ELLiptic CURVES AND THE Weil CONJECTURES

REBECCA GOLOVANOV

Abstract. This paper defines and explores arithmetic and geometric properties of elliptic curves. We will prove key results about elliptic curves, including their group law, and conclude with an application to a specific instance of the Weil Conjectures.

Contents

1. Introduction 1
2. Projective Varieties 2
3. Algebraic Curves 3
4. Divisors 4
5. Differentials and Riemann Roch Theorem 5
6. Elliptic Curves and Weierstrass Equations 7
7. Isogenies 10
8. Finite Fields and the Weil Conjectures 12
9. Appendix 17
Acknowledgments 18
References 18

1. Introduction

This paper provides a mostly self-contained exposition into elliptic curves, an essential component of algebraic geometry (we assume knowledge of some basic algebra). I will be adopting the algebraic geometry terminology and notation used in [1]. Elliptic curves are particularly interesting to study, as they are the first example of a variety that is also a group. This allows us to relate the geometry of the elliptic curve to its properties as an abelian group, which gives us an additional structure to work with. Their relation between different fields of mathematics has allowed for numerous theoretical advances, like the proof of Fermat’s Last Theorem, or as shown in this paper, their application to the Weil Conjectures.

In this paper we will briefly cover some definitions used in algebraic geometry. A canonical reference for this will be [2]. We will then develop some basic facts about curves which will be the foundation for constructing the group law on elliptic curves. Once we have the group law, it is natural to consider group homomorphisms between elliptic curves, known as isogenies. We will then apply this theory to the

Date: August 14, 2022.
Weil conjectures. In order to be rigorous, we need some terminology to build up machinery, which will be at the end of the paper in the form of an appendix.

2. Projective Varieties

This section will establish some preliminary terms we use throughout the paper. We let \( K \) denote a perfect field, and \( \bar{K} \) a fixed algebraic closure of \( K \). For the purposes of this paper, we will assume \( \text{char}(K) \neq 2 \) to avoid technical difficulties. The Galois group of the field extension \( \bar{K}/K \) is the set

\[
\{ \sigma : \bar{K} \to \bar{K} \mid \sigma \text{ is an automorphism over } \bar{K} \text{ fixing } K \}.
\]

We will denote this \( G_{\bar{K}/K} \).

**Remark 2.1.** As we transition to studying elliptic curves, \( K \) will be taken to be \( \mathbb{Q}, \mathbb{Q}_p, \mathbb{F}_p \), so it will be guaranteed to be perfect—refer to the appendix for why a perfect field is important.

Elliptic curves are defined in projective space, so it is necessary to establish what it means to work in projective space versus (the usual Euclidean) affine.

Affine \( n \)-space, denoted \( \mathbb{A}^n \), is also referred to as Cartesian \( n \)-space. Projective \( n \)-space can be intuitively understood as adding a point at infinity to affine space. Mathematically, a projective \( n \)-space, notated \( \mathbb{P}^n \), is the same as an affine \( n+1 \)-space modded out by an equivalence relation \((x_0, ..., x_n) \sim (y_0, ..., y_n)\) if there exists \( \lambda \in \bar{K} \) such that \( x_i = \lambda y_i \) for all \( i \). An equivalence class \( \{(\lambda x_0, ..., \lambda x_n) : \lambda \in \bar{K}\} \) is denoted \([x_0, ..., x_n]\) and \( x_0, ..., x_n \) are called homogeneous coordinates, which correspond to points in \( \mathbb{P}^n \).

**Remark 2.2.** \( G_{\bar{K}/K} \) acts on \( \mathbb{P}^n \) by acting on the homogeneous coordinates componentwise.

**Definition 2.3.** A polynomial \( f \in \bar{K}[x] = \bar{K}[x_0, ..., x_n] \) is homogeneous of degree \( d \) if \( f(\lambda x_0, ..., \lambda x_n) = \lambda^d f(x_0, ..., x_n) \) for all \( \lambda \in \bar{K} \). An ideal \( I \subset \bar{K}[x] \) is homogeneous if it is generated by homogeneous polynomials.

**Definition 2.4.** \( V \) is a projective variety if a homogeneous ideal \( I(V) \) is a prime ideal in \( \bar{K}[x_1, ..., x_n] \); in other words, it is the vanishing set of some homogeneous prime ideal in \( \bar{K}[x_1, ..., x_n] \).

We say \( V \) is smooth at a point \( P \) if \( V \cap \mathbb{A}^n \) is nonsingular at \( P \), i.e. the defining equations have at least one nonvanishing partial derivative. A function is regular at \( P \) if it is in the local ring of \( V \) at \( P \), denoted \( \bar{K}[V]_P \), which is \( \bar{K}[V] \) localized at \( P \). Regular functions can be locally defined by polynomials.

We want to restrict our study to Rational maps, which are geometric analogues for almost continuous maps that will allow us to associate varieties to their function fields. A rational map \( \phi : V_1 \to V_2 \) is a map that can be defined by \( \phi = [f_0, ..., f_n] \) where \( f_0, ..., f_n \in \bar{K}(V_1) \) and \( \phi(P) = [f_0(P), ..., f_n(P)] \in V_2 \), where \( \bar{K}(V_i) \) denotes the field of rational functions on \( V_i \). This domain \( \bar{K}(V) \) is the field of fractions of \( K[V] \), or the localization of \( K[V] \) at the ideal \((0)\). Essentially, these are maps that are locally fractions of polynomials. A rational map that is regular at every point (i.e. all \( f_i \) can be considered as elements of \( K[V_i] \)) is called a morphism. Morphisms will be the primary maps we use to study elliptic curves.
3. Algebraic Curves

A curve refers to a projective variety of dimension one—we use Hartshorne’s notion of dimension [2, I.1.6]. We begin by describing local rings at points on a smooth curve. We wish to construct a "valuation" on these rings which will give them the structure of discrete valuations rings (principal ideal domains with exactly one non-zero maximal ideal). This valuation will essentially mimic the role of an absolute value for functions which will give us information about the orders of the maximal ideals at points which the function divides. For more on this, read [2, I.6]

If $C$ is a curve and $P \in C$ is a smooth point, then it is known that $K[C]_P$ has the structure of a discrete valuation ring, i.e. there exists a valuation function on $K[C]_P$.

**Definition 3.1.** Let $C$ be a curve over the perfect field $K$, and let $M_P$ denote the maximal ideal of $P$ in the ring $K[C]$. The (normalized) valuation on $K[C]_P$ is given by

$$\ord_P : K[C]_P \to \mathbb{N} \cup \{\infty\},$$

$$\ord_P(f) = \sup\{d \in \mathbb{Z} : f \not\in M_P^d\}.$$  

Using $\ord_P(f/g) = \ord_P(f) - \ord_P(g)$, we can extend $\ord_P$ to $K(C)$:

$$\ord_P : K(C) \to \mathbb{Z} \cup \infty.$$  

A uniformizer for $C$ at $P$ is any function $t \in K(C)$ with $\ord_P(t) = 1$, or a generator for the ideal $M_P$.

