

The Group Structure of Elliptic Curves Defined over Finite Fields

A Senior Project submitted to
The Division of Science, Mathematics, and Computing
of
Bard College

by
Andrija Peruničić

Annandale-on-Hudson, New York
April 30, 2008

Abstract

An elliptic curve defined over a field k is the set of solutions to the polynomial equation $y^2 = x^3 + ax + b$ where a and b lie in k . There exists a well defined addition of points on each elliptic curve. In fact, points on an elliptic curve form an abelian group under this operation.

Typically, coordinates of our solutions lie in the closure of the field k over which the curve is defined. However, we can allow the coordinates of our points to lie only in a particular extension of k . The addition operation is well defined on this set as well, and thus we can associate a group to every extension k' of the base field k . For an elliptic curve E , denote this group by $E(k')$.

Now it makes sense to ask the following question. For an elliptic curve E defined over a finite field \mathbb{F}_p of characteristic p , to what extent does $E(\mathbb{F}_p)$ determine $E(\mathbb{F}_{p^2})$, where \mathbb{F}_{p^2} is a degree two extension of \mathbb{F}_p ? This project tackles exactly this question.

Contents

Abstract	1
Acknowledgments	4
1 Introduction	5
2 Preliminaries	10
2.1 Algebraic Geometry	10
2.2 Projective Geometry	15
3 Geometry of Elliptic Curves	23
3.1 Definition of an Elliptic Curve	23
3.2 The Group Structure of Elliptic Curves	27
3.3 Elliptic Curves Defined over Finite Fields	34
4 Behavior of Elliptic Curves Under Field Extensions	38
4.1 Statement of the Problem	38
4.2 The Supersingular Case	39
4.3 The $a_p = -1$ Case	40
4.4 The $a_p = 1$ Case	41
4.5 Further Research	48
A Connection of Elliptic Curves to Ellipses	49

List of Figures

1.0.1 Elliptic curves $y^2 = x^3 - x$ and $y^2 = x^3 - x + 1$ graphed over the real numbers	7
1.0.2 "Adding" two points on an elliptic curve	7
3.2.1 The addition law ($P + Q$) and a point of inflection ($P + P = \mathcal{O}$)	29
3.2.2 Inverse of a point P	31

Acknowledgments

I am particularly grateful to John Cullinan for introducing me to a lot of interesting mathematics and being such a great adviser! I would also like to thank the other two members of my board, Lauren Rose and Matthew Deady, for supporting me and my project. Finally, I owe a large debt of gratitude to Heidi Choi for her patience and love.

1

Introduction

The study of Diophantine equations deals with finding integer or rational number solutions to polynomial equations. This area of number theory is named after one of the great ancient Greek mathematicians, Diophantus of Alexandria, who solved many such problems. The simplest Diophantine equation is a polynomial equation in one variable:

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = 0.$$

These equations are easily solved by Gauss' lemma which states that if p/q is a rational solution written in lowest terms, then q divides a_n and p divides a_0 . By trying each of the possible solutions, we can quickly assemble all of the actual ones.

The situation changes greatly when we look at Diophantine equations in two variables, that is, polynomial equations of the form

$$f(x, y) = 0.$$

The set of real solutions to such an equation forms a curve in the Euclidean plane. The simplest curve arising from a polynomial equation in two variables is that of a line, and it

is given by a degree 1 polynomial of the form

$$ax + by = c.$$

There are always infinitely many rational solutions, there are no integer solutions if $\gcd(a, b)$ doesn't divide c , and there are infinitely many integer solutions otherwise. So, linear equations are also easy.

The next family of curves are conic sections, given by various degree 2 polynomials. It turns out, if there is one rational solution, then there are infinitely many. This can be shown using simple geometry (see [7, Chapter 1]) so the situation isn't yet all that bad.

The first interesting family of curves is given by degree 3 polynomial equations of the form

$$y^2 = x^3 + ax^2 + bx + c.$$

We call these curves **elliptic curves**, which are so named because they arise when computing the arclength of an ellipse (see Appendix A). For examples of elliptic curves graphed over the real numbers see Figure 1.0.1. The integer and rational solutions to these equations are still not completely understood. For example, it is known that there are only finitely many integer solutions and there is an explicit upper bound, but it is too large to be practical. Also, all of the (possibly infinitely many) rational solutions may be found by starting with a known set of solutions, and getting new ones by "adding" two solutions on the elliptic curve. This is done by finding the third intersection point of the line connecting the original two solutions and the elliptic curve as in Figure 1.0.2. However, there is no method to find the initial generating set of rational solutions: we have to guess. So, studying integer or rational solutions to the simplest family of cubic equations really is non-trivial.

In fact, proofs of the results mentioned in the previous paragraph are often very difficult and require techniques from area of mathematics as diverse as geometry, number theory

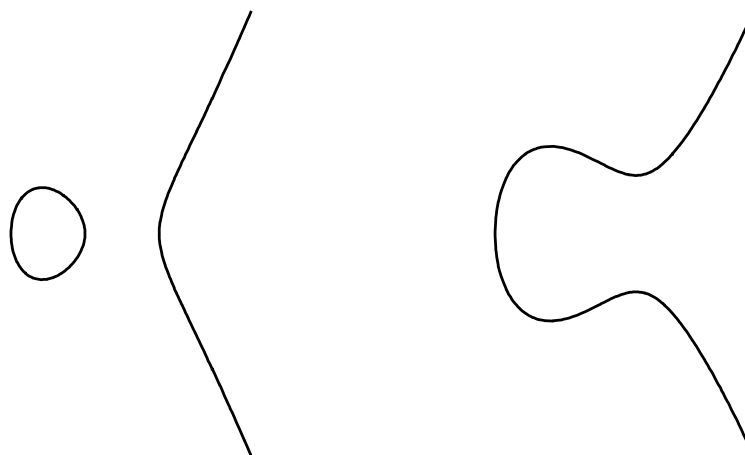


Figure 1.0.1. Elliptic curves $y^2 = x^3 - x$ and $y^2 = x^3 - x + 1$ graphed over the real numbers

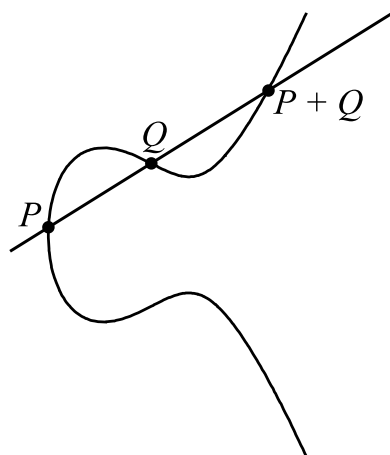


Figure 1.0.2. "Adding" two points on an elliptic curve

and algebra. Geometry enters because we can consider the solutions of our cubic equations as curves and because we get new solutions by intersecting various lines with our curve. Number theory is present in the fact that we are looking for integer and rational solutions. Algebra, however, has a more subtle role and provides us with a fundamentally important tool in studying elliptic curves.

