THE WEIL CONJECTURES FOR ELLIPTIC CURVES

ROMAIN AMZALLAG

Abstract. This paper explores various algebraic and geometric results of elliptic curves. We will prove that addition on elliptic curves gives it a group structure, and then shift our focus to elliptic curves over finite fields. We will prove the Weil conjectures for elliptic curves, and then discuss the conjectures in a more general setting. In particular, we will see how it links to the Riemann Hypothesis and zeta functions.

Contents

1. Introduction

1.1. **The Weil Conjectures.** This paper will explore the Weil conjectures for elliptic curves, proposed by André Weil in 1949 in his paper [18]. The importance of his work cannot be overstated, as it led into a decade long program aimed at proving them, which resulted in the advancement of studies in related fields. The program was a success, culminating with Pierre Deligne's 1980 paper [4]. The precise statement of the conjectures, found in Theorem 4.14, concerns the local zeta function of a projective variety V defined over some finite field $\mathbb{F}_q$. The conjectures claim the local zeta function

(i) is a rational function,

(ii) satisfies a certain functional equation,
(iii) has its zeros in restricted places.

The last two are analogues of the well known Riemann Hypothesis, which will be extensively discussed in the latter half of the paper. While the result is fairly straightforward to prove for elliptic curves, its generalization is still an open problem.

1.2. **History of Elliptic Curves.** As with many other geometric objects, the study of elliptic curves began with the ancient Greeks, most notably in Diophantus of Alexandria's *Arithmetica*. Problem 24 of Book IV reads as follows:

Problem 1.1. *To split a given number (6) into two parts such that their product is a cube minus it's side.*

Rewriting the above problem with an equation, one is tasked with find solutions to

$$y(6-y) = x^3 - x.$$

This is the equation of an elliptic curve! Other questions relating to elliptic curves were asked, such as by Apollonius, who wanted to find the arc length of an ellipse. However, it wasn't until the 17th century with the invention of integral calculus that mathematicians were able to exactly find the arc length of an ellipse. The integrals corresponding to the arc length of an ellipse are called **elliptic integrals**, and by studying the inverse of these elliptic integrals one gets doubly periodic functions, called **elliptic functions.** Karl Weierstrass defined an elliptic function in 1863 called the Weierstrass $\wp$-function. It satisfies a particular kind of differential equation. Indeed, by setting $x = \wp(z)$ and $y = \wp'(z)$ one gets

$$y^2 = 4x^3 - ax - b.$$

Thus, the $\wp$-function is a parametrization of elliptic curves! In 1901, Henri Poincaré published a landmark paper [9], in which he provided a comprehensive overview of all the work done on elliptic curves, effectively giving birth to a new area of study: elliptic curves.

It is then throughout the 20th century, with the advent of highly influential number theorists and algebraic geometers such as Louis Mordell and André Weil, that studying elliptic curves under a more general framework began. Using the language of schemes, Alexander Grothendieck developed the modern foundation of algebraic geometry in his treatise *Élements de Géometrie Algébrique* [8]. This framework is the one under which elliptic curves are studied in the modern lens.

The study of elliptic curves is rich and deep, having applications most notably in cryptography with elliptic curves cryptography (ECC). Whole books have been written on the subject, see for instance [10].

1.3. **Structure of Paper.** The paper is structured as follows. We begin in Section 2 with a general overview of elliptic curves using modern techniques, with the goal to prove that given an elliptic curve E, one can define an addition $+$ that makes $(E, +)$ into an abelian group. The proof of such a remarkable fact makes use of the theory of divisors (Section 2.1) and the Riemann-Roch theorem (Section 2.2), a foundational result in algebraic geometry giving a correspondence between topological data and algebraic data.

Section 3 then dives into elliptic curves over finite fields $\mathbb{F}_q$, introducing questions about counting the number of points on E that lie in $\mathbb{F}_{q^n}$ for $n \geq 1$. We provide an upper bound for the number of solutions to E over a finite field, known as the Hasse bound, in Section 3.2. We then state and prove the Weil conjectures for elliptic curves (Section 3.3) and how they link to the Riemann Hypothesis (Section 3.4). The proof makes use of the Tate module, which we discuss in Section 3.1.

Finally, Section 4 generalizes the Weil conjectures to curves of arbitrary genus in Section 4.1, expanding on how the local zeta function is related to the Riemann zeta function and how the Weil conjectures allow us to generalize Hasse's bound. We then quickly discuss the Weil conjectures for general projective varieties (Section 4.2) and explain how the conjectures for elliptic curves are a special case of the general statement.

We assume some knowledge of commutative algebra and Galois theory, as well as basic algebraic geometry. In particular, we assume the reader is familiar with introductory results about projective varieties. This paper is meant to be readable without too much knowledge beyond these subjects.

2. Elliptic Curves

2.1. **Definitions and Notation.** As the principal object of study, we must first define elliptic curves over a field. We will also introduce the notion of divisors, which will help with the exploration of elliptic curves. Throughout this paper, E will denote an elliptic curve, C a projective curve, and V a projective variety. Futhermore, K will denote a field, $\overline{K}$ its algebraic closure, and $K(C)$ the field of rational functions on a curve C.

Definition 2.1. Let $f(x)$ be a smooth cubic polynomial with coefficients in some field $\overline{K}$. The curve

$$y^2 = f(x)$$

defines an **elliptic curve**. An equivalent definition is that an **elliptic curve** (E, O) consists of a nonsingular curve E of genus one along with a specific basepoint $O \in E$. Given a field K, we say E **is defined over** K (denoted E/K) if E is defined over K as a curve and $O \in E(K)$.

The basepoint is often understood, and thus we henceforth denote the elliptic curve as E or E/K. We now define divisors on an algebraic curve C, which are simply elements of the free abelian group generated by points on C.

Definition 2.2. Let C be an algebraic curve. A **divisor** on C is a formal sum of points on C,

$$D = \sum_{P \in C} n_P(P),$$

where $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many $P \in C$. The group of divisors is $\mathrm{Div}(C)$. Given $D \in \mathrm{Div}(C)$, the **degree** of D is

$$\deg(D) = \sum_{P \in C} n_P.$$

The group of degree zero divisors is $\mathrm{Div}^0(C)$.

Now from a function in the field of rational functions $\overline{K}(C)$, we can construct divisors. Indeed, if $f \in \overline{K}(C)$, then we define

$$\begin{aligned} \mathrm{ord}_P : \overline{K}[C] &\to \mathbb{N} \cup \{\infty\} \\ f &\mapsto \sup_{d\in\mathbb{Z}}\{f \in M_P^d\}, \end{aligned}$$

where M_P is the maximal ideal of functions that vanish at P. We then extend this map to $\overline{K}(C)^*$ by letting $\mathrm{ord}_P(f/g) = \mathrm{ord}_P(f) - \mathrm{ord}_P(g)$. More simply, we view $\mathrm{ord}_P(f)$ as the order of P as a zero/pole of the function $f \in \overline{K}(C)^*$. Then we can define a divisor associated to f as follows.