Maximal ideals in $K[C]$, which consist of functions, correspond one to one with points on $C$. Thus, a point on $C$ corresponds to a maximal ideal $M_P$ in $K[C]$, which defines the valuation given by $P$. These facts are related to the Nullstellensatz, the theorem defining the relationship between geometry and algebra, and classical algebraic geometry.

**Definition 3.2.** Let $C$ and $P$ be as above, and let $f \in K(C)$. The order of $f$ at $P$ is $\ord_P(f)$. If $\ord_P(f) > 0$, then $f$ has a zero at $P$, and if $\ord_P(f) < 0$, then $f$ has a pole at $P$. If $\ord_P(f) \geq 0$, then $f$ is regular/defined at $P$ and we can evaluate $f(P)$. Otherwise $f$ has a pole at $P$ and $f(P) = \infty$.

**Proposition 3.3.** Let $C$ be a smooth curve and $f \in K(C)$ with $f \not= 0$. Then there are only finitely many poles or zeroes of $f$. If $f$ has no poles, then $f \in K$.

**Proof.** Look to [2, I.6.5] for a proof that there are finitely many poles. The proof is very similar for zeroes if we consider $1/f$ instead. Intuitively, the last statement makes sense because if $f$ has no poles, then $f(P)$ is defined for every $P$. There is no point at infinity, so values of $f$ can be defined solely in the affine coordinates of $K$. A rigorous proof can be found in [2, I.3.4a].

**Example 3.4.** Consider the curves $C_1 : Y^2 = X^3 + X$ and $C_2 : Y^2 = X^3 + X^2$. We will explicitly compute some orders on this curve to demonstrate how this works. Recall that $C_1$ and $C_2$ each have a single point at infinity. Let $P = (0, 0)$. The curve $C_1$ is smooth at $P$ and $C_2$ is not, because $C_2$ has a double root at $P$. We will calculate the orders of $Y$, $X$, and $2Y^2 - X$ for $C_1$ to demonstrate how this valuation works (since $C_1$ is nonsingular at $P$).
We are working in the ring of

\[ \frac{K[x, y]}{y^2 - x^3 - x}. \]

Let us begin with finding the order of \( Y \) at \( P \). We know \( y \notin M_P \) because \( M_P \) is generated by \((x, y)\). Now let us consider \( M_P^2 \), generated by \((x^2, y^2, xy)\). We can see \( Y \notin M_P^2 \) because \( Y \) cannot be generated by elements of the ideal or the ring. Then \( \text{ord}_P(Y) = 1 \)

We know \( X \in M_P \). Notice that \( X \in M_P^2 \) as well, because rearranging the polynomial yields \( x = y^2 - x^3 \), where \( x^3 \in M_P^2 \) because we can multiply \( x^2 \) by \( x \), an element of the ring, to get \( x^3 \). It then follows that \( x \in M_P^2 \). The maximal ideal of order 3 is \((x^3, y^3, xy^2, x^2y)\). It is clear \( x \not\in M_P^3 \), so \( \text{ord}_P(X) = 2 \)

Finally, let us consider \( 2Y^2 - X \). This expression is in \( M_P^2 \) because \( \text{ord}_P(Y^2) = 2 \) as we showed, as well as \( Y^2 \). It is not in \( M_P^3 \). Then \( \text{ord}_P(2Y^2 - X) = 2 \).

**Example 3.5.** Let a function \( f \in K(C) \) (where \( C/K \) is a smooth curve) define a rational map \( F : C \to \mathbb{P}^1 \) given explicitly by

\[
F(P) = \begin{cases} 
[f(P), 1] & \text{if } f \text{ is regular at } P, \\
[1, 0] & \text{if } f \text{ has a pole at } P.
\end{cases}
\]

Since \( C \) is smooth, \( F \) is a morphism.

If we define a rational map \( \phi : C \to \mathbb{P}^1 \), where \( \phi = [f, g] \), we have \( g = 0 \) where \( \phi \) is the constant map \( \phi = [1, 0] \). Otherwise, \( \phi \) corresponds to the function \( f/g \in K(C) \). When we denote \( \phi = [1, 0] \) by \( \infty \), hence ”adding a point at infinity”, we find a one to one correspondence

\[ K(C) \cup \{\infty\} \leftrightarrow \{\text{the maps } C \to \mathbb{P}^1 \text{ defined over } K\}. \]

**Theorem 3.6.** Let \( \phi : C_1 \to C_2 \) be a morphism of curves. Then \( \phi \) is either constant or surjective.

**Proof.** A proof can be found in [2, II.6.8] □

4. Divisors

We will now introduce the divisor group of a curve \( C \), denoted \( \text{Div}(C) \). A divisor \( D \in \text{Div}(C) \) is a summation of points on \( C \), formally denoted as

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

where \( n_P \in \mathbb{Z} \) and \( n_P = 0 \) for all but finitely many \( P \in C \). The degree of \( D \) is determined by the coefficient of each point, written as

\[ \deg D = \sum_{P \in C} n_P. \]

The divisors of degree 0 form a subgroup of \( \text{Div}(C) \), denoted by \( \text{Div}^0(C) \).

Let us assume \( C \) is smooth and let \( f \in \overline{K(C)}^* \). Then we can associate to \( f \) the divisor \( \text{div}(f) \), which we define to be

\[ \text{div}(f) = \sum_{P \in C} \text{ord}_P(f)(P). \]
If \( f \in K(C) \), then \( \text{div}(f) \in \text{Div}_K(C) \). Since each \( \text{ord}_P \) is a valuation, the map
\[
\text{div} : \overline{K}(C)^* \to \text{Div}(C)
\]
is a homomorphism of abelian groups. If \( f \in K(C) \) then it is not surjective to \( \mathbb{P}^1 \) because \( \text{div}(f) \) is defined over \( K \), so there are no poles.

**Definition 4.1.** A divisor \( D \in \text{Div}(C) \) is principal if it has the form \( D = \text{div}(f) \) for some \( f \in \overline{K}(C)^* \). Two divisors are linearly equivalent, written \( D_1 \sim D_2 \) if \( D_1 - D_2 \) is principal.

**Proposition 4.2.** Let \( C \) be a smooth curve and let \( f \in K(C)^* \).

1. \( \text{div}(f) = 0 \) if and only if \( f \in \overline{K}^* \).
2. \( \deg(\text{div}(f)) = 0 \).

**Proof.**

1. If \( \text{div}(f) = 0 \), then \( f \) has no poles, so the map \( f : C \to \mathbb{P}^1 \) is not surjective. Then by (3.8) the map is constant, so \( f \in \overline{K}^* \). The converse is the reverse: \( f \in \overline{K}^* \) implies a constant (and thus not surjective) map. Then \( f \) has no poles so \( \text{div}(f) \) must be 0.
2. Refer to [2, II.6.10]

The following example demonstrates a concrete use of the \( \text{div} \) function and Proposition 4.2.

