ELLIPTIC CURVES OVER FINITE FIELDS

CHRIS CALGER

A thesis submitted in partial fulfillment of the requirements for the degree of
Bachelor of Arts with Honors

Department of Mathematics
Colby College

Changningphaabi Namoijam, *advisor*
Nora Youngs, *reader*

Acknowledgements

I would like to thank my advisor Professor Changningphaabi Namoijam for her constant support and motivation. I would also like to thank Professor Nora Youngs for advising me during the first half of the project and for taking the time to read my thesis.

Contents

1. Introduction

The goal of this thesis is to give an expository report on elliptic curves over finite fields. An elliptic curve is defined as a smooth curve of genus 1 having a known point, denoted $\mathcal{O}$. It can also be defined as a smooth curve given by a Weierstrass equation.

We begin by giving an overview of the necessary background in algebraic geometry to understand the definition of an elliptic curve such as varieties, Weierstrass equations, and genus in Sections 2.1 and 2.2. We then explore the general theory of elliptic curves over arbitrary fields, such as the group structure in Section 3.1, isogenies in Section 3.2, and the endomorphism ring in Section 3.3. In Section 4, we study elliptic curves over finite fields. We focus on the number of $\mathbb{F}_q$-rational solutions, Tate modules, supersingular curves, and applications to elliptic curves over $\mathbb{Q}$. In particular, we approach the topic largely through the use of the Frobenius endomorphism. While Sections 2 and 3 are written so that the material is applicable to arbitrary fields, much of the presented information was chosen because of its utility to the theory of elliptic curves over finite fields.

The primary reference for Section 2 is Chapters I, II, and III of [5]. Chapter III of [5] is also the main reference for Sections 3.1 and 3.2. The primary reference for Sections 3.3, 4.2, and 4.3 is Chapters 12 and 13 of [2]. Chapter V of [5] is the main reference for Section 4.4. Lastly, the references used for Section 4.5 are Chapter VII of [5] and Chapter 16 of [3].

2. General Theory of Elliptic Curves

We will first state the definition of an elliptic curve. Although we have not yet defined some of the terms, this will allow the reader to make note of the important terms as they appear.

Definition 2.0.1. An *elliptic curve* $(E, \mathcal{O})$ is a smooth curve E of genus 1 having a known point $\mathcal{O}$.

The aim for Section 2.1 is to establish what a curve is. The genus of a curve will be thoroughly explained in Section 2.3.

2.1. **Projective Varieties.**

We will start by introducing *projective space*. This will serve as the foundation for elliptic curves and the majority of the objects in this thesis.

Unless otherwise specified, K will denote a perfect field, which means that every finite extension of K is separable. Examples of perfect fields include fields of characteristic zero, algebraically closed fields, and finite fields.

Definition 2.1.1. The *projective n-space* $\mathbb{P}^n$ over a field K, is the set of equivalence classes of $(n+1)$-tuples $(x_0, x_1, \ldots, x_n)$, where each entry $x_0, \ldots, x_n$ is an element of the algebraic closure $\overline{K}$ of K, under the following equivalence relation $\sim$:

$$(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n) \qquad \text{if there exists } \lambda \in \overline{K}^{\times} \text{ such that } x_i = \lambda y_i \text{ for all } i \in \{0, \ldots, n\}.$$

The equivalence class of a tuple $(x_0, \ldots, x_n)$ is denoted $[x_0, \ldots, x_n]$.

Note that $\mathbb{P}^n$ is dependent on the field K. If there is any ambiguity about the field we may write $\mathbb{P}^n(\overline{K})$. Also note that the elements (equivalences classes) of projective space over K have entries in $\overline{K}$. We write $\mathbb{P}^n(K)$ if we want to specify *only* the K-rational points in $\mathbb{P}^n$, i.e., the set of equivalences classes where each tuple has entries in K.

Example 2.1.2. We can think of $\mathbb{P}^n$ as describing the set of all lines in $(n+1)$-space passing through the origin. The elements of the real projective line $\mathbb{P}^1(\overline{\mathbb{R}})$, thought of as lines, can then be determined by their slope, which is a unique real number for all lines except for the vertical line $[0, 1] \in \mathbb{P}^1(\overline{\mathbb{R}})$ having corresponding "slope" ∞.

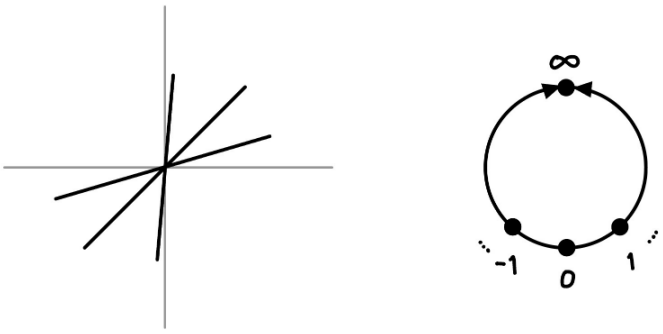

Figure 1. The real projective line $\mathbb{P}^1(\overline{\mathbb{R}})$.

From this, we see that the real projective line is homeomorphic to the circle $\mathbb{S}^1$ and to $\mathbb{R} \cup \{\infty\}$, where $[1, y] \in \mathbb{P}^1(\overline{\mathbb{R}})$ corresponds to $y \in \mathbb{R} \cup \{\infty\}$ and $[0, 1] \in \mathbb{P}^1(\overline{\mathbb{R}})$ corresponds to $\infty \in \mathbb{R} \cup \{\infty\}$.

In order to define varieties, we must consider *homogenous* polynomials in $\overline{K}[X_0, \ldots, X_n]$. For ease of notation, we will write $\overline{K}[X]$ to mean $\overline{K}[X_0, \ldots, X_n]$. By a (degree-$d$) homogenous polynomial, for $d \in \mathbb{Z}_{>0}$, we mean a polynomial $f \in \overline{K}[X]$ with the property that for each $\lambda \in \overline{K}$,

$$f(\lambda X_0, \ldots, \lambda X_n) = \lambda^d f(X_0, \ldots, X_n)\,.$$

Definition 2.1.3. A *projective variety* V is a set of the form

$$\{\, P \in \mathbb{P}^n(\overline{K}) \mid f_1(P) = 0, \ldots, f_m(P) = 0 \,\}\,,$$

for some homogenous polynomials $f_1, \ldots, f_m \in \overline{K}[X]$ satisfying the property that $I(V) = \langle f_0, \ldots, f_m \rangle \subset \overline{K}[X]$ is a prime ideal.

In this thesis we only consider projective varieties, and will as such refer to them only as "varieties". Note that projective space $\mathbb{P}^n$ is itself a variety.

We will write V/K to mean a variety whose ideal can be expressed as $I(V) = \langle f_1, \ldots, f_m \rangle$ where $f_1, \ldots, f_m \in K[X]$. We will say that such varieties are defined over K. In general, if we let $I(V/K) = I(V) \cap K[X]$, then V is defined over K when $I(V/K) = I(V)$.

Example 2.1.4. Consider the ideal in $\overline{K}[X, Y, Z]$ generated by $Y^2Z - X^3$. We write

$$V : Y^2Z = X^3$$

to mean the variety V with ideal $I(V) = \langle Y^2Z - X^3 \rangle$. Notice that $I(V)$ is generated by a homogeneous polynomial, so it is homogeneous. We can also check that $I(V)$ is prime to see that V is in fact a variety.

Definition 2.1.5. The *coordinate ring of a variety* V/K is

$$K[V] = \frac{K[X]}{I(V/K)}\,.$$

The quotient field of $K[V]$ is denoted $K(V)$.

Definition 2.1.6. The *dimension* $\dim V$ *of a variety* V is the transcendence degree of $\overline{K}(V)$ over $\overline{K}$.

As we will see from the next definition, in this thesis we only care about varieties of dimension one. In fact, if V is variety with $I(V) = \langle f \rangle$, where $f \in \overline{K}[X_0, X_1, X_2]$ is an irreducible (homogeneous) polynomial, then $\dim V = 1$.

Definition 2.1.7. A *curve* is a projective variety of dimension one.

Definition 2.1.8. A curve C with $I(C) = \langle f_1, \ldots, f_m \rangle$ is *smooth* if every point is non-singular. That is, if for all $P \in C$, the rank of the $m \times n$ matrix

$$\big(\partial f_i / \partial X_j(P)\big)_{1 \le i \le m\,, 1 \le j \le n}$$

is $n - 1$.

Specifically, if $I(C) = \langle f \rangle$, then C is smooth when

$$\Big(\frac{\partial f}{\partial X_1}(P) \dots \frac{\partial f}{\partial X_n}(P)\Big)$$

has rank $n-1$. Note that we will see a much nicer characterization of smoothness in Section 2.2.

Turning our attention to elliptic curves, the condition that there is a known point $\mathcal{O}$ can now restated as saying there is a fixed K-rational base point $\mathcal{O} \in E(K)$. With these definitions, we now understand most of the definition of an elliptic curve, except for the property that it is a genus 1 curve.

2.2. **Weierstrass Equations.** So far we have seen the definition of an elliptic curve and some information about curves. Before defining the genus of a curve, we aim to put elliptic curves into context by describing what they "look like": namely, curves given by Weierstrass equations. In fact, while the formal definition of an elliptic curve is important, we will often find it more practical to consider the (equivalent) definition in this section. Further, we will see in Section 2.3.5 that every elliptic curve can be expressed as a Weierstrass equation– and conversely, that every smooth curve given by a Weierstrass equation is an elliptic curve.

The labeling of the coefficients in the next definition may seem strange, but will be explained in Example 2.3.23. It is also not something to focus on as we will shortly change the coefficients to a different form.

Definition 2.2.1. A *Weierstrass equation* is an equation of the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3\,, \tag{1}$$

where $a_1, \dots, a_6 \in \overline{K}$.

We have mentioned that an elliptic curve has a specified base point $\mathcal{O}$. When an elliptic curve $(E, \mathcal{O})$ is given by a Weierstrass equation of the form (1), then the base point is $\mathcal{O} = [0, 1, 0]$. We can also make (1) easier to work with through the following process.

Definition 2.2.2. If $f(X_0, \dots, X_n) \in \overline{K}[X]$ is a polynomial written in homogeneous coordinates, then we can *dehomogenize* f with respect to X_i by setting $X_i = 1$, for some $i \in \{\, 0, \dots, n \,\}$ to get $f'(X_0, \dots, X_{i-1}, X_{i+1}, \dots, X_n)$. Afterwards, we say that f' is written in dehomogeneous coordinates.

Conversely, if we start with dehomogeneous $f'(X_0, \dots, X_{i-1}, X_{i+1}, \dots, X_n)$, we can *homogenize* f' by setting

$$f(X_0, \dots, X_n) = X_i^d f'\Big(\frac{X_0}{X_i}, \dots, \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i}, \dots, \frac{X_n}{X_i}\Big)\,,$$

where $d \in \mathbb{Z}$ is the least integer so that f is a polynomial.

By dehomogenizing (1), we get the equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\,, \tag{2}$$

where y represents Y/Z and x represents X/Z. Note that homogenizing (2) gives

$$Z^d\left(\Big(\frac{Y}{Z}\Big)^2 + a_1\Big(\frac{X}{Z}\Big)\Big(\frac{Y}{Z}\Big) + a_3\Big(\frac{Y}{Z}\Big) - \left(\Big(\frac{X}{Z}\Big)^3 + a_2\Big(\frac{X}{Z}\Big)^2 + a_4\Big(\frac{X}{Z}\Big) + a_6\right)\right),$$

$$=Y^2Z^{d-2} + a_1XYZ^{d-2} + a_3YZ^{d-1} - \left(X^3Z^{d-3} + a_2X^2Z^{d-2} + a_4XZ^{d-1} + a_6Z^d\right).$$

Then the least $d \in \mathbb{Z}$ making this a polynomial is $d = 3$, which is exactly (1).

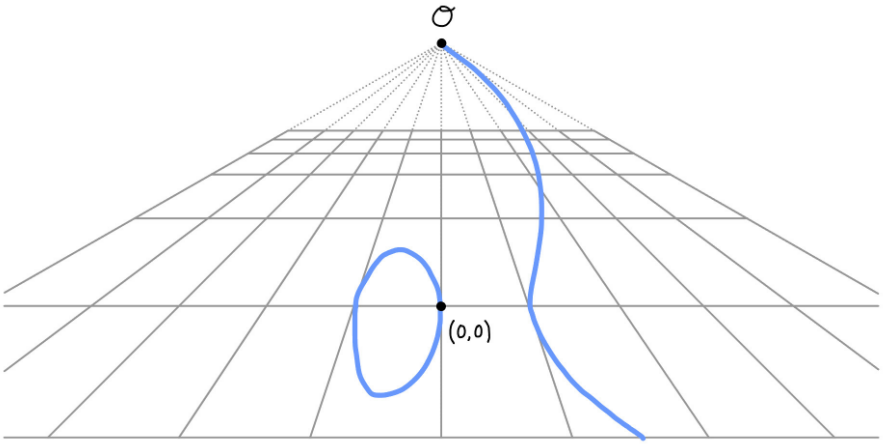

FIGURE 2. The elliptic curve $E : y^2 = x^3 - x$ with base point $\mathcal{O}$ included at infinity.

Of course, when we dehomogenize we are losing some information about the curve. In the case of an elliptic curve, when we dehomogenize (1) to get (2), we only "lose" the base point $\mathcal{O} = [0, 1, 0]$. Specifically, this means that every point on a curve given by a Weierstrass equation corresponds to a point on the dehomogenized curve *except* for $\mathcal{O}$, which is sent out to infinity. So, when working with a Weierstrass equation in dehomogenized coordinates, we must remember that the base point is also on the curve out at infinity.

So far, we have been working over an arbitrary field K. Now, suppose K has characteristic $\text{char}(K) \neq 2$. This allows us to simplify the Weierstrass equation by completing the square. If we set

$$y \mapsto \frac{1}{2}(y - a_1x - a_3),$$

then

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

simplifies to

$$E : y^2 = 4x^3 + (a_1^2 + 4a_2)x^2 + (2a_4 + a_1a_3)x + (a_3^2 + 4a_6).$$

Furthermore, if $\text{char}(K) \neq 2, 3$, then we can simplify even further to get an elliptic curve given by an equation of the form

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

where $A, B \in \overline{K}$. We call this a *short* Weierstrass equation and we will rewrite our elliptic curves into this form unless $\text{char}(K) = 2$ or 3.

In the previous section, we defined the property of a curve being smooth. You may wonder why we define this next definition in this way, but this will become apparent in the proof of Proposition 2.2.4.

