi]$.

By computation, $\mathbb{Z}[\pi]$ has discriminant $D=a^2-4p$. Write $D=\Delta f^2$ with Δ square-free, so that Δ is the discriminant of the imaginary quadratic field K containing $\mathbb{Z}[\pi]$. In running through the intermediate orders between $\mathcal{O}_K=\mathcal{O}_{K,1}$ and $\mathbb{Z}[\pi]=\mathcal{O}_{K,f}$, we hit all of the elliptic curves over $\mathbb{F}_p$, since $\mathcal{O}_K$ is the maximal order of K containing $\mathbb{Z}[\pi]$. More precisely, every elliptic curve $E/\mathbb{F}_p$ lifts—by 2.7.2—to an elliptic curve $E'/L_{K,f_0}$ for some $f_0 \mid f$, where L_{K,f_0} is the ring class field of $\mathcal{O}=\mathcal{O}_{K,f_0}$.

It suffices to show the number of elliptic curves over $\mathbb{F}_p$ with $a_p(E)=a$, that lift to a curve over $L=L_{K,f_0}$, must be $(p-1)h(\mathcal{O}_{K,f_0})/\#\mathcal{O}_{K,f_0}^\times$. Recall that by 2.6.6, if $\mathrm{End}_{\overline{\mathbb{F}}_p}(E)\cong\mathcal{O}$, then there are $h(\mathcal{O})$ possible j-invariants for E. By 2.7.5, curves with different j-invariants must be non-isomorphic, so we must show there are $(p-1)/\#\mathcal{O}^\times$ curves corresponding to each possible j-invariant j.

Suppose $\Delta_\mathcal{O}=\Delta f_0^2\neq -3,-4$, which implies $j(E)\neq 0,1728$. Let $\mathfrak{p}\mid p$ in L. Since L is the ring class field of $\mathcal{O}$, we know p splits completely in L and $\mathcal{O}_L/\mathfrak{p}\cong\mathbb{F}_p$. Let

$$k=\frac{27j}{j-1728}\in\mathbb{F}_p$$

and for all $c \in \mathcal{O}_L - \mathfrak{p}$, let $E_{j,c}/L$ be defined by

$$Y^2 = 4X^3 - kc^2X - kc^3$$

Then the $E_{j,c}$ form a family of elliptic curves over L with $j(E_{j,c}) = j$, of good reduction at $\mathfrak{p}$. Moreover, by 2.7.1 and 2.7.2, every curve over $\mathbb{F}_p$ with $\mathrm{End}_{\overline{\mathbb{F}}_p}(E) \cong \mathcal{O}$ and j-invariant j is the reduction of $E_{j,c}$ for some c (see also Exercise 14.16 in [2]). All told, the reductions of the $E_{j,c}$ for fixed j represent $p-1$ curves over $\mathbb{F}_p$. However, that these reduced curves have the same j-invariant does not imply that they are isomorphic, since 2.7.5 says we also need them to have the same size. In other words, not all of these curves have trace a, as the element of norm p in $\mathcal{O}$ corresponding to the Frobenius element of $\mathrm{End}_{\overline{\mathbb{F}}_p}(E)$ might not be $\pm\pi$ as needed.

Since $\mathcal{O} \neq \mathbb{Z}[i], \mathbb{Z}[\zeta_3]$, where ζ_3 is a primitive 3rd root of unity, we know $\mathcal{O}^\times = \{\pm 1\}$. Therefore, the only elements of norm p in $\mathcal{O}$ are $\pm\pi, \pm\overline{\pi}$. So the reductions of the $E_{j,c}$ fall into two isomorphism classes, corresponding to $\pm\pi$ and $\pm\overline{\pi}$ separately. (We can predict which class from whether c is a QR modulo $\mathfrak{p}$; see Exercise 14.18 in [2]). Ultimately, there are $(p-1)/2 = (p-1)/\mathcal{O}^\times$ curves over $\mathbb{F}_p$ with trace a and j-invariant j, completing this case of the proof. We leave the cases $j(E) = 0, 1728$ as exercises, with proofs on pp. 320-322 of [2]. □

Chapter 3

Extremal Traces of Frobenius

3.1 Motivation and Results

Throughout this chapter, we write "$\mathfrak{p} \mid p$ in K" to mean the prime $\mathfrak{p}$ of a number field K lies over the rational prime p.

Our investigation concerns the question: Given an elliptic curve $E/\mathbb{Q}$, which primes p cause the reduction of E modulo p to have the maximum or minimum number of points possible, among all elliptic curves defined over $\mathbb{F}_p$? Recall that, if p is a prime of good reduction for E, then the trace of Frobenius of the reduced curve $\overline{E}/\mathbb{F}_p$ is

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

understood to be the trace of the representation of the pth Frobenius endomorphism on the Tate module $T_\ell(\overline{E})$ for any prime $\ell \neq p$. (See Sections 4-5 of the previous chapter.) Hasse proved:

3.1.1 Theorem (Hasse)**.** *Let p be a prime of good reduction for $E/\mathbb{Q}$. Then*

$$|a_p(E)| \leq 2\sqrt{p}$$

The interval in the theorem, $[-2\sqrt{p}, +2\sqrt{p}]$, is sometimes called the Hasse interval. In asking which p yield the maximum/minimum number of points possible on $\overline{E}(\mathbb{F}_p)$, our motivating question is really: How often, for a fixed curve E, does Hasse's Theorem yield an *effective* bound? Note that in Section 7 of the previous chapter, we saw that for a fixed prime p, both ends of the Hasse interval can be obtained by some elliptic curves over $\mathbb{F}_p$. Hence, another way to phrase our motivation is as an inversion of the known results: Instead of fixing a prime and varying the curve, we are fixing a curve and running over primes of good reduction.

3.1.1 Definition. Let F be a number field. Let E/F an elliptic curve, and let $\mathfrak{p} \mid p$ be a prime of F of good reduction for E. We say $\mathfrak{p}$ is a extremal prime for E iff

$$|a_p(E)| = \lfloor 2\sqrt{p} \rfloor$$

In his 2012 masters' thesis [8], Jason Hedetniemi studies the primes p such that $a_p(E) = -\lfloor 2\sqrt{p} \rfloor$, which in his work are called "champion primes" since they correspond to having a maximum possible value of $\#E(\mathbb{F}_p)$. In Section 2.2 of the thesis, Hedetniemi considers the number of champion primes on average.