**Example 4.3.** Let \( e_1, e_2, e_3 \in \overline{K} \) be distinct, and consider the curve
\[
C : y^2 = (x - e_1)(x - e_2)(x - e_3).
\]
The curve \( C \) is smooth with a single point at infinity, which we denote \( P_\infty \) (in fact, this is an elliptic curve). For \( i = 1, 2, 3 \) let \( P_i = (e_1, 0) \in C \). Then
\[
\text{div}(x - e_i) = 2(P_i) - 2(P_\infty).
\]
We can consider \( f = x - e_i \) to be rational in \( \overline{K}(C)^* \), with a zero at \( e_i \) and a pole at \( \infty \). This holds because principal divisors have degree 0. Since \( x - e_i \) has a 0 of order 2 at \( P_i \) and a pole of order 2 at \( P_\infty \), we have our result. Similarly, for \( y \) we have
\[
\text{div}(y) = (P_1) + (P_2) + (P_3) - 3(P_\infty),
\]
where \( y \in K(C) \), and \( y \) has zeroes at \( P_1, P_2, P_3 \), and symmetrically a pole of order 3 at \( P_\infty \), meaning \( \deg \text{div}(y) = 0 \).

5. **Differentials and Riemann Roch Theorem**

We can now proceed to discuss the space of differential forms on a curve, which will be essential for illustrating the group law between points on a curve. Most of the differential analysis is beyond the scope of this paper, but this section is necessary to introduce canonical divisors. These particular divisors are meaningfully associated to an invariant of the curve, the genus. The Riemann Roch theorem, a fundamental result of algebraic geometry, will be the whole reason the group law works on elliptic curves, which are defined to be genus 1. The space of (meromorphic) differential forms on \( C \) is denoted by \( \Omega_C \).

Similarly to our original divisor definition, for an \( \omega \in \Omega_C \), the valuation \( \text{ord}_P(\omega) = 0 \) for all but finitely many \( P \in C \).
For an $\omega \in \Omega_c$, the associated divisor is
\[
\text{div}(\omega) = \sum_{P \in C} \text{ord}_P(\omega)(P) \in \text{Div}(C).
\]

The differential is regular and holomorphic if $\text{ord}_P(\omega) \geq 0$ for all $P \in C$. It is nonvanishing if $\text{ord}_P(\omega) \leq 0$ for all $P \in C$.

**Definition 5.1.** The canonical divisor class on $C$ is the image in $\text{Pic}(C)$ of $\text{div}(\omega)$ for any nonzero differential $\omega \in \Omega_C$. The group $\text{Pic}(C)$ (Picard group) denotes the quotient of $\text{Div}(C)$ by its subgroup of principal divisors. Any divisor in this divisor class is called a canonical divisor. A canonical class is an invariant associated to a curve.

We use these divisors to discuss Riemann Roch. Before doing that, we introduce a partial ordering on divisors. A divisor is positive if every coefficient $n_P$ is greater than or equal to 0. We can compare divisors $D_1, D_2$ by declaring $D_1 \geq D_2$ if $D_1 - D_2$ is positive.

Consider a function $f \in \overline{K}(C)^*$ with a pole of order at most $n$ at a point $P$. By the definition of $\text{div}(f)$, we can now say that
\[
\text{div}(f) \geq -n(P).
\]

We can also denote a 0 at a point $Q$ by writing
\[
\text{div}(f) \geq (Q) - n(P).
\]

**Definition 5.2.** Let $D \in \text{Div}(C)$. We define the set of functions
\[
\mathcal{L}(D) = \{f \in \overline{K}(C)^* : \text{div}(f) \geq -D\} \cup \{0\}.
\]

The set $\mathcal{L}(D)$ is a finite dimensional $\overline{K}$-vector space. We denote its dimension as a $\overline{K}$ vector space by
\[
\ell(D) = \dim_{\overline{K}} \mathcal{L}(D).
\]

This number is always finite.

We have the following facts about this vector space. If $\deg D < 0$, then
\[
\mathcal{L}(D) = 0 \text{ and } \ell(D) = 0.
\]

Moreover, this vector space is invariant under linear equivalence: in other words, if $D' \in \text{Div}(C)$ is linearly equivalent to $D$, then $\mathcal{L}(D) \cong \mathcal{L}(D')$, and so $\ell(D) = \ell(D')$. For a proof, see [1] [2,II.5.19].

**Example 5.3.** Let $K_C \in \text{Div}(C)$ be a canonical divisor on $C$, say $K_C = \text{div}(\omega)$. Then each function $f \in \mathcal{L}(K_C)$ has the property that
\[
\text{div}(f) \geq -\text{div}(\omega), \text{ so } \text{div}(f\omega) \geq 0.
\]

Then $f\omega$ is holomorphic. If $f\omega$ is holomorphic, then $f \in \mathcal{L}(K_C)$. Since every differential on $C$ has the form $f\omega$ for some $f$, we have an isomorphism of $\overline{K}$-vector spaces:
\[
\mathcal{L}(K_C) \cong \{\omega \in \Omega_C : \omega \text{ is holomorphic}\}.
\]

The dimension $\ell(K_C)$ is an important invariant of the curve $C$. 
Our combined analysis of differentials and divisors has now prepared us to state the Riemann Roch theorem. This theorem determines the genus of a curve, a major topological invariant. The genus is frequently referred to as the number of ‘holes’ of a surface, and its invariant nature is responsible for that joke about topologists being unable to differentiate between their donuts and their coffee mugs. Riemann Roch is also key in justifying the group law on elliptic curves.

**Theorem 5.4.** (Riemann-Roch) Let $C$ be a smooth curve and let $K_C$ be a canonical divisor on $C$. There is an integer $g \geq 0$, called the genus of $C$, such that for every divisor $D \in \text{Div}(C)$,

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

**Proof.** For an elementary proof by Weil, look to [4, 1]. There is a proof using Serre duality in [2, 4.1] □

**Corollary 5.5.**

1. $\ell(K_C) = g$.
2. $\deg K_C = 2g - 2$.
3. If $\deg D > 2g - 2$, then

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

**Proof.**

1. Take $D = 0$. Note that $\mathcal{L}(0) = \overline{K}$ from Proposition 3.3, so $\ell(0) = 1$. Putting this into the given equation of Theorem 5.4, we obtain the desired result.
2. Set $D = K_C$ and use part (1). We have

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

$$g - 1 = \deg K_C - g - 1$$

$$2g - 2 = \deg K_C$$

3. Since $\deg D > 2g - 2$, we have $\deg D > \deg K_C$ from (2), which implies $\deg(K_C - D) < 0$. Thus, we have $\ell(K_C - D) = 0$. When we apply Riemann Roch, the desired result immediately follows. □

### 6. Elliptic Curves and Weierstrass Equations

We can now define elliptic curves. **Elliptic curves** are smooth, projective algebraic curves of genus one that have a fixed base point. Every elliptic curve can be written as the locus in $\mathbb{P}^2$ of a cubic equation with one point (the base point) on the line at $\infty$. After $X$ and $Y$ are scaled, an elliptic curve has an (Weierstrass) equation of the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

where $O = [0, 1, 0]$ is the base point and $a_1, \ldots, a_6 \in \overline{K}$.