Polynomials are algebraic objects, but the connection of elliptic curves to algebra is less obvious. We have mentioned that by finding the intersection of the elliptic curve and the line connecting two rational points on the curve we can find a third rational point of intersection, which is guaranteed to exist by Bézout's theorem (*cf.* Theorem 3.2.2). This process, slightly modified, gives us *an abelian group of points on the elliptic curve!* Thus, we can use group theory to study rational solutions on elliptic curves. In fact, the proofs of the results mentioned above rely heavily on this fact.

However, there is nothing special about rational solutions. We can generalize our definition of the elliptic curve and work over any field.

Definition 1.0.1. An **elliptic curve** E defined over a field k is the set of \bar{k} solutions to the polynomial equation

$$y^2 = x^3 + ax^2 + bx + c$$

where $a, b, c \in k$.

△

Instead of looking only at solutions (or points) with coordinates in the closure of the field k over which the curve is defined, we can restrict our attention to those points with coordinates that lie only in a particular extension of k . The addition operation is well defined on this set as well, and thus we can associate a group to every extension k' of the base field k . For an elliptic curve E , denote this group by $E(k')$.

In this project, we consider curves defined over finite fields of characteristic p , denoted \mathbb{F}_p . We are interested in the set of points with coordinates in the degree two extension

of \mathbb{F}_p , denoted \mathbb{F}_{p^2} . More specifically, we are interested in the group structure of $E(\mathbb{F}_{p^2})$. Because we want to be able to easily determine this group, we ask the following question. Given $E(\mathbb{F}_p)$, to what extent is $E(\mathbb{F}_{p^2})$ determined? In general, this question has proven to be very difficult. However, we have successfully solved the problem for certain special cases of curves, classified based on the number of points on them.

A considerable amount of background theory is necessary to properly understand elliptic curves and the associated groups. The reader should be familiar with basic group and field theory, including basics of finite fields. See [3] for an excellent introduction to these subjects.

In Chapter 2 we introduce the necessary background to define elliptic curves. In the first section we define affine varieties, ideals and some associated concepts. We do this since we will eventually define elliptic curves as varieties arising from ideals generated by equations in the form of the one from Definition 1.0.1. In the second section we provide the connection between affine and projective varieties since elliptic curves live in projective space, if only just.

In Chapter 3 we use the first two sections to provide a general definition of elliptic curves, simplify it and show how to associate a group to an elliptic curve. In the last section, we state some useful results about elliptic curves over finite fields.

In Chapter 4 we finally formally state the central problem of this project and present the main results.

2

Preliminaries

2.1 Algebraic Geometry

In this section we provide an introduction to the algebraic geometry needed to define and understand elliptic curves. We begin with a definition of the space in which we are working.

Definition 2.1.1. Let k be a field. **Affine n -space (over k)** is the set of all n -tuples of elements of k , denoted \mathbb{A}_k^n or simply \mathbb{A}^n . \triangle

For example, if $k = \mathbb{R}$, then $\mathbb{A}^n(k) \cong \mathbb{R}^n$. We can start building up the definition of an affine variety. Let $k[\mathbf{x}] = k[x_1, \dots, x_n]$ be the ring in n variables over k and let T be any subset of $k[\mathbf{x}]$.

Definition 2.1.2. The **zero set of T** or an **(affine) algebraic set** is a subset of \mathbb{A}^n of the following form

$$Z(T) = \{P \in \mathbb{A}^n : f(P) = 0 \text{ for all } f \in T\}.$$

\triangle

We know that T generates an ideal \mathfrak{a} of $k[\mathbf{x}]$ and that this ideal has a finite set of generators f_1, \dots, f_m , since $k[\mathbf{x}]$ is a Noetherian ring (see [2, Theorem 2.5.4], for instance). Therefore, $Z(T) = Z(\mathfrak{a})$ is the set of common zeros of the polynomials f_1, \dots, f_m . We can also go the other way.

Definition 2.1.3. Let Z be an algebraic set. The **ideal of Z** is given by

$$I(Z) = \{f \in k[\mathbf{x}] : f(P) = 0 \text{ for all } P \in Z\}.$$

△

We want to explore the relationship between algebraic sets and their ideals. Shortly, we will prove a theorem telling us when the variety-ideal correspondence is bijective.

Example 2.1.4. Suppose we are working over the polynomial ring $\mathbb{C}[x, y]$ and let $f = x^2 + y^2 = (x + iy)(x - iy)$. Then $Z(f) = Z(x + iy) \cup Z(x - iy)$ (see [2, Lemma 1.2.2]). ◇

Definition 2.1.5. A **prime ideal** is an ideal I such that if $ab \in I$, either $a \in I$ or $b \in I$. △

Since multiplication corresponds to union in passing from ideals to varieties, the previous example suggests that we are only interested in irreducible polynomials, and more generally prime ideals, as generators of our algebraic sets. The following definitions and theorem show our intuition to be correct.

Definition 2.1.6. An algebraic set is **irreducible** if it cannot be expressed as a union of other algebraic sets. △

Consider $V(xz, yz)$ as a subset of \mathbb{R}^3 . This variety is the union of the xy -plane and the z -axis. Intuitively, it is natural to think of the line and the plane as more fundamental than $V(xz, yz)$. We formalize this notion.

Definition 2.1.7. An irreducible affine algebraic set V is called an **(affine) variety**. △

Theorem 2.1.8 (Hilbert's Nullstellensatz). *There is an injective, inclusion-reversing correspondence between algebraic sets in \mathbb{A}^n and radical ideals (i.e., ideals I in which $f^m \in I$ implies $f \in I$) in $k[\mathbf{x}]$, given by $V \rightarrow I(Z)$ and $\mathfrak{p} \rightarrow Z(\mathfrak{a})$. An algebraic set V is a variety if and only if its ideal $I(V)$ is prime.*

Proof. See either [4, Chapter 1] or [2, Chapter 4.2]. □

This theorem allows us to uniquely identify varieties, and later curves, with their generating prime ideals. Furthermore, we intuitively see a curve as being one dimensional, and a surface as two dimensional even if it is curved in three dimensional affine space for instance. We now develop the notion of the dimension of a variety. We start with an example.

