THE PENNSYLVANIA STATE UNIVERSITY
SCHREYER HONORS COLLEGE

DEPARTMENT OF MATHEMATICS

THE RIEMANN HYPOTHESIS FOR ELLIPTIC CURVES OVER FINITE FIELDS

CONNOR CASSADY
SPRING 2018

A thesis
submitted in partial fulfillment
of the requirements
for a baccalaureate degree
in Mathematics
with honors in Mathematics

Reviewed and approved* by the following:

Mihran Papikian
Associate Professor of Mathematics
Thesis Supervisor

Nathanial Brown
Professor of Mathematics
Associate Head of Diversity and Equity
Honors Advisor

*Signatures are on file in the Schreyer Honors College.

Abstract

The Riemann Hypothesis has been a result eluding mathematicians for nearly 200 years. Analogs of this result have been found for elliptic curves over finite fields, which is the subject of this thesis. We begin by establishing algebraic foundations that will be used to prove larger results regarding the Riemann Hypothesis. Next, we explore an elementary number theoretic approach to this problem, and deal with a very particular type of elliptic curve. The crux of this paper is found in the next chapter, where we state and prove the Riemann Hypothesis for elliptic curves over finite fields. Finally, we investigate some examples of specific elliptic curves to see the applications of the theorems proved earlier.

Table of Contents

Acknowledgements

First and foremost, I would like to thank my thesis supervisor, Dr. Mihran Papikian. I came to him with a very small idea of what I wanted to do for my thesis, and he immediately set me on the path for this project. This research project was an incredibly enjoyable experience, and Dr. Papikian pushed me to be a better student of mathematics at every step.

I would also like to thank my honors advisor Dr. Nathanial Brown for his continued support over the past four plus years. I know for a fact that I would not be where I am today without his guidance.

Finally, I would like to thank my family and close friends for all of their help both inside and outside of the classroom while I was at Penn State. They all pushed me higher than I could reach on my own, and I owe so much of my success to them.

Chapter 1

An Introduction to the Riemann Hypothesis

The Riemann zeta function $\zeta(s)$ is defined, for $\mathrm{Re}(s) > 1$, to be

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

and can be extended analytically to the whole complex plane. In 1859, Riemann stated in his seminal paper 'Über die Anzahl der Primazahlen unter einer gegebnen Grösse,' that all the nontrivial zeros of this zeta function lie on the line $\mathrm{Re}(s) = 1/2$. The motivation behind this work was to find an expression for the exact number of primes $\leq x$, or $\pi(x)$, from the estimate $x/\log x$ made by many other mathematicians. This statement remains unproven after nearly two hundred years, but certain analogs have been found that are much easier to work with.

In this thesis, we will consider the analog first proposed by Artin. Let p be a prime, n be a positive integer, and $q = p^n$. We consider the field $\mathbb{F}_q$ and an elliptic curve, E, over this field. In particular, we are interested in the number of points in our field that belong to this curve. Hasse proved the following result, which gives a fairly nontrivial estimate on this number of points. Letting $E(\mathbb{F}_q) =$ the set of points belonging to E with coordinates in $\mathbb{F}_q$:

$$\left|\#E(\mathbb{F}_q) - q - 1\right| \leq 2\sqrt{q}$$

How do we relate elliptic curves over finite fields to the Riemann Hypothesis? It starts with defining the zeta function for our elliptic curve. We define

$$Z(E/\mathbb{F}_q; T) = \exp\left(\sum_{n=1}^{\infty} \#E(\mathbb{F}_{q^n})\frac{T^n}{n}\right)$$

The Riemann Hypothesis can then be stated in a very simple manner, and becomes

$$Z(E/\mathbb{F}_q; T) = \frac{1 - aT + qT^2}{(1-T)(1-qT)} = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}, \quad |\alpha| = |\beta| = \sqrt{q}$$

where $a = q + 1 - \#E(\mathbb{F}_q)$. From this result we are able to easily deduce the "recognizable" Riemann Hypothesis; if $\zeta_E(s) = 0$, where $\zeta_E(s) := Z(E/\mathbb{F}_q; q^{-s})$, then $\mathrm{Re}(s) = 1/2$.

These results have been well established, so what will be done in this thesis? In Chapter 2, some fundamental results pertaining to finite fields are reviewed in order to be used later in Chapter 4. In Chapter 3, we explore this question of finding points on our elliptic curve using a number theoretic approach. This chapter follows the outline of George Andrews' *Number Theory*, exploring some general results about quadratic residues and the Legendre Symbol, and then using these results to provide an estimate on the number of consecutive triples of quadratic residues in a specified interval. This chapter concludes with investigating the congruence $y^2 \equiv x^3 + 3x^2 + 2x \mod p$, which is equivalent to counting $E(\mathbb{F}_p)$.

Chapter 4 follows the outline of Silverman's *The Arithmetic of Elliptic Curves*. In this chapter, algebraic techniques are utilized to prove Hasse's theorem regarding the bound on the number of solutions in $E(\mathbb{F}_q)$. We then move on to investigate the zeta function for our elliptic curve, and prove the Riemann Hypothesis for elliptic curves over finite fields.

We open Chapter 5 by revisiting the elliptic curve $y^2 = x^3 + 3x^2 + 2x$, verifying the general results proved in Chapter 4 in a specific example. Next, we will investigate the elliptic curve

$y^2 = x^2 + 2x^2 + 3$. Along with this example, we focus on other examples over $\mathbb{F}_5$. From Hasse's theorem, we know

$$(5+1) - 2\sqrt{5} \leq \#E(\mathbb{F}_5) \leq (5+1) + 2\sqrt{5}$$

Since we are counting the number of points on our curve, we can rewrite these bounds

$$1 \leq \#E(\mathbb{F}_5) \leq 10$$

We will investigate if, for each integer in this range, there exists an elliptic curve E over $\mathbb{F}_5$ having that number of rational points. To conclude, we will introduce the Honda-Tate theorem, which answers a very natural question that arises while exploring these examples.

Chapter 2

A Review of Finite Fields

In this chapter, we review some properties of finite fields that we will need when taking an algebraic approach to the Riemann Hypothesis, following Fraleigh's, *A First Course in Abstract Algebra* [2].

Definition 2.0.1. An extension field E of a field F is a **simple extension of** F if $E = F(\alpha)$ for some $\alpha \in E$.

The following theorem tells us how to construct such an extension using an irreducible polynomial over F.

Theorem 2.0.2. *Let E be a simple extension $F(\alpha)$ of a field F, and let α be algebraic over F. Let the degree of the irreducible polynomial for α over F be $n \geq 1$. Then every element β of $E = F(\alpha)$ can be uniquely expressed in the form*

$$\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$$

Proof. Let $a_0 + a_1x + ... + a_nx^n$, $a_n \neq 0$, be the irreducible polynomial for α over F.

$$a_0 + a_1\alpha + ... + a_n\alpha^n = 0 \iff \alpha^n = -\frac{1}{a_n}(a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1})$$

Now, consider $m \geq n$, i.e., $m = n + k$ for some nonnegative integer k. We proceed by induction on k, showing that α^m can be written as a linear combination of $\alpha^j, 0 \leq j \leq n-1$.

$$\begin{aligned}\alpha^{n+1} &= \alpha(\alpha^n) = \alpha(-\frac{1}{a_n}(a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1})) \\ &= -\frac{1}{a_n}(a_0\alpha + a_1\alpha^2 + ... + a_{n-1}\alpha^n) \\ &= -\frac{1}{a_n}(a_0\alpha + a_1\alpha^2 + ... + a_{n-1}(-\frac{1}{a_n}(a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1})))\end{aligned}$$

So, the base case has been proven.