We generally write the Weierstrass equation using non-homogeneous coordinates $x = X/Z$ and $y = Y/Z$.

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

If $a_1, \ldots, a_6 \in K$, then $E$ is said to be defined over $K$. Algebraic computations with these equations can be used to justify a number of theorems about elliptic curves (in fact, they have been used to prove the group law indeed creates an abelian
group), but those are both tedious and not relevant to this paper. [1, III] covers
them in depth for those curious.

There is a composition law on elliptic curves using Riemann Roch that is anal-
ogous to a geometric calculation.

Definition 6.1. Let $P, Q \in E$, let $L$ be the line through $P$ and $Q$ (if $P = Q$, let
$L$ be the tangent line to $E$ at $P$), and let $R$ be the third point of intersection of $L$
with $E$. Let $L'$ be the line through $R$ and $O$. Then $L'$ intersects $E$ at $R, O,$ and a
third point. Denote that third point by $P \oplus Q$.

The composition law makes $E$ into an abelian group with identity element $O$
There is a computational proof in [1,III.2.2].

We will first prove the algebraic group law, and then explain how the geometric
composition is identical. Recall that two divisors $P, Q$ are equivalent, denoted
$P \sim Q$, if $P - Q = \text{div}(f)$ for some $f \in \overline{K}(C)^*$

Proposition 6.2. Let $C$ be a smooth curve of genus one, and fix a base point
$P_0 \in C$. For all $P, Q \in C$ there exists a unique $R \in C$ such that

$$(P) + (Q) \sim (R) + (P_0).$$

Denote this point $R$ by $\sigma(P, Q)$.

Proof. Pick a divisor $D$ such that $D = P + Q - P_0$. Since $D$ is a point, we know
deg($D$) = 1, so deg($D$) > 2$g$ − 2 = 0. We can then use part 3 of Corollary 5.5 to
g et

$$\ell(D) = \text{deg}(D) - g + 1
= 1 - 1 + 1 = 1$$
Since $\ell(D) > 0$, there exist nonconstant, nontrivial functions in $L(D)$. Choose such
a function $f$. From our partial ordering on divisors, we see that

$$\text{div}(f) \geq -(P) - (Q) + (P_0).$$

We need deg div($f$) = 0 by part 1 of Proposition 4.2. $R$ is the unique point such that

$$\text{div}(f) = -(P) - (Q) + (P_0) + (R).$$
Since this difference is principal, we have $(P) + (Q) \sim (P_0) + (R)$. \hfill \Box

The function $\sigma : C \times C \to C$ makes an abelian group with identity element $P_0$.

Proof.

(1) **Commutativity:** This property is easy to see as the divisors themselves
are commutative, so for points $P, Q$ we know $P + Q = Q + P$, meaning
$P + Q \sim Q + P \sim R + P_0$.

(2) **Identity Element:** We want for every $P \in C$, $P + P_0 - P_0 \sim P$. Then the
$P_0$ cancels, and $P$ is understood to be linearly equivalent to itself $P \sim P$
so we are done.

(3) **Inverse:** We want to show that for every $P$, there exists a unique $P'$ such
that $P + P' - P_0 \sim P_0$. 


Pick a divisor \( D = 2(P_0) - P \). We know \( \ell(D) = 1 \) from Corollary 5.5, which means there is a nontrivial \( f \in L(D) \). Then we have

\[
\text{div}(f) \geq -D \\
\text{div}(f) \geq P - 2P_0
\]

Then \( P' \) is the unique point satisfying \( \text{div}(f) = P - 2P_0 + P' \), so we have \( P + P' \sim 2P_0 \). Since \( P_0 \) is the identity, we know \( P + P' \sim P_0 \), and we have proven the existence of an inverse.

(4) \textbf{Associativity} For clarity, I will define \( \oplus \) such that \( P \oplus Q \sim P + Q - P_0 \).

We want \( (P \oplus Q) \oplus R \sim P \oplus (Q \oplus R) \).

We know there are unique points \( U, V \), such that \( U \sim P \oplus Q \sim P + Q - P_0 \) and \( V \sim Q + R - P_0 \). While it seems trivial, let us note that \( P + Q - P_0 + R - P_0 \sim P + Q + R - P_0 - P_0 \). Using our definitions of \( U \) and \( V \), we have

\[
U + R - P_0 \sim P + V - P_0 \\
U \oplus R \sim P \oplus V \\
(P \oplus Q) \oplus R \sim P \oplus (Q \oplus R)
\]

and we have verified the last property of abelian groups.

\[\square\]

We know there exists a function \( f \in \overline{K}(C)^* \) such that \( \text{div}(f) = P + Q - O - R \).

We can define \( f \) as precisely the product of lines \( L \) and \( L' \), where the vanishing set is the geometry of the two lines. Then we have our unique \( R \).

\textbf{Proposition 6.3}. \textit{Suppose \( E \) is defined over \( K \). Then}

\[
E(K) = \{(x, y) \in K^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}
\]

is a subgroup of \( E \).

\textbf{Proof}. A proof can be found in [1, III.2.2] \[\square\]

From here, we replace \( \oplus \) and \( \ominus \) with \( + \) and \( - \) for the group operation on \( E \). For \( m \in \mathbb{Z} \) and \( P \in E \), we define

\[
[m]P = P + \ldots + P, \quad [m]P = -P - \ldots - P, \quad [0]P = O.
\]

In a way this is a "multiplication by \( m \)" operation on the elliptic curve. This will be quite important later and it an example of a group homomorphism from an elliptic curve to itself. We will now discuss group homomorphisms between elliptic curves in general.
7. Isogenies

We will now briefly study rational maps between elliptic curves which are also homomorphisms preserving the group structure. We want to obtain an injection of function fields such as $\phi^*: \overline{K}(E_2) \to \overline{K}(E_1)$ to more rigorously discuss isogenies. In particular, we want to be able to study the Frobenius morphism when considering elliptic curves over finite fields.

Let $C_1/K$ and $C_2/K$ be curves and let $\phi: C_1 \to C_2$ be a nonconstant rational map defined over $K$. Composition with $\phi$ induces an injection of function fields fixing $K$, $\phi^*: K(C_2) \to K(C_1)$, $\phi^* f = f \circ \phi$.

The basis of algebraic geometry is the ability to categorically relate maps between varieties to those between function fields. This injection allows us to "pull-back" rational functions along a rational map.

We use the following algebraic facts:

**Proposition 7.1.** Let $C/K$ be a curve, and let $t \in K(C)$ be a uniformizer at some nonsingular point $P \in C(K)$. Then $K(C)$ is a finite separable extension of $K(t)$.