Example 2.1.9. Consider the ideal

$$I = \langle yz, xz, xyz \rangle \subset k[x, y, z]$$

and let H_x be the plane defined by $x = 0$ with H_y and H_z defined similarly. Let H_{xy} be the line defined by $x = y = 0$. Then

$$\begin{aligned} V(I) &= V(xz) \cap V(yz) \cap V(xyz) \\ &= (H_y \cup H_z) \cap (H_x \cup H_z) \cap (H_x \cup H_y \cup H_z) \\ &= H_z \cup H_{xy} \end{aligned}$$

consists of the xy -plane H_z together with the z -axis $x = y = 0$. As subspaces of k^3 , these two have dimensions 2 and 1, respectively, and we take the bigger of the two as the dimension of V . In other words, $\dim(V) = 2$. ◇

Since a variety $V(I)$ of a monomial ideal $I \in k[\mathbf{x}]$ is a finite union of vector subspaces of k^n by [2, Proposition 9.1.1], we can generalize the process from the previous example and define the dimension of V as the dimension of the largest of the subspaces that compose

it. A crucial result due to Hilbert states that the dimension of a variety of a monomial ideal can be characterized by the growth of the number of monomials of certain degree *not* in $I(V)$, as their degree increases (see [2, Theorem 9.2.6]). We are able to fully generalize this notion to any ideal in $k[\mathbf{x}]$ using the following definition.

Definition 2.1.10. Let V be a variety and $R = k[\mathbf{x}]$. We define the **affine coordinate ring of V** to be

$$k[V] = \frac{R}{I(V)}.$$

△

The coordinate ring $k[V]$ of polynomial functions $f: V \rightarrow k$ is so called since every polynomial function on V is a k -linear combination of products of the coordinate functions $x_i: V \rightarrow k$ whose value at a point $P \in V$ is the i th coordinate of P .

To see how $k[V]$ relates to the dimension of V , let $I_{\leq s}$ be all polynomials of I of total degree $\leq s$. Both $k[\mathbf{x}]$ and $I(V)$ can be seen as infinite dimensional vector spaces over k . On the other hand, since there are only finitely many monomials for each s (see [2, Theorem 9.2.4]), restricting an ideal to polynomials of degree $\leq s$ gives us a finite dimensional vector space over k . Consider the injective linear map

$$\alpha_s: k[\mathbf{x}]_{\leq s} / I(V)_{\leq s} \rightarrow k[\mathbf{x}] / I(V) = k[V]$$

defined by $\alpha_s([f]) = [f]$ for each $s \geq 0$. This map allows us to say that $k[\mathbf{x}]_{\leq s} / I(V)_{\leq s}$ is a finite dimensional piece of $k[V]$ that approximates it more closely as s gets larger (see [2, Proposition 9.3.1] for a proof that a quotient of finite dimensional vector spaces is finite dimensional). Following Hilbert's result for monomial ideals, we want the dimension of V to measure how fast these finite dimensional approximations of $k[V]$ are growing, since our intuition about the quotient R/I of a polynomial ring R by an ideal $I \subset R$ tells us that it composes of exactly those polynomials of R not in I . Therefore, $\dim(V)$ conveys information about the size of $k[V]$, and vice-versa.

To find the size of $k[V]$, we notice that since $I(V)$ is a prime ideal, $k[V]$ is an integral domain and we make the following definition.

Definition 2.1.11. The quotient field of $k[V]$, denoted $k(V)$ is called the **function field of V** . In particular

$$k(V) = \{[f]/[g] : f, g \in k[\mathbf{x}], g \notin I(V)\},$$

where $[f]$ denotes the equivalence class of f . Similarly $\bar{k}[V]$ and $\bar{k}(V)$ are defined by replacing k with \bar{k} . △

Since $k(V)$ is the smallest field containing $k[V]$, we can gauge the size of $k[V]$ through $k(V)$ and define the dimension of a variety of an ideal by looking at the size of $k(V)$. We use the transcendence degree of $k(V)$ to accomplish this task.

Definition 2.1.12. The elements $\phi_1, \dots, \phi_r \in k[V]$ are **algebraically independent over k** if there is no nonzero polynomial p of r variables with coefficients in k such that $p(\phi_1, \dots, \phi_r) = 0$ in $k[V]$. △

Definition 2.1.13. Let K be a field extension of k . Then K has **transcendence degree d over k** provided that d is the largest number of elements of K that are algebraically independent over k . △

Definition 2.1.14. The **dimension of V** , denoted by $\dim(V)$, is the transcendence degree of $k(V)$ over k . △

For a more detailed description of dimension of a variety, see [2, Chapter 9]. We will return to dimension when showing that an elliptic curve has degree 1 as a variety. In addition to its dimension, when working with a geometric object we want to determine how smooth it is. We do this using the usual Jacobian criterion for the existence of a tangent plane from vector calculus.

Definition 2.1.15. Let V be a variety, and $f_1, \dots, f_m \in k[x_1, \dots, x_n]$ be a set of generators for $I(V)$. Then V is **non-singular (or smooth)** at $P \in V$ if the Jacobian matrix

$$\begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_m}{\partial x_1} & \cdots & \frac{\partial f_m}{\partial x_n} \end{pmatrix}$$

evaluated at P has rank $n - \dim(V)$. △

Example 2.1.16. Suppose that V is generated by a single polynomial equation $f \in k[x_1, \dots, x_n]$. Then $\dim(V) = n - 1$ and P is a singular point if and only if the Jacobian matrix evaluated at P has rank not equal to one. Hence, it has to have rank of zero, which is true only if

$$\frac{\partial f}{\partial x_1} = \dots = \frac{\partial f}{\partial x_n} = 0,$$

where each partial derivative is evaluated at P . ◇

We want to define elliptic curves as certain affine varieties of dimension one. In order to be able to associate a group to an elliptic curve, we need the concept of points at infinity. For this purpose we need to introduce projective space.

2.2 Projective Geometry

Historically, projective space arose through the process of adding points at infinity to affine space. Points at infinity are added to affine space in order to have every pair of lines, including parallel ones, intersect at one point. Thus, points at infinity can be seen as a set of directions in affine space corresponding to the directions of different classes of parallel lines. Throughout this section we will denote $k[x_0, \dots, x_n]$ by $k[\mathbf{x}]$ giving this notation double meaning, but this will not cause ambiguity as the use of $k[\mathbf{x}]$ will be clear from context.

Definition 2.2.1. **Projective n -space** (over k), denoted \mathbb{P}^n (or $\mathbb{P}^n(k)$) is the set of all $(n+1)$ -tuples

$$(x_0, \dots, x_n) \in \mathbb{A}_k^{n+1}$$

such that not all x_i are zero, under the equivalence relation given by

$$(x_0, \dots, x_n) \sim (y_0, \dots, y_n)$$

if there exists a $t \in \bar{k}$ with $x_i = ty_i$ for all i . An equivalence class is denoted $[x_0, \dots, x_n]$. \triangle

In projective space, we are naturally interested in polynomials f such that if $f(a_0, \dots, a_n) = 0$ then $f(ta_0, \dots, ta_n) = 0$ for all $t \in \bar{k}$, or in other words, the polynomials f that have a zero on the entire equivalence class $[a_0, \dots, a_n]$.