Definition 2.3. Let $f \in \overline{K}(C)^*$ be a function defined on a curve C. The **divisor** associated to f is

$$\mathrm{div}(f) = \sum_{P\in C} \mathrm{ord}_P(f)(P).$$

This is a divisor because any such function must have a finite number of zeros and poles. Let $D \in \mathrm{Div}(C)$, we say D is **principal** if there exists some $f \in \overline{K}(C)^*$ such that

$$D = \mathrm{div}(f).$$

Two divisors $D_1, D_2 \in \mathrm{Div}(C)$ are **linearly equivalent**, denoted $D_1 \sim D_2$, if $D_1 - D_2$ is principal. The group of principal divisors of C is denoted $\mathrm{Prin}(C)$.

Remark 2.4. Consider the div function defined as follows:

$$\begin{aligned} \mathrm{div} : \overline{K}(C)^* &\to \mathrm{Div}(C) \\ f &\mapsto \mathrm{div}(f). \end{aligned}$$

An important result about $f \in \overline{K}(C)^*$ tells us

$$\deg(\mathrm{div}(f)) = 0$$

(see [11, II.6.10] for a proof.) Hence the image of the div map, which is $\mathrm{Prin}(C)$ by construction, lies in $\mathrm{Div}^0(C)$. In fact, $\mathrm{ord}_P(f)$ is a valuation, which makes div a homomorphism of abelian groups. This means $\mathrm{Prin}(C)$ is an subgroup of $\mathrm{Div}^0(C)$, which motivates the following definition.

Definition 2.5. The **Picard Group** of a curve C is

$$\mathrm{Pic}(C) = \mathrm{Div}(C)/\,\mathrm{Prin}(C).$$

The **degree 0 part** of the Picard Group is

$$\mathrm{Pic}^0(C) = \mathrm{Div}^0(C)/\,\mathrm{Prin}(C)$$

which is well defined by Remark 2.4. The group $\mathrm{Pic}^0(E)$ for an elliptic curve E will be used to prove that we can make E into a group.

2.2. **Riemann-Roch Theorem.** Given a curve C and a divisor $D \in \mathrm{Div}(C)$, the Riemann-Roch theorem allows us to determine the existence (or non-existence) of functions on C having zeros and poles at points encoded in D. It does so by relating the degree of D and the genus of C to vector space of the following form.

Definition 2.6. Let $D \in \mathrm{Div}(C)$, we associate to D the set of functions

$$\mathcal{L}(D) = \{f \in \overline{K}(C)^* \mid \mathrm{div}(f) \geq -D\} \cup \{0\}.$$

Then $\mathcal{L}(D)$ forms a vector space over $\overline{K}$ of dimension $\ell(D)$.

We now have almost all the necessary machinery to express the Riemann-Roch theorem, as one would still have to define a **canonical divisor** K_C of C, which arises from differential forms on C. However, all that matters for our purpose is that $\ell(K_C)$ is an invariant of C, which will not play an important role when we take C to be an elliptic curve. We refer the reader to [15, II.4] for a more thorough discussion of K_C.

Theorem 2.7. *(Riemann-Roch) Let C be a smooth curve and K_C a canonical divisor on C. There is an integer $g \geq 0$, an invariant of the curve called the genus, such that for every $D \in \mathrm{Div}(C)$, one has*

$$\ell(D) - \ell(K_C - D) = \deg(D) - g + 1.$$

As we will see, the Riemann-Roch theorem is the theorem which fundamentally allows us to talk about the group law on an elliptic curve. It links the geometric properties of the curve to algebraic properties.

Corollary 2.8. *Using the same setting as above, $\ell(K_C) = g$ and $\deg(K_C) = 2g-2$.*

Proof. Taking $D = 0$ in Theorem 2.7, one gets

$$\ell(0) - \ell(K_C) = \deg(0) - g + 1.$$

As $\mathcal{L}(0) = \overline{K}$, we have $\ell(0) = 1$ and thus $\ell(K_C) = g$. Now, taking $D = K_C$, we get

$$\begin{aligned} \ell(K_C) - \ell(K_C - K_C) = \deg(K_C) - g + 1 &\implies g - 1 = \deg(K_C) - g + 1 \\ &\implies \deg(K_C) = 2g - 2. \end{aligned}$$

□

Lemma 2.9. *Let $D \in \mathrm{Div}(C)$ be a divisor such that $\deg(D) < 0$. Then*

$$\ell(D) = 0.$$

Proof. Let $D = \sum_{P \in C} n_P(P)$ such that $\deg(D) < 0$. Then

$$\mathcal{L}(D) = \left\{ f \in \overline{K}(C)^* \mid \mathrm{div}(f) \geq -\sum_{P \in C} n_P(P) \right\} \cup \{0\}.$$

Consider some $f \in \mathcal{L}(D) \setminus \{0\}$, then we must have

$$\mathrm{div}(f) \geq -\sum_{P \in C} n_P(P).$$

However, by considering the degree of both sides of the inequality, one gets

$$\deg(\mathrm{div}(f)) \geq -\sum_{P \in C} n_P.$$

The right hand side is strictly positive by the assumption $\deg(D) < 0$, but $\deg(\mathrm{div}(f)) = 0$, meaning no such f exists. Thus

$$\mathcal{L}(D) = \{0\} \implies \ell(D) = 0.$$

□

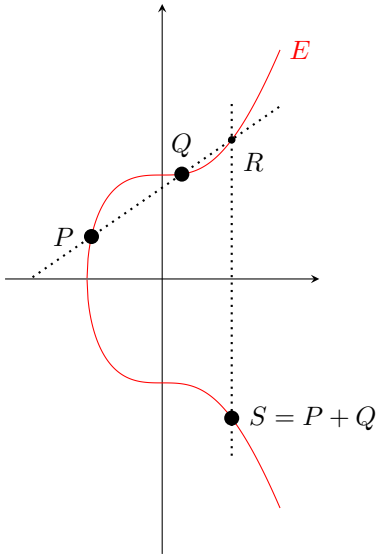

FIGURE 1. Addition of two points on elliptic curve

Remark 2.10. Henceforth, we will often be considering elliptic curves, i.e. smooth curves of genus 1. Furthermore, we will deal with divisors of strictly positive degree, which by Corollary 2.8 implies

$$\deg(K_C) = 0 \implies \deg(K_C - D) < 0,$$

and thus by Lemma 2.9

$$\ell(K_C - D) = 0.$$

Therefore, in the context described above, the Riemann-Roch theorem can be reduced to the simpler form

$$\ell(D) = \deg(D). \tag{2.11}$$

2.3. **Group Law on Elliptic Curves.** One may equip an elliptic curve (E, O) with an addition $+$ that makes $((E, O), +)$ into a group. We view E as being in the projective plane, so that by a simple application of Bezout's Theorem any line intersects E at exactly three points counting multiplicities.