3.1.2 Theorem (Hedetniemi)**.** *Let $A, B > 0$ satisfy the following growth conditions in X for some $\epsilon_1, \epsilon_2, \epsilon_3 > 0$:*

1. $A \gg \exp((1/4 + \epsilon_1)X)$.
2. $B \gg \exp((1/4 + \epsilon_2)X)$.
3. $AB \gg \exp((5/4 + \epsilon_3)X)$.

For all $a, b \in \mathbb{Z}$ with $4a^3 + 27b^2 \neq 0$, let $E_{a,b}$ be the elliptic curve defined by $Y^2 = X^3 + aX + b$. Then

$$\lim_{X\to\infty} \frac{\#\{E_{a,b} : |a| \leq A,\ |b| \leq B,\ E_{a,b} \text{ has a champion prime}\}}{\#\{E_{a,b} : |a| \leq A,\ |b| \leq B\}} = 1$$

We should note that the density of extremal primes for a fixed curve $E/\mathbb{Q}$ depends largely on whether E has complex multiplication (CM) or not. This is because the limiting distribution function of the normalized traces $a_p(E)/2\sqrt{p}$ is "semicircular" if E does not have CM, and is the roughly the "opposite" of that distribution if E does have CM. As stated in [10]: For all $[a, b] \subseteq [-1, +1]$, if E does not have CM, then

$$\lim_{X\to\infty} \frac{\#\{p \leq X : a_p(E)/2\sqrt{p} \in [a, b]\}}{\#\{p \leq X\}} = \frac{2}{\pi} \int_a^b \sqrt{1 - t^2}\, \mathrm{d}t$$

If E has CM, then there is a spike at $a_p(E) = 0$ of measure $1/2$, which corresponds to the supersingular primes, and

$$\lim_{X\to\infty} \frac{\#\{p \leq X : a_p(E)/2\sqrt{p} \in [a, b],\ a_p(E) \neq 0\}}{\#\{p \leq X\}} = \frac{1}{2\pi} \int_a^b \frac{1}{\sqrt{1 - t^2}}\, \mathrm{d}t$$

The latter result is classical, and was first established by Ernst Hecke in 1919 in the papers [6] and [7]. The non-CM case is substantially more difficult,

and was first achieved by Richard Taylor in 2006 in [22], after two other papers written in collaboration. We revisit their work in Chapter 5.

In short, the difference between the CM and non-CM cases means it is very difficult to find champion or extremal primes for non-CM curves—typically there are fewer than a dozen among all primes $\leq 100\,000$—whereas there are many such primes for CM curves. Using the Chinese Remainder Theorem, it is trivial to show that there exist elliptic curves without CM that have no extremal primes $\leq N$ given any $N \in \mathbb{Z}^+$. As of this writing, the following conjectures are open:

3.1.3 Conjecture. *Every elliptic curve $E/\mathbb{Q}$ without complex multiplication has an extremal prime.*

3.1.2 Definition. Let $\pi(X)$ be the usual prime-counting function, meaning the number of primes $\leq X$. Let $\pi_E^{\text{Hasse}}(X)$ be the number of extremal primes $\leq X$ for $E/\mathbb{Q}$.

3.1.4 Conjecture. *Every elliptic curve $E/\mathbb{Q}$ with complex multiplication has infinitely many extremal primes, and*

$$\pi_E^{Hasse}(X) \sim C_E^{Hasse} \frac{X^{3/4}}{\log X}$$

(Recall that there are only finitely many primes of bad reduction for E.)

3.1.5 Conjecture. *For all nonzero $b \in \mathbb{Z}$, let E_b be the elliptic curve defined by $Y^2 = X^3 + b$. Then there exists some $N > 0$ such that if $|b| \geq N$, then E_b has an extremal prime $\leq b$.*

By itself, each conjecture above is a question of great difficulty. In this chapter, we show that a weaker form of 3.1.4 holds, if we assume the truth of a classical conjecture of Hardy-Littlewood in [4].

3.1.6 Conjecture (Hardy-Littlewood Conjecture F, 1923)**.** *Let $f(T) = aT^2 + bT + c \in \mathbb{Z}[T]$, such that $a > 0$ and*

1. $\gcd(a, b, c) = 1$.
2. $4 \nmid (a + b)c$.
3. *$d_f = b^2 - 4ac$ is not a square.*

Let $\pi_f(X)$ be the number of primes $p \leq X$ of the form $p = f(n)$ with $n \in \mathbb{Z}$. Then

$$\pi_f(X) \sim \frac{\epsilon_f C_f}{\sqrt{a}} \prod_{\substack{p \mid \gcd(a,b) \\ p \neq 2}} \frac{p}{p-1} \frac{\sqrt{X}}{\log X}$$

where

$$\epsilon_f = \frac{1}{2}(3 + (-1)^{a+b})$$
$$C_f = \prod_{\substack{p \nmid a \\ p \neq 2}} \left(1 - \frac{1}{p-1}\left(\frac{d_f}{p}\right)\right)$$

3.1.7 Theorem (T-T-W)**.** *Assume that the Hardy-Littlewood Conjecture F holds. Let $E/\mathbb{Q}$ be an elliptic curve with $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \cong \mathcal{O}$, where $\mathcal{O}$ is an imaginary quadratic order of discriminant $\Delta_{\mathcal{O}} \neq -3, -4$. Then*

$$\pi_E^{Hasse}(X) = \Theta(X^{3/4}/\log X)$$

meaning $\pi_E^{Hasse}(X)(\log X)/X^{3/4}$ is bounded uniformly in X.

3.2 Proofs

3.2.1 Definition. For convenience, let $D(a, n) = a^2 - 4n$ for all $a, n \in \mathbb{Z}$. Abbreviate $D(n) = \lfloor 2\sqrt{n} \rfloor^2 - 4n$.

The following lemma is immediate from the work of Deuring presented in Section 7 of the previous chapter. However, it is infrequently written out in formal expositions, so we state it here.

3.2.1 Lemma. *Let $E/\mathbb{Q}$ be an elliptic curve with $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \cong \mathcal{O}$, where $\mathcal{O}$ is an imaginary quadratic order. Let $p \neq 2, 3$ be a prime of ordinary reduction for E. Then*

$$D(a_p(E), p) = a_p(E)^2 - 4p = \Delta_{\mathcal{O}} v^2$$

for some $v \in \mathbb{Z}$.