Now suppose this statement is true for $k = r$, and consider $k = r + 1$. $\alpha^k = \alpha(\alpha^r)$. Using the induction hypothesis and similar reasoning as seen in the base case above, α^k can be written as a linear combination of $\alpha^j, 0 \leq j \leq n-1$. Since $\beta \in F(\alpha)$, it is the linear combination of powers of α, so we have shown the existence of such a representation for β.

Now, we prove uniqueness. Take $\beta \in F(\alpha)$, and suppose two such representations exist. That is,

$$b_0 + b_1\alpha + ... + b_{n-1}\alpha^{n-1} = b'_0 + b'_1\alpha + ... + b'_{n-1}\alpha^{n-1}$$

This is equivalent to

$$(b_0 - b'_0) + (b_1 - b'_1)\alpha + ... + (b_{n-1} - b'_{n-1})\alpha^{n-1} = 0$$

which implies α is a root of the polynomial of degree $n-1$ with coefficients $b_j - b'_j$. This is a contradiction, since, by definition, $a_0 + a_1x + ... + a_nx^n$, the irreducible polynomial for α over F, has minimal degree. So, the above polynomial of degree $n-1$ must be identically zero, i.e., these two representations are identical. □

Remark 2.0.3. This theorem gives rise to a very natural approach to working with finite fields and finite field extensions. Because every $\beta \in E = F(\alpha)$ can be written uniquely as

$$b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$$

we can think of $F(\alpha)$ as a vector space over F, and think of the set $\{1, \alpha, ..., \alpha^{n-1}\}$ as a basis of this vector space.

Before moving into our discussion of the properties and classifications of finite fields, we need a few definitions and theorems regarding field extensions.

Definition 2.0.4. An extension field E of a field F is an **algebraic extension of** F if every element in E is algebraic over F.

Definition 2.0.5. If an extension field E of a field F is of finite dimension n as a vector space over F, then E is a **finite extension of degree** n **over** F.

Theorem 2.0.6. *A finite extension field E of a field F is an algebraic extension of F.*

Proof. We must show that each $\alpha \in E$ is algebraic over F. Let E be an extension of degree n. We have seen, if we think of E as a vector space over F, that $\{1, ..., \alpha^{n-1}\}$ can be thought of as a basis for E. Now consider the collection of $n + 1$ vectors

$$1, \alpha, ..., \alpha^n$$

As a vector space, E has dimension n, so these vectors are linearly dependent. That is, there exist $a_0, ..., a_n \in F$ not all zero such that

$$a_0 + a_1\alpha + ... + a_n\alpha^n = 0$$

From this equality, we see that α is a root of the polynomial

$$a_0 + a_1x + ... + a_nx^n \in F[x]$$

Therefore, α is algebraic over F, as desired, and E is an algebraic extension of F. □

Definition 2.0.7. A field F is **algebraically closed** if every nonconstant polynomial in $F[x]$ has a zero in F.

We are now ready to study and classify finite fields. In this section, we will show that for every prime, p, and every positive integer n, there is one field (up to isomorphism) of order p^n, which we will denote by $\mathbb{F}_{p^n}$.

Theorem 2.0.8. *Let E be a finite extension of degree n over a finite field F. If F has q elements, then E has q^n elements.*

Proof. Let $\{1, ..., \alpha^{n-1}\}$ be a basis of E as a vector space over F. By Theorem 2.0.2, every $\beta \in E$ can be uniquely expressed in the form

$$\beta = b_0 + \cdots + b_{n-1}\alpha^{n-1}$$

where $b_i \in F$ for all i. Each b_i can be any of the q elements in F, so the total number of distinct linear combinations of these α^i is q^n. □

Theorem 2.0.9. *If p is prime, $\mathbb{Z}_p$ is a field.*

Proof. It is clear that $\mathbb{Z}_p$ is a commutative ring with unity. We need only to show that each nonzero element of $\mathbb{Z}_p$ has an inverse. By contradiction, assume there exists $m \in \mathbb{Z}_p^\times$ with no inverse. That is, of the p elements $0, m, 2m, \ldots, (p-1)m$, none are equal to 1. There are $p-1$ elements of $\mathbb{Z}_p$ not equal to 1, so we know two of these multiples of m must be equal. That is, there are i, j, with $i \neq j$ such that $im \equiv jm \mod p$. This is equivalent to $(i-j)m \equiv 0 \mod p$. Hence, $p \mid (i-j)m$. $i \neq j$, so p does not divide $i-j$. Since p is prime, it must divide m, meaning $m \equiv 0 \mod p$, a contradiction. Thus, every nonzero element of $\mathbb{Z}_p$ must have an inverse. This tells us that $\mathbb{Z}_p$ is a field. □

Remark 2.0.10. As a field, we will denote $\mathbb{Z}_p$ by $\mathbb{F}_p$.

Lemma 2.0.11. *If E is a finite field of characteristic p, then E contains a subfield isomorphic to $\mathbb{F}_p$.*

Proof. E has characteristic p, so for any $e \in E, p \cdot e = 0$. Consider the subgroup generated by the unit, 1, of E. This group has p elements and is isomorphic to the additive group $\mathbb{Z}_p$, which we just saw is a field. Therefore, E contains a subfield isomorphic to $\mathbb{F}_p$. □

Corollary 2.0.12. *If E is a finite field of characteristic p, then E has exactly p^n elements for some positive integer n.*

Proof. Every finite field E is a finite extension of a prime field isomorphic to $\mathbb{F}_p$, where p is the characteristic of E. The corollary follows immediately from Theorem 2.0.8. □

The next theorem begins our understanding of the multiplicative structure of finite fields and tells us how to generate a finite field from a prime subfield.

Theorem 2.0.13. *Let E be a field of p^n elements contained in the algebraic closure $\overline{\mathbb{F}_p}$ of $\mathbb{F}_p$. The elements of E are precisely the zeros in $\overline{\mathbb{F}_p}$ of the polynomial $x^{p^n} - x$ in $\mathbb{F}_p[x]$.*

Proof. This is a direct consequence of Lagrange's Theorem and the fact that $E^\times$, the set of nonzero elements in E, is a multiplicative group of order $p^n - 1$. □

Theorem 2.0.14. *A finite extension E of a finite field F is a simple extension of F.*

Proof. This follows directly from the fact that the set of nonzero elements of a finite field is cyclic. Let α be a generator of $E^\times$. Then $E = F(\alpha)$. □

We now shift focus to showing the existence, and later uniqueness, of the finite field of order p^n.

Theorem 2.0.15. *If F is a field of prime characteristic p with algebraic closure $\overline{F}$, then $x^{p^n} - x$ has p^n distinct zeros in $\overline{F}$.*

Proof. $\overline{F}$ is algebraically closed, so $f(x) = x^{p^n} - x$ factors over $\overline{F}$ into linear factors $x - \alpha$. We must show that all of these roots have multiplicity 1. Observe $f'(x) = p^n x^{p^n - 1} - 1 \equiv -1 \mod p$ for all $x \in \overline{F}$. Therefore, each root of $f(x)$ has multiplicity 1. □

The roots of this polynomial are very special, and will be crucial to our classification of finite fields. The following lemma follows from the Binomial Theorem and induction on n.

Lemma 2.0.16. *If F is a field of prime characteristic p, then $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}$.*

We are now ready to prove the existence and uniqueness of $\mathbb{F}_{p^n}$.