Definition 2.2.2. A polynomial $f \in k[\mathbf{x}]$ is **homogeneous of degree d** if

$$f(\lambda x_0, \dots, \lambda x_n) = \lambda^d f(x_0, \dots, x_n).$$

Further, an ideal $I \subset k[\mathbf{x}]$ is a **homogeneous ideal** if it is generated by homogeneous polynomials. \triangle

One can easily verify that all monomials of a homogeneous polynomial are of the same degree. Using homogeneous polynomials, we can define projective algebraic sets, varieties and their ideals as we have similarly done in affine space.

Definition 2.2.3. A **(projective) algebraic set** is a subset of \mathbb{P}^n of the following form

$$V_I = \{P \in \mathbb{P}^n : f(P) = 0 \text{ for all } f \in I \text{ where } I \text{ is a homogeneous ideal}\}.$$

The **(homogeneous) ideal** of a projective algebraic set V_I is the ideal $I(V_I) \subset \bar{k}[\mathbf{x}]$ such that

$$I(V_I) = \{f \in \bar{k}[\mathbf{x}] : f \text{ is homogeneous and } f(P) = 0 \text{ for all } P \in V_I\}.$$

A projective algebraic set V is called a **(projective) variety** if its homogeneous ideal $I(V)$ is a prime ideal in $\bar{k}[\mathbf{x}]$. \triangle

It is not hard to see that \mathbb{P}^n contains many copies of \mathbb{A}^n . For each $0 \leq i \leq n$, there is an inclusion

$$\begin{aligned} \phi_i: \mathbb{A}^n &\longrightarrow \mathbb{P}^n \\ (x_1, \dots, x_n) &\longrightarrow [x_1, \dots, x_i, 1, x_{i+1}, \dots, x_n]. \end{aligned} \tag{2.2.1}$$

We can also project from \mathbb{A}^n into \mathbb{P}^n . Let U_i be the complement of the hyperplane $x_i = 0$ in \mathbb{P}^n ,

$$U_i = \{P = [x_0, \dots, x_n] \in \mathbb{P}^n : x_i \neq 0\}. \tag{2.2.2}$$

Then there is a natural bijection

$$\begin{aligned} \phi_i^{-1}: U_i &\longrightarrow \mathbb{A}^n \\ [x_0, \dots, x_n] &\longrightarrow \left(\frac{x_0}{x_i}, \dots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \dots, \frac{x_n}{x_i} \right). \end{aligned} \tag{2.2.3}$$

We see that the maps ϕ_i and ϕ_i^{-1} are inverses:

$$\begin{aligned} [x_0, \dots, x_n] &\xrightarrow{\phi_i^{-1}} \left(\frac{x_0}{x_i}, \dots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \dots, \frac{x_n}{x_i} \right) \\ &\xrightarrow{\phi_i} \left[\frac{x_0}{x_i}, \dots, \frac{x_{i-1}}{x_i}, 1, \frac{x_{i+1}}{x_i}, \dots, \frac{x_n}{x_i} \right] = [x_0, \dots, x_n], \end{aligned}$$

where the last equality follows because we are using homogeneous coordinates. Next, we show that this bijection gives us means of going between varieties in projective and affine space, losing track only of points on the hyperplane $x_i = 0$, which we will handle separately.

Lemma 2.2.4. *Let V be a projective algebraic set with homogeneous ideal $I(V) \subset \bar{k}[\mathbf{x}]$. Then $V \cap \mathbb{A}^n = \phi_i^{-1}(V \cap U_i)$ is an affine algebraic set with ideal $I(V \cap \mathbb{A}^n)$ where U_i and ϕ_i^{-1} are as defined in Equations (2.2.2) and (2.2.3).*

Proof. From the definitions of V and U_i we have

$$V \cap U_i = \{P \in \mathbb{P}^n : x_i \neq 0 \text{ and } f(P) = 0 \text{ for all } f \in I(V)\}$$

and consequently

$$V \cap \mathbb{A}^n = \phi_i^{-1}(V \cap U_i) = \left\{ \left(\frac{a_0}{a_i}, \dots, \frac{a_{i-1}}{a_i}, 1, \frac{a_{i+1}}{a_i}, \dots, \frac{a_n}{a_i} \right) : [a_0, \dots, a_n] \in V \right\}.$$

Next, assume that $f \in \bar{k}[\mathbf{x}]$ is a homogeneous polynomial of degree d and collect monomials having the same power of x_i :

$$\begin{aligned} f &= \sum_{j=0}^d x_i^j f_j \\ &= x_i^d \sum_{j=0}^d \frac{f_j}{x_i^j} \\ &= x_i^d \sum_{j=0}^d f_j \left(\frac{x_0}{x_i}, \dots, \frac{x_n}{x_i} \right) \\ &= x_i^d f \left(\frac{x_0}{x_i}, \dots, \frac{x_{i-1}}{x_i}, 1, \frac{x_{i+1}}{x_i}, \frac{x_n}{x_i} \right). \end{aligned}$$

Denote $f(\frac{x_0}{x_i}, \dots, \frac{x_{i-1}}{x_i}, 1, \frac{x_{i+1}}{x_i}, \frac{x_n}{x_i})$ by $f_*(y_0, \dots, y_{i-1}, 1, y_{i+1}, \dots, y_n)$, identifying $\frac{x_j}{x_i}$ with y_j . If $a = [a_0, \dots, a_n]$ is a zero of f , then $a_* = (\frac{a_0}{a_i}, \dots, \frac{a_{i-1}}{a_i}, 1, \frac{a_{i+1}}{a_i}, \dots, \frac{a_n}{a_i})$ is a zero of f_* since

$$0 = f(a) = a_i^d f_*(a_*).$$

Define $I_* = \{f_* : f = I(V)\}$. Clearly, I_* is an ideal and the affine variety it defines is precisely $V \cap \mathbb{A}^n$. \square

We see that in addition to giving us a way to pass from projective to affine varieties, Lemma 2.2.4 in its proof also gives us a way to pass from polynomials (and consequently ideas) in projective space to their counterparts in affine space. This process is called dehomogenization.

Definition 2.2.5. Let V be a projective algebraic set with homogeneous ideal $I(V) \subset \bar{k}[\mathbf{x}]$. Then $V \cap \mathbb{A}^n = \phi_i^{-1}(V \cap U_i)$ is an affine algebraic set with ideal $I(V \cap \mathbb{A}^n) \subset \bar{k}[\mathbf{x}]$ given by

$$I(V \cap \mathbb{A}^n) = \{f_*(x_0, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_n) : f(x_0, \dots, x_n) \in I(V)\}.$$

The process of replacing $f(x_0, \dots, x_n)$ with $f_*(x_0, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_n)$ is called **dehomogenization of f with respect to x_i** . \triangle

Note that the polynomial f_* is in n variables.