Construction 2.12. The addition of two points $P, Q \in E$ is described by the following construction.

- Draw the line (PQ), denoting the line through points P and Q.
- The line (PQ) intersects E at another point R (not necessarily distinct.)
- The line (RO) intersects E at another point S (not necessarily distinct.)
- We let $S = P + Q$.

The construction is illustrated in Figure 1.

Remark 2.13. A priori, it is not clear why Construction 2.12 equips E with a group structure. A proof using explicit formulas and coordinates is given in [15, III.2], but it is not particularly elegant. Instead, one may use the Riemann-Roch theorem to relate this 'geometric group law' to an 'algebraic' one.

We begin with a couple of lemmas.

Lemma 2.14. *Let E be an elliptic curve and $P, Q \in E$. Then*

$$(P) \sim (Q) \iff P = Q.$$

Proof. Assume $(P) \sim (Q)$, then there exists a function $f \in \overline{K}(E)^*$ such that

$$\operatorname{div}(f) = (P) - (Q).$$

Thus $\operatorname{div}(f) \geq -(Q)$, which implies $f \in \mathcal{L}((Q))$. By Riemann-Roch as in Equation (2.11), we have

$$\ell((Q)) = \deg((Q)) = 1.$$

Certainly, constant functions are in $\mathcal{L}((Q))$, which forces f to be constant, i.e. $f \in \overline{K}$. Hence $\operatorname{div}(f) = 0$ and $P = Q$. The converse is clear, as $P = Q$ implies $(P) - (Q) = 0 = \operatorname{div}(0)$. □

Lemma 2.15. *Let E be an elliptic curve and $D \in \operatorname{Div}^0(E)$. Then there exists a unique $P \in E$ such that*

$$D \sim (P) - (O).$$

Let

$$\sigma : \operatorname{Div}^0(E) \to E$$

be the map that sends D to the associated point P on the curve. This map is surjective.

Proof. The divisor $D + (O)$ has degree one, so by Equation (2.11) we get

$$\mathcal{L}(D + (O)) = 1$$

Let f be a nonzero element of this vector space, then $\{f\}$ forms a basis. Now we have

$$\operatorname{div}(f) \geq -(O) - D \quad \text{and} \quad \deg(\operatorname{div}(f)) = 0$$

which means there exists some point $P \in E$ such that

$$\operatorname{div}(f) = (P) - (O) - D.$$

Thus

$$D \sim (P) - (O).$$

If $P' \in E$ is another point with the above property, then

$$P' \sim D + (O) \sim P$$

which by Lemma 2.14 is equivalent to $P = P'$, hereby showing that P is unique. Hence σ is well defined. It is surjective because for any $P \in E$,

$$\sigma((P) - (O)) = (P).$$

□

Lemma 2.16. *With same setting as in Lemma 2.15, let $D_1, D_2 \in \operatorname{Div}^0(E)$. Then*

$$\sigma(D_1) = \sigma(D_2) \iff D_1 \sim D_2.$$

Proof. Let $P_i = \sigma(D_i)$ for $i = 1, 2$. Then $D_i \sim (P_i) - (O)$, which implies

$$(P_1) - (P_2) \sim D_1 - D_2.$$

If $P_1 = P_2$, then $D_1 \sim D_2$. Conversely, if $D_1 \sim D_2$, then $(P_1) \sim (P_2)$ which by Lemma 2.14 implies $P_1 = P_2$. □

Remark 2.17. In Definition 2.5, we have defined $\mathrm{Pic}^0(E)$ to be the quotient of $\mathrm{Div}^0(E)$ by the subgroup of principal divisors. By Lemma 2.16, principal divisors form the kernel of the σ map, so the induced map

$$\sigma^* : \mathrm{Pic}^0(E) \to E$$

is a bijection. It's inverse is

$$\begin{aligned} \kappa : E &\to \mathrm{Pic}^0(E) \\ P &\mapsto (\text{divisor class of } (P) - (O)). \end{aligned}$$

See [15, III.3.4 (d)] for a proof.

Theorem 2.18. *Let $P, Q \in E$, we have*

$$\kappa(P+Q) = \kappa(P) + \kappa(Q)$$

Proof. Let $f(X,Y,Z) = \alpha X + \beta Y + \gamma Z = 0$ be the equation of the line going through P, Q as viewed in $\mathbb{P}^2$. By Bezout's theorem there is another intersection point of multiplicity one, denoted R. Let $f'(X,Y,Z) = \alpha' X + \beta' Y + \gamma' Z = 0$ be the equation of the line going through O, R. At $Z = 0$, we are on the line at infinity, so E can only intersect $Z = 0$ at O, meaning the multiplicity of that intersection is three. Hence

$$\mathrm{div}(f/Z) = (P) + (Q) + (R) - 3(O).$$

Now from Construction 2.12, the line defined by $f'(X,Y,Z)$ intersects E at O, R, and $P + Q$. Thus

$$\mathrm{div}(f'/Z) = (R) + (P+Q) - 2(O).$$

Hence

$$0 \sim \mathrm{div}(f'/f) = (P+Q) - (P) - (Q) + (O)$$

and

$$(P+Q) \sim (P) + (Q) - (O).$$

Thus

$$\kappa(P+Q) = \kappa(P) + \kappa(Q)$$

which concludes the proof. □

Remark 2.19. The equation

$$\kappa(P+Q) = \kappa(P) + \kappa(Q)$$

holds much significance and proves that Construction 2.12 equips E with a group structure. Indeed, in $\kappa(P+Q)$, the addition of two points is done in E, so we are using the 'geometric group law'. However, when we add as in $\kappa(P) + \kappa(Q)$, we are adding in $\mathrm{Pic}^0(E)$, which we know is a group, hence it is the 'arithmetic group law'. Thus associativity of addition in E follows directly, as

$$\begin{aligned} \kappa((P+Q)+R) &= \kappa(P+Q) + \kappa(R) \\ &= (\kappa(P) + \kappa(Q)) + \kappa(R) \end{aligned}$$

Since $\mathrm{Pic}^0(E)$ is a group, we may use associativity.

$$\begin{aligned} &= \kappa(P) + (\kappa(Q) + \kappa(R)) \\ &= \kappa(P + (Q+R)) \end{aligned}$$

Thus, by bijectivity of κ, we must have

$$(P+Q)+R = P+(Q+R)$$

where addition is done in E. The precise statement would be to say that κ is a group homomorphism.

3. Elliptic Curves over Finite Fields

3.1. **Tate Module.** When studying elliptic curves over finite fields, such as $\mathbb{F}_q$, a natural consideration are torsion points, which can be defined because we know elliptic curves have an addition operation. The Tate Module encodes information about these torsion points, which will aid us in proving the Weil conjectures for elliptic curves rather easily. More specifically, the Tate module allows us to take an automorphism ϕ of E and get an associated matrix ϕ_ℓ over a ring of characteristic zero, making it possible to compute the determinant and trace, values which come up in the proof of the Weil conjectures for elliptic curves, see Section 3.3. We first introduce some notation.