Theorem 2.0.17. *A finite field $\mathbb{F}_{p^n}$ of p^n elements exists for every prime power p^n.*

Proof. Let $K = \{\text{zeros of } x^{p^n} - x\}$. By Theorem 2.0.15, $|K| = p^n$. To prove the theorem, we need only to show K is a field. The above lemma shows that K is closed under addition, and K is closed under multiplication since, for $\alpha, \beta \in K$, $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$. Also, 0 and 1 belong to K, so we have additive and multiplicative identities, respectively. To conclude, we must show that additive and multiplicative inverses of each $\alpha \in K, \alpha \neq 0$ belong to K. Consider $-\alpha$. $(-\alpha)^{p^n} = (-1)^{p^n}\alpha^{p^n} = (-1)^{p^n}\alpha$. We consider two cases: $p = 2$, and $p > 2$. If $p = 2, -1 \equiv 1 \mod p$, therefore $(-1)^{p^n}\alpha = -\alpha$. If $p > 2$, p is odd, so p^n is also odd for all n. So, once again, we have $(-1)^{p^n}\alpha = -\alpha$. Plugging $-\alpha$ into our polynomial shows that $-\alpha$ is also a zero, so $-\alpha \in K$. Finally, since $\alpha \neq 0$, and $\alpha^{p^n} = \alpha$, $1/a^{p^n} = 1/\alpha$. Plugging in $1/\alpha$, we see it, too, is a zero of our polynomial. Therefore, $1/\alpha \in K$. So, K is a field. □

Remark 2.0.18. In this proof, we have constructed the splitting field of the polynomial $x^{p^n} - x$.

We now prove the uniqueness of $\mathbb{F}_{p^n}$.

Theorem 2.0.19. *$\mathbb{F}_{p^n}$ is unique up to isomorphism.*

Proof. This result follows immediately from the above remark, Theorems 2.0.13 and 2.0.14, and the fact that the splitting field of a polynomial is unique. □

To make these ideas more concrete, let us construct the finite field with nine elements.

Example 2.0.20. Consider the field $\mathbb{F}_3$, and the irreducible polynomial $x^2 + 2x + 2$. Then,

$$\mathbb{F}_9 \simeq \frac{\mathbb{F}_3[x]}{\langle x^2 + 2x + 2\rangle}$$

or

$$\mathbb{F}_9 = \{a_0 + a_1\alpha \mid a_0, a_1 \in \mathbb{Z}_3, \alpha^2 = \alpha + 1\}$$

Chapter 3

A Number Theoretic Approach

Before we begin approaching the Riemann Hypothesis using algebraic techniques, we look to a more elementary approach, exhibited in George Andrews' book, *Number Theory* [1]. We are particularly interested in quadratic residues and their distributions in fields of prime order.

3.1 Quadratic Residues

We are interested in finding solutions to the congruence

$$x^2 \equiv a \mod p$$

where p is an odd prime and $\gcd(a, p) = 1$.

Definition 3.1.1. If p does not divide a and the above congruence has a solution, we say that a is a **quadratic residue** modulo p.

The following theorem describes Euler's criterion for a to be a quadratic residue modulo p.

Theorem 3.1.2. *The number a is a quadratic residue modulo p if and only if*

$$a^{\frac{p-1}{2}} \equiv 1 \mod p$$

This theorem implies the following result, which will be used later when we consider consecutive triples of quadratic residues in $[1, p-1]$.

Corollary 3.1.3. *Let g be a primitive root modulo p, and assume $\gcd(a, p) = 1$. Let r be any integer such that $g^r \equiv a \mod p$. Then r is even if and only if a is a quadratic residue modulo p.*

Proof. First, suppose that r is even. Then $r = 2s$ for some s, and we have

$$a \equiv g^r = g^{2s} = (g^s)^2 \mod p$$

Clearly a is a quadratic residue.

Conversely, suppose a is a quadratic residue. By Euler's criterion,

$$g^{\frac{r(p-1)}{2}} \equiv a^{\frac{p-1}{2}} \equiv 1 \mod p$$

$(p-1) \mid r(p-1)/2$ which implies that $r/2$ is an integer. This means that r is even. □

We now introduce the *Legendre symbol*, which provides a method by which we can "count" quadratic residues, which will be useful in later calculations.

Definition 3.1.4. If p is an odd prime, then the **Legendre symbol** is

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ 0 & \text{if } p \mid a \\ -1 & \text{otherwise} \end{cases}$$

The Legendre symbol has some important properties that will be very useful when performing calculations involving this symbol.

Theorem 3.1.5. *If p is an odd prime and a and b are relatively prime to p, then*

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right), \text{ if } a \equiv b \mod p$$
$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$
$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \mod p$$

Corollary 3.1.6. *If p is an odd prime, then*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

We now use these results to study the distributions of quadratic residues.

3.2 Distribution of Quadratic Residues

Our study of the distribution of quadratic residues is motivated by the following congruence:

$$y^2 \equiv x^3 + 3x^2 + 2x \mod p \tag{3.1}$$

If we factor the right hand side of this congruence, we get $x(x+1)(x+2)$. Considering this over $\mathbb{F}_p$, we see that if (3.1) has a solution we have three consecutive quadratic residues modulo p.

Let $v(p)$ denote the number of consecutive triples of quadratic residues in the interval $[1, p-1]$.

Theorem 3.2.1. *If p is an odd prime, then*

$$v(p) = \frac{1}{8}p + E_p$$

where $\left|E_p\right| < \frac{1}{4}\sqrt{p} + 2$

Proof. Define $C_p(n)$ by the formula

$$C_p(n) = \begin{cases} 1 \text{ if } n, n+1, n+2 \text{ are all quadratic residues modulo } p \\ 0 \text{ otherwise} \end{cases}$$

Then $v(p) = \sum_{n=1}^{p-3} C_p(n)$.

Notice that another way to write $C_p(n)$ is

$$C_p(n) = \frac{1}{8}\left(1 + \left(\frac{n}{p}\right)\right)\left(1 + \left(\frac{n+1}{p}\right)\right)\left(1 + \left(\frac{n+2}{p}\right)\right)$$

since both sides of this equation are 0 if $n, n+1, n+2$ are not all quadratic residues, and 1 if they are all quadratic residues.

This allows us to write, after some algebra,

$$8v_p(n) = \sum_{n=1}^{p-3} 1 + \sum_{n=1}^{p-3} \left(\frac{n}{p}\right) + \sum_{n=1}^{p-3} \left(\frac{n+1}{p}\right) + \sum_{n=1}^{p-3} \left(\frac{n+2}{p}\right) + \sum_{n=1}^{p-3} \left(\frac{n}{p}\right)\left(\frac{n+1}{p}\right) + \\ + \sum_{n=1}^{p-3} \left(\frac{n}{p}\right)\left(\frac{n+2}{p}\right) + \sum_{n=1}^{p-3} \left(\frac{n+1}{p}\right)\left(\frac{n+2}{p}\right) + \sum_{n=1}^{p-3} \left(\frac{n}{p}\right)\left(\frac{n+1}{p}\right)\left(\frac{n+2}{p}\right) \quad (3.2)$$

Since there are an equal number of quadratic residues and nonresidues in the interval $[1, p-1]$, $\sum_{n=1}^{p-1} \left(\frac{n}{p}\right) = 0$. Andrews also showed that $\sum_{n=1}^{p-2} \left(\frac{n}{p}\right)\left(\frac{n+1}{p}\right) = -1$ when proving a result related to the distribution of consecutive pairs of quadratic residues. From these two equalities, we can simplify (3.2) substantially:

$$8v_p(n) = (p-3) + \left(0 - \left(\frac{p-2}{p}\right) - \left(\frac{p-1}{p}\right)\right) + \left(0 - \left(\frac{1}{p}\right) - \left(\frac{p-1}{p}\right)\right) + \left(0 - \left(\frac{1}{p}\right) - \left(\frac{2}{p}\right)\right) + \\ + \left(-1 - \left(\frac{(p-2)(p-1)}{p}\right)\right) + \left(-1 - \left(\frac{(p-1)(p+1)}{p}\right)\right) + \left(-1 - \left(\frac{2}{p}\right)\right) + \sum_{n=1}^{p-3} \left(\frac{n(n+1)(n+2)}{p}\right) \quad (3.3)$$