**Proof.** We omit this proof for the focus of the paper, but one can be found [1, II.1.4].

A separable extension is generally a nice extension to work with because of its nonsingular nature. Refer to the appendix for a more detailed explanation.

**Proposition 7.2.** Let $C$ be a curve, let $V \subset \mathbb{P}^N$ be a variety, let $P \in C$ be a smooth point, and let $\phi: C \to V$ be a rational map. Then $\phi$ is regular at $P$. In particular, if $C$ is smooth, then $\phi$ is a morphism.

**Proof.** Let $\phi = [f_0, ..., f_N]$ with functions $f_i \in K(C)$, and choose a uniformizer $t \in K(C)$ for $C$ at $P$. Let $n = \min_{0 \leq i \leq N} \text{ord}_P(f_i)$. Then $\text{ord}_P(t^{-n} f_i) \geq 0$ for all $i$ and $\text{ord}_P(t^{-n} f_j) = 0$ for some $j$. Then every $t^{-n} f_i$ is regular at $P$, and $(t^{-n} f_j)(P) \neq 0$. Then $\phi$ is regular at $P$.

This injection and Corollary 7.5 demonstrate how we can analyze function fields through their corresponding curves.

**Definition 7.3.** Let $\phi: C_1 \to C_2$ be a map of curves defined over $K$. If $\phi$ is constant, the degree of $\phi$ is 0. Otherwise $\phi$ is a finite map and the degree is defined as $\text{deg} \phi = [K(C_1) : \phi^* K(C_2)]$.

**Definition 7.4.** Let $\phi: C_1 \to C_2$ be a nonconstant map of curves defined over $K$. We know $K(C_1)$ is a finite extension of $\phi^* K(C_2)$ [1,II.2.4a]. We can use the norm map relative to $\phi^*$ to define a map in the other direction:

$\phi_*: K(C_1) \to K(C_2)$, $\phi_* = (\phi^*)^{-1} \circ N_{K(C_1)/\phi^* K(C_2)}$.

Where $N_{K(C_1)/\phi^* K(C_2)}$ denotes the usual number theoretic norm map of field extensions.

**Corollary 7.5.** Let $C_1$ and $C_2$ be smooth curves, and let $\phi: C_1 \to C_2$ be a map of degree one. Then $\phi$ is an isomorphism.
Proof. By definition, deg $\phi = 1$ implies $\phi^* \overline{K}(C_2) = \overline{K}(C_1)$, so $\phi^*$ is an isomorphism of function fields. Then from [1, II.2.4b], there is a rational map $\psi : C_2 \to C_1$ that corresponds to $(\phi^*)^{-1} : \overline{K}(C_1) \to \overline{K}(C_2)$ such that $\psi^* = (\phi^*)^{-1}$. Since $C$ is smooth, we know it is a morphism. Since $(\phi \circ \psi)^* = \psi^* \circ \phi^*$ is the identity map on $\overline{K}(C_2)$ and $(\psi \circ \phi)^* = \phi^* \circ \psi^*$ is the identity map on $\overline{K}(C_1)$, it follows that $\phi \circ \psi$ and $\psi \circ \phi$ are, respectively, the identity maps on $C_2$ and $C_1$. Then $\phi$ and $\psi$ are isomorphisms. □

This corollary is particularly important, as the invertibility of an isomorphism implies an equivalence of categories, where smooth curves with rational maps correspond to finitely generated field extensions $K/K$ with field injections fixing $K$. We can visualize this as

$C/K \rightarrow K(C)$

$\phi : C_1 \rightarrow C_2 \rightarrow \phi^* : K(C_2) \rightarrow K(C_1)$

Isogenies are special because they preserve the unique 0 point of elliptic curves. In particular, isomorphisms between curves are also isogenies. Two curves $E_1, E_2$, are isogenous if there is a nonzero isogeny $\phi : E_1 \rightarrow E_2$. Then an isogeny is either $\phi(E_1) = \{O\}$ or $\phi(E_1) = E_2$,

so except for the zero isogeny ($(0)(P) = O$ for all $P \in E_1$), every other isogeny is a finite map of curves. Then we obtain the desired injection of function fields.

$\phi^* : \overline{K}(E_2) \rightarrow \overline{K}(E_1)$.

The degree of $\phi$, denoted by $\deg \phi$, is the degree of the finite extension $\overline{K}(E_1)/\phi^* \overline{K}(E_2)$. By convention we set $\deg[0] = 0$, so that $\deg(\psi \circ \phi) = \deg(\psi) \deg(\phi)$ for all chains of isogenies.

Elliptic curves are abelian groups, so maps between them preserve group structure. We denote this set of isogenies from $E_1$ to $E_2$ by

$\text{Hom}(E_1, E_2) = \{\text{isogenies } E_1 \rightarrow E_2\}$.

The sum of two isogenies is

$(\phi + \psi)(P) = \phi(P) + \psi(P)$.

The algebraic derivations of elliptic curves in [1, III.3] imply that $\phi + \psi$ is a morphism, so it is an isogeny. Then $\text{Hom}(E_1, E_2)$ is a group.

If $E_1 = E_2$, we can compose isogenies. We let the endomorphism ring $\text{End}(E) = \text{Hom}(E, E)$ have the same addition law as above and whose multiplication is the composition

$(\phi \psi)(P) = \phi(\psi(P))$.

The invertible elements of $\text{End}(E)$ form the automorphism group of $E$, denoted by $\text{Aut}(E)$.

Example 7.6. For each $m \in \mathbb{Z}$ we define the multiplication-by-$m$ isogeny

$[m] : E \rightarrow E$

in the natural way. One can inductively show $[m]$ is a morphism, hence an isogeny, as it sends $O$ to $O$.
Example 7.7. Let $K$ be a field of characteristic $p > 0$, let $q = p^r$, and let $E/K$ be an elliptic curve given by a Weierstrass equation. Recall that the curve $E^{(q)}/K$ is defined by raising the coefficients of the equation for $E$ to the $q^{th}$ power, and the Frobenius morphism $\phi_q$ is defined by

$$\phi_q : E \to E^{(q)}, \ (x, y) \mapsto (x^q, y^q).$$

Since $E^{(q)}$ is the zero locus of a Weierstrass equation, it will be an elliptic curve when the equation is nonsingular. We know the $q^{th}$-power map $K \to K$ is a homomorphism. The computation omitted here can be found in [1, III.1 and III.4.6], and we find that the equation for $E^{(q)}$ is nonsingular.

Suppose $K = F_q$ is a finite field with $q$ elements. Then the $q^{th}$-power map on $K$ is the identity and $\phi_q$ is an endomorphism of $E$, called the Frobenius endomorphism. The set of points fixed by $\phi_q$ is the finite group $E(F_q)$, an essential fact for estimating the cardinality of $E(F_q)$.