Definition 2.2.3. When E is an elliptic curve given by a short Weierstrass equation, we define the *discriminant* to be

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

Proposition 2.2.4. *Let E be a curve given by a Weierstrass equation. Then E is smooth if and only if $\Delta \neq 0$.*

Proof. Suppose E/K is smooth. We will prove this for when $\mathrm{char}(K) \neq 2$, as the proof in the general case is longer and no more interesting. When $\mathrm{char}(K) \neq 2$, then E may be given by a Weierstrass equation of the form

$$E : y^2 = 4x^3 + Ax^2 + 2Bx + C\,.$$

Recall that E is singular if the rank of the $m \times n$ matrix

$$\left(\partial f_i/\partial X_j(P)\right)_{1\leq i\leq m\,,1\leq j\leq n}$$

is $n-1$. So, E is singular exactly at the points $(a,0)$, when a is a multiplicity-two zero of

$$f(x) = 4x^3 + Ax^2 + 2Bx + C\,.$$

The polynomial f has such a zero if and only if its discriminant is zero– that is when

$$144ABC - 4A^3C + 4A^2B^2 - 128B^3 - 108C^2 = 0\,.$$

A computation reveals that the discriminant of f is equal to 16Δ, which finishes the proof. ∎

This proposition will be very useful in later sections such as Section 4.5 as it gives us a fast way to check if a curve given by a Weierstrass equation is non-singular and therefore an elliptic curve.

2.3. **Genus of Curves.** So far, we have seen in Section 2.1 the definition of elliptic curves as well as a brief introduction to the general theory of curves. The goal of this section is to provide more concepts from algebraic geometry to complete our understanding of the definition of an elliptic curve. Then, we will connect to the information in Section 2.2 by showing how the genus property of an elliptic curve guarantees it can be written in Weierstrass form.

Many of the theorems in this section will not be proven as they are results from algebraic geometry and, while necessary for defining elliptic curves, are not the focus of this thesis.

2.3.1. *Morphisms of Curves.* We turn our attention to maps between curves. Consider a function $f \in \overline{K}(C)$ in the function field of a curve C. For a point $P \in C$, if we can write f in the form $f = g/h$ for some $g, h \in \overline{K}[C]$ with $h(P) \neq 0$, then we say f is defined at P. More succinctly put, we say that f is defined at P when f is in the local ring at P, which is the ring

$$\overline{K}[C]_P = \{\, f \in \overline{K}(C) \mid f = g/h \text{ for some } g, h \in \overline{K}[C] \text{ with } h(P) \neq 0 \,\}\,.$$

The ring $\overline{K}[C]_P$ is a discrete valuation ring, so it is a principal ideal domain with exactly one maximal ideal $M_P = \langle t \rangle$ generated by a (not necessarily unique) element $t \in M_P$. We call t a uniformizer for C at P.

Definition 2.3.1. We define the *order of vanishing* of f at P,

$$\operatorname{ord}_P : \overline{K}(C) \to \mathbb{Z}_{\geq 0} \cup \{\infty\},$$

by $\operatorname{ord}_P(f/g) = \operatorname{ord}_P(f) - \operatorname{ord}_P(g)$, where

$$\operatorname{ord}_P(f) = \inf\{m \in \mathbb{Z} \mid t^{-m} f \in \overline{K}[C]_P \text{ for a uniformizer } t\ \}$$

for all $f \in \overline{K}[C]_P$.

Note that by definition, the order of a uniformizer t for P is $\operatorname{ord}_P(t) = 1$. We say that f is defined at P when $\operatorname{ord}_P(f) \geq 0$. More specifically, we say f has a zero at P when $\operatorname{ord}_P(f) > 0$. Otherwise, if $\operatorname{ord}_P(f) < 0$, we say that f has a pole at P.

The following two theorems will be of use in Section 2.3.5.

Proposition 2.3.2. *If C is a smooth curve and $f \in \overline{K}(C)$, then $\operatorname{ord}_P(C) = 0$ for all but finitely many points $P \in C$.*

Proposition 2.3.3. *If C is a smooth curve and $f \in \overline{K}(C)$ has no poles, then $f \in \overline{K}$.*

Definition 2.3.4. For two curves $C_1, C_2 \subset \mathbb{P}^n$, a map $\varphi : C_1 \to C_2$ is called a *rational map* if there exist $f_0, \ldots, f_n \in \overline{K}(C_1)$ such that φ is given by

$$\varphi(P) = [f_0(P), \ldots, f_n(P)]$$

whenever $f_0(P), \ldots, f_1(P)$ are all defined.

Definition 2.3.5. A rational map $\varphi : C_1 \to C_2$ is called a *birational map* if there exists an inverse $\varphi^{-1} : C_2 \to C_1$, that is also a rational map, satisfying $\varphi^{-1} \circ \varphi = \varphi \circ \varphi^{-1} = \mathrm{I}$.

Note that these rational maps may not be defined on all of C_1. However, it is most useful to us to only work with rational maps that *are* defined on all of C_1. We will refer to these types of rational maps as morphisms. A naïve approach to properly defining these morphisms would be to simply require that each $f_0, \ldots, f_n$ in Definition 2.3.4 be defined on all of C_1. The problem with this approach is that by choosing the $f_0, \ldots, f_n$, we may have described φ in such a way that the map appears to not be defined everywhere, even though it actually is.

As an analogy to this concept, suppose we were to define the constant-1 function on $\mathbb{R}$ by

$$\textsc{one} : \mathbb{R} \to \mathbb{R}, \qquad \textsc{one}(x) = \frac{x}{x}.$$

Written in this form, it may appear that ONE is not defined at 0, since $0/0$ is undefined, but if we rewrite ONE in the form $\textsc{one}(x) = 1$, then we see that it is indeed defined on all of $\mathbb{R}$.

So how do we "rewrite" rational maps as we did with our function in $\mathbb{R}$? Let $\varphi : C_1 \to C_2$ be a rational map given by $\varphi = [f_0, \ldots, f_n]$ and consider a point $P \in C_1$. If there exist homogeneous polynomials $g_0, \ldots, g_n \in \overline{K}[X_0, \ldots, X_n]$ all of the same degree such that $g_0(P), \ldots, g_n(P)$ are not all zero and

$$f_i g_j \equiv f_j g_i \,(\operatorname{mod} I(C_1)) \qquad \text{for every } i, j \in \{0, \ldots, n\},$$

then we say φ is defined at P and we may write

$$\varphi(P) = [g_0(P), \ldots, g_n(P)].$$

Definition 2.3.6. A rational map $\varphi : C_1 \to C_2$ between curves is a *morphism* if it is defined everywhere on C_1. Such a morphism is called an *isomorphism* if there exists an inverse $\varphi^{-1} : C_2 \to C_1$ such that $\varphi \circ \varphi^{-1} = \varphi^{-1} \circ \varphi = \mathrm{I}$.

Example 2.3.7. The map $\varphi : \mathbb{P}^2 \to \mathbb{P}^2$ given by

$$\varphi = [X^2, XY, Z^2]$$

is a rational map, but not a morphism. Note that X^2, XY, and Z^2 have no common factors. However the point $[0 : 1 : 0]$ is a zero of all three functions and since $I(\mathbb{P}^2) = (0)$, there is no way to modify the aforementioned functions modulo $I(\mathbb{P}^2)$.

Let V be the variety

$$V : Y^2Z = X^3 + Z^3 \,.$$

Then $\varphi : V \to \mathbb{P}^2$ given by

$$\varphi = [X^2, XY, Z^2]$$

does define a morphism of curves. To see this, we need to show that φ is defined everywhere on V. Notice that X^2, XY, and Z^2 all have the same degree. We only need to check if φ is defined at $[0, 1, 0]$ since the only solution to

$$X^2 = XY = Z^2 = 0$$

other than $X = Y = Z = 0$ is when $X = Z = 0$ and $Y \neq 0$. Notice that

$$\left(X^3\right)^2 \equiv \left(Z(Y^2 - Z^2)\right)^2 \pmod{I(V)} \,.$$

Then,

$$\begin{aligned}
\varphi &= [X^2, XY, Z^2] \\
&= [X^2(Y^2 - Z^2)^2, XY(Y^2 - Z^2)^2, Z^2(Y^2 - Z^2)^2] \\
&= [X^2(Y^2 - Z^2)^2, XY(Y^2 - Z^2)^2, X^6] \\
&= [X(Y^2 - Z^2)^2, Y(Y^2 - Z^2)^2, X^5] \,.
\end{aligned}$$

So, $\varphi([0, 1, 0]) = [0, 1, 0]$, which shows that φ is defined at $[0, 1, 0]$.

To reiterate our analogy with ONE : $\mathbb{R} \to \mathbb{R}$, we started with $\varphi([0, 1, 0]) = [0, 0, 0]$, which is undefined in $\mathbb{P}^2$ just as $0/0$ is in $\mathbb{R}$. Then we rewrote φ so that it was not undefined at $[0, 1, 0]$ just as we rewrote ONE.

An important result from algebraic geometry is the following theorem.

Theorem 2.3.8. *A morphism between curves is either constant or surjective.*

A morphism $\varphi : C_1 \to C_2$ also induces a map $\varphi^* : K(C_2) \to K(C_1)$, called the "follow by f map", given by $\varphi^*(f) = f \circ \varphi$. Using this, we can define the degree of a morphism.

Definition 2.3.9. The *degree of a morphism* of curves $\varphi : C_1 \to C_2$ is

$$\deg \varphi = \sum_{P \in \varphi^{-1}(Q)} \mathrm{ord}_P(\varphi^* t_{\varphi(p)})$$

where $Q \in C_2$ is any fixed point of C_2 and $t_{\varphi(P)}$ is a uniformizer at $\varphi(P) = Q$.

We call the summand $\mathrm{ord}_P(\varphi^* t_{\varphi(p)})$ the *ramification index* of φ at P. We may denote this by $e_\varphi(P)$. If $e_\varphi(P) = 1$, we say φ is unramified at P.

Example 2.3.10. Let $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$ be given by

$$\varphi([X, Y]) = [X^3(X - Y)^2, Y^5] .$$

Of course, $\mathbb{P}^1$ is a smooth curve and φ is non-constant, so we may use the above proposition to find the degree of φ. We can think of $\mathbb{P}^1$ as the points $[x, 1] \in \mathbb{P}^1$, which are determined solely by the coordinate x, together with $[1, 0]$. We call the collection of these x the affine line $\mathbb{A}^1$, so that $\mathbb{P}^1 \cong \mathbb{A}^1 \cup \{ \infty \}$.

Notice that the only point sent to $[1, 0]$ under φ is $[1, 0]$. Then φ sends every point of $\mathbb{P}^1$ other than $[1, 0]$, i.e., points on $\mathbb{A}^1$, to other points on $\mathbb{A}^1$. We can model the restriction of φ to $\mathbb{A}^1$ by setting $Y = 1$ and dropping the second coordinate. Denote this restriction by $\psi = \varphi\big|_{\mathbb{A}^1}$ so that $\psi : \mathbb{A}^1 \to \mathbb{A}^1$ is given by

$$\psi(x) = x^3(x - 1)^2 .$$

The zeros of ψ are 0 and 1 and it is easy to see that $\mathrm{ord}_0(\psi) = 3$ and $\mathrm{ord}_1(\psi) = 2$. The points $0, 1 \in \mathbb{A}^1$ correspond to $[0, 1], [1, 1] \in \mathbb{P}^1$, respectively, and are the only points in the preimage of $[0, 1] \in \mathbb{P}^1$. Applying the proposition we get

$$\deg \varphi = e_\varphi([0, 1]) + e_\varphi([1, 1]) = 3 + 2 = 5 .$$

The following is a useful result about the degree of a morphism of curves.

Proposition 2.3.11. *If $\varphi : C_1 \to C_2$ is a degree 1 map between smooth curves, then φ is an isomorphism.*

2.3.2. *Divisors.*

Definition 2.3.12. A *divisor D on a curve C* is a formal sum

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

of points on C, where each $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many terms. The degree of such a divisor is

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

Note that the degree $\deg(D)$ of a divisor is finite because $n_P = 0$ for all but finitely many terms. The divisors of C form a group denoted $\mathrm{Div}(C)$. The degree-0 divisors form a subgroup which is denoted $\mathrm{Div}^0(C)$.

Example 2.3.13. Let $P, Q \in C$. Then $3(P) + 2(Q)$ is a divisor on C. Another divisor is (P). We write the divisor in parentheses to distinguish between meaning the point P and the divisor (P).

Definition 2.3.14. A divisor is *principal* if it is of the form

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

for some $f \in \overline{K}(C)^\times$. We denote such a divisor by $\mathrm{div}(f)$. We say that two divisors D_1, D_2 are linearly equivalent if $D_1 - D_2$ is a principal divisor. When this occurs, we write $D_1 \sim D_2$.

Remark 2.3.15. Note that a divisor of f is an important device that keeps track of all of its zeros and poles. We will see in Theorem 2.3.30 that divisors can be used to construct functions with specific poles and zeros.

Definition 2.3.16. We say a divisor $D = \sum_{P \in C} n_P(P)$ is *positive* if $n_P \geq 0$ for each $P \in C$. When this occurs, we write $D \geq 0$.

Proposition 2.3.17. *Let C be a smooth curve and $f \in \overline{K}(C)^\times$. Then* $\deg(\mathrm{div}(f)) = 0$. *Also,* $\mathrm{div}(f) = 0$ *if and only if $f \in \overline{K}^\times$.*

The principal divisors form a normal subgroup of $\mathrm{Div}(C)$ and we denote the quotient of $\mathrm{Div}(C)$ by the principal divisors by $\mathrm{Pic}(C)$. Likewise, we define $\mathrm{Pic}^0(C)$ in the same way, replacing $\mathrm{Div}(C)$ with $\mathrm{Div}^0(C)$. We call $\mathrm{Pic}(C)$ the *Picard group* of C. The importance of the Picard group will be seen once we introduce differentials.

Now that we have defined isomorphisms of (elliptic) curves, we turn our attention briefly to an elliptic curve E given by a Weierstrass equation

$$E : y^2 = x^3 + Ax + B\,.$$

Definition 2.3.18. The j-invariant of an elliptic curve E given in short Weierstrass form is the value

$$j(E) = \frac{1728(4A)^3}{\Delta}\,.$$

The j-invariant is called such because it is invariant under isomorphism of curves. In fact, we also have the following stronger statement.

Proposition 2.3.19. *Let E and E' be elliptic curves. Then E and E' are isomorphic if and only if $j(E) = j(E')$.*

We omit the proof of the next proposition.

Proposition 2.3.20. *Any two Weierstrass equations for E are related by a change of variables of the form*

$$(x, y) \mapsto (u^2x + r, u^3y + su^2x + t)\,,$$

where $r, s, t \in K$ and $u \in K^\times$.