Let $E_p = v(p) - \frac{1}{8}p$. Applying the Triangle Inequality to (3.3), we see that

$$|E_p| < \frac{3}{8} + 6\left(\frac{1}{4}\right) + \frac{1}{8}\left|\sum_{n=1}^{p-3} \left(\frac{n(n+1)(n+2)}{p}\right)\right| < 2 + \frac{1}{8}\left|\sum_{n=1}^{p-3} \left(\frac{n(n+1)(n+2)}{p}\right)\right|$$

To prove the theorem, we need only to show

$$\left|\sum_{n=1}^{p-3} \left(\frac{n(n+1)(n+2)}{p}\right)\right| \leq 2\sqrt{p}$$

Now, define $S(m)$ by the formula

$$S(m) = \sum_{(n \mod p)} \left(\frac{n(n^2-m)}{p}\right)$$

First, letting $m = 1$, we have

$$S(1) = \sum_{(n \mod p)} \left(\frac{n(n-1)(n+1)}{p}\right) = \sum_{(n \mod p)} \left(\frac{n(n+1)(n+2)}{p}\right) = \sum_{n=1}^{p-3} \left(\frac{n(n+1)(n+2)}{p}\right)$$

We can split this sum "in half," as follows:

$$\begin{aligned} S(m) &= \sum_{n=1}^{(p-1)/2} \left(\frac{n(n^2-m)}{p}\right) + \sum_{(p+1)/2}^{p-1} \left(\frac{n(n^2-m)}{p}\right) \\ &= \sum_{n=1}^{(p-1)/2} \left(\frac{n(n^2-m)}{p}\right) + \sum_{n=1}^{(p-1)/2} \left(\frac{(p-n)((p-n)^2-m)}{p}\right) \\ &= \sum_{n=1}^{(p-1)/2} \left(\frac{n(n^2-m)}{p}\right) + \left(\frac{-1}{p}\right) \sum_{n=1}^{(p-1)/2} \left(\frac{n(n^2-m)}{p}\right) \end{aligned}$$

If $p \equiv 3 \mod 4$, then $\left(\frac{-1}{p}\right) = -1$, so $S(m) = 0$ for such p. Consequently, we have found an incredibly simple bound for E_p in this case: $\left|E_p\right| < 2$.

As such, we turn our attention to p such that $p \equiv 1 \mod 4$. Take any integer $k \not\equiv 0 \mod p$. Then $\left(\frac{k^4}{p}\right) = 1$. So,

$$S(m) = \sum_{(n \mod p)} \left(\frac{k^4}{p}\right)\left(\frac{n(n^2-m)}{p}\right) = \sum_{(n \mod p)} \left(\frac{kkn(n^2k^2-k^2m)}{p}\right)$$

Let $h = kn$. Since n takes all values modulo p, so does h. Then

$$S(m) = \left(\frac{k}{p}\right) \sum_{(h \mod p)} \left(\frac{h(h^2-k^2m)}{p}\right) = \left(\frac{k}{p}\right) S(k^2m)$$

Consequently, if j is a quadratic residue modulo p, then $c^2 \equiv j \mod p$ for some c. This implies that

$$S(1) = \left(\frac{c}{p}\right) S(c^2) = \left(\frac{c}{p}\right) S(j) \implies \left|S(1)\right| = \left|S(j)\right|$$

If we take quadratic nonresidues l and r modulo p , then by Corollary 3.1.3,

$$l \equiv g^{2a+1} \mod p \text{ and } r \equiv g^{2b+1} \mod p$$

WLOG, assume $b \geq a$, and let $t = g^{b-a}$. Then $r \equiv lt^2 \mod p$, and

$$S(l) = \left(\frac{t}{p}\right) S(lt^2) = \left(\frac{t}{p}\right) S(r) \implies \left|S(l)\right| = \left|S(r)\right|$$

These arguments tell us that the absolute value of $S(m)$ depends only on whether or not m is a quadratic residue modulo p.

Now, since there are an equal number of quadratic residues and nonresidues in $[1, p-1]$,

$$\begin{aligned}\frac{p-1}{2}S(1)^2 + \frac{p-1}{2}S(l)^2 &= \sum_{m=1}^{p-1} S(m)^2 = \sum_{m \mod p} S(m)^2 \\ &= \sum_{(m \mod p)} \sum_{(s \mod p)} \left(\frac{s(s^2-m)}{p}\right) \sum_{(t \mod p)} \left(\frac{t(t^2-m)}{p}\right) \\ &= \sum_{(m \mod p)} \sum_{(s \mod p)} \sum_{(t \mod p)} \left(\frac{st}{p}\right) \left(\frac{(m-s^2)(m-t^2)}{p}\right) \\ &= \sum_{(s \mod p)} \sum_{(t \mod p)} \left(\frac{st}{p}\right) \sum_{(m \mod p)} \left(\frac{(m-s^2)(m-t^2)}{p}\right)\end{aligned}$$

Andrews showed that

$$\sum_{n=0}^{p-1} \left(\frac{(n-a)(n-b)}{p}\right) = \begin{cases} p-1 & \text{if } a \equiv b \mod p \\ -1 & \text{if } a \not\equiv b \mod p \end{cases}$$

Applying this result, we get

$$\begin{aligned}\frac{p-1}{2}S(1)^2 + \frac{p-1}{2}S(l)^2 &= \sum_{(s \mod p)} \sum_{\substack{(t \mod p) \\ t^2 \equiv s^2 \mod p}} \left(\frac{st}{p}\right)(p-1) + \sum_{(s \mod p)} \sum_{\substack{(t \mod p) \\ t^2 \not\equiv s^2 \mod p}} \left(\frac{st}{p}\right)(-1) \\ &= 2(p-1)(p-1) - \left(0 - \sum_{(s \mod p)} \sum_{\substack{(t \mod p) \\ t^2 \equiv s^2 \mod p}} \left(\frac{st}{p}\right)\right) \\ &= 2(p-1)^2 + 2(p-1) = 2p(p-1)\end{aligned}$$

Therefore, $S(1)^2 + S(l)^2 = 4p$. From this equality, we can conclude that $\left|S(1)\right| \leq 2\sqrt{p}$, as desired. □

Remark 3.2.2. Before using this result, let us show why the following equality from the above proof is true:

$$\sum_{(s \mod p)} \sum_{\substack{(t \mod p) \\ t^2 \equiv s^2 \mod p}} \left(\frac{st}{p}\right) = 2(p-1) \text{ for } p \equiv 1 \mod 4$$

First, notice that if $s = 0$ or $t = 0$, our summand is zero, so we consider only nonzero values of s and t. The congruence $s^2 \equiv t^2 \mod p$ implies that $t = s$ or $t = -s$. If $t = s$,

$$\left(\frac{st}{p}\right) = \left(\frac{s^2}{p}\right) = 1$$

Now, if $t = -s$,

$$\left(\frac{st}{p}\right) = \left(\frac{-s^2}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{s^2}{p}\right) = \left(\frac{s^2}{p}\right) = 1$$

since $p \equiv 1 \mod 4$.