Proof. Let $\overline{E}$ be the reduction of E modulo p, and let $a = |a_p(E)|$. We know $\mathrm{End}_{\overline{\mathbb{F}}_p}(\overline{E})$ contains the Frobenius element π, satisfying $\pi^2 \pm a\pi + p = 0$. So $\mathbb{Z}[\pi] \subseteq \mathrm{End}_{\overline{\mathbb{F}}_p}(\overline{E})$, where we compute that $D(a, p)$ is the discriminant of $\mathbb{Z}[\pi]$. But by hypothesis, p does not divide the conductor of $\mathcal{O}$ and $\overline{E}$ is ordinary, from which $\mathrm{End}_{\overline{\mathbb{F}}_p}(\overline{E}) \cong \mathcal{O}$ by Chapter 13, Theorem 12 of [13]. This proves $D(a, p) = \Delta v^2$ for some $v \in \mathbb{Z}$. □

3.2.2 Lemma. *Let D be a nonpositive integer such that $D \equiv 0, 1 \pmod 4$. Then for all $n \in \mathbb{Z}_{\geq 0}$,*

$$D(n) = D \iff n = \begin{cases} u^2 + \dfrac{|D|}{4},\ u \geq \dfrac{|D|}{4} & D \equiv 0 \pmod 4 \\ u^2 + u + \dfrac{|D|+1}{4},\ u \geq \dfrac{|D|+1}{4} & D \equiv 1 \pmod 4 \end{cases}$$

for some $u \in \mathbb{Z}_{\geq 0}$.

Proof. Suppose $u^2 \leq n < (u+1)^2$, where $u \in \mathbb{Z}$. Write $n = u^2 + n_0$. If $n_0 \leq u$, then $2u \leq 2\sqrt{n} < \sqrt{4u^2 + 4u + 1} = 2u+1$, from which $\lfloor \sqrt{4n} \rfloor = 2u$. Similarly, if $n_0 > u$, then $\lfloor \sqrt{4n} \rfloor = 2u + 1$. Altogether,

$$D_n = \begin{cases} -4n_0 & n_0 \leq u \\ -4(n_0 - u) & n_0 > u \end{cases}$$

and the result follows. □

3.2.2 Definition. Let $\mathcal{O}$ be an imaginary quadratic order. We define

$$\Delta'_{\mathcal{O}} = \begin{cases} 2^2 \Delta_{\mathcal{O}} & \Delta_{\mathcal{O}} = -7 \\ \Delta_{\mathcal{O}} & \text{otherwise} \end{cases}$$

3.2.3 Corollary (T-T-W)**.** *Let $E/\mathbb{Q}$ be an elliptic curve with $\mathrm{End}_{\mathbb{C}}(E) \cong \mathcal{O}$, where $\mathcal{O}$ is an imaginary quadratic order with $\Delta_{\mathcal{O}} \neq -3, -4$. Let $p \neq 2, 3$ be a prime of ordinary reduction for E. Then p is a extremal prime for E if and only if there exist $u, v \in \mathbb{Z}$, where $u \geq 0$, such that either of the following holds:*

1. $p = u^2 + \dfrac{|\Delta'_{\mathcal{O}}| v^2}{4}$ *and* $u \geq \dfrac{|\Delta'_{\mathcal{O}}| v^2}{4}$.
2. $p = u^2 + u + \dfrac{|\Delta'_{\mathcal{O}}| v^2 + 1}{4}$ *and* $u \geq \dfrac{|\Delta'_{\mathcal{O}}| v^2 + 1}{4}$.

Proof. By 3.2.2, it suffices to prove that p is a extremal prime for E if and only if $D(p) = \Delta'_{\mathcal{O}} v^2$ for some $v \in \mathbb{Z}$. Note that 3.2.1 proves the "only if" direction and proves the "if" direction in the case where $\Delta_{\mathcal{O}} \neq -7$. If $\Delta_{\mathcal{O}} = -7$, then we check using 3.2.2 that $D(a_p(E), p) = -7v^2$ can occur for p odd only if $2 \mid v$. So we can write $D(p) = \Delta'_{\mathcal{O}} v^2$, where $\Delta'_{\mathcal{O}} = 2^2 \Delta_{\mathcal{O}}$. □

3.2.1 Remark. With 3.2.3, we have shown that the problem of computing $\pi_E^{\text{Hasse}}(X)$ for a CM curve E is equivalent to determining how often members of a family of quadratic polynomials attain prime values. The fact that the error bounds on the Prime Number Theorem are, in the best case, $X^{1/2}\log X$ assuming the Riemann Hypothesis, is what causes this and Hardy-Littlewood's problem to remain wide open.

Proof of 3.1.7. We will use the conditions above guaranteeing that a prime p is an extremal prime for a CM curve of discriminant $\Delta \neq -3, -4$. For some v, we compute the number of primes $p \leq n$ with $D(p) = \Delta v^2$. For Δv^2 odd, this equals the number of primes p that can be written in the form $n^2 + n + (1 - \Delta v^2)/4$ with $4\sqrt{p} \geq \Delta v^2$, denoted $E(\Delta v^2, n)$. (It's easy to see that $|D(p)| \leq 4\sqrt{p}$.) We note that the discriminant of this quadratic is Δv^2 and apply 3.1.6. We also use that $\left(\frac{\Delta v^2}{p}\right) = \left(\frac{\Delta}{p}\right)$ to get

$$E(\Delta v^2, n) \sim 2c\left(\frac{\sqrt{n}}{\log n} - \frac{\frac{\Delta v^2}{4}}{2\log\frac{\Delta v^2}{4}}\right)$$

where c is a constant depending on Δ.

Now, when Δv^2 is even, we do the same thing but with $n^2 - \Delta/4$ and so we have

$$E(\Delta v^2, n) \sim c\left(\frac{\sqrt{n}}{\log n} - \frac{\frac{\Delta v^2}{4}}{2\log\frac{\Delta v^2}{4}}\right)$$

From this, we can see that we can compute the number of external primes by summing $E(\Delta v^2, n)$ over v. Since we will be computing a θ bound, we can ignore the 2 for the case when Δv^2 is odd. Our sum can only go up to when $\Delta v^2/4 \leq \sqrt{n}$, in which case $v \leq v_{\max} = 2n^{1/4}/\sqrt{\Delta}$.