Definition 3.1. Let E_1, E_2 be elliptic curves with basepoint O. An **isogeny** ϕ is a group homomorphism

$$\phi : E_1 \to E_2$$

such that $\phi(O) = O$.

There are many isogenies, for instance the trivial map $\phi : E_1 \to E_2$ defined by $\phi(P) = O$. We will study the **multiplication by m** isogeny, which is defined using the group law. It is given by

$$[m] : E \to E$$

$$P \mapsto \begin{cases} \underbrace{P+P+\ldots+P}_{m \text{ times}} & \text{if } m \geq 0, \\ \underbrace{-P-P-\ldots-P}_{m \text{ times}} & \text{if } m < 0. \end{cases}$$

One may now ask about m-torsion points, defined as the kernel of $[m]$ (and thus a group), which we denote by

$$E[m] = \{P \in E \mid [m]P = 0\}.$$

Proposition 3.2. *If $m \neq 0$ in K and $\mathrm{char}(K) \nmid m$, then*

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

Proof. See [15, III.6.4] □

Remark 3.3. Proposition 3.2 is an important statement, as it gives us a fundamental description for $E[m]$. The torsion points form a group of order m^2. This matters, because if m is a prime different than $\mathrm{char}(K)$, say ℓ, then

$$E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$$

and thus the set of automorphisms of the group $E[\ell]$ is the matrix group $GL_2(\mathbb{Z}/\ell\mathbb{Z})$, a well studied group. However, there is an issue here. The representation we get by looking at the set of automorphisms is over a ring of positive characteristic, meaning we would have to use modular representation theory to study these representations.

This makes it much harder and therefore we would like to work over rings of characteristic zero. The natural way to do so is by mimicking the construction of the ℓ-adic integers. One may use an inverse limit to induce a representation over $\mathbb{Z}_\ell$ instead of $\mathbb{Z}/\ell\mathbb{Z}$, and through the inclusion $\mathbb{Z}_\ell \hookrightarrow \mathbb{Q}_\ell$ we get a representation over a ring of characteristic zero as desired.

Construction 3.4. *(Tate Module)* While Proposition 3.2 tells us $E[\ell]$ and $(\mathbb{Z}/\ell\mathbb{Z})^2$ are isomorphic as groups, it turns out $E[\ell]$ has more structure than just a group. Indeed, it is acted on by the Galois group $G = \mathrm{Gal}(\overline{K}/K)$ and hence we get a representation

$$G \to \mathrm{Aut}(E[\ell]) \cong GL_2(\mathbb{Z}/\ell\mathbb{Z})$$

as explained above. Consider the family of groups $\{E[\ell^n]\}$ and the map

$$[\ell] : E[\ell^{n+1}] \to E[\ell^n].$$

We have the necessarily data to take an inverse limit.

Definition 3.5. With the setting described above, let the (ℓ-adic) **Tate Module** of E be the group

$$T_\ell(E) = \varprojlim_n E[\ell^n]$$

where the inverse limit is taken with respect to the maps $[\ell]$.

Remark 3.6. From Proposition 3.2 and by properties of the inverse limit, one easily gets

$$T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell.$$

We know the Galois group G acts on $E[\ell^n]$, and it turns out that action commutes with the multiplication by $[\ell]$ map, i.e. the following diagram commutes.

$$\begin{array}{ccc} G \times E[\ell^{n+1}] & \longrightarrow & E[\ell^{n+1}] \\ \downarrow & & \downarrow \\ G \times E[\ell^n] & \longrightarrow & E[\ell^n] \end{array}$$

The action of G therefore passes to $T_\ell(E)$. If given a representation $\rho : G \to GL_2(\mathbb{Z}/\ell\mathbb{Z})$, we get an induced representation

$$\rho_\ell : G \to GL_2(\mathbb{Z}_\ell) \hookrightarrow GL_2(\mathbb{Q}_\ell).$$

Thus our representation is over a ring of characteristic zero, as desired.

Remark 3.7. All of this may seem quite arbitrary, but it matters for the following reason. If we are given an endomorphism $\phi \in \mathrm{Aut}(E)$, it maps torsion points to torsion points, so we can restrict it to a map $\phi \in \mathrm{End}(E[\ell])$. Now by the above comments, this induces a map

$$\phi_\ell \in \mathrm{End}(T_\ell(E)).$$

By choosing a $\mathbb{Z}_\ell$ basis, we can therefore write ϕ_ℓ as an element of $GL_2(\mathbb{Z}_\ell)$, which means that the values $\det(\phi_\ell)$ and $\mathrm{Tr}(\phi_\ell)$ are computable. These values play a crucial role in the proof of the Weil conjectures for elliptic curves in the case where ϕ is the Frobenius automorphism, motivating why we needed to discuss the Tate module.

3.2. **Hasse Bound.** Let $E/\mathbb{F}_q$ be an elliptic curve. Since we are working over a finite field, an important question to ask about this curve is how many points on E have coordinates in $\mathbb{F}_q$, or in other words, how many solutions in $\mathbb{F}_q$ does the equation defining E have. Let us denote the set of such points

$$E(\mathbb{F}_q).$$

A trivial upper bound for $|E(\mathbb{F}_q)|$ is q^2, since we have q^2 choices for coordinates of points $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$. However, we would like to improve this bound, something Hasse has done in 1930 by proving the following theorem.

Theorem 3.8. *(Hasse) Let $E/\mathbb{F}_q$ be an elliptic curve defined over a finite field. Then*

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

Before, we need a simple lemma which is a version of Schwartz's inequality.

Lemma 3.9. *Let A be an abelian group, and let*

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

be a positive definite quadratic form. Then

$$|d(\alpha - \beta) - d(\alpha) - d(\beta)| \leq 2\sqrt{d(\alpha)d(\beta)}$$

for all $\alpha, \beta \in A$.

The proof is not particularly illuminating, it can be found at [15, V.1.2]. We can now prove Hasse's theorem.

Proof. (of Theorem 3.8) Let

$$\begin{aligned} \phi : E &\to E \\ (x, y) &\mapsto (x^q, y^q) \end{aligned}$$

be the q-th power Frobenius automorphism of E. This automorphism topologically generates the Galois group $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. Hence, for any $P \in E(\overline{\mathbb{F}}_q)$, one has

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

Thus $E(\mathbb{F}_q) = \ker(1 - \phi)$. The map $1 - \phi$ is separable (see [15, III.5.5]) and thus

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

with the second equality coming from [16, 6.7], Recall that the degree map is a positive definite form, so using Lemma 3.9 with $\alpha = 1$ and $\beta = \phi$, one gets

$$|\deg(1 - \phi) - 1 - q| \leq 2\sqrt{q}$$

as $\deg(1) = 1$ and $\deg(\phi) = q$. Therefore

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

as desired. □

Remark 3.10. The above result may be generalized to the Hasse-Weil bound, which holds not only for elliptic curves, but higher genus algebraic curves. Given a curve C of genus g, for all $n \geq 1$, one has

$$||C(\mathbb{F}_{q^n})| - q^n - 1| \leq 2gq^{n/2}.$$

Then Theorem 3.8 is simply when $n = 1$ and C is an elliptic curve. The result is a consequence of the Weil conjectures proposed in 1949 by André Weil in [18]. We

will discuss the conjectures in the case of elliptic curves in the next section, and later on derive the Hasse-Weil bound (see Corollary 4.11).