The following corollary is used in proofs of Hasse’s theorem as well as in the Weil conjectures; the proof relies on the invariant differential and is in [1,III.5.5]

Corollary 7.8. Let $E$ be an elliptic curve defined over a finite field $F_q$ of characteristic $p$, let $\phi : E \to E$ be the $q^{th}$-power Frobenius morphism, and let $m, n \in \mathbb{Z}$. Then the map

$$m + n\phi : E \to E$$

is separable if and only if $p \nmid m$. The map $1 - \phi$ is separable.

The fact that $1 - \phi$ is separable is essential to understand how the Frobenius endomorphism relates to the number of solutions to elliptic curves over finite fields.

8. Finite Fields and the Weil Conjectures

We now have enough information to discuss an important result about elliptic curves. First, we will discuss properties of the Frobenius map of elliptic curves over finite fields, followed by a proof of one of Hasse’s theorems, estimating the number of points on the elliptic curve in a finite field. We will then proceed to the Weil conjectures, which generally concern the number of points on varieties defined over finite fields. While parts are still open, it has been solved for elliptic curves. Throughout this section, we let $q$ be a power of a prime $p$, and let $\overline{F}_q$ be a finite field with $q$ elements. As usual, $\overline{F}_q$ will denote a fixed algebraic closure of $F_q$.

Let us define the Frobenius map. Let $q = p^r$. For any polynomial $f \in K[X]$, let $f^{(q)}$ be the polynomial obtained from $f$ by raising each coefficient of $f$ to the $q^{th}$ power. Then for any curve $C/K$, we can define a new curve $C^{(q)}/K$ as the curve whose homogeneous ideal is given by

$$I(C^{(q)}) = \text{ideal generated by } \{f^{(q)} : f \in I(C)\}.$$ 

There is a natural map from $C$ to $C^{(q)}$, called the $q^{th}$ -power Frobenius morphism, given by

$$\phi : C \to C^{(q)}, \ \phi([x_0, ..., x_n]) = [x_0^q, ..., x_n^q].$$

When working in fields of characteristic $p > 0$, especially finite fields, we find that the Galois Group of the field is cyclic, generated by the Frobenius map. The Frobenius automorphism will be useful for our proof of the Weil Conjectures on elliptic curves over finite fields.
Proposition 8.1. Let $K$ be a field of characteristic $p > 0$, let $q = p^r$, let $C/K$ be a curve, and let $\phi : C \to C^{(q)}$ be the $q^{th}$-power Frobenius morphism.

1. $\phi^* K(C^{(q)}) = K(C)^q = \{ f^q : f \in K(C) \}$.
2. $\phi$ is purely inseparable.
3. $\deg \phi = q$.

Proof.

(1) Since $K(C)$ consists of quotients $f/g$ (1.2.9) of homogeneous polynomials of the same degree, we see that $\phi^* K(C^{(q)})$ is the subfield of $K(C)$ given by quotients

$$\phi^* \left( \frac{f}{g} \right) = \frac{f(X_0^q, \ldots, X_n^q)}{g(X_0^q, \ldots, X_n^q)}.$$

We then see that $K(C)^q$ is the subfield of $K(C)$ given by the quotients

$$\frac{f(X_0^q, \ldots, X_n^q)}{g(X_0^q, \ldots, X_n^q)}$$

but since $K$ is perfect, we know every element of $K$ is a $q^{th}$ power, so

$$(K[X_0, \ldots, X_n])^q = K[X_0^q, \ldots, X_n^q].$$

Then the sets $f(X_i^q)/g(X_i^q)$ and $f(X_i)/g(X_i)$ give the same subfield of $K(C)$.

(2) Immediately follows from (1).

(3) In [1, II.2.11c]

□

Corollary 8.2. Every map $\psi : C_1 \to C_2$ of (smooth) curves over a field of characteristic $p > 0$ factors as

$$C_1 \xrightarrow{\phi} C_1^{(q)} \xrightarrow{\lambda} C_2,$$

where $q = \deg(\psi)$, the map $\phi$ is the $q^{th}$-power Frobenius map, and the map $\lambda$ is separable.

Proof. Let $K$ be the separable closure of $\psi^* K(C_2)$ in $K(C_1)$. Then $K(C_1)/K$ is purely inseparable of degree $q$, so $K(C_1)^q \subset K$. From parts 1 and 3 of Proposition 8.1 we have

$$K(C_1)^q = \phi^* (K(C_1^{(q)}))$$

and $\left[ K(C_1) : \phi^* (K(C_1^{(q)})) \right] = q$.

Then $K = \phi^* (C_1^{(q)})$. We then have a tower of function fields

$$K(C_1)/\phi^* K(C_1^{(q)})/\psi^* K(C_2),$$

and from [1, II.2.4b] this corresponds to maps

$$C_1 \xrightarrow{\phi} C_1^{(q)} \xrightarrow{\lambda} C_2 \xrightarrow{\psi} C_2.$$

□

This corollary shows that the only inseparable part of any map $\psi : C_1 \to C_2$ is the Frobenius map. Factoring it out leaves us with a nice separable map. Let $E/F_q$ be an elliptic curve defined over a finite field. We want to estimate the number of
points in $E(\mathbb{F}_q)$, which is also the number of solutions to the equation defining $E$ plus the point at infinity. A trivial upper bound is
\[ #E(\mathbb{F}_q) \leq 2q + 1, \]
as each value of $x$ would yield at most two values for $y$. However, we believe the order of magnitude should be $q$ instead, as there is an approximately 50% chance a quadratic equation will be solvable in $\mathbb{F}_q$. Hasse’s theorem rigorously justifies this reasoning.

**Theorem 8.3. (Hasse)** Let $E/\mathbb{F}_q$ be an elliptic curve defined over a finite field. Then
\[ |#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}. \]
We are on an order of magnitude $q$, with a maximum error of $2\sqrt{q}$.

**Proof.** Choose a Weierstrass equation for $E$ defined over $\mathbb{F}_q$, and let $\phi : E \to E$, $(x, y) \mapsto (x^q, y^q)$, be the $q$th-power Frobenius morphism (Example 7.7). Since the Galois group $G_{\mathbb{F}_q}/\mathbb{F}_q$ is generated by the $q$th-power map on $\mathbb{F}_q$, then for any point $P \in E(\mathbb{F}_q)$, the point $P$ is in $P \in E(\mathbb{F}_q)$ if and only if $\phi(P) = P$. Then $E(\mathbb{F}_q) = \ker(1 - \phi)$.

Using Corollary 7.8 and [1, III.4.10c] (which states that if $\phi$ is separable, then $\# \ker \phi = \deg \phi$), we have
\[ #E(\mathbb{F}_q) = \# \ker(1 - \phi) = \deg(1 - \phi). \]
The degree map on $\text{End}(E)$ is a positive definite quadratic form and $\deg \phi = q$. A version of the Cauchy Schwarz inequality, detailed in [1, V.1.2], yields our result. \qed

We will now proceed to studying the Weil Conjectures, which, if generally proven, have immense number-theoretical implications, such as proving the Riemann Hypothesis for varieties over finite fields. We will prove them for elliptic curves, and adopt the following notation from [1.V]:

For each integer $n \geq 1$, let $\mathbb{F}_{q^n}$ be the extension of $\mathbb{F}_q$ of degree $n$, meaning $\# \mathbb{F}_{q^n} = q^n$. We define $V/\mathbb{F}_q$ to be a projective variety, where $V(\mathbb{F}_{q^n})$ is the set of points of $V$ with coordinates in $\mathbb{F}_{q^n}$.