Example 2.2.6. Let $f(x, y, z) = y^2z - x^3 + z^3 \in \bar{k}[\mathbf{x}]$. Then $f_*(x, y) = y^2 - x^3 + 1$ is the dehomogenization of f with respect to z . \diamond

We now give the counterpart to Lemma 2.2.4 that allows us to project varieties from affine to projective space.

Definition 2.2.7. Let V be an affine algebraic set with ideal $I(V)$. Then the set \bar{V} obtained from V via the map

$$V \subset \mathbb{A}^n \xrightarrow{\phi_i} \mathbb{P}^n$$

is called **the projective closure of V** . \triangle

Lemma 2.2.8. *Let V be an affine algebraic set with ideal $I(V)$. Then the projective closure of V , denoted \bar{V} , is a projective algebraic set.*

Proof. From the definition of projective closure,

$$\bar{V} = \{[a_1, \dots, a_{i-1}, 1, a_i, \dots, a_n] : (a_1, \dots, a_n) \in V\}.$$

Let $f \in \bar{k}[x_1, \dots, x_n]$ be a polynomial of degree d and write f by collecting all monomials having common degree. Denote each such homogeneous component of f by f_j , so that $f = f_0 + \dots + f_d$. Then define $f^* \in \bar{k}[x_1, \dots, x_{i-1}, y, x_i, \dots, x_n]$ so that

$$\begin{aligned} f^* &= y^d f_0 + y^{d-1} f_1 + \dots + f_d \\ &= y^d \sum_{j=1}^d \frac{f_j}{y^j} \\ &= y^d \sum_{j=1}^d f_j \left(\frac{x_1}{y}, \dots, \frac{x_n}{y} \right) \\ &= y^d f \left(\frac{x_1}{y}, \dots, \frac{x_n}{y} \right). \end{aligned}$$

Clearly, f^* is homogeneous and if $a = (a_1, \dots, a_n)$ is a zero of f , then $a^* = [a_1, \dots, a_{i-1}, 1, a_i, \dots, a_n]$ is a zero of f^* . Define $I^* = \{f^* : f \in I(V)\}$. Clearly, I^* is an ideal and the affine variety it defines is precisely \bar{V} . \square

Similarly as before, we see that the proof of Lemma 2.2.8 reveals how to project polynomials (and ideals) from affine to projective space. This process is called homogenization.

Definition 2.2.9. For any $f(x) \in \bar{k}[\mathbf{x}]$, let

$$f^*(x) = f^*(x_0, \dots, x_n) = x_i^d f\left(\frac{x_0}{x_i}, \dots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \dots, \frac{x_n}{x_i}\right),$$

where $d = \deg(f)$ is the smallest integer for which f^* is a polynomial. We say that f^* is the **homogenization of f with respect to x_i** . \triangle

Example 2.2.10. Let $f(x_1, x_2) = \sum a_{ij}x_1^i x_2^j$. Then the homogenization of f with respect to x_3 is given by

$$f^*(x_1, x_2, x_3) = \sum_{i,j} a_{ij}x_1^i x_2^j x_3^{d-i-j},$$

where $d = \deg(f)$. \diamond

With Lemmas 2.2.4 and 2.2.8 and Definitions 2.2.5 and 2.2.9 we have a way to pass varieties and ideals from projective to affine space and vice-versa. Because we can choose the coordinate x_i with respect to which we homogenize and dehomogenize, we simply set $i = n$. As we have remarked above, however, we lose track of points on the hyperplane $x_n = 0$. We give these points a name.

Definition 2.2.11. The points in the set

$$\mathcal{O} = \{[x_0, \dots, x_{n-1}, 0] \in \mathbb{P}^n : \text{at least one } x_i \neq 0\}$$

are called **points at infinity of \mathbb{P}^n** . \triangle

Clearly, $\mathcal{O} \cong \mathbb{P}^{n-1}$ and since $\mathbb{P}^n \cong U_n \cup \mathcal{O}$ and $U_n \cong \mathbb{A}^n$ by ϕ , then $\mathbb{P}^n \cong \mathbb{A}^n \cup \mathcal{O}$ or equivalently $\mathbb{P}^n \cong \mathbb{A}^n \cup \mathbb{P}^{n-1}$. Furthermore, an equivalence class $[a_0, \dots, a_n]$ of \mathbb{P}^n

corresponds to a line through the origin in \mathbb{A}^{n+1} and since we can identify all parallel lines with a unique line through the origin, we can also identify equivalence classes of \mathbb{P}^n with directions in \mathbb{A}^{n+1} . But since $\mathcal{O} \cong \mathbb{P}^{n-1}$, we identify \mathcal{O} with directions in \mathbb{A}^n . Intuitively, this means that parallel lines intersect at a unique point at infinity corresponding to their direction. Technically, this means that we can finally establish a bijection between \mathbb{P}^n and $\mathbb{A}^n \cup \mathbb{P}^{n-1}$.

Theorem 2.2.12. *There is a bijective correspondence $\mathbb{P}^n \leftrightarrow \mathbb{A}^n \cup \mathbb{P}^{n-1}$ given by*

$$[x_0, \dots, x_n] \rightarrow \begin{cases} \phi_n^{-1}([x_0, \dots, x_n]) \in \mathbb{A}^n, & \text{if } x_n \neq 0; \\ [x_0, \dots, x_{n-1}] \in \mathbb{P}^{n-1}, & \text{if } x_n = 0, \end{cases}$$

in one direction, and in the other by

$$\begin{aligned} (x_0, \dots, x_{n-1}) \in \mathbb{A}^n &\rightarrow \phi_n(x_0, \dots, x_{n-1}), \\ [x_0, \dots, x_{n-1}] \in \mathbb{P}^{n-1} &\rightarrow [x_0, \dots, x_{n-1}, 0]. \end{aligned}$$

Proof. The theorem follows directly from Lemmas 2.2.4 and 2.2.8 as well as the remarks following Definition 2.2.11. □

Now that we can pass between affine space and projective space, we can extend our definition of smooth affine varieties to projective ones.

Definition 2.2.13. A projective variety V is **non-singular (or smooth)** if all embeddings $V \cap \mathbb{A}^n$ of V are non-singular as an affine varieties. △

We end this section with an intuitive example of the bijection stated in Theorem 2.2.12.

Example 2.2.14. For our purposes, we are interested in $\mathbb{P}^2 \cong \mathbb{A}^2 \cup \mathbb{P}^1$. Suppose the field we are working over is \mathbb{R} . We verify that it makes sense to call \mathbb{P}^1 the set of directions in \mathbb{R}^2 . Every line in \mathbb{R}^2 is parallel to a unique line through the origin which is given by an equation of the form

$$ax = by,$$

where $a, b \in \mathbb{R}$ are not both zero. In fact, the points (a, b) and (A, B) are on the same line if and only if there exists a non-zero t such that $A = ta$ and $B = tb$, which means that both points belong to the same equivalence class in \mathbb{P}^1 , namely $[a, b]$.