3.3. **Weil Conjectures for Elliptic Curves.** Just as in the previous section, we are concerned with $|E(\mathbb{F}_q)|$, but this time we will also consider $|E(\mathbb{F}_{q^n})|$ for $n \geq 1$. We first encode these values in a generating function.

Definition 3.11. The **zeta function** of $E/\mathbb{F}_q$ is the power series

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

Remark 3.12. This definition may seem arbitrary, but the name of the function should be indicative that it is related to known zeta functions, and in particular to the Riemann Hypothesis. This will extensively be discussed when generalizing to curves of genus $g \geq 1$ in Section 4.1.

It turns out the zeta function of $E/\mathbb{F}_q$ has a very simple form.

Theorem 3.13. *(Weil conjectures for E.) Let $E/\mathbb{F}_q$ be an elliptic curve. There exists an $a \in \mathbb{Z}$ such that*

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

with $1 - aT + qT^2 = (1 - \alpha T)(1 - \beta T)$ where $|\alpha| = |\beta| = \sqrt{q}$.

The goal of this part is to prove Theorem 3.13. To do so, we will make use of the Tate module. Recall from Remark 3.7 that one has the following map

$$\begin{aligned} \mathrm{End}(E) &\to \mathrm{End}(T_\ell(E)) \\ \phi &\mapsto \phi_\ell. \end{aligned}$$

By choosing a $\mathbb{Z}_\ell$-basis, we can write ϕ_ℓ as a 2×2 matrix with coefficients in $\mathbb{Z}_\ell$.

Lemma 3.14. *Let $\phi \in \mathrm{End}(E)$, then*

$$\det(\phi_l) = \deg(\phi)$$

and

$$\mathrm{Tr}(\phi_l) = 1 + \deg(\phi) - \deg(1 - \phi).$$

In particular, the quantities are independent of ℓ.

Proof. See [15, III.8.6] □

Lemma 3.15. *Let $E/\mathbb{F}_q$ be an elliptic curve and let*

$$\begin{aligned} \phi : E &\to E \\ (x, y) &\mapsto (x^q, y^q) \end{aligned}$$

be the q-th power Frobenius. Let

$$a = q + 1 - |E(\mathbb{F}_q)|$$

and let $\alpha, \beta \in \mathbb{C}$ be the roots of $T^2 - aT + q$. Then α and β satisfy $|\alpha| = |\beta| = \sqrt{q}$.

Proof. First recall from the proof of Theorem 3.8 that

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

Using Lemma 3.14 one gets

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

and

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

Therefore, the characteristic polynomial $\det(T\cdot I - \phi_\ell)$ of ϕ_ℓ is

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

whose roots are α and β by assumption. Thus we may write

$$T^2 - aT + q = (T-\alpha)(T-\beta).$$

In particular, for every rational $m/n \in \mathbb{Q}$, we have

$$\det(m/n\cdot I - \phi_\ell) = \frac{\det(m\cdot I - n\phi_\ell)}{n^2} = \frac{\deg(m\cdot I - n\phi_\ell)}{n^2} \geq 0.$$

It follows that $T^2 - aT + q$ is non negative for all $T \in \mathbb{R}$ (by continuity), so it either has conjugate complex roots or a double root. In either case $|\alpha| = |\beta|$. Finally

$$\alpha\beta = \det(\phi_\ell) = q \implies |\alpha| = |\beta| = \sqrt{q}.$$

□

Lemma 3.16. *For every $n \geq 1$, we have*

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

where α, β are defined as in Lemma 3.15.

Proof. For each $n \geq 1$, we have

$$|E(\mathbb{F}_{q^n})| = \deg(1-\phi^n) = \det(1-\phi_\ell^n).$$

Since $\det(\phi_\ell) = \alpha\beta$ as in Lemma 3.15, there is a basis of $\mathbb{Z}_\ell$ such that

$$\phi_\ell = \begin{pmatrix}\alpha & 1\\ 0 & \beta\end{pmatrix}.$$

Hence

$$\phi_\ell^n = \begin{pmatrix}\alpha^n & 1\\ 0 & \beta^n\end{pmatrix}$$

which shows

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

Therefore

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

. □

We now have all the required machinery to prove Theorem 3.13.

Proof. (of Theorem 3.13) We simply compute

$$\log(Z(E/\mathbb{F}_q,T)) = \sum_{n=1}^{\infty} |E(\mathbb{F}_{q^n})| \frac{T^n}{n}$$

$$\text{(from Lemma 3.16)} \quad = \sum_{n=1}^{\infty} (q^n + 1 - \alpha^n - \beta^n) \frac{T^n}{n}$$

$$= -\log(1-T) - \log(1-qT) + \log(1-\alpha T) + \log(1-\beta T).$$

Thus, taking the exponential on both sides, we get

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

Since $a = \alpha + \beta = \mathrm{Tr}(\phi_\ell)$ from the proof of Lemma 3.15, we indeed get $a \in \mathbb{Z}$ and $|\alpha| = |\beta| = \sqrt{q}$. □

We will explain why Theorem 3.13 is called the Weil conjecture for elliptic curves in Remark 4.15.

3.4. **Riemann Hypothesis for Elliptic Curves.** In Theorem 3.13, the conclusion $|\alpha| = |\beta| = 1/2$ is called the Riemann Hypothesis for elliptic curves, but it is not immediately obvious how it is related to the famous Riemann Hypothesis. This part will explain the terminology. As a reminder, the Riemann Hypothesis is the following open problem.

Problem 3.17. *Let*

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

be the ***Riemann zeta function****. All the nontrivial zeros of $\zeta(s)$ lie on the line $\Re(s) = 1/2$.*

Now in the expression for $Z(E/\mathbb{F}_q,T)$, set $T = q^{-s}$ and define a function in s, which suggestively will be named $\zeta_{E/\mathbb{F}_q}(s)$.

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

One may check the following claim through simple algebra.

Claim 3.18. *The above zeta function satisfies the functional equation*

$$\zeta_{E/\mathbb{F}_q}(s) = \zeta_{E/\mathbb{F}_q}(1-s).$$

Proof. Just multiply $\zeta_{E/\mathbb{F}_q}(1-s)$ by $\frac{q^{1-2s}}{q^{1-s}\cdot q^{-s}} = 1$. □

Now the original Riemann zeta function satisfies a functional equation of the same form, namely

$$\varepsilon(s) = \varepsilon(1-s)$$

where $\varepsilon(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$ (see [6] for details). This similarity should suggest why the Riemann Hypothesis is related to our result on elliptic curve. Another important observation to make is the following.