When E is given by a short Weierstrass equation, any such map has $r = s = t = 0$. We can see this by expanding the Weierstrass equation

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

The left hand side becomes

$$\big(u^3y + su^2x + t\big)^2 = u^6y^2 + s^2u^4x^2 + t^2 + 2su^5yx + 2tu^3y + 2tsu^2x\,,$$

and the right hand side becomes

$$\big(u^2x + r\big)^3 + A\big(u^2x + r\big) + B = u^6x^3 + 3u^4x^2r + 3u^2xr^2 + r^3 + Au^2x + Ar + B\,.$$

Putting them together we get

$$\begin{aligned} &u^6y^2 + s^2u^4x^2 + t^2 + 2su^5yx + 2tu^3y + 2tsu^2x \\ =\,&u^6x^3 + 3u^4x^2r + 3u^2xr^2 + r^3 + Au^2x + Ar + B\,, \end{aligned}$$

which simplifies to

$$\begin{aligned} &u^6y^2 + 2su^5yx + 2tu^3y \\ =&u^6x^3 + (3u^4r - s^2u^4)x^2 + (3u^2r^2 + Au^2 - 2tsu^2)x + (r^3 + Ar + B - t^2)\,. \end{aligned}$$

This new equation is in short Weierstrass form when $u \neq 0$, $2su^5 = 0$, $2tu^3 = 0$, and $3u^4r - s^2u^4 = 0$. So, we must have $r = s = t = 0$. Consequently, any two short Weierstrass equations are related by a change of variables of the form

$$(x, y) \mapsto (u^2x, u^3y)\,,$$

which is dependent solely on $u \in K^\times$.

2.3.3. *Differentials.*

Definition 2.3.21. The *space of differential forms of a curve* C is the set Ω_C generated by symbols of the form dx where $x \in \overline{K}(C)$. For all $z \in \overline{K}$ and all $x, y \in \overline{K}(C)$, we have the following relations:

(1) $dz = 0$.
(2) $d(x + y) = dx + dy$.
(3) $d(xy) = x\,dy + y\,dx$.

Ω_C is a $\overline{K}$-vector space of dimension one.

Some intuition for these relations, specifically 2 and 3, is that they resemble the sum and product rules, respectively, for derivatives of functions from $\mathbb{R}$ to $\mathbb{R}$.

Definition 2.3.22. For a divisor $D \in \mathrm{Div}(C)$, we define the *vector space associated to* D to be

$$\mathcal{L}(D) = \{\, f \in \overline{K}(C)^\times \mid D + \mathrm{div}(f) \geq 0 \,\} \cup \{\, 0 \,\},$$

which is a $\overline{K}$-vector space of finite dimension. Notice that if we take some non-zero $f \in \mathcal{L}(D)$, then

$$0 = -\deg \mathrm{div}(f) \leq -\deg(-D) = \deg(D)\,.$$

This means that if $\deg(D) < 0$, then $\mathcal{L}(D) = \{\, 0 \,\}$.

Example 2.3.23. Consider the spaces $\mathcal{L}\big(n(\mathcal{O})\big)$ for $n = 0, 1, \ldots$. When $n = 0$, this space has dimension 1. For all other n, this space has dimension n. We will see what a basis for this space looks like for each $n = 0, 1, \ldots, 6$.

When $n = 0$, $\dim\Big(\mathcal{L}\big(n(\mathcal{O})\big)\Big) = 0$, so the vector space contains just the constant functions and has basis $\{\, 1 \,\}$. When $n = 1$, the dimension does not change, so we do not get any new functions in the basis.

When $n = 2$, the dimension is 2, so we get a new function, which we will denote x, that has a pole of order 2. Likewise, when $n = 3$, we get a new function, denoted y, with a pole of order 3. So far we have the basis $\{\, 1, x \,\}$ when $n = 2$ and $\{\, 1, x, y \,\}$ when $n = 3$.

When $n = 4$, it may appear as though we should get a new function with a pole of order 4, but we do not, since x^2 has a pole of order 4, so we have $\{\, 1, x, y, x^2 \,\}$. Likewise, for $n = 5$, we have xy, which has a pole of order 5, so we have $\{\, 1, x, y, x^2, xy \,\}$. For $n = 6$, we have y^2, which has a pole of order 6, but we also have x^3. Thus, for $n = 6$ we have seven functions: $\{\, 1, x, y, x^2, xy, y^2, x^3 \,\}$. We are stopping at $n = 6$ for reasons that will become clear in Theorem 2.3.31.

Proposition 2.3.24. *Let $\omega \in \Omega_C$ be a non-zero differential and let t be a uniformizer for a point $P \in C$. Then there exists a unique function $g \in \overline{K}(C)$ such that $\omega = gdt$. We denote g by ω/dt. Furthermore,* $\mathrm{ord}_P(g)$ *is independent of choice of t, i.e., it depends only on ω. We then denote* $\mathrm{ord}_P(\omega) = \mathrm{ord}_P(g)$.

Definition 2.3.25. For a differential $\omega \in \Omega_C$, we can associate to it the divisor $\mathrm{div}(\omega)$ defined by

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

Notice that for a non-zero differential $\omega \in \Omega_C$, we have a map $\omega \mapsto \mathrm{div}(\omega)$ which sends $\Omega_C \to \mathrm{Div}(C)$. Then, we can evaluate $\mathrm{Div}(C) \to \mathrm{Pic}(C)$ to get a map $\Omega_C \to \mathrm{Pic}(C)$.

Definition 2.3.26. The *canonical divisor class* on C is the image in $\mathrm{Pic}(C)$ of the map $\Omega_C \to \mathrm{Pic}(C)$. The elements of the canonical divisor class on C are called canonical divisors.

The idea behind canonical divisors is that if we take two (non-zero) differentials $\omega, \varpi \in \Omega_C$ such that $\omega = f\varpi$, for some $f \in \overline{K}(C)^\times$, then

$$\mathrm{div}(\omega) = \mathrm{div}(f) + \mathrm{div}(\varpi)\,.$$

The result of this is that canonical divisors of a curve C are all linearly equivalent.

2.3.4. *Riemann-Roch.* We finally have a sufficient amount of theory to state the Riemann-Roch Theorem, which defines the genus of a curve.

Theorem 2.3.27 (Riemann-Roch)**.** *Let C be a smooth curve and K_C a canonical divisor on C. There exists an integer $g \geq 0$ such that for every divisor $D \in \mathrm{Div}(C)$,*

$$\dim\big(\mathcal{L}(D)\big) - \dim\big(\mathcal{L}(K_C - D)\big) = \deg(D) - g + 1\,.$$

The integer $g \geq 0$ is called the *genus of C*. Notice that in general, when $D = 0$, we have $\mathcal{L}(D) = \{\,0\,\}$, so

$$1 - \dim\big(\mathcal{L}(K_C)\big) = 0 - g + 1\,,$$

which means $\dim\big(\mathcal{L}(K_C)\big) = 1$. Furthermore, if we set $D = K_C$, then the Riemann-Roch theorem tells us that

$$\dim\big(\mathcal{L}(K_C)\big) - 1 = \deg(K_C) - g + 1\,,$$

so $\deg(K_C) = 2g - 2$.

Now suppose $\deg(D) > 2g - 2$. In particular, this means that $\deg(K_C - D) < 0$, so $\mathcal{L}(K_C - D) = \{\,0\,\}$. Then,

$$\dim\big(\mathcal{L}(D)\big) = \deg(D) - g + 1\,.$$

The above discussion can be summarized as the following corollary to Theorem 2.3.27.

Corollary 2.3.28.

(1) $\dim\big(\mathcal{L}(K_C)\big) = g$.
(2) $\deg(K_C) = 2g - 2$.
(3) If $\deg(D) > 2g - 2$, *then* $\dim\big(\mathcal{L}(D)\big) = \deg(D) - g + 1$.

Now that we have defined the genus of a curve, we can give the following two theorems. In particular, they show a distinction between genus 1 and genus 0 curves.

Theorem 2.3.29. *Let C be a curve of genus 1 and let $P, Q \in C$. Then $(P) \sim (Q)$ if and only if $P = Q$.*

Proof. If $P = Q$, then clearly $(P) \sim (Q)$. If $(P) \sim (Q)$, then there exists $f \in \overline{K}(C)$ such that $\operatorname{div}(f) = (P) - (Q)$. Notice that $f \in \mathcal{L}\big((Q)\big)$. The Riemann-Roch theorem tells us that

$$\dim \mathcal{L}\big((Q)\big) = \deg(Q) = 1\,,$$

so $\mathcal{L}\big((Q)\big)$ contains only constant functions. Then f is constant and $P = Q$. ∎

Theorem 2.3.30. *Let C/K be a smooth curve. The following are equivalent over $\overline{K}$:*

(i) C has genus 0.
(ii) There exist $P, Q \in C$ such that $(P) \sim (Q)$ but $P \neq Q$.
(iii) $C \cong \mathbb{P}^1$.

Proof. (i) ⇒ (ii). Suppose C has genus $g = 0$ and let $Q \in C$. By the Riemann-Roch theorem, since $\deg(Q) = 1 > 2g - 2$,

$$\dim \mathcal{L}\big((Q)\big) = \deg(Q) - g + 1 = 2\,.$$

Then $\mathcal{L}\big((Q)\big)$ contains all constant functions in $\overline{K}$ as well as the function X.

(ii) ⇒ (iii). If $(P) \sim (Q)$, then there exists $f \in \overline{K}(C)$ such that $\operatorname{div}(f) = (P) - (Q)$. Using f we can construct a morphism $F : C \to \mathbb{P}^1$ by

$$F(x) = \begin{cases} [1,0] & x = Q \\ [f(x),1] & x \neq Q \end{cases}.$$

It suffices to show that $\deg F = 1$. Recall that for any choice of $S \in \mathbb{P}^1$,

$$\deg F = \sum_{R \in F^{-1}(S)} e_F(R) = \sum_{R \in F^{-1}(S)} \operatorname{ord}_R(t_S \circ F)\,,$$

where $t_S \in \overline{K}(\mathbb{P}^1)$ is a uniformizer for $\mathbb{P}^1$ at S. If we take S to be $[0,1] \in \mathbb{P}^1$, then $F^{-1}([0,1]) = P$ because P is the only zero of f. Notice that the maximal ideal $M_{[0,1]}$ in the local ring $\overline{K}[\mathbb{P}^1]_{[0,1]}$ is generated by $X \in \overline{K}(\mathbb{P}^1)$, so X is a uniformizer for $\mathbb{P}^1$ at $[0,1]$. Then, $X \circ F = f$, so P is a multiplicity 1 zero of $X \circ F$. Thus,

$$\deg F = e_F(P) = 1\,,$$

so $C \cong \mathbb{P}^1$.

(iii) ⇒ (i). By a corollary to the Riemann-Roch Theorem, the genus of C is equal to the dimension of the $\mathcal{L}(K_C)$ as a $\overline{K}$-vector space, for any canonical divisor K_C.

Let t be a coordinate function on $\mathbb{P}^1$. Notice that

$$\operatorname{ord}_\infty(dt) = \operatorname{ord}_\infty\big(-t^2 d(1/t)\big) - 2\,,$$

and every $P \in \mathbb{P}^1 \setminus \{\infty\}$,

$$\operatorname{ord}_P(dt) = \operatorname{ord}_P\big(d(t-P)\big) = 0\,.$$

So, $\operatorname{div}(dt) = -2(\infty)$. Then, for every non-zero divisor $\omega \in \Omega_{\mathbb{P}^1}$,

$$\deg\big(\operatorname{div}(\omega)\big) - \deg\big(\operatorname{div}(dt)\big) = -2\,,$$

so ω is not regular by definition. Let $K_C \in \mathbb{P}^1$. Then

$$\mathcal{L}(K_C) = \{\,\omega \in \Omega_{\mathbb{P}^1} \mid \omega \text{ regular}\,\} = \emptyset\,.$$

Since C is isomorphic to $\mathbb{P}^1$, there exists some canonical divisor $K_{C'}$ for C with $\mathcal{L}(K_{C'}) = \emptyset$. By a corollary to the Riemann-Roch Theorem, the genus of C is the dimension of the $\mathcal{L}(K_{C'})$ as a $\overline{K}$-vector space, for any canonical divisor $K_{C'}$. Thus, the genus of C is $\dim(\emptyset) = 0$. ■

2.3.5. *Connection to Weierstrass Equations.* We are finally ready to prove the connection between elliptic curves given by Weierstrass equations and elliptic curves defined as genus one curves.

Theorem 2.3.31. *Let E/K be an elliptic curve. Then E is isomorphic to some curve*

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

with $a_1, \ldots, a_6 \in K$ and the base point $\mathcal{O}$ corresponding with $[0, 1, 0] \in \mathbb{P}^2$.

Proof. Recall that in Example 2.3.23 we showed that $\mathcal{L}\big(6(\mathcal{O})\big)$ has dimension 6 and contains the seven functions $1, x, y, x^2, xy, y^2, x^3$. Thus, there exists $A_1, \ldots, A_7 \in K$ such that

$$A_1 + A_2x + A_3y + A_4x^2 + A_5xy + A_6y^2 + A_7x^3\,.$$

There exists a change of variables which puts this equation into a Weierstrass form. Specifically, we replace (x, y) with $(-A_6A_7x, A_6A_7^2y)$ to get

$$\begin{aligned}
&A_1 + A_2(-A_6A_7x) + A_3(A_6A_7^2y) + A_4(-A_6A_7x)^2 \\
&+ A_5(-A_6A_7x)(A_6A_7^2y) + A_6(A_6A_7^2y)^2 + A_7(-A_6A_7x)^3 \\
&= A_1 - A_2A_6A_7x + A_3A_6A_7y + A_4A_6^2A_7^2x^2 - xyA_6^2A_7^2A_5xy + A_6^3A_7^2y^2 - A_7^4A_6^3x^3\,.
\end{aligned}$$

Then dividing by $A_7^4A_6^3$ gives

$$\begin{aligned}
&\frac{A_1}{A_7^4A_6^3} - \frac{A_2A_6A_7}{A_7^4A_6^3}x + \frac{A_3A_6A_7}{A_7^4A_6^3}y + \frac{A_4A_6^2A_7^2}{A_7^4A_6^3}x^2 - \frac{A_6^2A_7^2A_5}{A_7^4A_6^3}xy + \frac{A_6^3A_7^2}{A_7^4A_6^3}y^2 - \frac{A_7^4A_6^3}{A_7^4A_6^3}x^3 \\
&= \frac{A_1}{A_7^4A_6^3} - \frac{A_2}{A_7^3A_6^2}x + \frac{A_3}{A_7^3A_6^2}y + \frac{A_4}{A_7^2A_6^1}x^2 - \frac{A_5}{A_7^2A_6^1}xy + \frac{1}{A_7^2}y^2 - x^3\,.
\end{aligned}$$

So, we have a map $\varphi : E \to \mathbb{P}^2$ given by $\varphi = [x, y, 1]$ whose image is given by a Weierstrass equation. Say C is the curve given by this Weierstrass equation. The restriction $\varphi : E \to C$ is a morphism of curves, so it is surjective.