Denote an equivalence class in \mathbb{P}^2 by $[x, y, z]$. The bijection $\phi : \mathbb{P}^2 \leftrightarrow \mathbb{A}^2 \cup \mathbb{P}^1$ is given by

$$[x, y, z] \rightarrow \begin{cases} (\frac{x}{z}, \frac{y}{z}) \in \mathbb{A}^2 & \text{if } z \neq 0; \\ [x, y] \in \mathbb{P}^1 & \text{if } z = 0, \end{cases}$$

with the other direction given by

$$[x, y, 1] \rightarrow (x, y) \in \mathbb{A}^2,$$

$$[x, y, 0] \rightarrow [x, y] \in \mathbb{P}^1.$$

◇

With this we conclude all the preliminaries necessary to define elliptic curves.

3

Geometry of Elliptic Curves

3.1 Definition of an Elliptic Curve

We are finally ready to define our main object of study.

Definition 3.1.1. An **elliptic curve** E **defined over a field** k , denoted E/k is the smooth projective variety of the homogeneous ideal generated by a Weierstrass equation of the form

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

where $a_1, a_2, a_3, a_4, a_6 \in k$.

△

Our first lemma shows that each elliptic curve intersects the line at infinity at exactly one point. Later on, this point will serve as the identity in the group associated with each elliptic curve.

Lemma 3.1.2. *Let E/k be an elliptic curve. Then $E \cap \mathcal{O} = [0, 1, 0]$.*

Proof. From our definition of \mathcal{O} , we see that $Z = 0$ in the polynomial equation from Definition 3.1.1. Using this in the equation gives us $0 = X^3$ and thus $X = 0$ as well. Since

there is no constraint on Y and we are working in projective space (with homogeneous coordinates), we conclude that the only point at infinity intersecting E is $[0, 1, 0]$. \square

We will slightly abuse notation and call this point \mathcal{O} , after the set of points at infinity defined previously. Lemma 3.1.2 provides us with a more intuitive way of thinking about elliptic curves as affine curves with an added point at infinity. Using non-homogeneous coordinates $x = X/Z$ and $y = Y/Z$, the affine part of E/k is given by

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \quad (3.1.1)$$

We can simplify our view of elliptic curves even further if the characteristic of the field k over which the curve is defined is different than 2 or 3.

Lemma 3.1.3. *Let E/k be an elliptic curve and let $\text{char}(k) \neq 2, 3$. Then the variety from Definition 3.1.1 is identical to the variety given by*

$$E: y^2 = x^3 + ax + b$$

where

$$b_2 = a_1^2 + 4a_2,$$

$$b_4 = 2a_4 + a_1a_3,$$

$$b_6 = a_3^2 + 4a_6,$$

as well as

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$

$$c_4 = b_2^2 - 24b_4^2,$$

$$c_6 = -b_2^3 + 36b_2b_4 - 216b_6,$$

finally give us $a = -27c_4$ and $b = -54c_6$.

Proof. Since $\text{char}(k) \neq 2$ we can complete the square in Equation (3.1.1) by replacing y with $y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$. This produces

$$E: y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6.$$

We can also eliminate the x^2 term by replacing x and y by $(x - 3b_2)/36$ and $y/108$, respectively. Note that we need $\text{char}(k) \neq 2, 3$ and that the equation for our elliptic curve simplifies to

$$E: y^2 = x^3 - 27c_4x - 54c_6,$$

which is as stated in the theorem with a simple renaming of the coefficients. \square

We will be working with elliptic curves defined over finite fields of characteristic p . Sometimes, these curves can be attained by reduction (modulo p) of the coefficients of a curve defined over a field of characteristic 0 such as \mathbb{Q} . We are not guaranteed that a curve obtained in this way will stay smooth. Before we give a theorem that provides a simple condition under which a cubic curve is singular, we examine two types of singularities that can occur. If P is a singular point on a cubic curve E/k given by a Weierstrass equation $f(x, y)$, then

$$\left. \frac{\partial f}{\partial x} \right|_{(0,0)} = \left. \frac{\partial f}{\partial y} \right|_{(0,0)} = 0$$

and the Taylor expansion of $f(x, y)$ at (x_0, y_0) is given by

$$\begin{aligned} f(x, y) - f(x_0, y_0) &= \lambda_1(x - x_0)^2 + \lambda_2(x - x_0)(y - y_0) + \lambda_3(y - y_0) - (x - x_0)^3 \\ &= [(y - y_0) - \alpha(x - x_0)][(y - y_0) - \beta(x - x_0)] - (x - x_0)^3 \end{aligned} \quad (3.1.2)$$

for some λ_i in k and $\alpha, \beta \in \bar{k}$.

Example 3.1.4. The cubic curve given by the equation $f: y^2 = x^3$ has a singular point at the origin since

$$\left. \frac{\partial f}{\partial x} \right|_{(0,0)} = \left. 3x^2 \right|_{(0,0)} = 0$$

and

$$\left. \frac{\partial f}{\partial y} \right|_{(0,0)} = -2y \Big|_{(0,0)} = 0.$$

We see that $\alpha = \beta = 0$ as defined in Equation (3.1.2). This type of singularity is called a cusp. \diamond

Example 3.1.5. The curve given by $g: y^2 = x^3 + x^2$ also has the origin as a singular point as differentiation can show. Writing g as $(y - x)(y + x) - x^3 = 0$ gives us $\alpha = 1$ and $\beta = -1$ as defined in Equation (3.1.2). This type of singularity is called a node. \diamond

Definition 3.1.6. With notation of Equation (3.1.2), the singular point P is a **node** if $\alpha \neq \beta$, in which case the tangent lines at P are defined by

$$y - y_0 = \beta(x - x_0) \quad \text{and} \quad y - y_0 = \alpha(x - x_0).$$

If $\alpha = \beta$ then P is a **cusp** and there is a unique tangent line at P defined by

$$y - y_0 = \alpha(x - x_0).$$

\triangle

The following quantity is of fundamental importance in recognizing singular curves.