**Definition 8.4.** The zeta function of $V/\mathbb{F}_q$ is the power series
\[ Z(V/\mathbb{F}_q; T) = \exp \left( \sum_{n=1}^{\infty} \frac{\# V(\mathbb{F}_{q^n})}{n} T^n \right). \]

For any power series $F(T) \in \mathbb{Q}[[T]]$ with no constant term, the power series $\exp(F(T))$ is defined to be $\sum_{k \geq 0} F(T)^k / k!$. If we know the series $Z(V/\mathbb{F}_q; T)$, then we can find $\# V(\mathbb{F}_{q^n})$ with the formula
\[ \# V(\mathbb{F}_{q^n}) = \frac{1}{(n-1)!} \frac{d^n}{dT^n} \log Z(V/\mathbb{F}_q; T) \big|_{T=0}. \]

**Example 8.5.** Let $V = \mathbb{P}^N$. A point of $V(\mathbb{F}_{q^n})$ is given by homogeneous coordinates $[x_0, ..., x_N]$ with at least one $x_i$ nonzero. Then
\[ \# V(\mathbb{F}_{q^n}) = \frac{q^n(N+1)}{q^n - 1} = \sum_{i=0}^{N} q^{ni}, \]
so
\[
\log Z(\mathbb{P}^n/\mathbb{F}_q; T) = \sum_{n=1}^{\infty} \left( \sum_{i=0}^{N} q^{ni} \right) \frac{T^n}{n} = \sum_{i=0}^{N} \frac{-\log(1 - q^i T)}{n}.
\]

Then we have
\[
Z(\mathbb{P}^n/\mathbb{F}_q; T) = \frac{1}{(1 - T)(1 - qT) \cdots (1 - q^N T)}.
\]

where the zeta function is in \( \mathbb{Q}(T) \). If there are numbers \( \alpha_1, \ldots, \alpha_r \in \mathbb{C} \) such that \( \# V(\mathbb{F}_q^n) = \pm \alpha_1^n \pm \cdots \pm \alpha_r^n \) for all \( n \in \mathbb{Z}, n > 0 \), then the zeta function is rational.

**Theorem 8.6. (Weil Conjectures)** Let \( V/\mathbb{F}_q \) be a smooth projective variety of dimension \( N \).

1. **Rationality**
   
   \( Z(V/\mathbb{F}_q; T) \in \mathbb{Q}(T) \).

2. **Functional Equation**
   There is an integer \( \epsilon \), called the Euler characteristic of \( V \), such that
   \[
   Z(V/\mathbb{F}_q; 1/q^N T) = \pm q^{N\epsilon/2} Z(V/\mathbb{F}_q; T).
   \]

3. **Riemann Hypothesis**
   The zeta function factors as
   \[
   Z(V/\mathbb{F}_q; T) = \frac{P_1(T) \cdots P_{2N-1}(T)}{P_0(T) P_2(T) \cdots P_{2N}(T)}
   \]
   with each \( P_i(T) \in \mathbb{Z}[T] \), with \( P_0(T) = 1 - T \) and \( P_{2N}(T) = 1 - q^N T \), and for every \( 0 \leq i \leq 2N \), the polynomial \( P_i(T) \) factors over \( \mathbb{C} \) as
   \[
   P_i(T) = \prod_{j=1}^{b_i} (1 - \alpha_{ij} T) \text{ with } |\alpha_{ij}| = q^{\frac{i}{2}}.
   \]

We want to prove the above conjectures for elliptic curves, but we have to prove some key results about elliptic curves first. [1, III.7] discusses \( l \)-adic numbers regarding elliptic curves. This is beyond the scope of the paper, but the following proposition takes the ability to compute the determinant \( (\det(\psi_1)) \) and trace \( (\text{tr}(\psi_1)) \) of an \( l \)-adic map \( \psi_1 \) when \( \psi \in \text{End}(E) \), and demonstrates the values are independent of \( l \). It allows us to compute these values without worrying about the \( l \)-adic number system.

**Proposition 8.7.** Let \( \psi \in \text{End}(E) \). Then \( \det(\psi_1) = \deg(\psi) \) and \( \text{tr}(\psi_1) = 1 + \deg(\psi) - \deg(1 - \psi) \). In fact, \( \det(\psi_1) \) and \( \text{tr}(\psi_1) \) are in \( \mathbb{Z} \) and are independent of \( l \).

**Proof.** See [1, III.8.6] \( \square \)

We can apply the above proposition to an elliptic curve over a finite field, which will lead us to an important property of the Frobenius endomorphism.

**Theorem 8.8.** Let \( E/\mathbb{F}_q \) be an elliptic curve, let \( \phi : E \to E, (x, y) \mapsto (x^q, y^q) \), be the \( q \)-th power Frobenius endomorphism, and let \( a = q + 1 - \# E(\mathbb{F}_q) \).

1. Let \( \alpha, \beta \in \mathbb{C} \) be the roots of the polynomial \( T^2 - aT + q \). Then \( \alpha \) and \( \beta \) are complex conjugates satisfying \( |\alpha| = |\beta| = \sqrt{a} \), and for every \( n \geq 1 \),
   \[
   \# E(\mathbb{F}_q^n) = q^n + 1 - \alpha^n - \beta^n.
   \]

2. The Frobenius endomorphism satisfies \( \phi^2 - a\phi + q \in \text{End}(E) \).
Proof. We observed earlier that \( \#E(\mathbb{F}) = \deg(1 - \phi) \). We can use Proposition 8.7 to compute
\[
\det(\phi_l) = \deg(\phi) = q
\]
\[
\text{tr}(\phi_l) = 1 + \deg(\phi) - \deg(1 - \phi) = 1 + q - \#E(\mathbb{F}_q) = a.
\]
So the characteristic polynomial of \( \phi_l \) is
\[
\det(T - \phi_l) = T^2 - \text{tr}(\phi_l)T + \det(\phi_l) = T^2 - aT + q.
\]
(1) Since the characteristic polynomial of \( \phi_l \) has coefficients in \( \mathbb{Z} \), we can factor it over \( \mathbb{C} \) as
\[
\det(T - \phi_l) = (T - \alpha_n)(T - \beta_n).
\]
Then the polynomial \( \det(T - \phi_l) = T^2 - aT + q \in \mathbb{Z}[T] \) is nonnegative for all \( T \in \mathbb{R} \), so either it has complex conjugate roots or it has a double root. Either way, we have \( |\alpha| = |\beta| \), and from
\[
\alpha \beta = \det \phi_l = \deg \phi = q,
\]
we find that
\[
|\alpha| = |\beta| = \sqrt{q},
\]
which proves the first part of a).