We now want to show that φ is a degree-one morphism. From Example 2.3.23 we know that x has one pole, namely an order 2 pole at $\mathcal{O}$. Likewise, y has only an order 3 pole at $\mathcal{O}$. Then, the ramification index of φ at $\mathcal{O}$ is 1, since only 1 divides both 2 and 3. Thus,

$$\deg(\varphi) = e_\varphi(\mathcal{O}) = 1\,.$$

Then φ is a degree-one morphism, so it is an isomorphism by Proposition 2.3.11.

The last thing we need to show is that C is smooth. Suppose, by contradiction, that C is singular. A fact from algebraic geometry is that whenever a curve is singular, we can find a degree-one rational map $\psi : C \to \mathbb{P}^1$. Then $\psi \circ \varphi : E \to \mathbb{P}^1$ is a degree-one map of smooth curves, so it is an isomorphism. However, Theorem 2.3.30 then tells us that E has genus 0, which contradicts that it is an elliptic curve. ■

Lemma 2.3.32. *Let E be given by the Weierstrass equation*

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

Then the differential $\omega = dx/(2y + a_1x + a_3)$ *satisfies* $\operatorname{div}(\omega) = 0$. *This is called the invariant differential.*

The next theorem is the converse of Theorem 2.3.31, which proves the relationship between Weierestrass equations and elliptic curves.

Theorem 2.3.33. *Let*

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

be a smooth curve with $a_1, \ldots, a_6 \in K$. *Then* C *is an elliptic curve over* K *with base point* $\mathcal{O} = [0, 1, 0]$.

Proof. The above lemma says that the invariant differential has $\operatorname{div}(\omega) = 0$. The Riemann-Roch theorem tells us that

$$\deg\big(\operatorname{div}(\omega)\big) = 2g - 2\,,$$

so $g = 1$ is the genus of E. We then have that E is a smooth curve of genus 1 with base point $\mathcal{O} = [0, 1, 0]$, so it is an elliptic curve. ■

3. Isogenies

3.1. **Group Structure.** Our goal for this section is to establish a group structure for the points of E and for $E(K)$, the K-rational points on E. We will then introduce isogenies in 3.2 and see how they relate to the group of points on an elliptic curve.

Consider an elliptic curve in short Weierstrass form

$$E : y^2 = x^3 + Ax + B$$

defined over a field K. Suppose we have two distinct K-rational points $P = (p_1, p_2)$ and $Q = (q_1, q_2)$ on E and draw the line

$$L : y - p_2 = \left(\frac{p_2 - q_2}{p_1 - q_1}\right)(x - p_1)$$

connecting P and Q. For now, ignore the possibility of $p_1 = q_1$, so that we do not divide by zero. It is easy to see that L will always intersect E at a third point $R = (r_1, r_2)$. Moreover, R will also be another K-rational point, since L has slope

$$\frac{p_2 - q_2}{p_1 - q_1} \in K\,.$$

When $p_1 = q_1$, the line L does not appear to intersect E at a third point. However, we have to remember that when our Weierstrass equation is written in non-homogeneous coordinates, we still have the base point $\mathcal{O} \in E(K)$ out at infinity. Then the third point where L intersects E will be $\mathcal{O}$.

Definition 3.1.1. Using the information from the above discussion, we can define a *"composition rule"* $* : E \times E \to E$ as follows: Draw the line L from P to Q. Then $P * Q$ is the third point on $L \cap E$.

It may seem at first that this composition rule could be a group operation on E. However, notice that, for example, we would not be able to define an identity element, as $P * Q$ is never P or Q. Instead, we perform one extra step to define the group law.

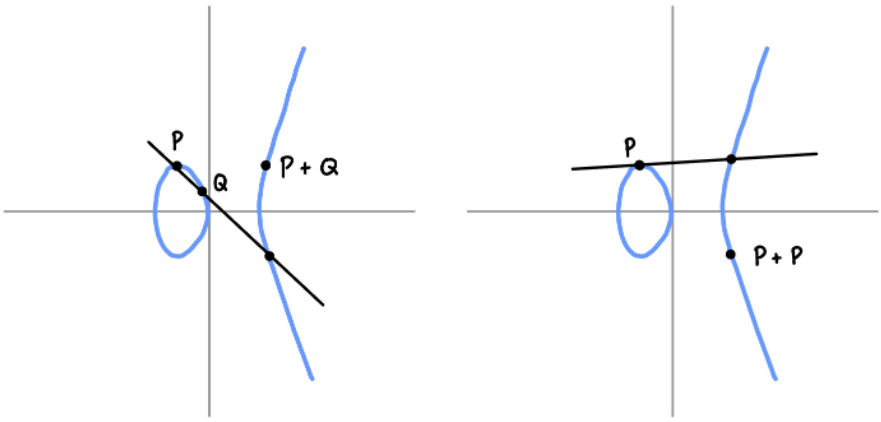

Figure 3. Illustration of the group law on an elliptic curve.

Definition 3.1.2. Let $+ : E \times E \to E$ be defined by

$$P + Q = \mathcal{O} * (P * Q)\,.$$

When E is given by a Weierstrass equation, then $\mathcal{O}$ is sent out to infinity, so our group law becomes:

$$P + Q = -(P * Q)\,.$$

Theorem 3.1.3. $\big(E, +\big)$ *is an abelian group, with* $+$ *defined as above.*

Proof. Notice that the operation $+$ is well-defined, because $*$ is a well-defined operation on $E(K)$. The identity of this group is $\mathcal{O}$ and it is obvious that $\mathcal{O} + \mathcal{O} = \mathcal{O}$. It is also clear that every element $P \in E(K)$ has an inverse, namely $P * \mathcal{O}$. Notice that $P * Q = Q * P$, so

$$P + Q = \mathcal{O} * (P * Q) = \mathcal{O} * (Q * P) = Q + P\,.$$

It remains to show that $+$ is an associative operation, which we will omit as it is long and not very interesting. ■

Corollary 3.1.4. *The* K*-rational points* $E(K)$ *form a subgroup of* E*.*

Proof. In the discussion at the beginning of this section we explained that $*$ also defines an operation on $E(K)$, i.e., that $P * Q \in E(K)$ if $P, Q \in E(K)$. Then this extends to $+$ to say that $P + Q \in E(K)$ if $P, Q \in E(K)$. ■

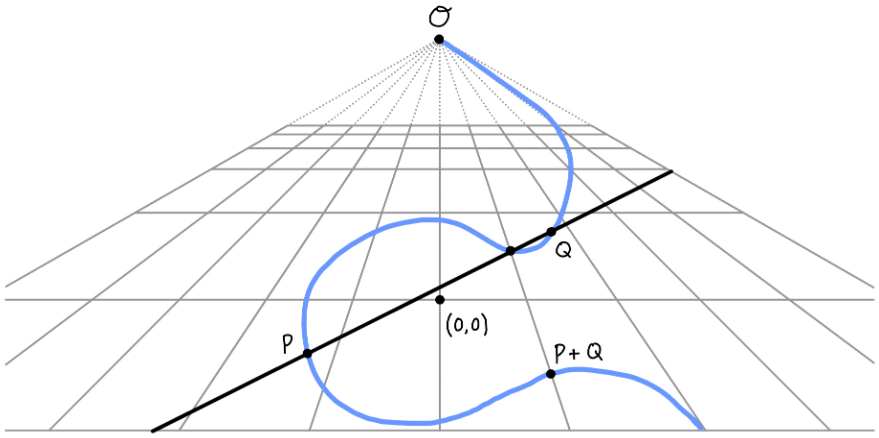

FIGURE 4. The group law with the base point included at infinity.

3.2. **Introduction to Isogenies.**

Definition 3.2.1. An *isogeny* is a morphism $\varphi : E_1 \to E_2$ of elliptic curves which preserves the base point, i.e., $\varphi(\mathcal{O}) = (\mathcal{O})$.

Notice that there is a trivial constant isogeny which sends every point to $\mathcal{O}$. Since this is the only constant isogeny, Theorem 2.3.8 tells us that every non-trivial isogeny is surjective.

Recall that since isogenies are morphisms of curves, we already know some information about them from Section 2.3.1.

Example 3.2.2. An important isogeny is the multiplication-by-m map $[m] : E \to E$ defined by

$$[m](P) = \begin{cases} \underbrace{P + P + \cdots + P}_{m \text{ times}} & m > 0 \\ \underbrace{(-P) + (-P) + \cdots + (-P)}_{-m \text{ times}} & m < 0 \\ \mathcal{O} & m = 0 \end{cases}.$$

The map $[m]$ is defined on all of E and satisfies $[m](\mathcal{O}) = (\mathcal{O})$, so it is indeed an isogeny. Note that the trivial isogeny is [0]. We will see in Proposition 3.2.5 that $\deg([m]) = m^2$, where the degree was given in Definition 2.3.9.

The kernel of $[m]$ is called the *m-torsion points* of E and is denoted $E[m]$. The *torsion subgroup* of E is the subgroup E_{tors} containing all elements of finite order. That is, it is the union

$$E_{\text{tors}} = \bigcup_{m \in \mathbb{Z}_{\geq 0}} E[m]\,.$$

The set of isogenies between two elliptic curves E_1 and E_2 is denoted $\text{Hom}(E_1, E_2)$. In fact, $\big(\text{Hom}(E_1, E_2), +\big)$ is an abelian group with $+$ defined by

$$(\varphi + \psi)(P) = \varphi(P) + \psi(P)\,,$$

The group operation on $\big(\text{Hom}(E_1, E_2), +\big)$ is well-defined since

$$(\varphi + \psi)(\mathcal{O}) = \varphi(\mathcal{O}) + \psi(\mathcal{O}) = \mathcal{O}\,,$$

making $\varphi + \psi$ an isogeny. The identity element is the trivial isogeny [0] and the inverse of an isogeny φ is the map $(-\varphi)$ defined by

$$(-\varphi)(P) = -\varphi(P)\,.$$

Associativity and commutativity easily follow from the group structure on elliptic curves.

We have just seen that isogenies are closely related to the group structure of $E(K)$. In fact, isogenies respect the group law on $E(K)$. Since every isogeny is a morphism that fixes $\mathcal{O}$, which is the identity of $E(K)$, we have that the isogenies are exactly the group homomorphisms of $E(K)$.

The set $\text{Hom}(E, E)$ of isogenies from an elliptic curve E to itself forms a ring with multiplication given by composition of isogenies. We call $\text{Hom}(E, E)$ the endomorphism ring of E and denote it by $\text{End}(E)$. This ring is one of our principal objects of interest in this thesis. The group of units in the endomorphism ring is called the *automorphism group* and is denoted $\text{Aut}(E)$.

Definition 3.2.3. Every degree-m isogeny $\varphi : E_1 \to E_2$ comes with a unique isogeny $\widehat{\varphi} : E_2 \to E_1$, called the *dual isogeny* to φ, which satisfies $\widehat{\varphi} \circ \varphi = [m]$.

To see that this isogeny $\widehat{\varphi}$ is unique, suppose by contradiction that there exists another isogeny $\psi : E_2 \to E_1$ satisfying $\psi \circ \varphi = [m]$. Specifically, we would have

$$\widehat{\varphi} \circ \varphi = \psi \circ \varphi = [m]\,,$$

so

$$(\widehat{\varphi} \circ \varphi) - (\psi \circ \varphi) = [m] - [m] = [0]\,.$$

Then,

$$(\widehat{\varphi} - \psi) \circ \varphi = [0]\,,$$

so either $\varphi = 0$ or $\widehat{\varphi} - \psi = 0$.

Proposition 3.2.4. *Let $\varphi, \psi : E_1 \to E_2$ and $\lambda : E_2 \to E_3$ be isogenies. Then*

$$\widehat{\lambda \circ \varphi} = \widehat{\varphi} \circ \widehat{\lambda} \quad \text{and} \quad \widehat{\varphi + \psi} = \widehat{\varphi} + \widehat{\psi}\,.$$

We now have enough information to show that the degree of the multiplication-by-m map is m^2.

Proposition 3.2.5. $\widehat{[m]} = [m]$ *and* $\deg[m] = m^2$.

Proof. It is clear that $\widehat{[0]} = [0]$ and $\widehat{[1]} = [1]$. From Proposition 3.2.4, we know that

$$\widehat{[m+1]} = \widehat{[m]} + \widehat{[1]} = \widehat{[m]} + [1]\,.$$

In particular, this means

$$\widehat{[m]} = \overbrace{[1 + 1 + \cdots + 1]}^{m \text{ times}} = \underbrace{\widehat{[1]} + \widehat{[1]} + \cdots + \widehat{[1]}}_{m \text{ times}} = \underbrace{[1] + [1] + \cdots + [1]}_{m \text{ times}} = [m]\,.$$

We then have

$$\big[\deg([m])\big] = \widehat{[m]} \circ [m] = [m] \circ [m] = [m^2]\,,$$

so $\deg([m]) = m^2$. ∎

3.3. **Endomorphism Ring.** As mentioned when we introduced the endomorphism ring, it is one of the main objects of interest in this thesis. This section serves to provide useful theory of the endomorphism ring and explain why it is interesting.

Proposition 3.3.1. $\mathrm{End}(E)$ *has no zero divisors.*

Proof. If $\varphi, \psi \in \mathrm{End}(E)$ are such that $\varphi\psi = 0$, then $0 = \deg(\varphi\psi) = \deg(\varphi)\deg(\psi)$. So, either $\deg(\varphi)$ or $\deg(\psi)$ must be 0, which implies that either φ or ψ is 0. ∎

Proposition 3.3.2. *Let E/K be an elliptic curve and let $\varphi, \psi \in \mathrm{End}(E)$. Then the degree map* $\deg : \mathrm{End}(E) \to \mathbb{R}$ *has the following properties:*

(1) $\deg(0) = 0$.
(2) $\deg(\psi) \geq 0$.
(3) $\deg(\psi + \varphi) = \deg(\psi) + \deg(\varphi) + \widehat{\psi}\varphi + \widehat{\varphi}\psi$.
(4) $\deg(m\psi) = m^2 \deg(\psi)$.