From this, we have

$$\sum_{(s \mod p)} \sum_{\substack{(t \mod p) \\ t^2 \equiv s^2 \mod p}} \left(\frac{st}{p}\right) = \sum_{s=1}^{p-1}\left(\left(\frac{s^2}{p}\right) + \left(\frac{-s^2}{p}\right)\right) = \sum_{s=1}^{p-1} 2 = 2(p-1)$$

Remark 3.2.3. The above remark gives us the following equality

$$\sum_{(s \mod p)} \sum_{\substack{(t \mod p) \\ t^2 \not\equiv s^2 \mod p}} \left(\frac{st}{p}\right)(-1) = 2(p-1)$$

We know that the sum over all s and t is 0. Therefore, the sum over all s and t with $t^2 \not\equiv s^2 \mod p$ is equal to the difference of the sum over all s and t, 0, and the sum over all s and t with $t^2 \equiv s^2 \mod p$, $2(p-1)$. That is

$$\begin{aligned}\sum_{(s \mod p)} \sum_{\substack{(t \mod p) \\ t^2 \not\equiv s^2 \mod p}} \left(\frac{st}{p}\right) &= \sum_{(s \mod p)}\sum_{(t \mod p)} \left(\frac{st}{p}\right) - \sum_{(s \mod p)} \sum_{\substack{(t \mod p) \\ t^2 \equiv s^2 \mod p}} \left(\frac{st}{p}\right) \\ &= 0 - 2(p-1) = -2(p-1)\end{aligned}$$

With these tools at our disposal, we turn our attention back to (3.1).

Proposition 3.2.4. *The congruence*

$$y^2 \equiv x^3 + 3x^2 + 2x \mod p$$

has p mutually incongruent solutions if $p \equiv 3 \mod 4$, and at least $p - 2\sqrt{p}$ mutually incongruent solutions if $p \equiv 1 \mod 4$

To prove this proposition, we need a small generalized result regarding the number of solutions of this type of congruence.

Lemma 3.2.5. *Suppose $Y(f)$ denotes the number of mutually incongruent solutions (x, y) of the congruence $y^2 \equiv f(x) \mod p$, p an odd prime, where $f(x)$ is a polynomial with integral coefficients. Then*

$$Y(f) = p + \sum_{n=0}^{p-1}\left(\frac{f(n)}{p}\right)$$

Proof. First, suppose we have a solution, (x, y), i.e., $y^2 \equiv f(x) \mod p$. It is easy to see that the $(x, -y)$ is also a solution to this congruence. We are interested in counting the number of solutions to this congruence. If $y = 0$, then we have only one solution; however, if $y \neq 0$, we have two solutions. These solutions, $(x, y), (x, -y)$ are mutually incongruent because p is an odd prime.

Now, we consider the Legendre symbol. We know that if we have a solution (x, y) with $y \neq 0$, then $\left(\frac{f(x)}{p}\right) = 1$. If $y = 0$, then $\left(\frac{f(x)}{p}\right) = 0$. If we do not have a solution, then $\left(\frac{f(x)}{p}\right) = -1$. From the above reasoning we see that, in order to count our solutions, we must add one to the Legendre symbol. So, the total number of solutions to the congruence $y^2 \equiv f(x) \mod p$ is

$$Y(f) = \sum_{n=0}^{p-1} \left(1 + \left(\frac{f(n)}{p}\right)\right) = p + \sum_{n=0}^{p-1} \left(\frac{f(n)}{p}\right)$$

□

We are now ready to prove our proposition.

Proof of Proposition. From the above lemma, we know that the number of mutually incongruent solutions to (3.1) is given by

$$Y(f) = p + \sum_{n=0}^{p-1} \left(\frac{f(n)}{p}\right)$$

As we noted at the beginning of this section, $f(x) = x^3 + 3x^2 + 2x = x(x+1)(x+2)$. Therefore,

$$Y(f) = p + \sum_{x=0}^{p-3} \left(\frac{x(x+1)(x+2)}{p}\right)$$

Recall $S(m)$. If we let $m = 1, n = x$, we have

$$S(1) = \sum_{x \mod p} \left(\frac{x(x^2-1)}{p}\right) = \sum_{x \mod p} \left(\frac{x(x+1)(x-1)}{p}\right) = \sum_{x \mod p} \left(\frac{(x+1)(x+2)x}{p}\right)$$

This last equality holds simply due to the fact that if x runs through all residues modulo p, so does $x + 1$. Therefore

$$Y(f) = p + S(1)$$

In the proof of Theorem 3.2.1, we showed that, if $p \equiv 3 \mod 4$, then $S(m) = 0$ for all m. So, for $p \equiv 3 \mod 4, Y(f) = p$. We now consider the case when $p \equiv 1 \mod 4$. In the proof of Theorem 3.2.1, we showed that $\left|S(1)\right| \leq 2\sqrt{p}$. This can be rewritten

$$-2\sqrt{p} \leq S(1) \leq 2\sqrt{p}$$

Adding p everywhere, we find

$$Y(f) = p + S(1) \geq p - 2\sqrt{p}$$

which is our desired result. □

Example 3.2.6. Let us consider a concrete example. Let $p = 5$, and consider $y^2 \equiv x^3 + 3x^2 + 2x \mod p$. Straightforward calculations show that the following points are solutions to this congruence:

$$(0,0), (1,1), (1,4), (2,2), (2,3), (3,0), (4,0)$$

So, we have seven solutions to our congruence. $5 - 2\sqrt{5} < 7 < 5 + 2\sqrt{5}$, so these calculations agree with the above results.

Now, let $p = 7$, and consider the same congruence, mod 7. We should find seven solutions to this congruence. The following points are solutions to this congruence:

$$(0,0), (3,2), (3,5), (4,1), (4,6), (5,0), (6,0)$$

There are exactly seven solutions, as expected.

Finally, as a prelude to the next chapter, where we investigate this problem for fields of *prime power* order, consider our curve over $\mathbb{F}_{25} = \{a+b\alpha | a, b \in \mathbb{F}_5\}$ where $\alpha \in \overline{\mathbb{F}_5}$ is a root of x^2+x+1. When $b = 0$, we work in "$\mathbb{F}_5$", and we have seen that we have 7 solutions. Straightforward calculations show that the following points are solutions to this congruence:

$$(0,0), (1,1), (1,4), (2,2), (2,3), (3,0), (4,0), (1+\alpha, 1), (1+\alpha, 4), (3+\alpha, 2), (3+\alpha, 3),$$
$$(1+2\alpha, 3+2\alpha), (1+2\alpha, 2+3\alpha), (3+2\alpha, 1+\alpha), (3+2\alpha, 4+4\alpha), (4+2\alpha, 1+2\alpha), (4+2\alpha, 4+3\alpha),$$
$$(3\alpha, 2+2\alpha), (3\alpha, 3+3\alpha), (1+3\alpha, \alpha), (1+3\alpha, 4\alpha), (2+3\alpha, 1+4\alpha), (2+3\alpha, 4+\alpha), (4+3\alpha, 1+3\alpha),$$
$$(4+3\alpha, 4+2\alpha), (4\alpha, 1), (4\alpha, 4), (2+4\alpha, 2), (2+4\alpha, 3), (3+4\alpha, 1+2\alpha), (3+4\alpha, 4+3\alpha)$$

So, over $\mathbb{F}_{5^2}$, we have 31 solutions to the congruence.

We now leave this number theoretic approach, and look at this problem from a much more abstract viewpoint, using the tools of abstract algebra and algebraic geometry to investigate the Riemann Hypothesis for elliptic curves over finite fields.

Chapter 4

An Abstract Algebraic Approach

We now consider this problem using the tools of abstract algebra. First, let us introduce some notation we will use throughout this section: q is a power of a prime, p; $\mathbb{F}_q$, as usual, is the finite field with q elements, whose closure is $\overline{\mathbb{F}_q}$; $E/\mathbb{F}_q$ is an elliptic curve defined over the finite field $\mathbb{F}_q$, and $E(\mathbb{F}_q)$ is the set of points in our finite field that belong to the elliptic curve.

We proceed following the outline of Silverman's, *The Arithmetic of Elliptic Curves* [4].