Observation 3.19. The Riemann Hypothesis for elliptic curves (Theorem 3.13) tells us the zeros are $T = \frac{1}{\alpha}, \frac{1}{\beta}$ where $|\alpha| = |\beta| = \sqrt{q}$. Therefore, if T is a zero, then

$$|T| = \left|\frac{1}{\alpha}\right| = q^{-1/2}.$$

Now

$$Z(E/\mathbb{F}_q, T) = 0 \iff Z(E/\mathbb{F}_q, q^{-s}) = 0 \iff \zeta_{E/\mathbb{F}_q}(s) = 0,$$

which means $\zeta_{E/\mathbb{F}_q}(s) = 0$ if and only if $|T| = q^{-1/2}$. Through the usual change of variable $T = q^{-s}$, we see that $\zeta_{E/\mathbb{F}_q}(s) = 0$ if and only if $|q^{-s}| = q^{-1/2}$, i.e. $\Re(s) = 1/2$. This is the Riemann Hypothesis, as we are saying the zeros of our zeta function are on the line $\Re(s) = \frac{1}{2}$.

4. Generalizations

4.1. **Weil Conjectures for Curves.** This part will generalize Theorem 3.13 to curves of genus $g \geq 1$, culminating in the Weil conjectures for curves. We will look more precisely at where the zeta function comes from and relate it to the Riemann Hypothesis. We will then derive the Hasse-Weil bound introduced in Remark 3.10 from the Weil Conjectures for Curves.

Definition 4.1. The **Riemann zeta function** is the sum

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

Remark 4.2. It is common result that the zeta function may be rewritten as

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

This form of the zeta function makes it easier to generalize to number fields by generalizing from prime elements to prime ideals.

Definition 4.3. Let K be any number field (finite extension of $\mathbb{Q}$) and $\mathcal{O}_K$ be the ring of integers of K. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. The **Dedekind zeta function** is defined to be the product

$$\zeta(K, s) = \prod_{\mathfrak{p} \text{ prime}} \frac{1}{1 - |\mathcal{O}_K/\mathfrak{p}|^{-s}},$$

where the product is taken of all prime ideals. We call $\mathcal{O}_K/\mathfrak{p}$ the **quotient ring** of $\mathcal{O}_K$ and $\mathfrak{p}$.

Remark 4.4. Let K be the simplest number field possible, the rationals $\mathbb{Q}$. It's ring of integers is $\mathbb{Z}$. Thus, the prime ideals of $\mathcal{O}_{\mathbb{Q}}$ are (p) for prime $p \in \mathbb{Z}$. The quotient rings are therefore

$$\mathbb{Z}/(p) = \mathbb{Z}/p\mathbb{Z}$$

which have order p. Hence, the associated Dedekind zeta function is

$$\zeta(\mathbb{Q}, s) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}},$$

which is just the usual zeta function!

Let C be a nonsingular projective curve over $\mathbb{F}_q$. We are now going to relate the Dedekind zeta function to the zeta function of a curve C, defined just like in the case of elliptic curves by

$$Z(C/\mathbb{F}_q, T) = \exp\left(\sum_{n=1}^{\infty} |C(\mathbb{F}_{q^n})| \frac{T^n}{n}\right).$$

We must somehow relate the curve to a ring, which we do in the following observation.

Observation 4.5. Let $C/\mathbb{F}_q$ be our curve. We can consider the ring of functions on that curve, denoted $\mathbb{F}_q[C]$. This is a polynomial ring, with field of fractions $\mathbb{F}_q(C)$. for every point $P \in C$, we can consider the ideal in $\mathbb{F}_q[C]$ of functions that vanish at P. This ideal, denoted $\mathfrak{p}_P$ is prime. This result is a consequence of Hilbert's Nullstellensatz, see [1, 7.10].

Let $K = \mathbb{F}_p(C)$, then $\mathcal{O}_K = \mathbb{F}_p[C]$ and we can write

$$\zeta(\mathbb{F}_p[C], s) = \prod_{\mathfrak{p} \text{ prime}} \frac{1}{1 - |\mathbb{F}_p[C]/\mathfrak{p}|^{-s}}.$$

As explained in Observation 4.5, the prime ideals $\mathfrak{p}$ correspond to points P. The quotient ring $\mathbb{F}_p[C]/\mathfrak{p}$ is actually a finite field of order q^m. We call m the **degree** of P, denoted $\deg(P)$ or $\deg(\mathfrak{p})$ depending on if we are talking about the points or the prime ideals, but it doesn't matter since they are defined to be the same. We can thus rewrite our zeta function as

$$\zeta(\mathbb{F}_p[C], s) = \prod_{P \in C} \frac{1}{1 - (q^{\deg(P)})^{-s}}.$$

Now we claim we have the following equality.

Theorem 4.6. *With the above setting, one has the equality*

$$\zeta(\mathbb{F}_p[C], s) = Z(C/\mathbb{F}_q, q^{-s})$$

Proof. Making the change of variable $T = q^{-s}$, we get

$$\zeta(\mathbb{F}_p[C], s) = \prod_{P \in C} \frac{1}{1 - T^{\deg(P)}}$$

and thus the above result boils down to showing

$$Z(C/\mathbb{F}_q, T) = \prod_{P \in C} \frac{1}{1 - T^{\deg(P)}}.$$

Although an abuse of notation, when writing $Z(C/\mathbb{F}_q, T)$ we will mean the product form, and from the product form we will get to the power series form through some algebraic manipulations.

We first work over the prime ideals rather than points and take the logarithm to get

$$\log Z(C/\mathbb{F}_q, T) = -\sum_{\mathfrak{p}} \log(1 - T^{\deg(\mathfrak{p})}).$$

Now the Taylor expansion of $\log(1 - x)$ gives us

$$\log Z(C/\mathbb{F}_q, T) = \sum_{\mathfrak{p}} \sum_{k=1}^{\infty} \frac{(T^{\deg(\mathfrak{p})})^k}{k}.$$

Finally, taking the derivative with respect to T we have

$$\frac{d}{dT}\log Z(C/\mathbb{F}_q,T)=\frac{1}{T}\sum_{\mathfrak{p}}\sum_{k=1}^{\infty}\deg(\mathfrak{p})T^{k\cdot\deg(\mathfrak{p})}.$$

Remark 4.7. We define a_d to be the number of prime ideals of degree d, i.e.

$$a_d=|\{\mathfrak{p}\subset\mathbb{F}_q[C]\mid \deg(\mathfrak{p})=d\}|.$$

There is another and more useful way to view a_d. Consider a point $P\in C$. It is acted on by a permutation in the Galois group $G=\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. This action gives us an orbit of size $\deg(P)$. Therefore, a_d is just the number of orbits of size exactly d under the Galois action. This way of viewing a_d will allow us to relate the product form of $Z(C/\mathbb{F}_q,T)$ to the power series form. Indeed, we make the following observation, relating a_d to the number of points on C with coordinates in $\mathbb{F}_{q^n}$, denoted $|C(\mathbb{F}_{q^n})|$.