We get an easy upper bound on the number $E(n)$ of external primes less than n, by

$$E(n) \leq \sum_{v=1}^{v_{\max}} 2c\frac{\sqrt{n}}{\log n} = O(n^{3/4}\log n)$$

Now to get a lower bound, we recall that we want only primes satisfying the quadratics above that are greater than $\Delta^2 v^4/16$.

$$\sum_{v=1}^{v_{\max}} E(\Delta v^2, n) \sim \sum_{v=2}^{v_{\max}} c\left(\frac{\sqrt{n}}{\log n} - \frac{\frac{\Delta v^2}{4}}{2\log\frac{\Delta v^2}{4}}\right) > cv_{\max}\frac{\sqrt{n}}{\log n} - \frac{\Delta c}{16}\sum_{v=2}^{v_{\max}}\frac{v^2}{\log v}$$

We must compute $\sum_{v=2}^{X} \frac{v^2}{\log v}$. We can approximate this with

$$\int_{v=2}^{X} \frac{v^2}{\log v} dv = \frac{X^3}{3\log X} + \int_{v=2}^{X} \frac{v^2}{3(\log v)^2} = \frac{X^3}{3\log X} + O\left(\frac{X^3}{(\log X)^2}\right)$$
$$< \frac{2X^3}{3\log X}$$

Plugging in $X = v_{\max}$, we get $E(n) > c(v_{\max}\sqrt{n}/\log n - 2v_{\max}^3/3\log v_{\max})$. Since $v_{\max} < n^{1/4}$, this is $\Omega(n^{3/4}/\log n)$. Therefore, we conclude that $E(n) = \theta(n^{3/4}/\log n)$. □

3.3 Future Work

By algebraic number theory, we find that the extremal primes of an elliptic curve $E/\mathbb{Q}$ with $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \cong \mathcal{O}$, an imaginary quadratic order, are precisely the primes that split in $\mathcal{O}$, such that the primes that lie over them live in the interior of parabolic regions in $\mathbb{C}$, with axis along the real axis. These regions arise because of the condition $u \geq |\Delta'_{\mathcal{O}}|v^2/4$ or $u \geq (|\Delta'_{\mathcal{O}}|v^2 + 1)/4$ encountered in 3.2.3.

The problem of merely showing there are infinitely many extremal primes for E, without the assumption of Conjecture F, is equivalent to showing that these parabolic regions contain infinitely many primes of the quadratic field K to which $\mathcal{O}$ belongs. This is analogous to viewing Conjecture F as a statement about the density of primes of K along horizontal lines in $\mathbb{C}$ through points of $\mathcal{O}$—a stronger statement.

The solution of these density problems will undoubtedly use much more advanced tools of number theory than the theorems of Deuring on which our work is based. In fact, these problems point at the natural improvement on the Chebotarev Density Theorem, which predicts the asymptotic density of primes of K as their maximum norm tends to ∞, but says nothing regarding the distribution of their angles in $\mathbb{C}$. The Hardy-Littlewood Conjecture F, and by extension our result 3.1.7, agree with the belief that the primes of K should be *roughly equidistributed* with respect to their angles, after accounting for natural symmetries.

In the vein of these observations, let us conclude with this conjecture:

3.3.1 Conjecture. *Let D be a nonpositive integer with $D \equiv 0, 1 \pmod 4$. Then there exists $C_D > 0$ such that*

$$\pi_D(X) = \#\{p \leq X : D(p) = D, \, p \text{ is prime}\} \sim C_D \frac{X^{1/2}}{\log X}$$

Chapter 4

Prime Traces of Frobenius [Attached]

[Please see the attached file, `3_PrimeTraces.pdf`, for the main content.]

4.1 Results

4.1.1 Definition. For all $a, b \in \mathbb{Z}$ such that $4a^3 + 27b^2 \neq 0$, let $E_{a,b}$ be the elliptic curve defined by $Y^2 = X^3 + aX + b$. Let $\pi_{a,b}(\alpha; X)$ denote the number of primes $p \leq X$ such that $a_p(E_{a,b}) \leq 2\alpha\sqrt{p}$ and is prime.

4.1.1 Theorem (T-T-W)**.** *Let*

$$S_\alpha(U, V, A, B; X) = \frac{1}{AB} \sum_{\substack{a \in (U, U+A] \\ b \in (V, V+B]}} \pi_{a,b}(\alpha; X)$$

Then

$$S_\alpha(U, V, A, B; X) \sim c(\alpha)\pi(X)$$

where

$$c(\alpha) = \frac{16C}{\pi} \int_0^\alpha \sqrt{1 - t^2}\, \mathrm{d}t = \frac{8C}{3\pi} \left(\alpha\sqrt{1 - \alpha^2} + \arcsin(\alpha) \right)$$
$$\pi(X) = \int_2^X \frac{\mathrm{d}t}{(\log t)^2} = (1 + O((\log X)^{-1})) \frac{X}{(\log X)^2}$$

and

$$C = \sum_{k:2\nmid k} \frac{\mu(k)\tau(k)}{\phi(k)k} \sum_{\substack{u:2\nmid u \\ \gcd(u,k)=1}} \frac{\mu(u)^2}{u^4} \sum_{\substack{v:2\nmid v \\ \gcd(v,uk)=1}} \frac{\mu(v)^2}{\phi(v)v} D(k,u,v)$$

$$D(k,u,v) = \sum_{f':\gcd(f',2k)=1} \frac{1}{f'^3} \sum_{\substack{w:2\nmid w \\ (w,v)=1}} \frac{\phi(w)\gcd(k,w)\gcd(v,w)}{\phi(k,w)\phi(u,w)w^3}$$

where ϕ, τ, μ are the classical arithmetic functions and $\phi(a,b) = \phi(\gcd(a,b))$ for all nonzero $a, b \in \mathbb{Z}$.

4.1.2 Theorem (T-T-W)**.** *Suppose $A, B > (X \log X)^2$. Then*

$$\frac{1}{AB} \sum_{\substack{a\in(U,U+A] \\ b\in(V,V+B]}} |\pi_{a,b}(\alpha; X) - c(\alpha)\pi(X)|^2 = o(\pi(X)^2)$$

4.2 Analytic Techniques

We outline the version of the Hardy-Littlewood Circle Method that inspires our own approach, largely following the procedure of K. James and G. Yu in Section 2 of [9]. In the 1920s, G. H. Hardy and J. E. Littlewood developed a broad paradigm to deal with questions in additive number theory related to Waring's Problem. Specifically, they proposed using complex analysis to estimate the number of ways to write an integer as a sum of a fixed number of elements from a fixed subset of the integers.