4.1 Number of Rational Solutions

When we are looking for points $(x, y) \in \mathbb{F}_q^2$ on $E/\mathbb{F}_q$, we are looking for the number of solutions to the general equation

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

We can create a trivial upper bound on the number of points on E by noticing that every value of x gives at most two values of y. We also note that E, being an elliptic curve, is a projective object, and therefore, along with points belonging to $\mathbb{F}_q$, we must also consider the point at infinity in the projective plane. So, including this point at infinity, we have:

$$\#E(\mathbb{F}_q) \leq 2q + 1$$

We will see that this bound is not very precise. The following theorem gives a much less trivial upper bound on the number of solutions on E.

Theorem 4.1.1 (Hasse)**.** *Let $E/\mathbb{F}_q$ be an elliptic curve defined over a finite field. Then*

$$\left|\#E(\mathbb{F}_q) - q - 1\right| \leq 2\sqrt{q}$$

Proof. Let

$$\phi : E \to E, (x, y) \mapsto (x^q, y^q)$$

be the qth power Frobenius map.

Proposition 4.1.2. *Let $P = (x, y) \in E(\overline{\mathbb{F}_q})$.*

$$P \in E(\mathbb{F}_q) \iff \phi(P) = P$$

Proof. Suppose $P \in E(\mathbb{F}_q)$. This implies $P \in \mathbb{F}_q^2$. By Lagrange's Theorem, for any $a \in \mathbb{F}_q, a^q = a$. Therefore, $\phi(P) = P$.

Now, suppose $\phi(P) = P$. This means that $x^q - x = 0$ and $y^q - y = 0$. q is a prime power, and by Theorem 2.0.13, we see that $E(\mathbb{F}_q)$ consists precisely of the zeros of this polynomial. So, $P \in E(\mathbb{F}_q)$. □

From this proposition we see that

$$E(\mathbb{F}_q) = \ker(1 - \phi)$$

We will take the following result, and the fact that the degree map is a positive definite quadratic form, as a "black box":

$$\#E(\mathbb{F}_q) = \#\ker(1 - \phi) = \deg(1 - \phi)$$

The fact that $\deg(1 - \phi) = q$ and the following inequality give us our result. □

Lemma 4.1.3. *If A is an abelian group, and*

$$d : A \to \mathbb{Z}$$

is a positive definite quadratic form, then for any $\psi, \phi \in A$,

$$\left|d(\psi - \phi) - d(\phi) - d(\psi)\right| \leq 2\sqrt{d(\phi)d(\psi)}$$

Proof. For $\psi, \phi \in A$, let

$$L(\psi, \phi) = d(\psi - \phi) - d(\phi) - d(\psi)$$

be the bilinear form associated to the quadratic form d. Because d is positive definite, for all $m, n \in \mathbb{Z}$,

$$0 \leq d(m\psi - n\phi) = d(m\psi) + L(m\psi, n\phi) + d(n\phi) = m^2 d(\psi) + mnL(\psi, \phi) + n^2 d(\phi)$$

If we take $m = -L(\psi, \phi)$, and $n = 2d(\psi)$, we have

$$0 \leq d(\psi)\left(4d(\psi)d(\phi) - L(\psi, \phi)^2\right)$$

which gives us the desired inequality if $\psi \neq 0$. If $\psi = 0$, the inequality is trivial. □

The degree map is a positive definite quadratic form, so, taking $\psi = 1$, and ϕ as the qth-power Frobenius map, we have found our desired upper bound.

We now move on to the Riemann Hypothesis for Elliptic Curves over Finite Fields.

4.2 The Riemann Hypothesis

For each positive integer n, let $\mathbb{F}_{q^n}$ be the extension of $\mathbb{F}_q$ of degree n, so $\mathbb{F}_{q^n}$ has q^n elements.

Definition 4.2.1. The **Zeta function** of $E/\mathbb{F}_q$ is the power series

$$Z(E/\mathbb{F}_q; T) = \exp\left(\sum_{n=1}^{\infty} \#E(\mathbb{F}_{q^n})\frac{T^n}{n}\right)$$

The following results are motivated by the Weil Conjectures, which are stated for general projective varieties. However, we are interested only in these conjectures for our elliptic curve. Before we state and prove these facts for $E/\mathbb{F}_q$, we need to establish some preliminary results.

Take ℓ to be a prime different than p, the characteristic of $\mathbb{F}_q$, and let $T_\ell(E)$ be the Tate module of E, our elliptic curve. The next two results are proven in Chapter 3 of Silverman and are well beyond the scope of this thesis:

Proposition 4.2.2. *There is a representation*

$$End(E) \to End(T_\ell(E)), \phi \mapsto \phi_\ell$$

and choosing an ℓ-adic basis for $T_\ell(E)$, we can write ϕ_ℓ as a 2x2 matrix.

Proposition 4.2.3. *Let $\phi \in End(E)$. Then*

$$\det \phi_\ell = \deg(\phi) \text{ and } \mathrm{tr}(\phi_\ell) = 1 + \deg(\phi) - \deg(1 - \phi)$$

We can apply these results to an elliptic curve over a finite field to estimate the number of points on this curve.

Theorem 4.2.4. *Let $E/\mathbb{F}_q$ be an elliptic curve, ϕ be the q-th power Frobenius map, and $a = q + 1 - \#E(\mathbb{F}_q)$.*

Let $\alpha, \beta \in \mathbb{C}$ be the roots of the polynomial $T^2 - aT + q$. Then α and β are complex conjugates satisfying $|\alpha| = |\beta| = \sqrt{q}$, and for every $n \geq 1$

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - \alpha^n - \beta^n$$

Proof. We have seen that

$$\#E(\mathbb{F}_q) = \deg(1 - \phi)$$

From Proposition 4.2.3, we have

$$\begin{aligned} \det \phi_\ell &= \deg(\phi) = q \\ \mathrm{tr}(\phi_\ell) &= 1 + \deg(\phi) - \deg(1 - \phi) = 1 + q - \#E(\mathbb{F}_q) = a \end{aligned}$$

Therefore, the characteristic polynomial of ϕ_ℓ is

$$\det(T - \phi_\ell) = T^2 - \mathrm{tr}(\phi_\ell)T + \det \phi_\ell = T^2 - aT + q$$

The characteristic polynomial is an element of $\mathbb{Z}[T]$, and therefore factors into linear factors over $\mathbb{C}$. That is,

$$T^2 - aT + q = (T - \alpha)(T - \beta), \alpha, \beta \in \mathbb{C}$$

For every rational number $\frac{m}{n} \in \mathbb{Q}$ we have

$$\det\left(\frac{m}{n} - \phi_\ell\right) = \frac{\det(m - n\phi_\ell)}{n^2} = \frac{\deg(m - n\phi)}{n^2} \geq 0$$

The rationals are dense in the reals, so for any $T \in \mathbb{R}$, the characteristic polynomial is non-negative, which implies that there is either a double root, or complex conjugate roots. In either case, $|\alpha| = |\beta|$, and we have

$$\alpha\beta = \det \phi_\ell = \deg(\phi) = q$$

So, $|\alpha| = |\beta| = \sqrt{q}$.

Remark 4.2.5. It is clear from this argument that α and β are the eigenvalues of ϕ_ℓ. The remaining arguments follow immediately from this observation.

Now, for each integer $n \geq 1$, the (q^n)-th power Frobenius map satisfies

$$\#E(\mathbb{F}_{q^n}) = \deg(1 - \phi^n)$$

Therefore, the characteristic polynomial of ϕ_ℓ^n is

$$\det(T - \phi_\ell^n) = (T - \alpha^n)(T - \beta^n)$$

This follows from putting ϕ_ℓ into Jordan normal form (in which we have α^n and β^n on the main diagonal of an upper triangular matrix).