Remark 3.3.3. A map that satisfies properties 1-4 is called a quadratic form.

Definition 3.3.4. The *characteristic polynomial* of an isogeny $\psi \in \mathrm{End}(E)$ is

$$c_\psi(x) = x^2 - \mathrm{Tr}(\psi)x + \deg(\psi)\,,$$

where its trace is $\mathrm{Tr}(\psi) = \psi + \widehat{\psi}$.

Proposition 3.3.5. *An isogeny $\psi \in \mathrm{End}(E)$ is a zero of its own characteristic polynomial, i.e., $c_\psi(\psi) = 0$.*

Theorem 3.3.6 (Hasse)**.** *If $\psi \in \mathrm{End}(E)$, then $|\,\mathrm{Tr}(\psi)| \leq 2\sqrt{\deg(\psi)}$, where $|\cdot|$ denotes the standard absolute value.*

Proof. Let $\psi \in \mathrm{End}(E)$ and $x \in \mathbb{Q}$ be given and set $x = m/n$. Recall that the degree map deg is non-negative. Then

$$c_\psi(x) = \frac{m^2}{n^2} - \frac{m}{n}\operatorname{Tr}(\psi) + \deg(\psi)\,,$$

so using the properties of a quadratic form given in Proposition 3.3.2 we get

$$\begin{aligned} n^2 c_\psi(x) &= m^2 - nm\operatorname{Tr}(\psi) + n^2\deg(\psi)\,, \\ &= \deg(m) + \deg(n\psi) - nm\operatorname{Tr}(\psi)\,, \\ &= \deg(m) + \deg(n\psi) + m(-n\psi) + (-n\widehat{\psi})m\,, \\ &= \deg(m) + \deg(n\psi) + \widehat{m}(-n\psi) + (\widehat{-n\psi})m\,, \\ &= \deg(m - n\psi) \\ &\geq 0\,. \end{aligned}$$

The result of this is that either $c\psi(x)$ has 0 or 1 roots in $\mathbb{Q}$, so the discriminant of c_ψ is $(-\operatorname{Tr}(\psi))^2 - 4\deg(\psi) \leq 0$. We then conclude that $|\operatorname{Tr}(\psi)| \leq 2\sqrt{\deg(\psi)}$. ∎

Our goal now is to explain what the structure of $\mathrm{End}(E)$ looks like.

Definition 3.3.7. Let $\mathscr{A}$ be a finite-dimensional algebra over $\mathbb{Q}$. An *order* $\mathscr{R}$ of $\mathscr{A}$ is a subring of $\mathscr{A}$ which is $\mathbb{Z}$-lattice in $\mathscr{A}$ and satisfies $\mathscr{R} \otimes \mathbb{Q} = \mathscr{A}$.

Definition 3.3.8. A *quadratic imaginary field* is a number field of the form $\mathbb{Q}(\sqrt{d})$, where $d < 0$.

Definition 3.3.9. A *quaternion algebra* (over $\mathbb{Q}$) is an algebra $\mathscr{A}$ of the form

$$\mathscr{A} = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta\,,$$

with $\alpha^2, \beta^2 \in \mathbb{Q}$ both less than 0, and $\beta\alpha = -\alpha\beta$. In particular, α and β commute with every element of $\mathbb{Q}$.

Example 3.3.10. Let $\mathscr{A} = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta$ be a quaternion algebra and consider the set

$$\mathscr{R} = \{\, w + x\alpha + y\beta + z\alpha\beta \mid w, x, y, z \in \mathbb{Z} \,\}$$

Clearly $\mathscr{R}$ is a subring of $\mathscr{A}$ and is a $\mathbb{Z}$-lattice in $\mathscr{A}$. We also have $\mathscr{R} \otimes \mathbb{Q} = \mathscr{A}$, so $\mathscr{R}$ is an order in $\mathscr{A}$.

With these definitions in place, we can now state the following result:

Theorem 3.3.11. *Let E be an elliptic curve. Then* $\mathrm{End}(E)$ *is one of the following: $\mathbb{Z}$, an order in a quadratic imaginary field, or an order in a quaternion algebra.*

It turns out that if $\mathrm{char}(K) = 0$, then $\mathrm{End}(E)$ cannot be an order in a quaternion algebra. This is one of the reasons why studying elliptic curves over finite fields is interesting, as we can have elliptic curves with these unusually large endomorphism rings. This is explored in greater depth in Section 4.4.

We now turn our attention briefly to the automorphism group of an elliptic curve. Recall that $\mathrm{Aut}(E)$ is the group (under composition) of invertible elements of the ring $\mathrm{End}(E)$.

Theorem 3.3.12. *Let E/K be an elliptic curve. The size of its automorphism group depends on the characteristic of K and the j-invariant of E. Specifically:*

$$\#\operatorname{Aut}(E) = \begin{cases} 24 & \operatorname{char}(K) = 2 \\ 12 & \operatorname{char}(K) = 3 \\ 6 & j(E) = 0 \text{ and } \operatorname{char}(K) \neq 2,3 \\ 4 & j(E) = 1728 \text{ and } \operatorname{char}(K) \neq 2,3 \\ 2 & j(E) \neq 0, 1728 \text{ and } \operatorname{char}(K) \neq 2,3 \end{cases}$$

Proof. We will show the case when $\operatorname{char}(K) \neq 2, 3$. Let E be given by the short Weierstrass equation

$$E : y^2 = x^3 + Ax + B\,,$$

for some $A, B \in \overline{K}$. Recall from Proposition 2.3.20 that every change of variables between two Weierstrass equations is of the form

$$(x, y) \mapsto (u^2x + r, u^3y + su^2x + t)\,,$$

for some $r, s, t \in \overline{K}$ and $u \in \overline{K}^\times$. We have also seen that when E is given by a short Weierstrass equation, any such map has $r = s = t = 0$. The image of the map $(x, y) \mapsto (u^2x, u^3y)$ is the curve given by the equation

$$u^6y^2 = u^6x^3 + Au^2x + B\,,$$

which is birationally equivalent to

$$y^2 = x^3 + Au^4x + Bu^6\,.$$

Thus, this map is an automorphism exactly when $A = Au^4$ and $B = Bu^6$. If $j(E) = 1728$, then $B = 0$, so u must satisfy $u^4 = 1$. Then $\#\operatorname{Aut}(E) = 4$ and $\operatorname{Aut}(E)$ has an element of order 4, so $\operatorname{Aut}(E) \cong \mathbb{Z}/4\mathbb{Z}$. If $j(E) = 0$, then $A = 0$, so $u^6 = 1$ and $\operatorname{Aut}(E) \cong \mathbb{Z}/6\mathbb{Z}$. Lastly, if $j(E) \neq 0, 1728$, then we only have $u = 1$ or $u = -1$, so $\operatorname{Aut}(E) \cong \mathbb{Z}/2\mathbb{Z}$. ■

Remark 3.3.13. The proof for the cases when $\operatorname{char}(K) = 2, 3$ are omitted because they are significantly longer, yet do not provide much additional insight. The idea is to mimic the same process, but for the much longer equations resulting from Proposition 2.3.20. The important difference to make note of when $\operatorname{char}(K) = 2, 3$ is that $\operatorname{Aut}(E)$ is not necessarily cyclic like it was in the proof above. Furthermore, $\operatorname{Aut}(E)$ is not necessarily abelian.

The proof of Theorem 3.3.12 also gave us some information about the structure of $\operatorname{Aut}(E)$. Specifically, when $\operatorname{char}(K) \neq 2, 3$, $\operatorname{Aut}(E)$ is cyclic. Notice that the isogeny $[1] : E \to E$ given by $P \mapsto P$ is always in $\operatorname{Aut}(E)$. Specifically, it is the identity element of the group. Another isogeny that is always in $\operatorname{Aut}(E)$ is $[-1] : E \to E$ given by $P \mapsto -P$. So when $\#\operatorname{Aut}(E) = 2$, it is the set $\operatorname{Aut}(E) = \{\,[1], [-1]\,\}$.

4. Elliptic Curves Over Finite Fields

We have now learned a significant amount about the theory of elliptic curves over an arbitrary field K. The rest of this thesis is dedicated to the case when K is a finite field. Before we explore elliptic curves, we give a brief overview of finite fields.

4.1. **Preliminary Theory of Finite Fields.**

From here on out, unless otherwise specified, $p \in \mathbb{Z}$ will be a prime and $q = p^r$ will be the rth power of p for some positive integer $r \in \mathbb{Z}_{>0}$.

Proposition 4.1.1. *For every prime p, there exists a unique field of order p (up to isomorphism). We denote this field $\mathbb{F}_p$ and call it the finite field of order p. Specifically, $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$, with the usual addition and multiplication.*

Remark 4.1.2. $\mathbb{F}_p$ is sometimes denoted $\mathrm{GF}(p)$, where GF stands for "Galois field".

By taking finite extensions of $\mathbb{F}_p$, we obtain finite fields whose order is a prime power. Specifically, if $L/\mathbb{F}_p$ is a field extension with $[L : \mathbb{F}_p] = r$, then L is a finite field of order p^r and is denoted $\mathbb{F}_{p^r} = \mathbb{F}_q$. There is a unique field of order p^r (up to isomorphism) for each prime p and power r. The characteristic of $\mathbb{F}_{p^r}$ is p for every $r \in \mathbb{Z}_{>0}$.

Explicitly we can construct $\mathbb{F}_{p^r}$ by

$$\mathbb{F}_{p^r} \cong \frac{\mathbb{F}_p[X]}{f(X)}\,,$$

where $f(X) \in \mathbb{F}_p[X]$ is an irreducible polynomial of degree r.

Example 4.1.3. Let $f(X) \in \mathbb{F}_2(X)$ be given by $f(X) = X^2 + X + 1$. Then $f(X)$ is an irreducible polynomial of degree 2, so

$$\mathbb{F}_4 \cong \frac{\mathbb{F}_2[X]}{X^2 + X + 1}\,.$$

Proposition 4.1.4. *If $n \in \mathbb{Z}$ is not a prime power, then there is no field of order n.*

To summarize, Propositions 4.1.1 and 4.1.4 tell us that there exists a unique finite field of order $\mathbb{F}_q$ if and only if $q \in \mathbb{Z}_{>0}$ is a prime power.

Proposition 4.1.5. *$\mathbb{F}_q$ is not algebraically closed.*

Proof. Let $\mathbb{F}_q = \{\, \alpha_1, \ldots, \alpha_q \,\}$ and consider the polynomial $f(x) \in \mathbb{F}_q[x]$ given by

$$f(x) = 1 + (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_q)\,.$$

Then $f(\alpha_i) = 1$ for all $\alpha_i \in \mathbb{F}_q$, so $\mathbb{F}_q$ is not algebraically closed. ∎

So, the closure of $\mathbb{F}_q$ cannot be a finite field. Specifically, the closure of $\mathbb{F}_q$ is

$$\overline{\mathbb{F}}_q = \bigcup_{m \in \mathbb{Z}_{>0}} \mathbb{F}_{q^m}\,.$$

4.2. **Inverse Limits.** In this section we introduce inverse limits which we will use to construct useful objects, specifically, the ℓ-adic integers and the Tate module of an elliptic curve. These constructions will lead to Theorem 4.2.9, Tate's Isogeny Theorem, which gives us a lot of information regarding isogeneous elliptic curves over $\mathbb{F}_q$.

Definition 4.2.1. Let $\{ G_i \}_{i \in D}$ be a set of groups and $\{ \varphi_{ji} : G_j \to G_i \}_{i \leq j \in D}$ a set of group homomorphisms, indexed by a directed set D. The pair $(\{ G_i \}_{i \in D}, \{ \varphi_{ji} : G_j \to G_i \}_{i \leq j \in D})$ is called an *inverse system of groups* if for all $i, j, k \in D$,

(1) $\varphi_{ii}(g) = g$ for all $g \in G_i$,
(2) $\varphi_{ki} = \varphi_{ji} \circ \varphi_{kj}$ whenever $i \leq j \leq k$.

Definition 4.2.2. Let $\mathbb{G} = (\{ G_i \}_{i \in D}, \{ \varphi_{ji} : G_j \to G_i \}_{i \leq j \in D})$ be an inverse system of groups. The *inverse limit* of $\mathbb{G}$ is

$$\varprojlim(\mathbb{G}) = \left\{ \alpha \in \prod_{i \in D} G_i \,\middle|\, \alpha_i = \varphi_{ji}(\alpha_j) \text{ whenever } i \leq j \right\}.$$

With this definition in place, we can construct the *ℓ-adic integers*.

Definition 4.2.3. Let $\ell \in \mathbb{Z}$ be a prime. The *ring of ℓ-adic integers* is

$$\mathbb{Z}_\ell = \varprojlim \left(\{ \mathbb{Z}/\ell^n\mathbb{Z} \}_{n \in \mathbb{Z}_{>0}}, \{ \text{ev} : \mathbb{Z}/\ell^j\mathbb{Z} \to \mathbb{Z}/\ell^i\mathbb{Z} \}_{i \leq j \in \mathbb{Z}_{>0}} \right),$$

where ev is the evaluation map. Specifically, this inverse limit is

$$\begin{aligned} \mathbb{Z}_\ell &= \left\{ \alpha \in \prod_{n \in \mathbb{Z}_{>0}} \mathbb{Z}/\ell^n\mathbb{Z} \,\middle|\, \text{ev}_{ji}(\alpha_j) = \alpha_i \text{ for all } i \leq j \right\}, \\ &= \left\{ (a_n) : \mathbb{Z}_{>0} \to \mathbb{Z} \,\middle|\, a_i \equiv a_j \pmod{\ell^i} \text{ for all } i \leq j \right\}. \end{aligned}$$

Being an inverse limit, the ℓ-adic integers carry information about $\mathbb{Z}/\ell^n\mathbb{Z}$ for every $n \in \mathbb{Z}_{>0}$. The following example serves to explain what that means.

Example 4.2.4. In this example, we will show that by generalizing statements to $\mathbb{Z}/\ell^n\mathbb{Z}$ for every n, then we can learn information about the inverse limit $\mathbb{Z}_\ell$. Specifically, we will deduce something about the 5-adic integers $\mathbb{Z}_5$. To begin, we will show that for every $k \geq 1$, there exists $x_k \in \mathbb{Z}/5^k\mathbb{Z}$ such that

$$(\dagger) \qquad x_k^2 + 1 \equiv 0 \pmod{5^k}.$$

We prove this by induction. For the base case, notice that $(2)^2 + 1 \equiv 0 \pmod 5$.