Though our problem does not have this additive nature, the analytic techniques used in the Circle Method are still fruitful. Let $n \equiv 0, 1 \pmod 4$ be negative, and fix a subset $\mathcal{R} \subseteq \mathbb{Z}$. We wish to estimate the number of representations of n in the form $r^2 - 4p$, where $r \in \mathcal{R}$ and p is prime. Note that $r \leq 2\sqrt{p}$. We fix $X > 0$ and $\alpha \in (0,1)$, and count the representations of n with $p \leq X$ and $r \leq 2\sqrt{p}\alpha$, weighted by $\log p$:

$$R(n) = \sum_{\substack{p\leq X,\, r\leq 2\sqrt{p}\alpha \\ r^2-4p=n}} \log p$$

Here and throughout the rest of the article, it is implicitly understood that a sum over r and p only runs over $r \in \mathcal{R}$ and p prime. Before using contour integration, we must rewrite $R(n)$ in a nicer form. Let $g = 1 + (\log X)^{-5}$,

and let $L = \lfloor \log_g(4X/n) \rfloor \ll (\log X)^5 \log\log X$. Then $R(n) = \sum_{\ell=0}^{L} R_\ell(n)$, where

$$R_\ell(n) = \sum_{\substack{p \in (X/g^{\ell+1},\, X/g^\ell] \\ r \le 2\sqrt{p}\alpha \\ r^2 - 4p = n}} \log p$$

Let us modify R_ℓ to

$$R_\ell^*(n) = \sum_{\substack{p \in (X/g^{\ell+1},\, X/g^\ell] \\ r \le 2\sqrt{X/g^\ell}\alpha \\ r^2 - 4p = n}} \log p$$

The difference is bounded: $0 \le R_\ell^*(n) - R_\ell(n) \ll \log X + \sqrt{X/g^\ell} \log X)^{-4}$. In particular, the number of ℓ such that $R_\ell^*(n) - R_\ell(n) > 0$ is constant in α. Altogether, then,

$$R(n) = \sum_{\ell=0}^{L} R_\ell^*(n) + O(\sqrt{X}(\log X)^{-3})$$

We now explain the actual estimation of $R_\ell^*(n)$. Let Γ be the circle of radius 1 centered at 0 in the complex plane. By Cauchy's Integral Formula, $\int_\Gamma z^{m-1}\,\mathrm{d}z$ equals $2\pi i$ if $m = 0$ and 0 if otherwise. We rewrite this integral as $2\pi i \int_0^1 e(m\beta)\,\mathrm{d}\beta$, where $e(\beta) = e^{2\pi i \beta}$. The trick is:

$$\begin{aligned} R_\ell^*(n) &= \sum_{\substack{p \in (X/g^{\ell+1},\, X/g^\ell] \\ r \le 2\sqrt{X/g^\ell}\alpha}} \int_0^1 e((r^2 - 4p - n)\beta) \log p \,\mathrm{d}\beta \\ &= \int_0^1 s_{\ell,1}(\beta) s_{\ell,2}(-4\beta) e(-n\beta)\,\mathrm{d}\beta \end{aligned}$$

where

$$\begin{aligned} s_{\ell,1}(\beta) &= \sum_{p \in (X/g^{\ell+1},\, X/g^\ell]} e(p\beta) \log p \\ s_{\ell,2}(\beta) &= \sum_{r \le 2\sqrt{X/g^\ell}\alpha} e(r^2\beta) \end{aligned}$$

It is useful to translate the interval of integration to $I = [P/X, 1 + P/X]$, where $P = (\log X)^A$ for some large fixed A to be chosen later.

The idea of Hardy and Littlewood is to partition I into "major arcs" $\mathfrak{M}$ and "minor arcs" $\mathfrak{m}$ (the term "arc" comes from the circle Γ), chosen so that the contribution to the integral from $\mathfrak{m}$ is small compared to that from $\mathfrak{M}$. In particular, on the major arcs, we estimate $R_\ell^*(n)$ as the product of a singular sum $\mathfrak{S}(n)$ and a singular integral $J_\ell^*(n)$, following the notation given by R. C. Vaughan in [23]. On both major and minor arcs, the first objective is to bound

$$f(\alpha) = \sum_{p \leq X} e(p\alpha) \log p$$

In our work, of course, $\mathcal{R}$ is the set of primes.

Outside of the standard techniques covered in R. C. Vaughan's textbook [23], we also rely on the following results, found as Theorem 2 in [12] and Theorem 2 in [3], respectively:

4.2.1 Theorem (Kumchev)**.** *Let $\alpha, Q \in \mathbb{R}$ and $k \in \mathbb{Z}^+$ such that*

$$\left|\alpha - \frac{a}{q}\right| < \frac{Q}{qY^k}$$

for some $a/q \in \mathbb{Q}$ in lowest terms such that $1 \leq q \leq Q \leq Y$. Then for all $\epsilon > 0$,

$$\sum_{p \in [Y, 2Y)} e(\alpha p^k) \leq C_{k,\epsilon} Q^{1/2} Y^{11/20+\epsilon} + \frac{q^\epsilon Y (\log Y)^c}{(q + Y^k |q\alpha - a|)^{1/2}}$$

where c is an absolute constant and $C_{k,\epsilon}$ depends at most on k, ϵ.

4.2.2 Theorem (Ghosh)**.** *Let $\Lambda(n)$, the von Mangoldt function, equal $\log p$ if $n = p^m$ is a prime power and 0 if otherwise. Let $\alpha \in \mathbb{R}$ and $N \in \mathbb{Z}^+$. Then for all $\epsilon > 0$,*

$$\sum_{n \leq N} \Lambda(n) e(n^2 \alpha) \leq C_\epsilon N^{1+\epsilon} (q^{-1} + N^{-1/2} + qN^{-2})^{1/4}$$

where C_ϵ depends at most on ϵ.

4.3 Future Work

While the proofs of 4.1.1 and 4.1.2 are interesting in their own right, the theorems themselves are relatively specialized results, unless we consider the question of the density of prime traces of Frobenius part of a broader goal, of predicting densities of traces of Frobenius belonging to certain infinite

subsets of the integers. We believe that, under sufficiently strong conditions of equidistribution analogous to those of Kumchev and Ghosh, we should find generalizations of 4.1.1 and 4.1.2 to other infinite subsets of the integers that—like the prime numbers—are predicted to behave mostly "randomly" with respect to the sequence of traces of Frobenius of a typical $E/\mathbb{Q}$.

Chapter 5

The Akiyama-Tanigawa Conjecture

This chapter is a shortened exposition of Shigeki Akiyama and Yoshiro Tanigawa's 1999 result, that a stronger form of the Sato-Tate Conjecture—one that proposes the rate of convergence of the normalized traces to their limiting distribution—implies the Riemann Hypothesis for elliptic curves over $\mathbb{Q}$ without complex multiplication. To conclude, we describe a plan of future exploration of this work.