Taking $T = 1$, we have

$$\begin{aligned}\#E(\mathbb{F}_{q^n}) = \deg(1-\phi^n) = \det(1-\phi_\ell^n) = (1-\alpha^n)(1-\beta^n) = \\ = 1-\alpha^n-\beta^n+(\alpha\beta)^n = 1-\alpha^n-\beta^n+q^n\end{aligned}$$

□

We can now use this theorem to prove a portion of the Weil Conjectures for elliptic curves over finite fields.

Theorem 4.2.6. *Let $E/\mathbb{F}_q$ be an elliptic curve. There exists $a \in \mathbb{Z}$ such that*

$$Z(E/\mathbb{F}_q;T) = \frac{1-aT+qT^2}{(1-T)(1-qT)} = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}$$

where $|\alpha| = |\beta| = \sqrt{q}$.

Proof. By definition,

$$Z(E/\mathbb{F}_q;T) = \exp\left(\sum_{n=1}^{\infty} \#E(\mathbb{F}_{q^n})\frac{T^n}{n}\right)$$

We take the logarithm of the zeta function,

$$\log Z(E/\mathbb{F}_q;T) = \sum_{n=1}^{\infty} \#E(\mathbb{F}_{q^n})\frac{T^n}{n} = \sum_{n=1}^{\infty} \frac{(1-\alpha^n-\beta^n+q^n)T^n}{n}$$

from the previous theorem. Now, we rewrite this sum using power series:

$$\log Z(E/\mathbb{F}_q;T) = -\log(1-T) + \log(1-\alpha T) + \log(1-\beta T) - \log(1-qT)$$

Therefore,

$$Z(E/\mathbb{F}_q;T) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}$$

where, as we saw in the previous theorem, α and β are complex conjugates whose absolute values are $\sqrt{q}$ and

$$a = \alpha + \beta = \mathrm{tr}(\phi_\ell) = q + 1 - \#E(\mathbb{F}_q)$$

□

But why is this called the Riemann Hypothesis? To see the relation of these results to the Riemann Hypothesis, let $T = q^{-s}$, and define

$$\zeta_{E/\mathbb{F}_q}(s) = Z(E/\mathbb{F}_q;q^{-s}) = \frac{1-aq^{-s}+q^{1-2s}}{(1-q^{-s})(1-q^{1-s})}$$

Theorem 4.2.7 (Riemann Hypothesis)**.** *If $\zeta_{E/\mathbb{F}_q}(s) = 0$, then $\mathrm{Re}(s) = 1/2$.*

Proof. $\zeta_{E/\mathbb{F}_q}(s) = 0$ is equivalent to

$$Z(E/\mathbb{F}_q; q^{-s}) = \frac{(1-\alpha q^{-s})(1-\beta q^{-s})}{(1-q^{-s})(1-q^{1-s})} = 0$$

This equality holds true when the numerator is zero; that is, when one of the factors in the numerator is zero. We consider the case when $(1-\alpha q^{-s}) = 0$, as the other case follows in exactly the same fashion.

$$1-\alpha q^{-s} = 0 \iff \alpha q^{-s} = 1 \implies \left|\alpha q^{-s}\right| = 1 \implies \frac{\sqrt{q}}{|q^s|} = 1 \implies |q^s| = \sqrt{q}$$

Writing $q^s = e^{s\log(q)}$ and taking the modulus gives us that $\mathrm{Re}(s) = 1/2$, as desired. □

Chapter 5

Examples

In this chapter, we will investigate specific elliptic curves and apply the general results proven above. To start, let us revisit the elliptic curve first investigated in Chapter 3:

Example 5.0.1.

$$y^2 = x^3 + 3x^2 + 2x$$

Using brute force, in Chapter 3 we saw that the congruence $y^2 \equiv x^3 + 3x^2 + 2x \mod 5^2$ had 31 solutions over $\mathbb{F}_{5^2}$. Now, let us look at this from an algebraic perspective and investigate the elliptic curve $E : y^2 = x^3 + 3x^2 + 2x$ over $\mathbb{F}_{25}$. First off, elliptic curves are projective objects, so we must include the point at infinity. With this in mind, we will use Theorem 4.2.4 to find the number of solutions on this elliptic curve.

Over $\mathbb{F}_5$, we saw in Chapter 3 that the congruence had 7 solutions. Translating this to elliptic curves, this means $\#E(\mathbb{F}_5) = 7 + 1 = 8$. Following Theorem 4.2.4, our characteristic polynomial is $T^2 - aT + 5$, where $a = 5 + 1 - 8 = -2$. Solving for T, we find

$$T = -1 \pm 2i \implies T^2 + 2T + 5 = (T - \alpha)(T - \beta), \alpha = -1 + 2i, \beta = -1 - 2i$$

Clearly $\beta = \overline{\alpha}$, and $|\alpha| = |\beta| = \sqrt{5}$, as predicted by Theorem 4.2.4. With this information, we know

$$\#E(\mathbb{F}_{5^2}) = 5^2 + 1 - (-1 + 2i)^2 - (-1 - 2i)^2 = 26 - (1 - 4i - 4) - (1 + 4i - 4) = 32 = 31 + 1$$

Recalling that brute force calculation showed the congruence $y^2 \equiv x^3 + 3x^2 + 2x \mod 5^2$ had 31 solutions, if we include the point at infinity, these two results agree.

This example shows the power and utility of Theorem 4.2.4. Computing all solutions to the above congruence is very time consuming, and this was for a small prime power. However, finding the number of solutions for the prime p takes very little time. If we know the number of solutions for p, we can use Theorem 4.2.4 to quickly and easily determine the number of solutions for any power of p.

For instance, consider E over $\mathbb{F}_{49}$. Computing all solutions to the congruence $y^2 \equiv x^3 + 3x^2 + 2x \mod 7^2$ over this field would take a long time. But, we have a better method. We saw that this congruence has 7 solutions over $\mathbb{F}_7$, i.e., $\#E(\mathbb{F}_7) = 8$. The characteristic polynomial is $T^2 + 7 = (T + \sqrt{7}i)(T - \sqrt{7}i)$. So, $\alpha = \sqrt{7}i$, $\beta = -\sqrt{7}i$. Using this information, we find

$$\#E(\mathbb{F}_{7^2}) = 49 + 1 + 7 + 7 = 64$$

The number of solutions on E includes the point at infinity, so the number of solutions to the congruence is $64 - 1 = 63$.

Let us consider one more example to see this theorem at work.

Example 5.0.2. Consider the curve

$$E : y^2 = x^3 + 2x^2 + 3 \text{ over } \mathbb{F}_5$$

Simple calculations show that $\#E(\mathbb{F}_5) = 7$. Therefore, $a = 5 + 1 - 7 = -1$, making our characteristic polynomial $T^2+T+5 = (T-\alpha)(T-\beta)$, where $\alpha = -\frac{1}{2}+\frac{\sqrt{19}}{2}i$, and $\beta = -\frac{1}{2}-\frac{\sqrt{19}}{2}i$. Finding $\#E(\mathbb{F}_{25})$ is easy:

$$\#E(\mathbb{F}_{25}) = 25 + 1 - \alpha^2 - \beta^2 = 26 - (-\frac{9}{2} - \frac{\sqrt{19}}{2}i) - (-\frac{9}{2} + \frac{\sqrt{19}}{2}i) = 35$$

This result tells us that we would expect the congruence

$$y^2 \equiv x^2 + 2x^2 + 3 \mod 25$$

to have 34 solutions over $\mathbb{F}_{25}$.