Now suppose there exists a solution $x_k \in \mathbb{Z}/5^k\mathbb{Z}$ to $x^2 + 1 \equiv 0 \pmod{5^k}$ for some $k \geq 1$. Note that either $x_k \equiv 2$ or $-x_k \equiv 2 \pmod 5$, so suppose that $x_k \equiv 2 \pmod 5$. Then, by definition, there exists integers $m, n \in \mathbb{Z}$ such that $x_k = m5 + 2$ and $x_k^2 = n5^k - 1$. I claim that $(x_k + n5^k)^2 + 1 \equiv 0 \pmod{5^{k+1}}$.

$$\begin{aligned} (x_k + n5^k)^2 + 1 &= x_k^2 + 2x_k n5^k + n^2 5^{2k} + 1 \\ &= (n5^k - 1) + 2(m5 + 2)n5^k + n^2 5^{2k} + 1 \\ &\equiv 5^k\big(n + 2n(m5 + 2)\big) && \pmod{5^{k+1}} \\ &\equiv n5^k(1 + 2m5 + 4) && \pmod{5^{k+1}} \\ &\equiv n5^{k+1}(1 + 2m) && \pmod{5^{k+1}} \\ &\equiv 0 && \pmod{5^{k+1}} \end{aligned}$$

This completes the induction step and proves (†).

Notice in the above proof that we can find two solutions to the congruence modulo 5^k, for every k. In fact, it is not difficult to show that these are the *only* two solutions. This allows us to make the following conclusion about the 5-adic integers: The equation $x^2 + 1 = 0$ has exactly two solutions in $\mathbb{Z}_5$.

The second useful object constructed by an inverse limit we will look at is the Tate module of an elliptic curve.

Definition 4.2.5. Let $\ell \in \mathbb{Z}$ be a prime, E an elliptic curve, and $\mathbb{E}$ the inverse system

$$\mathbb{E} = \left(\{\, E[\ell^n] \,\}_{n \in \mathbb{Z}_{>0}}, \{\, [\ell^{j-i}] : E[\ell^j] \to E[\ell^i] \,\}_{i \leq j \in \mathbb{Z}_{>0}} \right).$$

Then the *(ℓ-adic) Tate module of E* is $T_\ell(E) = \varprojlim(\mathbb{E})$.

Much like how the ℓ-adic integers carry information about $\mathbb{Z}/\ell^n\mathbb{Z}$, the Tate module carries information about the torsion of an elliptic curve. We will see what this structure looks like in Corollary 4.3.11.

Definition 4.2.6. Let L/K be a normal, separable extension. Then the set of automorphisms

$$\mathrm{Gal}(L/K) = \{\, \alpha \in L \to L \mid \alpha(x) = x \text{ for all } x \in K \,\}$$

is a group under composition called the *Galois group of L/K*.

Example 4.2.7. We will determine the Galois group

$$G = \mathrm{Gal}\left(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}\right).$$

Let $f(x) \in \mathbb{Q}[x]$ be given and consider an element $u \in \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ that is a root of $f(x)$. If $\sigma \in G$, then $\sigma(u)$ is also a root of $f(x)$. Thus, for each $\ell \in \{\, 2, 3, 5 \,\}$, we have $\sigma(\sqrt{\ell}) = \sqrt{\ell}$ or $-\sqrt{\ell}$. Let $\ell \in \{\, 2, 3, 5 \,\}$. Then,

$$\sigma\big(\sigma(\sqrt{\ell})\big) = \sigma(\pm\sqrt{\ell}) = \pm\sigma(\sqrt{\ell}) = \pm(\pm\sqrt{\ell}) = \sqrt{\ell}\,.$$

Hence the elements of G are self-invertible. Furthermore, G has six elements, so

$$G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\,.$$

Example 4.2.8. We will show that the Galois group of $\overline{\mathbb{F}}_q/\mathbb{F}_q$ is

$$\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \cong \widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/m\mathbb{Z} \cong \prod_{\ell \text{ prime}} \mathbb{Z}_\ell\,,$$

where the inverse limit is taken over all $m \in \mathbb{Z}_{>0}$ and the morphisms in the inverse system are the evaluation maps used in defining the ℓ-adic integers. The ring $\widehat{\mathbb{Z}}$ is called the *profinite integers*.

We first need to show that

$$\mathrm{Gal}(\mathbb{F}_{p^k}/\mathbb{F}_p) \cong \mathbb{Z}/k\mathbb{Z}$$

for every $k \in \mathbb{Z}_{>0}$. Let π be defined by $\pi(x) = x^p$. This morphism is explored in greater depth in Section 4.3. Specifically, in the discussion after Definition 4.3.2, we show that π is a field automorphism of $\mathbb{F}_p$. Furthermore, $\alpha^k = \alpha$ for all $\alpha \in \mathbb{F}_{p^k}$, so π is a field automorphism of $\mathbb{F}_{p^k}$ as well. Fermat's Little Theorem tells us that π fixes all elements of $\mathbb{F}_p$, so $\pi \in \mathrm{Gal}(\mathbb{F}_{p^k}/\mathbb{F}_p)$.

Galois theory tells us that

$$|\operatorname{Gal}(\mathbb{F}_{p^k}/\mathbb{F}_p)| = [\mathbb{F}_{p^k} : \mathbb{F}_p] = k\,.$$

Let $i, j \in \{0, 1, \ldots, k-1$ with $i \neq j$ be given. If $\pi^i = \pi^j$, then π^{i-j} is the identity of $\operatorname{Gal}(\mathbb{F}_{p^k}/\mathbb{F}_p)$. Recall that

$$\mathbb{F}_{p^k} \cong \frac{\mathbb{F}_p[X]}{f(X)}\,,$$

where $f(X) \in \mathbb{F}_p[X]$ is an irreducible polynomial of degree k. Under this construction, the polynomial $g(X) = X^{i-j} - X$ has exactly p^k roots, since π^{i-j} is the identity of $\operatorname{Gal}(\mathbb{F}_{p^k}/\mathbb{F}_p)$. Then, $g(X)$ must be the zero polynomial, so $i - j = 0$. This shows that all powers $0, 1, \ldots, k-1$ of π are distinct, so $\operatorname{Gal}(\mathbb{F}_{p^k}/\mathbb{F}_p)$ is generated by π and therefore is cyclic with order k. Note that if $q = p^r$, then

$$\operatorname{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) \subset \operatorname{Gal}(\mathbb{F}_q/\mathbb{F}_p) \cong \mathbb{Z}/r\mathbb{Z}$$

is a subgroup, so it is also cyclic and has order m.

Recall from Section 4.1 that

$$\overline{\mathbb{F}}_q = \bigcup_{m \in \mathbb{Z}_{>0}} \mathbb{F}_{q^m}\,.$$

Thus, we get that

$$\operatorname{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \cong \widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/m\mathbb{Z}\,.$$

Lastly, we will not show this, but it is interesting to note that

$$\widehat{\mathbb{Z}} \cong \prod_{\ell \text{ prime}} \mathbb{Z}_\ell\,.$$

The next theorem shows the utility of the Tate module. The proof is beyond the scope of the thesis [8].

Theorem 4.2.9 (Tate [8])**.** *If $E_1, E_2/\mathbb{F}_q$ are elliptic curves, then the natural map*

$$\operatorname{Hom}_{\mathbb{F}_q}(E_1, E_2) \otimes \mathbb{Z}_\ell \to \operatorname{Hom}_{\operatorname{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)}\big(T_\ell(E_1), T_\ell(E_2)\big)$$

is an isomorphism.

Remark 4.2.10. The above theorem is also true if $\mathbb{F}_q$ is replaced with a number field. Over an arbitrary field, the map in the above theorem is injective.

Let $\mathbb{Q}_\ell$ denote the ℓ-adic numbers, which are the field of fractions of $\mathbb{Z}_\ell$. Define the module V_ℓ by $V_\ell(E) = T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. Then we get the corollary:

Corollary 4.2.11. *If $E_1, E_2/\mathbb{F}_q$ are elliptic curves, then the natural map*

$$\operatorname{Hom}_{\mathbb{F}_q}(E_1, E_2) \otimes \mathbb{Q}_\ell \to \operatorname{Hom}_{\operatorname{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)}\big(V_\ell(E_1), V_\ell(E_2)\big)$$

is an isomorphism.

This means Tate's theorem tells us that E_1 and E_2 are isogeneous if and only if $V_\ell(E_1)$ and $V_\ell(E_2)$ are isomorphic as $\operatorname{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$-modules. We can also use this to say more about E_1 and E_2. From Example 4.2.8, we have the fact that the Galois group $\operatorname{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ is (topologically) generated by π_E, where π_E is the morphism defined by $\pi_E(P) = P^q$. Then, for a point $P \in E(\overline{\mathbb{F}}_q)$, this means that $P \in E(\mathbb{F}_q)$ if and only if $\pi_E(P) = P$. In particular, this discussion yields the following corollary:

Corollary 4.2.12. *Two elliptic curves E_1 and E_2 over $\mathbb{F}_q$ are isogeneous if and only if $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$.*

4.3. **Frobenius Endomorphism.** We now consider an elliptic curve $E/\mathbb{F}_q$. A natural question to ask is how many elements are in the group $E(\mathbb{F}_q)$. That is, how many $\mathbb{F}_q$-rational points are on the elliptic curve?

Example 4.3.1. Let E be the elliptic curve defined over $\mathbb{F}_p$ given by

$$E : y^2 = x^3 + x\,.$$

We will show that $\#E(\mathbb{F}_p) \equiv 0 \pmod 4$ for every odd prime p. First notice that we always have one point for free, namely the base point $\mathcal{O} \in E(\mathbb{F}_p)$. There are also three trivial solutions $(0,0)$, $(\zeta_1, 0)$, and $(\zeta_2, 0)$, where $\zeta_1, \zeta_2 \in \mathbb{F}_p$ are the two solutions to $\zeta^3 + \zeta = 0$.

Lastly, we count the number of elements $x \in \mathbb{F}_p$ such that $x^3 + x$ is a square (not zero). Of course, there must be an even number of these elements since for every such element, the map $x \mapsto -x$ produces another distinct element. Then there are twice as many points (x, y) which solve $y^2 = x^3 + x$, so the number of non-trivial points (i.e., not including $\mathcal{O}$ and those with $y = 0$) is divisible by 4. This, together with the four trivial points, shows that the total number of $\mathbb{F}_p$-rational points is divisible by 4, so $\#E(\mathbb{F}_p) \equiv 0 \pmod 4$.

We now turn to a particular endomorphism of an elliptic curve over a finite field called the Frobenius endomorphism. As we will see in this section and the next, there are many advantages to studying this particular morphism.

Definition 4.3.2. The *Frobenius endomorphism* of an elliptic curve $E/\mathbb{F}_q$ is the morphism $\pi_E : E \to E$ given by

$$\pi_E(x, y) = (x^q, y^q)\,.$$

We will first verify that π_E is an endomorphism. If E (as a variety) has ideal $I(E)$, then denote $E^{(q)}$ to be the curve with ideal generated by $\{\, f^{(q)} \mid f \in I(E) \,\}$. In other words, if E is given by a Weierstrass equation

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

then $E^{(q)}$ is given by raising each coefficient to the qth power:

$$E^{(q)} : y^2 + a_1^q xy + a_3^q y = x^3 + a_2^q x^2 + a_4^q x + a_6^q\,.$$

Then π_E is a morphism $\pi_E : E \to E^{(q)}$.

Let $\varphi : \mathbb{F}_q \to \mathbb{F}_q$ denote the qth power map, that is $\varphi(x) = x^q$. By Fermat's Little Theorem, φ is the identity on $\mathbb{F}_q$ when q is prime. Clearly, φ is a homomorphism of rings, so its kernel must be an ideal of $\mathbb{F}_q$, which can be either $\{\,0\,\}$ or all of $\mathbb{F}_q$, since $\mathbb{F}_q$ is a field. Note that $\varphi(1) = 1$, so $1 \notin \ker\varphi$. Then it must be that $\ker\varphi = \{\,0\,\}$, so φ is an injective morphism between finite fields of the same size, so it is therefore an isomorphism.

We then have $E^{(q)} \cong E$ which means π_E is an endomorphism of E. The Frobenius endomorphism also fixes the base point $\mathcal{O}$, so $\pi_E \in \mathrm{End}(E)$. Recall from Section 3.3 that $\mathrm{Tr}(\pi_E) = \pi_E + \widehat{\pi}_E$, where $\widehat{\pi}_E$ is its dual isogeny.

Definition 4.3.3. When $E/\mathbb{F}_q$, where $\mathrm{char}(\mathbb{F}_q) = p$, we define a similar *Frobenius map* $\pi : E \to E^{(p)}$ by $\pi(x, y) = (x^p, y^p)$. Note that when $p = q$, then $\pi = \pi_E$.

Recall that in order to define the degree of a morphism $\varphi : C_1 \to C_2$, in Definition 2.3.9, we introduced an induced map $\varphi^* : K(C_2) \to K(C_1)$ given by $\varphi^*(f) = f \circ \varphi$.

Definition 4.3.4. We say that a morphism of curves $\varphi : C_1 \to C_2$ is *purely inseparable* if $K(C_1)$ is purely inseparable over $\varphi^* K(C_2)$. We define separable and inseparable morphisms in a similar way, by replacing "purely inseparable" in the definition.

Proposition 4.3.5. $\deg(\pi) = p$ *and* π *is purely inseparable.*

Proof. Let $E/\mathbb{F}_q$ be an elliptic curve. We know that $\pi : E \to E^{(p)}$. It suffices to show that $\pi^* \mathbb{F}_q(E^{(p)}) = \mathbb{F}_q(E)^p$, where $\mathbb{F}_q(E)^p = \{ f^p \mid f \in \mathbb{F}_q(E) \}$.

Notice that $\mathbb{F}_q(E)$ consists of quotients of homogeneous polynomials $f, g \in \mathbb{F}_q[E]$ of the same degree, namely

$$f/g = f(X, Y, Z)/g(X, Y, Z)\,.$$

Then $\pi^* \mathbb{F}_q(E^{(p)})$ consists of quotients

$$\pi^*(f/g) = f(X^p, Y^p, Z^p)/g(X^p, Y^p, Z^p)\,.$$

Observe that $\mathbb{F}_q[X, Y, Z]^p = \mathbb{F}_q[X^p, Y^p, Z^p]$, so we then have

$$f(X^p, Y^p, Z^p)/g(X^p, Y^p, Z^p) = f(X, Y, Z)^p/g(X, Y, Z)^p = (f/g)^p\,,$$

which shows $\pi^* \mathbb{F}_q(E^{(p)}) = \mathbb{F}_q(E)^p$. Lastly, we have that $\mathbb{F}_q(E)^p$ is purely inseparable over $\mathbb{F}_q(E)$, which means π_E is purely inseparable.