5.1 Strengthening the Sato-Tate Conjecture

Since March 2006, the Sato-Tate Conjecture has largely been proven via the joint work of Michael Harris, Laurent Clozel, Nicholas Shepherd-Barron, and Richard Taylor. We state a weaker form of their result here (Theorem 1 in [15]):

5.1.1 Theorem (Harris-Clozel-Shepherd-Barron-Taylor)**.** *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication, having at least one prime of multiplicative reduction. Then for all $[a, b] \subseteq [-1, +1]$,*

$$\lim_{X\to\infty} \frac{\#\{p \leq X : a_p(E)/2\sqrt{p} \in [a, b]\}}{\#\{p \leq X\}} = \frac{2}{\pi}\int_a^b \sqrt{1-t^2}\,\mathrm{d}t$$

where p runs over the primes of good reduction for E.

Above, $a_p(E)/2\sqrt{p}$ is the pth trace of Frobenius, $a_p(E)$, normalized by the size of the Hasse interval. Hence, 5.1.1 says that the normalized traces

for an elliptic curve without complex multiplication follow a semicircular distribution. In what follows, it will be useful for us to reparametrize:

5.1.1 Definition. Let p be a prime of good reduction for $E/\mathbb{Q}$. We define $\theta_p(E) \in [0, \pi]$ by

$$\cos \theta_p = \frac{a_p(E)}{2\sqrt{p}}$$

After a change of variables, we find 5.1.1 is equivalent to saying that the $\theta_p(E)$ have limiting density $(2/\pi) \sin^2 \theta \, \mathrm{d}\theta$, running over the primes $\leq X$ of good reduction, as $X \to \infty$. In this exposition, we are interested in the *rate* of convergence to the limiting distribution. Towards this goal, we introduce the following terminology and notation:

5.1.2 Definition. Let $(x_n)_{n=1}^{\infty}$ be a sequence in $\mathbb{R}$. The Nth empirical distribution function of (x_n) is

$$F_N(t; x_n) = \frac{\#\{n \leq N : x_n \leq t\}}{N}$$

(See [11], p. 31.) The asymptotic distribution function of (x_n) is defined by $F(t; x_n) = \lim_{N \to \infty} F_N(t; x_n)$, when that limit exists.

5.1.3 Definition. Let (x_n) be a sequence. The discrepancy of $(x_n)_{n=1}^{N}$ with respect to $F : \mathbb{R} \to \mathbb{R}$ is

$$\delta(N; x_n, F) = \sup_{t \in \mathbb{R}} |F_N(t; x_n) - F(t)|$$

We abbreviate $\delta(x_n, F) = \lim_{N \to \infty} \delta(N; x_n, F)$.

Note that F is the asymptotic distribution function of (x_n) if and only if $\delta(x_n, F) = 0$. As Chris Swierczewski states in [21], the use of a discrepancy function was proposed by Harold Niederreiter, in a paper on quasi-Monte Carlo integration methods.

Let (p_n) be the sequence of primes of good reduction for $E/\mathbb{Q}$. We find the Sato-Tate Conjecture is equivalent to stating: $(\theta_{p_n}(E))$ has the asymptotic distribution function

$$F_{\mathrm{ST}}(t) = \frac{2}{\pi} \int_0^t \sin^2 \theta \, \mathrm{d}\theta$$

for all $t \in [0, \pi]$. Written in full, $\delta(N; \theta_{p_n}(E), F_{\mathrm{ST}}) \to 0$ as $N \to \infty$. Shigeki Akiyama and Yoshiro Tanigawa propose the following refinement in [1]:

5.1.2 Conjecture (Akiyama-Tanigawa)**.** *Let $E/\mathbb{Q}$ be an elliptic curve that does not have complex multiplication. Then*

$$\delta(N; \theta_{p_n}(E), F_{\mathrm{ST}}) = O(N^{-(1/2-\epsilon)})$$

for all $\epsilon > 0$, where $F_{\mathrm{ST}}(t) = (2/\pi)\int_0^t \sin^2\theta \, \mathrm{d}\theta$.

We will see this conjecture has a deep connection to one form of the Riemann Hypothesis—specifically, for L-functions attached to elliptic curves.

5.2 A Riemann Hypothesis for Elliptic Curves

5.2.1 Definition. Let p be a prime of bad reduction for $E/\mathbb{Q}$. We generalize

$$a_p(E) = \begin{cases} 0 & \text{additive reduction} \\ +1 & \text{split reduction} \\ -1 & \text{non-split reduction} \end{cases}$$

(Recall that E has split reduction at p iff the slopes of the tangent lines to the node of $\overline{E}/\mathbb{F}_p$ live in $\mathbb{F}_p$. See [18], VII.5.)

5.2.2 Definition. The L-series of the elliptic curve $E/\mathbb{Q}$ of discriminant Δ is

$$L(s; E/\mathbb{Q}) = \prod_p L(s; E/\mathbb{F}_p)$$

where

$$L(s; E/\mathbb{F}_p) = \begin{cases} \dfrac{1}{1 - a_p(E)p^{-s} + p^{1-2s}} & p \nmid \Delta \\ \\ \dfrac{1}{1 - a_p(E)p^{-s}} & p \mid \Delta \end{cases}$$

is the local factor of $L(s; E/\mathbb{Q})$ at p.

Recall that, whenever we are given an L-series, we seek to construct the meromorphic continuation—called the associated L-function—of the series to all of the complex plane. In particular, we want a functional equation, which will tell us a transformation under which the L-function has symmetry across a vertical axis in $\mathbb{C}$. For instance, the original Riemann ζ function has a functional equation with symmetry about $\mathrm{Re}(s) = 1/2$. We then want to determine the zeroes and poles of the L-function, using this equation.

The Generalized Riemann Hypothesis for $E/\mathbb{Q}$ states: The zeroes of $L(s; E/\mathbb{Q})$ in the critical strip $0 \leq \mathrm{Re}(s) \leq 2$ all live on the functional

axis of symmetry. Akiyama and Tanigawa prove an approximation to the functional equation of $L(s; E/\mathbb{Q})$, which confirms the expectation that the axis of symmetry is $\mathrm{Re}(s) = 1$. (By the Modularity Theorem, elliptic curves over $\mathbb{Q}$ are in correspondence with newforms in $\mathcal{S}_2(\Gamma_0(N))$. Per Theorem 16.1.4 of [16], the functional equation for a cusp form of weight k for $\Gamma_1(N)$ is known, with symmetry about $\mathrm{Re}(s) = k/2$.)