Observation 4.8. A point P lies in $C(\mathbb{F}_{q^n})$ if and only if it lies an a Galois orbit as described above. Every prime ideal $\mathfrak{p}$ of degree d gives us exactly d points in $C(\mathbb{F}_{q^d})$. Moreover, if $d\mid n$, then these points will also lie in $C(\mathbb{F}_{q^n})$. These give us all the points in $C(\mathbb{F}_{q^n})$, and since we have a_d prime ideals of degree d, one gets

$$|C(\mathbb{F}_{q^n})|=\sum_{d|n}d\cdot a_d.$$

We want to introduce a_d in our expression for $\frac{d}{dT}\log Z(C/\mathbb{F}_q,T)$, but this is not too complicated as we have

$$\frac{d}{dT}\log Z(C/\mathbb{F}_q,T)=\frac{1}{T}\sum_{\mathfrak{p}}\sum_{k=1}^{\infty}\deg(\mathfrak{p})T^{k\cdot\deg(\mathfrak{p})}.$$

There are a_d prime ideals of degree d:

$$\begin{aligned}&=\frac{1}{T}\sum_{d=1}^{\infty}a_d\cdot\left[dT^d+dT^{2d}+\ldots\right]\\&=\frac{1}{T}\sum_{d=1}^{\infty}d\cdot a_d\sum_{n=1}^{\infty}T^{d\cdot n}.\end{aligned}$$

Through simple rearranging exercise:

$$=\frac{1}{T}\sum_{n=1}^{\infty}\left(\sum_{d|n}a_d\cdot d\right)T^n.$$

By Observation 4.8:

$$\begin{aligned}&=\frac{1}{T}\sum_{n=1}^{\infty}|C(\mathbb{F}_{q^n})|T^n\\&=\frac{d}{dT}\sum_{n=1}^{\infty}|C(\mathbb{F}_{q^n})|\frac{T^n}{n}.\end{aligned}$$

This gives us the desired expression for $Z(C/\mathbb{F}_q, T)$, as by cancelling out the derivatives and taking the exponential we get

$$Z(C/\mathbb{F}_q, T) = \exp\left(\sum_{n=1}^{\infty} |C(\mathbb{F}_{q^n})| \frac{T^n}{n}\right).$$

This shows that

$$\zeta(\mathbb{F}_p[C], s) = Z(C/\mathbb{F}_q, q^{-s})$$

as desired. □

Just like for elliptic curves, we have the Weil conjectures for curves.

Theorem 4.9. *(Weil conjectures for C, [17, 2.1]) Let $C/\mathbb{F}_q$ be a nonsingular curve of genus g. Then*

$$Z(C/\mathbb{F}_q, T) = \frac{P(T)}{(1-T)(1-qT)}$$

where

$$P(T) = \prod_{i=1}^{2g}(1 - \alpha_i T) \in \mathbb{Z}[T]$$

is a polynomial of degree $2g$ with reciprocal roots $\alpha_i \in \mathbb{C}$ that are algebraic integers satisfying $|\alpha_i| = q^{1/2}$. The zeta function also satisfies the function equation

$$Z\left(C/\mathbb{F}_q, \frac{1}{qT}\right) = \frac{1}{(qT^2)^{g-1}} Z(C/\mathbb{F}_q, T).$$

Remark 4.10. One must use intersection theory to prove *Theorem* 4.9. See [11, Appendix C] for more details about the necessary prerequisites.

As promised, we conclude this part with the proof of the Hasse-Weil bound mentioned in Remark 3.10.

Corollary 4.11. *(Hasse - Weil Bound, [17, 2.2]) Let $C/\mathbb{F}_q$ be a nonsingular projective curve of genus g. Then for all $n \geq 1$ we have*

$$||C(\mathbb{F}_{q^n})| - q^n - 1| \leq 2gq^{n/2}.$$

Proof. Taking the logarithmic derivative of $Z(C/\mathbb{F}_q, T)$ gives us

$$\frac{d}{dT} \log Z(C/\mathbb{F}_q, T) = \sum_{n=1}^{\infty} |C(\mathbb{F}_q)| T^{n-1}.$$

Doing the same manipulation but using Theorem 4.9 we get

$$\begin{aligned}
\frac{d}{dT} \log Z(C/\mathbb{F}_q, T) &= \frac{1}{1-T} + \frac{q}{1-qT} - \sum_{i=1}^{2g} \frac{\alpha_i}{1-\alpha_i T} \\
&= \sum_{n=0}^{\infty} (1 + q^{n+1}) T^n - \sum_{n=1}^{\infty} \left(\sum_{i=1}^{2g} \alpha_i^{n+1}\right) T^n \\
&= \sum_{n=1}^{\infty} \left(1 + q^n - \sum_{i=1}^{2g} \alpha_i^n\right) T^{n-1}.
\end{aligned}$$

Equating the two expressions gives us

$$\sum_{n=1}^{\infty} |C(\mathbb{F}_q)|T^{n-1} = \sum_{n=1}^{\infty} \left(1 + q^n - \sum_{i=1}^{2g} \alpha_i^n\right) T^{n-1}.$$

Hence

$$||C(\mathbb{F}_{q^n})| - q^n - 1| \leq \left|\sum_{i=1}^{2g} \alpha_i^n\right| \leq 2g|\alpha_i|^n \leq 2gq^{n/2}$$

as desired. □

4.2. **Weil Conjectures for Projective Varieties.** This part will introduce the Weil Conjectures for any projective variety and illustrate how Theorem 3.13 is a special case of it.

Let $V/\mathbb{F}_q$ be a projective variety and $\mathbb{F}_{q^n}$ be the field extension of $\mathbb{F}_q$ of degree n. As before, we care about the number of points in our finite field on our variety, that is to say we care about the value of

$$|V(\mathbb{F}_{q^n})|$$

for different values of n. We are going to encode these values in a generating function.

Definition 4.12. The **zeta function** of $V/\mathbb{F}_q$ is the power series

$$Z(V/\mathbb{F}_q, T) = \exp\left(\sum_{n=1}^{\infty} |V(\mathbb{F}_{q^n})| \frac{T^n}{n}\right).$$

Remark 4.13. If we know the power series $Z(V/\mathbb{F}_q, T)$, then we can recover $|V(\mathbb{F}_{q^n})|$ through the equation

$$|V(\mathbb{F}_{q^n})| = \frac{1}{(n-1)!} \frac{d^n}{dT^n} \log(Z(V/\mathbb{F}_q, T))\Big|_{T=0}.$$

Therefore, knowing more about the power series will undoubtedly prove to be useful.

In [18], André Weil conjectured the following results about $Z(V/\mathbb{F}_q, T)$.