We will not show that $\deg(\pi_E) = p$ as the proof relies on a different characterization of the degree of a morphism from the one we have been using. Specifically, we may define the degree to be

$$\deg(\pi_E) = [\mathbb{F}_q(E) : \pi_E^* \mathbb{F}_q(E^{(p)})]\,,$$

which can be shown to be p. ∎

Specifically, this proposition tells us that $\deg(\pi_E) = q$ and π_E is purely inseparable.

Proposition 4.3.6. *Let $\varphi : E \to E'$ be an isogeny of elliptic curves $E, E'/\mathbb{F}_q$. Then there exists a separable isogeny φ_s and an integer $n \geq 0$ such that*

$$\varphi = \varphi_s \circ \pi^n\,.$$

Definition 4.3.7. Let $\varphi = \varphi_s \circ \pi^n$ be an isogeny of elliptic curves over $\mathbb{F}_q$. We define the *separable and inseparable degrees of* φ to be

$$\deg_s(\varphi) = \deg(\varphi_s) \quad \text{and} \quad \deg_i(\varphi) = p^n\,,$$

respectively.

In particular, note that $\deg(\varphi) = \deg_s(\varphi) \deg_i(\varphi)$. Also, φ is purely inseparable exactly when $\deg_s(\varphi) = 1$.

Proposition 4.3.8. *Let $\varphi : E_1 \to E_2$ be an isogeny. Then*

$$\#\big(\varphi^{-1}(P)\big) = \deg_s(\varphi)$$

for every $P \in E_2$.

Notice that when we set $P = \mathcal{O}$, Proposition 4.3.8 tells us that $\#\ker(\varphi) = \deg_s(\varphi)$. Applying this to $[m] : E \to E$ tells us that $\#E[m] = \deg_s([m])$.

Proposition 4.3.9. *Let E be an elliptic curve and let $F \subset E$ be a finite subgroup. Then there exists a unique elliptic curve E' and a separable isogeny $\varphi : E \to E'$ with*

$$\ker(\varphi) = F\,.$$

Proposition 4.3.10. *Let $E/\mathbb{F}_q$ be an elliptic curve and let $m \in \mathbb{Z}$ be nonzero. If m and p are coprime, then $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Furthermore, either $E[p] \cong \mathbb{Z}/p\mathbb{Z}$ or $E[p] \cong \{\,0\,\}$.*

Proof. First, suppose $m \in \mathbb{Z}$ is a nonzero integer coprime to p. Then $[m]$ is separable and Proposition 4.3.9 tells us

$$\#E[m] = \deg[m] = m^2\,.$$

Likewise for any divisor $d \in \mathbb{Z}$ of m, we have

$$\#E[d] = \deg[d] = d^2\,.$$

Thus, it must be that $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

Now consider the multiplication-by-p map $[p]$. Since $\mathrm{char}(\mathbb{F}_q) = p$, $[p]$ is not separable. Recall from Proposition 4.3.5 that π is purely inseparable and $\deg(\pi) = [p]$. This means $\deg_s(\pi) = 1$ and $[p] = \widehat{\pi} \circ \pi$. Then,

$$\#E[p] = \deg_s[p] = \deg_s(\widehat{\pi} \circ \pi) = \deg_s(\widehat{\pi}) \deg_s(\pi) = \deg_s(\widehat{\pi})\,.$$

Notice that

$$\deg_s(\widehat{\pi}) = \begin{cases} 1 & \widehat{\pi} \text{ is purely inseparable;} \\ p & \text{else.} \end{cases}$$

So, this tells us that either $\#E[p] = 0$ or $\#E[p] = p$. A small modification of the above proof shows that $\#E[p^a] = \deg_s(\widehat{\pi})^a$ for every $a \in \mathbb{Z}_{>0}$. Thus, when $E[p] = p$ we have $E[p] \cong \mathbb{Z}/p\mathbb{Z}$. ■

The next corollary follows immediately.

Corollary 4.3.11. *The Tate module of an elliptic curve E/K is a $\mathbb{Z}_\ell$-module. If $\ell \in \mathbb{Z}$ is a prime not equal to p, then $T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$. Otherwise, we have $T_p(E) \cong \{\,0\,\}$ or $\mathbb{Z}_p$.*

Now that we are equipped with information about the Frobenius endomorphism, we will use it to study the number of $\mathbb{F}_q$-rational points on an elliptic curve over $\mathbb{F}_q$.

Proposition 4.3.12. *Let $E/\mathbb{F}_q$ be an elliptic curve and π_E the Frobenius endomorphism. Then*

$$\#E(\mathbb{F}_q) = q + 1 - \mathrm{Tr}(\pi_E)\,.$$

Proof. Using the properties of the degree map, we have the following:

$$\#E(\mathbb{F}_q) = \deg(1 - \pi_E) = \deg(\pi_E) - \mathrm{Tr}(\pi_E) + 1 = 1 + q - \mathrm{Tr}(\pi_E)\,.$$

■

Example 4.3.13. Let $E/\mathbb{F}_5$ be the elliptic curve

$$E : y^2 = x^3 + 2\,.$$

We will see later in Example 4.4.8 that $\#E(\mathbb{F}_5) = 6$. In this case, π_E is the map given by $\pi_E(x, y) = (x^5, y^5)$. Since $\pi_E \in \mathrm{End}(E)$, we know that it is a root of its characteristic polynomial

$$c_{\pi_E}(x) = x^2 - \mathrm{Tr}(\pi_E)x + \deg(\pi_E)\,.$$

But, we also know from the above proposition that $\operatorname{Tr}(\pi_E) = 5 + 1 - \#E(\mathbb{F}_5) = 0$. So, $\pi_E \circ \pi_E = [-5]$. The dual $\widehat{\pi}_E$ is the unique map such that $\widehat{\pi}_E \circ \pi_E = [5]$, so it must be that $\widehat{\pi}_E = -\pi_E$.

Theorem 4.3.14 (Hasse)**.** *Let $E/\mathbb{F}_q$ be an elliptic curve. Then*

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

Proof. Theorem 3.3.6 tells us that $|\operatorname{Tr}(\psi)| \leq 2\sqrt{\deg(\psi)}$ for any $\psi \in \operatorname{End}(E)$. We have just seen that $\pi_E \in \operatorname{End}(E)$, $\deg(\pi_E) = q$, and $\operatorname{Tr}(\pi_E) = q + 1 - \#E(\mathbb{F}_q)$, which proves the result. ∎

The next result was also proved by Hasse and is a generalization of the previous theorem.

Theorem 4.3.15 (Riemann Hypothesis for Elliptic Curves)**.** *Let $E/\mathbb{F}_q$ be an elliptic curve. Then for all integers $m \geq 1$, we have*

$$|\#E(\mathbb{F}_{q^m}) - q^m - 1| \leq 2\sqrt{q^m}\,.$$

4.4. **Supersingular Curves.** We have mentioned several times that one of the interests in exploring elliptic curves over finite fields is that the endomorphism ring may be unusually large. Specifically, Theorem 3.3.11 tells us that $\operatorname{End}(E)$ may be an order in a quaternion algebra. The main result of this section, Theorem 4.4.4, tells us exactly when this occurs.

Recall Proposition 4.3.10 which says that when m and p are coprime, then $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, and if we set $m = p$, then depending on E we have either $E[p] \cong \mathbb{Z}/p\mathbb{Z}$ or $E[p] \cong \{\,0\,\}$.

Definition 4.4.1. An elliptic curve $E/\mathbb{F}_q$ is *supersingular* if $E[p] \cong \{\,0\,\}$. If E is not supersingular, then it is called ordinary.

Remark 4.4.2. There is no relation between singular curves and supersingular elliptic curves, since all elliptic curves are non-singular. The term supersingular is historic, and comes from describing the j-invariants of certain elliptic curves as "singular" when they correspond to elliptic curves of unusual endomorphism rings [6].

Lemma 4.4.3. *If $\widehat{\pi}$ is separable, then the natural map $\operatorname{End}(E) \to \operatorname{End}\big(T_p(E)\big)$ is injective.*

The next theorem gives many equivalences for supersingular curves.

Theorem 4.4.4. *Let $E/\mathbb{F}_q$ be an elliptic curve. The following are equivalent.*

(1) E is supersingular, i.e., $E[p] \cong \{\,0\,\}$.
(2) $\widehat{\pi}$ is purely inseparable.
(3) $[p]$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$.
(4) $\operatorname{End}_{\overline{\mathbb{F}}_q}(E)$ is an order in a quaternion algebra.
(5) $\operatorname{End}_{\overline{\mathbb{F}}_q}(E)$ is not commutative.
(6) $\operatorname{Tr}(\pi_E) \equiv 0 \pmod{p}$.

Proof. (1 $\iff$ 2) From Proposition 4.3.8 we know

$$\#E[p] = \#\big([p]^{-1}(\mathcal{O})\big) = \deg_s([p])\,,$$

Remember that $[p] = \widehat{\pi} \circ \pi$ by definition of the dual isogeny. We showed in Proposition 4.3.5 that π is purely inseparable, so $\deg_s(\widehat{\pi}) = \deg_s([p])$. This means

$$\#E[p] = \deg_s(\widehat{\pi})\,,$$

so $\widehat{\pi}$ is purely inseparable if and only if $\#E[p] = 1$, which occurs exactly when E is supersingular.

(2 $\implies$ 3) If $\widehat{\pi}$ is purely inseparable, then since π is always purely inseparable, we have $[p] = \widehat{\pi} \circ \pi$ is purely inseparable. It remains to show that $j(E) \in \mathbb{F}_{p^2}$.

$\widehat{\pi}$ factors as $\widehat{\pi} = \widehat{\pi}_s \circ \pi$ and $\deg_s(\widehat{\pi}) = 1$ because $\widehat{\pi}$ is purely inseparable. Then,

$$[p] = \widehat{\pi} \circ \pi = \left(\widehat{\pi}_s \circ \pi\right) \circ \pi = \widehat{\pi}_s \circ \pi^2\,,$$

which means $\widehat{\pi}_s : E^{(p^2)} \to E$ is an isomorphism. Theorem 2.3.19 tells us

$$j(E) = j(E^{(p^2)}) = j(E)^{p^2}\,,$$

so $j(E) \in \mathbb{F}_{p^2}$.

(3 $\implies$ 4) Suppose, by way of contradiction, that $\mathrm{End}(E)$ is not an order in a quaternion algebra. Then by Theorem 3.3.11, either $\mathrm{End}(E) = \mathbb{Z}$ or is an order in an imaginary quadratic number field. This means that either $\mathrm{End}(E) \otimes \mathbb{Q} = \mathbb{Q}$ or $\mathbb{Q}(\sqrt{d})$, for some $d < 0$.

We now want to show that the isogeny class of E is finite. Let $\psi : E \to E'$ be an isogeny to some elliptic curve E'. By assumption, we have that $[p]$ is purely inseparable on E and $j(E) \in \mathbb{F}_{p^2}$. The proof of Corollary 4.4.7 shows that $[p]$ is also purely inseparable on E', which means $\#E'[p] = \deg_s[p]$. The proof of (2 $\implies$ 3) shows that we also have $j(E') \in \mathbb{F}_{p^2}$, so there are only finitely-many possibilities for the isogenous elliptic curve E'.

Let $\ell \in \mathbb{Z}$ be any prime $\ell \neq p$ such that ℓ is prime in $\mathrm{End}(E')$ for all elliptic curves E' isogenous to E. We proved in Proposition 4.3.10 that

$$E[\ell^i] \cong \mathbb{Z}/\ell^i\mathbb{Z} \times \mathbb{Z}/\ell^i\mathbb{Z}\,.$$

Since $E[\ell^i] \subset E(\overline{\mathbb{F}}_q)$, there exist subgroups $F_1 \subset F_2 \subset \cdots \subset E$ such that each $F_i \cong \mathbb{Z}/\ell^i$. Denote $E_i = E/F_i$. By Proposition 4.3.9, there exists a unique isogeny $\varphi_i : E \to E_i$ with $\ker(\varphi_i) = F_i$.

Since, as $j(E_i) \in \mathbb{F}_{p^2}$, there are only finitely-many possibilities (up to isomorphism) of isogeneous elliptic curves E_i, there exists positive integers $m, n \in \mathbb{Z}_{>0}$ such that $\iota : E_{m+n} \to E_m$ is an $\mathbb{F}_q$-isomorphism. Since we have started with $F_1 \subset F_2 \subset \cdots \subset E$, there is a natural projection

$$\varpi : E_m \to E_{m+n}$$

which gives an endomorphism $\lambda = \iota \circ \varpi$ with $\ker(\lambda) = F_{m+n}/F_m$. Then $\ker(\lambda)$ is cyclic with order ℓ^n. Remember we chose ℓ to remain prime in $\mathrm{End}(E_m)$. Then, notice that since

$$\ker(\lambda) = F_{m+n}/F_m \subset E[\ell^{m+n}]$$

is a subgroup, there exists an isogeny τ such that

$$\varpi \circ \tau = [\ell^{m+n}]\,.$$

So there must exist $u \in \mathrm{Aut}(E_m)$ such that $\lambda = u \circ [\ell^{n/2}]$. However, $\ker([\ell^{n/2}])$ is never cyclic, which is a contradiction.

($4 \iff 5$) This equivalence is immediate from the characterization of $\mathrm{End}(E)$ in Theorem 3.3.11. Either $\mathrm{End}(E)$ is commutative, in which case $\mathrm{End}(E) \otimes \mathbb{Q} = \mathbb{Q}$ or $\mathbb{Q}(\sqrt{d})$, or $\mathrm{End}(E)$ is not commutative, in which case $\mathrm{End}(E) \otimes \mathbb{Q}$ is a quaternion algebra.

($5 \implies 2$) We prove this direction contrapositively. If $\widehat{\pi}$ is not purely inseparable then $E[p] \neq \{0\}$. Corollary 4.3.11 tells us that either $T_p(E) = \{0\}$ or $\mathbb{Z}_p$. Notice that

$$E[p] \cong T_p(E)/pT_p(E)\,,$$

so we must have $T_p \cong \mathbb{Z}_p$. By Lemma 4.4.3, $\mathrm{End}(E)$ injects into $\mathrm{End}(T_p) \cong \mathrm{End}(\mathbb{Z}_p)$. We know $\mathrm{End}(\mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}$, and taking the inverse limit gives $\mathrm{End}(\mathbb{Z}_p) \cong \mathbb{Z}_p$. Thus, $\mathrm{End}(E)$ injects into $\mathbb{Z}_p$, which is commutative, so $\mathrm{End}(E)$ is commutative.