In light of the functional equation for $L(s; E/\mathbb{Q})$, the following conjecture implies the GRH for $E/\mathbb{Q}$:

5.2.1 Conjecture. $\log L(s; E/\mathbb{Q})$ *is holomorphic in the open half-plane* $\mathrm{Re}(s) > 1$. *(We use the principal branch of the complex logarithm.)*

In their 1999 article, Akiyama and Tanigawa show that their conjecture 5.1.2 implies 5.2.1, and by extension the Generalized Riemann Hypothesis for elliptic curves. The next section discusses the proof of this result:

5.2.2 Theorem (Akiyama-Tanigawa)**.** *5.1.2 implies 5.2.1 for all elliptic curves* $E/\mathbb{Q}$ *without complex multiplication.*

5.3 Proof of the Akiyama-Tanigawa Theorem

5.3.1 Lemma (Koksma, for Continuous Functions)**.** *Let* $f : [0,1] \to \mathbb{R}$ *be continuous with total variation* $V_f < \infty$*, and let* $\mathrm{d}\mu$ *be an a. e. nonzero density function on* $[0,1]$*. Then*

$$\left| \frac{1}{N} \sum_{n=1}^{N} f(x_n) - \int_0^1 f(t)\,\mathrm{d}\mu(t) \right| \leq V_f \delta(N; x_n, \mu)$$

for every sequence $(x_n)_{n \in \mathbb{Z}^+}$ *in* $[0,1]$.

5.3.1 Remark. Recall that the total variation of f is defined to be $V_f = \sup_{\mathcal{P}} \sum |f(p_{j+1}) - f(p_j)|$, where the supremum is taken over all partitions $\mathcal{P} = \{0 = p_0 < \ldots < p_J = 1\}$ of $[0,1]$. See [19], p. 117.

Proof. Define

$$\delta_t(N; x_n, \mu) = F_N(t; x_n) - \mu(t)$$

Let $\chi_{[0,t]} : \mathbb{R} \to \{0,1\}$ be the indicator of $[0,t]$, meaning $\chi_{[0,t]}(x) = 1$ if

$x \in [0,t]$ and $\chi_{[0,t]}(x) = 0$ otherwise. We integrate by parts:

$$\begin{aligned}\int_0^1 \delta_t(N;x_n,\mu)\,\mathrm{d}f(t) &= \frac{1}{N}\sum_{n=1}^{N}\int_0^1 \chi_t(x_n)\,\mathrm{d}f(t) - \int_0^1 \mu(t)\,\mathrm{d}f(t)\\ &= \frac{1}{N}\sum_{n=1}^{N}(f(1)-f(x_n)) - f(1)\mu(1) + \int_0^1 f(t)\,\mathrm{d}\mu(t)\\ &= -\frac{1}{N}\sum_{n=1}^{N} f(x_n) + \int_0^1 f(t)\,\mathrm{d}\mu(t)\end{aligned}$$

Bound $|\int_0^1 \delta_t(N;x_n,\mu)\,\mathrm{d}f(t)| \le V_f \sup_{t\in[0,1]}|\delta_t(N;x_n,\mu)| = V_f\delta(N;x_n,\mu)$ to complete the proof. □

5.3.2 Theorem. *Let (α_n) be a sequence in $\mathbb{C}$ such that*

$$\left|\sum_{n=1}^{N}\alpha_n\right| = O(N^{1/2+\epsilon})$$

for all $\epsilon > 0$. Then the Dirichlet series $\sum_{n=1}^{\infty}\alpha_n n^{-s}$ is holomorphic on $\mathrm{Re}(s) > 1/2$.

5.3.3 Lemma. *Let $s \in \mathbb{C}$ such that $\sigma = \mathrm{Re}(s) > 0$. Then for all $n \in \mathbb{Z}^+$,*

$$\left|\frac{1}{n^s} - \frac{1}{(n+1)^s}\right| \le \frac{|s|}{\sigma}\left(\frac{1}{n^\sigma} - \frac{1}{(n+1)^\sigma}\right)$$

Proof. Let $a = (n+1)/n$. Multiplying on both sides by $|(n+1)^s|$, we see it suffices to prove $|a^s - 1| \le (|s|/\sigma)(a^\sigma - 1)$. After rearranging, this is equivalent to

$$\frac{|a^s-1|^2}{(a^\sigma-1)^2} - 1 \le \frac{|s|^2}{\sigma^2} - 1 = \frac{\tau^2}{\sigma^2}$$

where $\tau = \mathrm{Im}(s)$. Observe that $a^s = a^\sigma e^{i\tau\ln a}$, from which we compute $|a^s-1|^2 = a^{2\sigma} + 1^2 - 2a^\sigma\cos(\tau\ln a)$ by the Law of Cosines. Substituting,

$$\frac{|a^s-1|^2}{(a^\sigma-1)^2} - 1 = \frac{2a^\sigma(1-\cos(\tau\ln a))}{(a^\sigma-1)^2} = -\frac{1-\cos(\tau\ln a)}{1-\cosh(\sigma\ln a)}$$

But by Taylor expansion, we know that $(1-\cos(\tau\ln a))/\tau^2 \le (\ln a)^2/2 \le -(1-\cosh(\sigma\ln a))/\sigma^2$, which concludes the proof. □

Proof of 5.3.2. It suffices to prove that the partial sums $A_n = \sum_{n=1}^{N} \alpha_n n^{-s}$ converge uniformly on every compact subset of $\mathrm{Re}(s) > 1/2$. We do this by proving uniform convergence in the region

$$\Gamma_{\sigma_0,R} = \{s \in \mathbb{C} : \mathrm{Re}(s) > \sigma_0 \text{ and } |s| < R\}$$

for all $\sigma_0 > 1/2$ and R large.

Fix $R > \sigma_0 > 1/2$. Let $s \in \Gamma_{\sigma_0,R}$. By hypothesis, there exists $A > 0$ such that $|A_N| \leq AN^{\sigma_0}$. Using summation by parts and 5.3.3,

$$\begin{aligned}\left|\sum_{n=1}^{N} \frac{\alpha_n}{n^s}\right| &\leq \frac{|A_N|}{N^\sigma} + \sum_{n=1}^{N-1} |A_n| \left|\frac{1}{n^s} - \frac{1}{(n+1)^s}\right| \\ &\leq A + \sum_{n=1}^{N-1} \frac{An^{\sigma_0}|s|}{\sigma} \left(\frac{1}{n^\sigma} - \frac{1}{(n+1)^\sigma}\right)\end{aligned}$$

Above, $n^{-\sigma} - (n+1)^{-\sigma} = O(n^{-(1+\sigma)})$ from combining terms and applying binomial expansion. So the sum in the last expression is $O(n^{-(1+\sigma-\sigma_0)})$, where $\sigma - \sigma_0 > 0$. As $N \to \infty$, we find the sum converges, which proves $\sum_{n=1}^{\infty} \alpha_n n^{-s}$ converges.