Theorem 4.14. *(Weil Conjectures) Let $V/\mathbb{F}_q$ be a smooth projective variety of dimension N. Then the following statements about $Z(V/\mathbb{F}_q, T)$ hold.*

(a) Rationality: One has $Z(V/\mathbb{F}_q, T) \in \mathbb{Q}(T)$.

(b) Functional Equation: Let $\varepsilon = \chi(V)$ be the Euler characteristic of the variety V. Then

$$Z\left(V/\mathbb{F}_q, \frac{1}{q^N T}\right) = \pm q^{N\varepsilon/2} T^{\varepsilon} Z(V/\mathbb{F}_q, T).$$

(c) Riemann Hypothesis: The zeta function factors as

$$Z(V/\mathbb{F}_q, T) = \frac{P_1(T)P_3(T)\cdots P_{2N-1}(T)}{P_0(T)P_2(T)\cdots P_{2N}(T)}$$

with $P_i(T) \in \mathbb{Z}[T]$, and

$$P_0(T) = 1 - T, \quad P_{2N}(T) = 1 - q^N T.$$

Over $\mathbb{C}$, each $P_i(T)$ factors as

$$P_i(T) = \prod_{j=1}^{b_i}(1 - \alpha_{ij}T) \quad \textit{with } |\alpha_{ij}| = q^{i/2}.$$

*The degree b_i of P_i is called the **i-th Betti number**. They are related to the Euler characteristic ε by the following equation, taken from* [12, II.26]*:*

$$\varepsilon = \sum_i (-1)^i b_i.$$

Remark 4.15. We can see that Theorem 3.13 and Theorem 4.9 are special cases of the Weil conjectures. We will explicitly check the case of elliptic curve, as the way it is written makes it not as obvious. Indeed, since $a \in \mathbb{Z}$, we indeed have

$$Z(E/\mathbb{F}_q, T) \in \mathbb{Q}(T),$$

giving us rationality. Moreover, since

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

setting $P_1(T) = 1 - aT + qT^2$, we get

$$Z(E/\mathbb{F}_q, T) = \frac{P_1(T)}{P_0(T)P_2(T)}$$

with $P_0(T) = 1 - T$ and $P_2(T) = 1 - qT$ as desired (since the dimension of E is $N = 1$.) Furthermore, because $P_1(T) = (1 - \alpha T)(1 - \beta T)$ and $|\alpha| = |\beta| = q^{1/2}$, each $P_i(T)$ factors as desired. We have the Riemann Hypothesis. Finally, for the functional equation, the Euler characteristic of E is given by

$$\varepsilon = \sum_{i=1}^{3}(-1)^i b_i = -1 + 2 - 1 = 0$$

so we should have the equation

$$Z\left(E/\mathbb{F}_q, \frac{1}{qT}\right) = Z(E/\mathbb{F}_q, T).$$

An immediate check shows the above functional equation holds.

Acknowledgments

I would like to thank my mentor Wei Yao for her guidance and support during this REU. Her detailed explanations have brought me invaluable insights and deepened my appreciation of algebraic geometry. Moreover, I would like to thank Peter May for organizing this wonderful REU, providing me with the opportunity to explore a subject I am passionate about.

References

[1] Atiyah, Michael, and Ian Macdonald. Introduction to Commutative Algebra. CRC Press, 1969.
[2] Brown, Ezra, and Bruce T. Myers. "Elliptic Curves from Mordell to Diophantus and Back." The American Mathematical Monthly, vol. 109, no. 7, Aug. 2002, p. 639, www.jstor.org/stable/3072428, https://doi.org/10.2307/3072428.
[3] Chahal, Jasbir S, and Brian Osserman. "The Riemann Hypothesis for Elliptic Curves." American Mathematical Monthly, vol. 115, no. 5, 1 May 2008, pp. 431–442, www.jstor.org/stable/27642503, https://doi.org/10.1080/00029890.2008.11920545.

[4] Deligne, Pierre. “La Conjecture de Weil. II.” Publications Mathématiques de L’IHÉS, vol. 52, no. 1, Dec. 1980, pp. 137–252, https://doi.org/10.1007/bf02684780. Accessed 30 Jan. 2023.
[5] Dummit, David Steven, and Richard M Foote. Abstract Algebra. Danvers, John Wiley & Sons, 2004.
[6] Elkies, Noam D. ”The Riemann zeta function and it’s functional equation”. 2003. ”https://people.math.harvard.edu/ elkies/M259.02/zeta1.pdf”
[7] Gathmann, Andreas. ”14. Divisors on Curves”. 2014. https://agag-gathmann.math.rptu.de/class/alggeom-2014/alggeom-2014-c14.pdf.
[8] Grothendieck, A., and J. Dieudonné. “Éléments de Géométrie Algébrique.” Publications Mathématiques de L’IHÉS, vol. 4, no. 1, Jan. 1960, pp. 5–214, https://doi.org/10.1007/bf02684778.
[9] H. Poincaré. “Sur Les Propriétés Arithmétiques Des Courbes Algébriques.” Journal de Mathématiques Pures et Appliquées, vol. 7, 1 Jan. 1901, pp. 161–234.
[10] Hankerson, Darrel R, et al. Guide to Elliptic Curve Cryptography. New York ; London, Springer, 2011.
[11] Hartshorne, Robin. Algebraic Geometry. Springer Science & Business Media, 29 June 2013.
[12] Milne, James S. Lectures on Étale Cohomology, V2.21. 22 Mar. 2013. https://www.jmilne.org/math/CourseNotes/LEC.pdf.
[13] Milne, James S. “The Riemann Hypothesis over Finite Fields: From Weil to the Present Day.” Notices of the International Congress of Chinese Mathematicians, vol. 4, no. 2, 2016, pp. 14–52, https://doi.org/10.4310/iccm.2016.v4.n2.a4.
[14] Rice, Adrian, and Ezra Brown. “Why Ellipses Are Not Elliptic Curves.” Mathematics Magazine, vol. 85, no. 3, June 2012, pp. 163–176, www.jstor.org/stable/10.4169/math.mag.85.3.163, https://doi.org/10.4169/math.mag.85.3.163.
[15] Silverman, Joseph H. The Arithmetic of Elliptic Curves. 2nd ed., New York, Springer-Verlag, 29 May 2009.
[16] Sutherland, Andrew. ”Isogeny kernels and division polynomials”. 2017. https://math.mit.edu/classes/18.783/2017/LectureNotes6.pdf
[17] Voight, John. “Curves over Finite Fields with Many Points: An Introduction.” CiteSeer X (the Pennsylvania State University), 1 Aug. 2005, math.dartmouth.edu/ jvoight/articles/pointscurves-moscow.pdf, ”https://doi.org/10.1142/9789812701640_0010.”
[18] Weil, André. ”Numbers of solutions of equations in finite fields.” Bulletin of the American Mathematical Society, 55(5) 497-508 May 1949.