For each integer \( n \geq 1 \), the \((q^n)^{th}\)-power Frobenius endomorphism satisfies \( \#E(\mathbb{F}_{q^n}) = \deg(1 - \phi^n) \). Putting \( \phi_l \) into Jordan normal form, so it is upper triangular with \( \alpha \) and \( \beta \) on the diagonal, shows that the characteristic polynomial of \( \phi_l^n \) is given by
\[
\det(T - \phi_l^n) = (T - \alpha^n)(T - \beta^n).
\]
In particular,
\[
\#E(\mathbb{F}_{q^n}) = \deg(1 - \phi^n)
\]
\[
= \det(1 - \phi_l^n) \text{ from Proposition 8.7}
\]
\[
= 1 - \alpha^n - \beta^n + q^n.
\]
(2) By the Cayley-Hamilton theorem, we know \( \phi_l \) satisfies its characteristic polynomial, so \( \phi_l^2 - a\phi_l + q = 0 \). Applying Proposition 8.7 yields
\[
\deg(\phi^2 - a\phi + q) = \det(\phi_l^2) - a\phi_l + q = \det(0) = 0.
\]
Thus, \( \phi^2 - a\phi + q \) is the zero map in \( \text{End}(E) \).

Using Part 1 of Theorem 8.8, we are now ready to verify the Weil conjectures for elliptic curves.

**Theorem 8.9.** Let \( E/\mathbb{F}_q \) be an elliptic curve. Then there is an \( a \in \mathbb{Z} \) such that
\[
Z(E/\mathbb{F}_q; T) = \frac{1 - aT + qT^2}{(1 - T)(1 - qT)}.
\]
Further,
\[
Z(E/\mathbb{F}_q; 1/qT) = Z(E/\mathbb{F}_q; T),
\]
and
\[
1 - aT + aT^2 = (1 - \alpha T)(1 - \beta T) \text{ with } |\alpha| = |\beta| = \sqrt{q}.
\]
Proof. We compute
\[
\log Z(E/\mathbb{F}_q; T) = \sum_{n=1}^{\infty} \frac{\#E(\mathbb{F}_{q^n}) T^n}{n}
\]
by definition,
\[
= \sum_{n=1}^{\infty} \frac{1 - \alpha^n - \beta^n + q^n T^n}{n} \quad \text{(part 1 of Theorem 8.8)},
\]
\[
= -\log(1 - T) + \log(1 - \alpha T) + \log(1 - \beta T) - \log(1 - q T).
\]
Then
\[
Z(E/\mathbb{F}_q; T) = \frac{(1 - \alpha T)(1 - \beta T)}{(1 - T)(1 - q T)},
\]
satisfying the Rationality conjecture. In [1], (V.2.3.1a) says \(\alpha\) and \(\beta\) are complex conjugates of absolute value \(\sqrt{q}\) and that they satisfy
\[
a = \alpha + \beta = \operatorname{tr}(\phi) = 1 + q - \deg(1 - \phi) \in \mathbb{Z}.
\]
Then we have verified the Riemann Hypothesis. Finally, setting \(\epsilon = 0\) immediately reveals the functional equation. \(\square\)

Remark 8.10. To connect Theorem 8.6 to the Riemann hypothesis, we can make a change of variables by setting \(T = q^{-s}\) to give a function of \(s\):
\[
\zeta_{E/\mathbb{F}_q}(s) = Z(E/\mathbb{F}_q; q^{-s}) = \frac{1 - aq^{-s} + q^{1-2s}}{1 - q^{-s})(1 - q^{1-s})}.
\]
The functional equation reads
\[
\zeta_{E/\mathbb{F}_q}(s) = \zeta_{E/\mathbb{F}_q}(1 - s).
\]
Further, the Riemann hypothesis for \(Z(E/\mathbb{F}_q; T)\) says if \(\zeta_{E/\mathbb{F}_q}(s) = 0\), then \(|q^s| = \sqrt{q}\), which is equivalent to \(\Re(s) = \frac{1}{2}\).

9. Appendix

Definition 9.1. A field \(F\) is algebraically closed if every nonconstant polynomial in \(F[x]\) has a root in \(F\).

Definition 9.2. A field extension \(E/K\) is finite if \(E\) is a finite dimensional vector space over \(K\).

Definition 9.3. A field extension \(E/K\) is separable if every \(\alpha \in K\) is separable. Every \(\alpha\) is separable if its minimal polynomial over \(F\) has distinct roots.

Definition 9.4. A field \(K\) is perfect if any of the following hold:

1. Every finite or algebraic extension of \(K\) is separable.
2. Every irreducible polynomial over \(K\) is separable or has distinct roots.
3. The separable closure of \(K\) is algebraically closed.
4. Either \(K\) has characteristic \(p = 0\), or when \(p \neq 0\), every element of \(K\) is a \(p\)th power.
5. If \(K\) has characteristic \(p \neq 0\), then the Frobenius endomorphism \(x \mapsto x^p\) is an automorphism.
We assume $K$ is perfect mainly to simplify the machinery required for this paper, just as we assume the characteristic $p$ of $K$ is not 2 or 3. When every finite extension is separable, this makes our relation between function fields and curves easier to see. Additionally, the Frobenius map being an automorphism is essential to how we use elliptic curves over finite fields to prove an instance of the Weil Conjectures.

**Definition 9.5.** A field extension $E/K$ where $K$ has characteristic $p > 0$ is purely inseparable if every element of $K$ is the root of an equation of the form $x^q = a$, where $q$ is a power of $p$ and $a \in E$.

**Definition 9.6.** The coordinate ring of $V/K$ for a variety $V$ is denoted $K[V] = \frac{K[x]}{I(V/K)}$ where $K[V]$ is an integral domain. The quotient field is denoted by $K(V)$ and called the function field of $V/K$.

**Definition 9.7.** A meromorphic form is a holomorphic form with at most countably many poles.

**Remark 9.8.** We will also detail Galois actions on curves due to their algebraic importance.

1. If $\sigma \in G_{\overline{K}/K}$, then $\text{div}(f^\sigma) = (\text{div}(f))^\sigma$.
2. If a curve $C$ is defined over $K$, then $G_{\overline{K}/K}$ acts on $\text{Div}(C)$ and $\text{Div}^0(C)$ as

\[D^\sigma = \sum_{P \in C} n_P(P^\sigma).\]

This only holds if $C$ is defined over $K$ because $G_{\overline{K}/K}$ only fixes $K$. The divisor $D$ is defined over $K$ if $D^\sigma = D$ for all $\sigma \in G_{\overline{K}/K}$, meaning $D$ is also fixed by $G_{\overline{K}/K}$.

**Acknowledgments**

It is a pleasure to thank my mentor, Wei Yao, for her guidance and help writing this paper. I would also like to thank Peter May for organizing the University of Chicago REU and giving me this opportunity.

**References**