Again using summation by parts, we compute $|\sum_{n=N+1}^{\infty} \alpha_n n^{-s}| = A + 2AR \sum_{n=N+1}^{\infty} n^{\sigma_0}(n^{-\sigma} - (n+1)^{-\sigma}) = O(N^{-(\sigma-\sigma_0)})$. Thus, the convergence is uniform. □

Proof of 5.2.2. Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. Let $\sigma \in \mathbb{C}$ with $\sigma = \mathrm{Re}(s) > 1$. By Taylor expansion and Hasse's bound on the $a_p(E)$ (recall that $|a_p(E)| \leq 1$ for all primes p of bad reduction),

$$\log L(s; E/\mathbb{Q}) = \sum_p a_p(E) p^{-s} + O\left(\sum_{p \nmid \Delta} p^{1-2\sigma}\right)$$

Since there are only finitely many primes of bad reduction, we ignore them along with the error term in the above expression. Then it suffices to prove $\sum_{p \nmid \Delta} a_p(E) p^{-s}$ is holomorphic in the half-plane $\mathrm{Re}(s) > 1$.

We see $\mathrm{d}F_{\mathrm{ST}}(t) = (2/\pi)\sin^2 t, \mathrm{d}t$, from which $\int_0^\pi \cos\theta \, \mathrm{d}F_{\mathrm{ST}}(\theta) = 0$. As before, let (p_n) be the sequence of primes of good reduction for E. After a change of variables, 5.3.1 yields

$$\begin{aligned}\left|\frac{1}{N}\sum_{n=1}^{N} \frac{a_{p_n}(E)}{2\sqrt{p}}\right| &= \left|\frac{1}{N}\sum_{n=1}^{N} \cos\theta_{p_n}(E) - \int_0^\pi \cos\theta \, \mathrm{d}F_{\mathrm{ST}}(\theta)\right| \\ &\leq V_f \delta(N; \theta_{p_n}(E), F_{\mathrm{ST}}) \\ &\leq 2\delta(N; \theta_{p_n}(E), F_{\mathrm{ST}})\end{aligned}$$

Then 5.1.2 implies $(1/N)\sum_{n=1}^{N} a_{p_n}(E)/2\sqrt{p_n} = O(N^{-(1/2-\epsilon)})$ for all $\epsilon > 0$. That is,

$$\sum_{n=1}^{N} \frac{a_{p_n}(E)}{2\sqrt{p_n}} = O(N^{1/2+\epsilon})$$

Therefore, after a second change of variables, 5.3.2 says $\sum_{n=1}^{\infty} a_{p_n}(E)p_n^{-s}$ is holomorphic in the half-plane $\mathrm{Re}(s) > 1$, as needed. □

5.4 Future Work

According to a presentation of William Stein, accessible at

http://wiki.l-functions.org/talks/20071016-convergence/talk.pdf

an email from Akiyama to Barry Mazur says that the converse to 5.2.2 holds at least for the the L-functions we have defined. In this email, Akiyama states that Hirofumi Nagoshi expects it to follow from the Erdös-Turán Inequality, which can be used to bound the discrepancy. However, this converse result has been neither submitted nor published.

We are unsure of Nagoshi's claim, because preliminary work indicates that, while the GRH for $E/\mathbb{Q}$ without complex multiplication does imply a bound on the rate of convergence of the 1st moment of the normalized traces to its limit—that is, the rate at which the mean of the first N traces tends to 0—it does not appear to give information about the higher moments of the normalized traces. Indeed, information about all the higher moments would be needed to use the Erdös-Turán Inequality to prove 5.1.2 from 5.2.1. Admittedly, one might use the Wiener-Ikehara Theorem and/or other powerful analytic tools to obtain this information from the assumption of the GRH.

References

[1] Shigeki Akiyama and Yoshiro Tanigawa. Calculation of values of L-functions associated to elliptic curves. *Mathematics of Computation*, 68(227):1201–1231, Feb 1999.

[2] David A. Cox. *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication.* John Wiley & Sons, Inc., New York, 1989.

[3] A. Ghosh. The distribution of ap^2 modulo 1. *Proceedings of the London Mathematical Society*, S3-42(2):252–269, March 1981.

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

[5] Robin Hartshorne. *Algebraic Geometry.* Springer-Verlag, New York, 1977.

[6] Ernst Hecke. Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen. *Mathematische Zeitschrift*, pages 357–376, 1918.

[7] Ernst Hecke. Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen. *Mathematische Zeitschrift*, pages 11–51, 1919.

[8] Jason Hedetniemi. Champion primes for elliptic curves over fields of prime order. Master's thesis, Clemson University, Clemson, SC, 2012.

[9] Kevin James and Gang Yu. Average Frobenius distribution of elliptic curves. *Acta Arithmetica*, 124(1):79–100, 2006.

[10] Kiran S. Kedlaya and Andrew V. Sutherland. Hyperelliptic curves, L-polynomials, and random matrices. *Contemporary Mathematics*, 487, 2009.

[11] Leonid Koralov and Yakov Sinai. *Theory of Probability and Random Process*. Springer-Verlag, Berlin, 2007.

[12] Angel V. Kumchev. On Weyl sums over primes and almost primes. *Michigan Mathematical Journal*, 54(2):243–268, 2006.

[13] Serge Lang. *Elliptic Functions, 2nd. Ed.* Springer-Verlag, New York, 1987.

[14] J. S. Milne. *Elliptic Curves*. BookSurge Publishers, 2006.

[15] M. Ram Murty and V. Kumar Murty. The Sato-Tate Conjecture and generalizations. *Current Trends in Science*, Nov 2009.

[16] Kenneth A. Ribet and William A. Stein. *Lectures on Modular Forms and Hecke Operators*. http://wstein.org, 2011.

[17] Pierre Samuel. *Algebraic Theory of Numbers*. Hermann, Paris, 1970.

[18] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 1986.

[19] Elias M. Stein and Rami Shakarchi. *Real Analysis: Measure Theory, Integration, and Hilbert Spaces*. Princeton University Press, Princeton, NJ, 2005.

[20] William Stein. A Brief Introduction to Classical and Adelic Algebraic Number Theory, 2004. Based heavily on works of Swinnerton-Dyer and Cassels.

[21] Christopher Swierczewski. Connections between the Riemann Hypothesis and the Sato-Tate Conjecture. Master's thesis, University of Washington, Seattle, Washington, 2008.

[22] Richard Taylor. Automorphy for some ℓ-adic lifts of automorphic mod ℓ Galois representations, II. http://www.math.ias.edu/, 2006.

[23] R. C. Vaughan. *The Hardy-Littlewood Method, 2nd. Ed.* Cambridge University Press, Cambridge, 1997.