($2 \iff 6$) We already know π_E is always purely inseparable. If $\widehat{\pi}$ is purely inseparable, then setting $p = q^r$ gives $(\widehat{\pi})^r = \widehat{\pi}_E$. This shows that $\widehat{\pi}_E$ is purely inseparable. Then, $[\mathrm{Tr}(\pi_E)]$ is inseparable, which means $\mathrm{Tr}(\pi_E) \equiv 0 \pmod{p}$. A similar line of reasoning shows that the converse of this is true. ■

Equivalence 6 can be strengthened when π_E is the pth power map, that is when E is defined over $\mathbb{F}_p$.

Corollary 4.4.5. *If $p > 3$. $E/\mathbb{F}_p$ is supersingular if and only if $E(\mathbb{F}_p) = p + 1$.*

Proof. If $p > 3$, then Theorem 4.3.14 says

$$|\,\mathrm{Tr}(\pi_E)| \leq 2\sqrt{p}\,,$$

so, $|\,\mathrm{Tr}(\pi_E)| = 0$ because $p > 2\sqrt{q}$ when $p > 3$. To finish the proof, recall that Proposition 4.3.12 says

$$\#E(\mathbb{F}_p) = p + 1 - \mathrm{Tr}(\pi_E) = p + 1\,.$$

■

Remark 4.4.6. Corollary 4.4.5 fails if $p \leq 3$. For example, it can be seen that

$$E : y^2 + y = x^3 + x \qquad \text{and} \qquad E' : y^2 + y = x^3 + x$$

are both elliptic curves over $\mathbb{F}_2$, but the $\#E(\mathbb{F}_2) = 3 \neq 5 = \#E(\mathbb{F}_2)$.

Using equivalence 3, we obtain another corollary:

Corollary 4.4.7. *If $E_1, E_2/\mathbb{F}_q$ are supersingular, then they are isogenous. That is, the supersingular curves form a single isogeny class.*

Proof. Let $\varphi : E_1 \to E_2$ be an isogeny and suppose E_1 is supersingular. Let $[p]_1 \in \mathrm{End}(E_1)$ and $[p]_2 \in \mathrm{End}(E_2)$ be the multiplication-by-p maps. Then, $[p]_1 \circ \varphi = \varphi \circ [p]_2$, so

$$\deg_s([p]_1)\deg_s(\varphi) = \deg_s(\varphi)\deg_s([p]_2)\,.$$

It follows that $\deg_s([p]_1) = \deg_s([p]_2)$. Then since E_1 is supersingular, $E[p] = \{0\}$, so $\deg_s([p]_1) = 1 = \deg_s([p]_2)$. Thus, E_2 is supersingular as well. ■

In the next two examples, we will use Corollary 4.4.5 to show that specific classes of elliptic curves are supersingular.

Example 4.4.8. Let $p \equiv 2 \pmod 3$ be a prime, let $B \in \mathbb{F}_p^\times$, and let E be the elliptic curve

$$E : y^2 = x^3 + B \,.$$

We will show that $\#E(\mathbb{F}_p) = p+1$. As always, we start by noting $\mathcal{O} \in E(\mathbb{F}_p)$. Note that $\#(\mathbb{F}_p^\times) = p-1$, and since $p \equiv 2 \pmod 3$, we have that $\#(\mathbb{F}_p^\times)$ is coprime to 3.

Under the birational map $(x, y) \mapsto (x, y + 1/2)$, E is equivalent to

$$E' : y^2 + y = x^3 + B \,.$$

This means that for each $y \in \mathbb{F}_p$, there exists a unique $x \in \mathbb{F}_p$ such that $y^2 + y = x^3 + B$. This gives us p points in $E(\mathbb{F}_p)$ in addition to the base point $\mathcal{O}$, so we can conclude that $\#E(\mathbb{F}_p) = p + 1$.

Example 4.4.9. Let $p \equiv 3 \pmod 4$ be a prime and let E be the elliptic curve

$$E : y^2 = x^3 - x \,.$$

We will show that $\#E(\mathbb{F}_p) = p + 1$. Again, we clearly have $\mathcal{O} \in \mathbb{E}(\mathbb{F}_p)$. There are also three trivial solutions, which are $(0, 0)$, $(1, 0)$, and $(-1, 0)$.

Next we count the number of non-zero squares in $\mathbb{F}_p$ equal to $x^3 - x$, for some x. Consider an element $x \in \mathbb{F}_p$ such that $x \neq 0, 1, p-1$. Note that either $x^3 - x$ or (not inclusive) $(-x)^3 - (-x)$ is a square in $\mathbb{F}_p$. Then there are are $(p-3)/2$ non-zero squares equal to $x^3 - x$.

This gives us $2(p-3)/2 = p - 3$ non-trivial solutions to $y^2 = x^3 - x$. Adding the four trivial solutions we counted in the beginning yields $\#E(\mathbb{F}_p) = p + 1$.

The next theorem gives us information about how many supersingular curves there are, up to isomorphism, modulo p, for each prime p.

Theorem 4.4.10 (Deuring, Eichler)**.** *The following sum is taken over supersingular curves up to isomorphism.*

$$\frac{p-1}{24} = \sum_{\substack{E/\overline{\mathbb{F}}_p \\ \textit{supersingular}}} \frac{1}{\#\operatorname{Aut}(E)} \,.$$

The above theorem gives us a few notable corollaries. First, since

$$\#\operatorname{Aut}(E) = \begin{cases} 24 & p = 2\,; \\ 12 & p = 3\,, \end{cases}$$

we have that there is exactly one supersingular curve over $\overline{\mathbb{F}}_2$ and one supersingular curve over $\overline{\mathbb{F}}_3$ (up to isomorphism). Specifically, these curves are given by the equations

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

and

$$y^2 = x^3 - x \,,$$

respectively. Note that this does not mean that there is one supersingular curve over $\mathbb{F}_2$ and over $\mathbb{F}_3$. For example, over $\mathbb{F}_2$ there are three supersingular curves up to isomorphism, namely the curves given by

$$y^2 + y = x^3 + x + 1\,, \quad y^2 + y = x^3 + 1\,, \quad \text{and} \quad y^2 + y = x^3 + x\,.$$

4.5. **Elliptic Curve Reduction.** We conclude this thesis by showing an application of elliptic curves over finite fields to the theory of elliptic curves over $\mathbb{Q}$.

Theorem 4.5.1 (Mordell, 1923)**.** *$E(\mathbb{Q})$ is a finitely generated group.*

We also know that $E(\mathbb{Q})$ is abelian, so Theorem 4.5.1 specifically implies that

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r \,,$$

for some non-negative integer $r \in \mathbb{Z}_{r\geq 0}$ called the rank of E. In general, this type of decomposition into the torsion subgroup and finitely-many copies of $\mathbb{Z}$ is a property of finitely generated abelian groups.

Definition 4.5.2. If E is given by a Weierstrass equation with smallest possible discriminant, then we say E has a minimal model.

Suppose we have an elliptic curve $E/\mathbb{Q}$ given by a minimal model

$$E : y^2 = x^3 + Ax + B \,,$$

for some $A, B \in \overline{\mathbb{Q}}$, and we want to ask if

$$\widetilde{E} : y^2 = x^3 + A'x + B'$$

is an elliptic curve over $\mathbb{F}_p$, where $A' \equiv A \,(\text{mod}\, p)$ and $B' \equiv B \,(\text{mod}\, p)$. The only condition we need to verify is if the discriminant of this new (possibly singular) curve is non-zero. That is,

$$\Delta_{\widetilde{E}} = -16(4A'^3 + 27B'^2) \not\equiv 0 \,(\text{mod}\, p) \,.$$

if and only if $\widetilde{E}/\mathbb{F}_p$ is an elliptic curve. Of course, this is entirely dependent on our choice of prime p.

Definition 4.5.3. If p is a prime such that $\widetilde{E}/\mathbb{F}_p$ is an elliptic curve, we say p is a *prime of good reduction.* If $\widetilde{E}/\mathbb{F}_p$ is not an elliptic curve, we say p is a *prime of bad reduction.*

Example 4.5.4. Let E be the elliptic curve

$$E : y^2 = x^3 - 4x + 4 \,.$$

If we reduce E over $\mathbb{F}_3$, we get

$$\widetilde{E}_3 : y^2 = x^3 + 2x + 1 \,,$$

which has discriminant

$$\Delta_{\widetilde{E}_3} = -16(4(2)^3 + 27(1)^2) = -944 \equiv 1 \,(\text{mod}\, 3) \,.$$

This means 3 is a prime of good reduction.

If we reduce E over $\mathbb{F}_2$, we get

$$\widetilde{E}_2 : y^2 = x^3 \,,$$

which has discriminant $\Delta_{\widetilde{E}_2} = 0$, so 2 is a prime of bad reduction. A quick calculation shows that there is also bad reduction at 11.

Proposition 4.5.5. *An elliptic curve over $\mathbb{Q}$ has bad reduction at prime p if and only if p divides the discriminant of the elliptic curve.*

An immediate corollary is that an elliptic curve has only finitely many primes of bad reduction.

Note that when we introduced $\widetilde{E}$ we required that E be given by a minimal Weierstrass model. The next example shows what would have happened if we did not have this condition.

Example 4.5.6. Let $E/\mathbb{Q}$ be the elliptic curve given by

$$E : y^2 = x^3 + 5^6 \,,$$

which has discriminant $\Delta = -2^4 \cdot 3^3 \cdot 5^{12}$. If we reduced E over $\mathbb{F}_5$, then we would get the curve

$$\widetilde{E} : y^2 = x^3 \,,$$

which is singular. So it appears as though E has bad reduction at 5. However, since Δ contains 5^{12} as a factor, we can use a change of variables

$$(x, y) \mapsto (5^2 x, 5^3 y)$$

to see that E is also given by the model

$$E : y^2 = x^3 + 1$$

in which 5 is no longer a bad prime. So, the original bad-prime could be "removed" by switching to a different model. Specifically, we removed the factor 5^{12} from the discriminant. These removable bad-primes do not appear when we remove all factors p^{12} from the discriminant, which is exactly what it means for E to be given by a minimal model.

Proposition 4.5.7. *Whenever p is not a prime of bad reduction, there is an injection*

$$E(\mathbb{Q})_{tors} \to E(\mathbb{F}_p) \,.$$

Example 4.5.8. Let $n \in \mathbb{Z}_{>0}$ and consider the elliptic curve

$$E_n : y^2 = x^3 - n^2 x \,.$$

We will try to determine the structure of $E_n(\mathbb{Q})_{\text{tors}}$. Of course, we always have $\mathcal{O} \in E_n(\mathbb{Q})_{\text{tors}}$. First, notice that by looking at the equation defining E_n, we get three more points in $E_n(\mathbb{Q})$ for free, namely $(0, 0)$, $(n, 0)$, and $(-n, 0)$. Furthermore, each of these points has order 2 in $E_n(\mathbb{Q})$, so they are all in $E_n(\mathbb{Q})_{\text{tors}}$.

Recall Example 4.4.9, which tells us that whenever $p \equiv 3 \pmod 4$ is a prime, we have $\#E_n(\mathbb{F}_p) = p+1$. Whenever p is a prime of good reduction, $E_n(\mathbb{Q})_{\text{tors}}$ injects into $E_n(\mathbb{F}_p)$. This means that $\#E_n(\mathbb{Q})_{\text{tors}}$ divides $p+1$ for all but finitely-many primes $p \equiv 3 \pmod 4$.

A result from elementary number theory is that if $k > 4$ is an integer, then there exists infinitely many primes $p \equiv 3 \pmod 4$ such that $p + 1$ is *not* divisible by k.

With this fact, we see that $\#E_n(\mathbb{Q})_{\text{tors}}$ cannot be larger than 4 or else we would contradict our original deductions. Thus, $E_n(\mathbb{Q})_{\text{tors}}$ consists only of the four points we found earlier, which shows

$$E_n(\mathbb{Q})_{\text{tors}} = \{\, \mathcal{O}, (0, 0), (n, 0), (-n, 0) \,\} \,.$$

Given an elliptic curve over $\mathbb{Q}$, we may want to ask for which primes p is the reduction $\widetilde{E}$ over $\mathbb{F}_p$ supersingular.

Example 4.5.9. Consider the elliptic curve

$$E : y^2 = x^3 + x\,.$$

Notice that E has only one prime of bad reduction, namely 2. Whenever $p \neq 2$ is a prime, it is equivalent to either 1 or 3 modulo 4. Recall that in Example 4.3.1 we showed $\#\widetilde{E}(\mathbb{F}_p) \equiv 0 \pmod 4$. Then $\widetilde{E}$ is supersingular over $\mathbb{F}_p$ exactly when $p \equiv 3 \pmod 4$.

Conclusion

In this thesis, we examined the theory of elliptic curves over finite fields. We explored what it means for elliptic curves to be isogeneous and developed the theory of isogenies which included dual isogenies, the endomorphism ring, the Frobenius endomorphism, and separable/purely inseparable isogenies. Over finite fields, we used the Tate module to show that elliptic curves are isogeneous over $\mathbb{F}_q$ exactly when they have the same number of $\mathbb{F}_q$-rational points.

We saw what the possible structure of the endomorphism ring is over arbitrary fields and gave a more detailed description of the ring when the field is finite. In particular, we classified elliptic curves over finite fields as either supersingular or ordinary and saw many equivalences for determining this characterization.

Lastly, as we have just seen in the previous section, we explored an application of finite fields. Specifically, we used our knowledge of finding the number of $\mathbb{F}_q$-rational points on an elliptic curve to help us understand elliptic curves over $\mathbb{Q}$.

I will close this thesis by stating there is much more to learn about elliptic curves over finite fields. An important and interesting topic that was not covered is the Weil conjectures, which involve zeta functions associated to elliptic curves. A good reference for this is Chapter V.2 of [5].

References

[1] D.S. Dummit and R.M. Foote, *Abstract Algebra*, Wiley, Hoboken, 2004.

[2] D. Husemöller, *Elliptic Curves*, Graduate Texts in Math., Vol. 111, 2nd ed., Springer, New York, 2004.

[3] A. Lozano-Robled, *Number Theory and Geometry: An Introduction to Arithmetic Geometry*, Pure and Applied Undergraduate Texts, American Mathematical Society, 2019.

[4] S. Roman, *An Introduction to the Language of Category Theory*, Compact Textbooks in Math., Birkhäuser, 2017.

[5] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math., Vol. 106, 1st ed., Springer-Verlag, New York, 1986.

[6] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Math., Vol. 151, 1st ed., Springer-Verlag, New York, 1994.

[7] J. H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Undergraduate Texts in Math., 2nd ed., Springer, Switzerland, 2015.

[8] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Inventiones Math. **160**, 134–144 (1966).