Definition 3.1.7. The quantity

$$\Delta = -b^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

associated with a Weierstrass equation is called the **discriminant** associated with that curve. For an cubic curve given by the simplified equation $f: y^2 = x^3 + ax + b$ the discriminant is given by

$$\Delta = -16(4a^3 + 27b^2).$$

\triangle

Example 3.1.8. The curves given by f and g in Examples 3.1.4 and 3.1.5 have the discriminant $\Delta = 0$. This is true in general! \diamond

Theorem 3.1.9. *The curve given by a Weierstrass equation can be classified as follows.*

(i) *It is non-singular if and only if $\Delta \neq 0$.*

(ii) *It has a node if and only if $\Delta = 0$ and $c_4 \neq 0$.*

(iii) *It has a cusp if and only if $\Delta = c_4 = 0$.*

Proof. See [6, Proposition 3.1.4]. \square

In addition to the statement of the theorem, the proof cited above also shows that the point at infinity \mathcal{O} is never singular. To see this, consider the curve in \mathbb{P}^2 with a homogeneous equation

$$f(X, Y, Z): Y^2Z - X^3 - aXZ^2 - bZ^3 = 0$$

and the point $\mathcal{O} = [0, 1, 0]$. Since

$$\partial f / \partial Z(\mathcal{O}) = 1 \neq 0,$$

we see that \mathcal{O} is a non-singular point on E . In addition, an elliptic curve can have at most one singular point. In the proof we learn that a singular point $P = (x_0, y_0)$ has a double root x_0 of $f(x)$ where the elliptic curve is given by $E: y^2 = f(x)$. Since $f(x)$ is cubic, it cannot have two double roots.

3.2 The Group Structure of Elliptic Curves

There is a well defined addition of points on an elliptic curve. In fact, points on an elliptic curve form a group under this operation. Thus, we can associate a group to each elliptic curve and study properties of the curve through the algebraic structure of the associated

group. In order to define addition of points on an elliptic curve we need the fact that a line intersects an elliptic curve exactly three times.

Definition 3.2.1. A **projective line** is a projective variety defined by a homogeneous polynomial of degree 1. △

Of course, we can intuitively think of the line as belonging in affine space in the usual way with an extra point at infinity.

Theorem 3.2.2 (Bézout’s Theorem). *Let $L \in \mathbb{P}^2$ be a projective line and $V \in \mathbb{P}^2$ be a projective variety defined by a homogeneous polynomial $f(x, y, z)$ of degree 3. Then*

$$\#V \cap L = 3.$$

Proof. As stated here, this theorem is actually a special case of Bézout’s theorem. For the proof see [2, Theorem 8.7.8], or see [7, A.4] for a more elementary treatment. □

Since we are working in projective space, the point at infinity \mathcal{O} of an elliptic curve could be a point of intersection. However, the theory developed previously allows us to consider our line and elliptic curve as subsets of the affine plane with an additional point at infinity. In this scenario, lines passing through \mathcal{O} are vertical (see Figure 3.2.1). In addition, the three points of intersection of the line L and an elliptic curve E don’t have to be distinct. That is, we count intersections with multiplicity: an inflection point (which can only be \mathcal{O}) has multiplicity 3, a point tangent to the curve has multiplicity 2 (Figure 3.2.1) and all other points have multiplicity one. Over certain fields we don’t have an appropriate picture for the group law, but we will give explicit formulas and these can be verified algebraically.

We can now describe the **addition law** of points on an elliptic curve E . Let $P, Q \in E$, L be the line connecting P and Q (tangent line to E if $P = Q$), and R the third point of intersection of L with E . Let L' be the line connecting R and \mathcal{O} . Then $P \oplus Q$ is the point

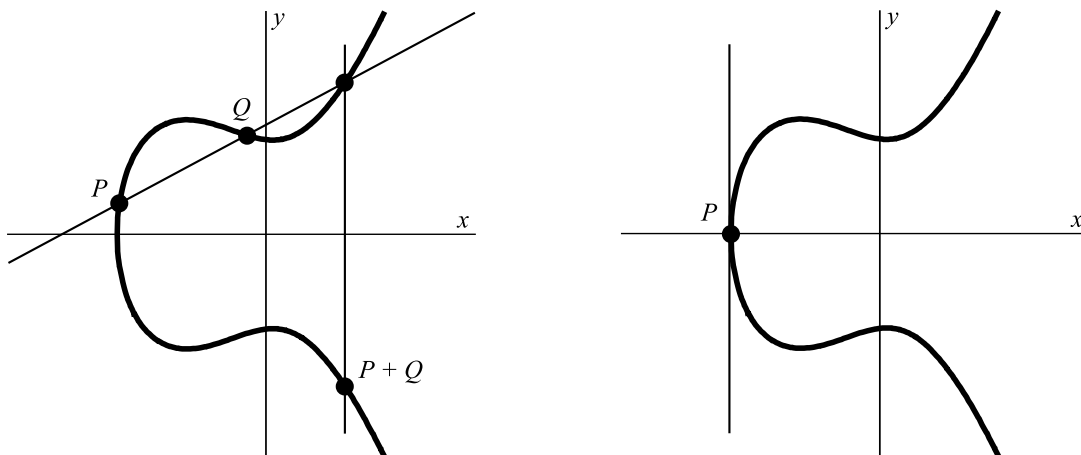


Figure 3.2.1. The addition law ($P + Q$) and a point of inflection ($P + P = \mathcal{O}$)

such that L' intersects E at R, \mathcal{O} and $P \oplus Q$. See Figure 3.2.1 for an illustration of this rule.

Proposition 3.2.3. *An elliptic curve E endowed with the operation \oplus described above forms an abelian group.*

(a) *If a line L intersects E at the (not necessarily distinct) points P, Q, R , then*

$$(P \oplus Q) \oplus R = \mathcal{O}.$$

(b) *$P \oplus \mathcal{O} = P$ for all $P \in E$.*

(c) *Let $P \in E$. There is a point of E , denoted $\ominus P$, such that*

$$P \oplus (\ominus P) = \mathcal{O}.$$

(d) *Let $P, Q, R \in E$. Then*

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R).$$

(e) *$P \oplus Q = Q \oplus P$ for all $P, Q \in E$.*

Proof. See [6, Proposition 3.2.2]. The proof can be verified using Figure 3.2.1, as well as through direct computation with the formulas given below. \square

Throughout the rest of the project we will simply use $+$ and $-$ instead of \oplus and \ominus , respectively. We now derive explicit formulas for the group operations, directly following [6, Section 3.2]. Suppose that E is given by a simplified Weierstrass equation

$$E(x, y): y^2 = x^3 + ax + b$$

and let $P = (x_0, y_0) \in E$.