From our theoretical results, we know, for an elliptic curve E over $\mathbb{F}_5$,

$$1 \leq \#E(\mathbb{F}_5) \leq 10$$

A natural question to ask is if, for each integer from 1 to 10, there is an elliptic curve with this number of solutions over this field. Each curve is guaranteed to contain the point at infinity, but is there an elliptic curve with no other points in $\mathbb{F}_5^2$? Is there a curve with 10 points? It turns out that elliptic curves E_i exist for $i = 1, 2, ..., 10$ such that $\#E_i(\mathbb{F}_5) = i$. Below are examples of these curves:

$$\begin{aligned}
E_1 &: y^2 = x^3 + 4x + 2 \\
E_2 &: y^2 = x^3 + 3x^2 + 3 \\
E_3 &: y^2 = x^3 + 2x^2 + 2x + 2 \\
E_4 &: y^2 = x^3 + x \\
E_5 &: y^2 = x^3 + x^2 + 1 \\
E_6 &: y^2 = x^3 + 3x^2 + 3x \\
E_7 &: y^2 = x^3 + 2x^2 + 1 \\
E_8 &: y^2 = x^3 + 3x^2 + 2x \\
E_9 &: y^2 = x^3 + 4x^2 + 3x + 1 \\
E_{10} &: y^2 = x^3 + x^2 + 4
\end{aligned}$$

This example lends itself to the following question: Given a finite field, what are the achievable number of rational points on elliptic curves over this field? This question is answered in [3] by the Honda-Tate Theorem.

Theorem 5.0.3 (Honda-Tate)**.** *Let $q = p^a$ for some prime p and positive integer a. For integers in the interval $[-2\sqrt{q}, 2\sqrt{q}]$, the achievable integer values, t, of the quantity $q + 1 - \#E(\mathbb{F}_q)$ are:*

1. *t coprime to p;*
2. *If a is even, $t = \pm 2\sqrt{q}$;*
3. *If a is even and $p \not\equiv 1 \mod 3, t = \pm\sqrt{q}$;*
4. *If a is odd and $p = 2$ or 3, $t = \pm p^{\frac{a+1}{2}}$;*
5. *If either a is odd, or a is even and $p \not\equiv 1 \mod 4$, $t = 0$.*

Immediately, we see that if $q = p$, then, for every integer t in the interval $[-2\sqrt{p}, 2\sqrt{p}]$, there exists an elliptic curve E_t over $\mathbb{F}_p$ such that $t = p + 1 - \#E(\mathbb{F}_p)$. We will now apply this theorem to specific prime powers.

Examples 5.0.4. 1. $p = 2$.

- By the above observation, if $a = 1$, we know every integer $t \in [-2, 2]$ is achieved for some elliptic curve over $\mathbb{F}_2$.
- If $a = 2$, we are interested in the interval $[-4, 4]$. By (5.0.3)(1), $-3, -1, 1$, and 3 are achieved. By (5.0.3)(2) and (3), $-4, -2, 2$, and 4 are achieved. Finally, by (5.0.3) (5), 0 is achieved. Once again, we see that every integer $t \in [-4, 4]$ is achieved for some elliptic curve over $\mathbb{F}_4$.
- If $a = 3$, we consider $t \in [-5, 5]$. (5.0.3) shows that the achievable values of t in this interval are $-5, -4, -3, -1, 0, 1, 3, 4$, and 5. In particular, we see that $t = 2$ does not belong to this list. That means that there is no elliptic curve E over $\mathbb{F}_8$ with 7 rational points in this finite field.

2. $p = 5$.

- Once again, by the above observation, applying the Honda-Tate Theorem with $p = 5$ and $a = 1$ agrees with the direct calculation work done above. That is, for every $t \in [-4, 4]$, there exists an elliptic curve E_t such that $5 + 1 - \#E_t(\mathbb{F}_5) = t$.
- Now, if we take $a = 2$, we are interested in the interval $[-10, 10]$. By (5.0.3), we see that $\pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 7, \pm 8, \pm 9$, and ± 10 are all achieved. However, since $p = 5 \equiv 1 \mod 4$, 0 is not achieved. So, there is no elliptic curve E over $\mathbb{F}_{25}$ such that $\#E(\mathbb{F}_{25}) = 26$. Recalling our consideration of the elliptic curve $E : y^2 = x^3 + 2x^2 + 3$ over $\mathbb{F}_{25}$, we saw that $\#E(\mathbb{F}_{25}) = 35$. This agrees with the Honda-Tate Theorem, as -9 is an achievable value of t.

3. $p = 7$.

- As we have seen, the Honda-Tate Theorem guarantees that for all $t \in [-5, 5]$, there exists an elliptic curve E_t such that $7 + 1 - \#E_t(\mathbb{F}_7) = t$.
- Now, if we take $a = 2$, we are interested in the interval $[-14, 14]$. By (5.0.3), we see that $0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 8, \pm 9, \pm 10, \pm 11, \pm 12, \pm 13$, and ± 14 are all achieved. However, since $p \equiv 1 \mod 3$, ± 7 are not achievable. So, there is no elliptic curve E over $\mathbb{F}_{49}$ such that $\#E(\mathbb{F}_{49}) = 43$. However, this result does agree with our above observation that there exists an elliptic curve E over $\mathbb{F}_{49}$ such that $\#E(\mathbb{F}_{49}) = 49 + 1 + 14 = 64$.

References

[1] Andrews, George E.: *Number Theory*. 115-140. Dover Books on Mathematics, United States (1994)

[2] Fraleigh, John B.: *A First Course in Abstract Algebra, Seventh Edition*. 300-304. Pearson Education, London, United Kingdom (2003)

[3] Papikian, Mihran.: *Honda-Tate Theorem for Elliptic Curves*. 6. Pennsylvania State University (2012).

[4] Silverman, J.: *The Arithmetic of Elliptic Curves, 2nd Edition*, Graduate Texts in Mathematics **106**, 51-52, 98-99, 137-144. Springer, New York, New York (2009)

Academic Vita
Connor Cassady

cdc5402@psu.edu, (570) 977-0620

Objective Obtain a graduate assistantship and acquire my Ph.D. in theoretical mathematics, specializing in algebraic or analytic number theory.

Education

The Pennsylvania State University – May 2018
Eberly College of Science, Mathematics
Schreyer Honors College
Millennium Scholars Program

Work Experience

William G. Pritchard Fluid Mechanics Laboratory: January – May 2015
Used differential equations to model the dissipative behavior of standing water waves in a three-foot long tank.

Penn State Applied Mathematics REU: May – July 2016
Worked under Dr. Alberto Bressan and Dr. Tim Reluga and used differential game theory to study fishery and forest management.

Mathematics Advanced Study Semesters (MASS): August – December 2016
MASS is a one-semester program designed to introduce specially selected, highly motivated students to life as mathematics graduate students.

Millennium Scholars Calculus II Tutor: January – May 2017

Undergraduate Thesis Research: January 2017 – Present
Inspecting specific examples of the Riemann Hypothesis for elliptic curves.

Summer Research with Dr. Nathanial Brown: May – July 2017
Investigated STEM faculty perceptions of diversity and diversity initiatives at universities in the United States.

Millennium Scholars Mathematics Learning Assistant: May – July 2017

Activities and Honors

Schreyer Honors College: 2014 – Present
Millennium Scholars Program: 2014 – Present
Penn State Marching Blue Band, Snare Drum: 2014 – Present
Dean's List: Fall 2014, 2015, 2016, 2017, Spring 2015, 2016, 2017
Graduation with Distinction – MASS Program: 2016
William B. Forest Honors Scholarship in Mathematics: 2017, 2018
Evan Pugh Scholar Junior/Senior Award: 2017, 2018
Presented to the top 0.5% of Penn State's Junior and Senior Classes.
Student Marshal for the Department of Mathematics: Spring 2018