We first compute the coordinates of $-P$. Let L be the line going through P and \mathcal{O} . By Proposition 3.2.3 (a) and (b)

$$\mathcal{O} = (P + \mathcal{O}) + (-P) = P + (-P),$$

so the third point of intersection is $-P$. Since $\mathcal{O} = [0, 1, 0]$, the line L is given by

$$L: x - x_0 = 0.$$

Substituting this into the equation for E , we see that the quadratic polynomial $E(x_0, y): y^2 - x_0^3 - ax_0 - b = 0$ has roots y_0 and y'_0 , where $-P = (x_0, y'_0)$. Writing out

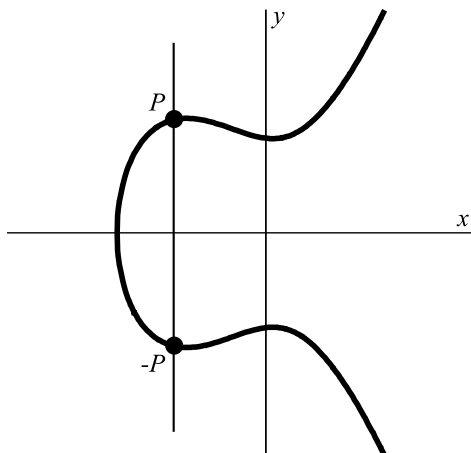
$$E(x_0, y) = (y - y_0)(y - y'_0) = y^2 - (y_0 + y'_0)y + y_0y'$$

and comparing coefficients for y gives $y'_0 = -y_0$ which means that

$$-P = (x_0, -y_0).$$

We see that $-P$ is just the reflection of P around the x -axis, or the third point of intersection of the line passing through P and \mathcal{O} and our elliptic curve (see Figure 3.2.2).

Next we derive a formula for the addition law. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points of E . If $x_1 = x_2$ and $y_1 = -y_2$, then $P + (-P) = \mathcal{O}$. Otherwise the line L through

Figure 3.2.2. Inverse of a point P

P_1 and P_2 (tangent line to E if $P_1 = P_2$) has an equation of the form

$$L: y = \lambda x + \nu$$

where

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \quad \text{and} \quad \nu = y_1 - \lambda x_1 = y_2 - \lambda x_2.$$

To get the third point of intersection $P'_3 = (x_3, y'_3)$ we substitute $\lambda x + \nu$ for y into $E(x, y)$ to get

$$E(x, \lambda x + \nu): (\lambda x + \nu)^2 = x^3 + ax + b.$$

Since the roots of $E(x, \lambda x + \nu)$ are x_1, x_2, x_3 it follows that

$$x^3 - \lambda^2 x^2 + (a - 2\lambda\nu)x + (b - \nu) = (x - x_1)(x - x_2)(x - x_3).$$

By equating coefficients we find that $\lambda^2 = x_1 + x_2 + x_3$. Thus,

$$x_3 = \lambda^2 - x_1 - x_2 \quad \text{and} \quad y'_3 = \lambda x_3 + \nu.$$

By the addition law stated above, we want $P_1 + P_2$ to be the third point of intersection of the line passing through P'_3 and \mathcal{O} . We have already shown this point to be $-P'_3 = (x_3, -y'_3)$

while computing the inverse of an arbitrary point on the elliptic curve. Let $y_3 = -y'_3$. Then $P_3 = P_1 + P_2 = (x_3, y_3)$. We summarize our results.

Theorem 3.2.4 (Group Law Algorithm). *Let E be an elliptic curve given by a Weierstrass equation*

$$E: y^2 = x^3 + ax + b.$$

(a) *Let $P = (x_0, y_0) \in E$. Then*

$$-P_0 = (x_0, -y_0).$$

Now let

$$P_1 + P_2 = P_3 \quad \text{with} \quad P_i = (x_i, y_i) \in E.$$

(b) *If $x_1 = x_2$ and $y_1 = -y_2$, then*

$$P_1 + P_2 = \mathcal{O}.$$

Otherwise, let

$$\begin{aligned} \lambda &= \frac{y_2 - y_1}{x_2 - x_1}, \quad \nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1} && \text{if } x_1 \neq x_2; \\ \lambda &= \frac{a}{2y}, \quad \nu = \frac{-x_1^3 + ax_1 + 2b}{2y_1} && \text{if } x_1 = x_2. \end{aligned}$$

(Then $y = \lambda x + \nu$ is the line through P_1 and P_2 , or tangent to E if $P_1 = P_2$.)

(c) $P_3 = X_1 + X_2$ *is given by*

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = -\lambda x_3 - \nu.$$

(d) *As special cases of (c), we have the **duplication formula** for $P = (x_0, y_0) \in E$,*

$$x(P + P) = \frac{x_0^4 - 2ax_0^2 - 8bx_0 + a^2}{4x_0^3 + 4ax_0 + 4b}.$$

Proof. The proof follows from simple manipulation of the expressions derived in the discussion preceding the theorem. \square

Example 3.2.5. Let E be defined over \mathbb{R} by $y^2 = x^3 + 17$. Let $P_1 = (-1, 4)$ and $P_2 = (2, 5)$.

To compute $P_1 + P_2$ we first find the line through the two points,

$$y = \frac{1}{3}x + \frac{13}{3} \quad \text{so}$$

$$\lambda = \frac{1}{3} \quad \text{and} \quad \nu = 133.$$

Next we have

$$x_3 = \lambda^2 - x_1 - x_2 = -\frac{8}{9} \quad \text{and} \quad y_3 = \lambda x_3 + \nu = \frac{109}{27},$$

and finally $P_1 + P_2 = (x_3, -y_3) = (-\frac{8}{9}, -\frac{109}{27})$.

To compute $P_1 + P_1 = 2P_1$ we can use the duplication formula given above, or simply compute the slope of the line tangent to P_1 by implicit differentiation of $y^2 = f(x)$,

$$\lambda = \frac{dy}{dx} = \frac{f'(x)}{2y}.$$

Now we have $\lambda = \frac{f'(-1)}{8} = \frac{3}{8}$ and by following the same steps we used to compute $P_1 + P_2$, we also compute $2P_1 = (\frac{137}{64}, -\frac{2651}{512})$. \diamond

We have been implicitly assuming that the coordinates of points on an elliptic curve E defined over k lie in the closure \bar{k} of k . However, we can allow the coordinates of points on E to lie only in a particular extension k' of k and still have a well defined addition law on this set.

Theorem 3.2.6. *Let $E: y^2 = x^3 + ax + b$ be an elliptic curve defined over k , and let k' be any field extension of k . Then*

$$E(k') = \{(x, y) \in k'^2: y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$$

is a subgroup of E . In fact, $E(k') \leq E(k'')$, for any extension k'' of k' .

Proof. The proof is as in [6, Proposition 3.2.2(f)]. Let $P, Q \in E$. If P and Q have coordinates in k , then the equation of the line connecting them has coefficients in k . If further E is defined over k , then the third point of intersection will have coordinates given by a rational combination of the coefficients of the line and of E , so will be in k . \square

We are now ready to present the results about elliptic curves defined over finite fields that will be useful in our research.

3.3 Elliptic Curves Defined over Finite Fields

Let E be an elliptic curve and let \mathbb{F}_q be the finite field of $q = p^n$ elements, where p is a prime and n is a positive integer. There are some basic results concerning the group structure of elliptic curves over finite fields.

In general, $E(\mathbb{F}_q)$ is a finite abelian group, but there are still many possibilities for what group it could be because it is a subset of $\mathbb{P}^2(\mathbb{F}_q)$ and since there are many abelian groups of order less than or equal to $\#\mathbb{P}^2(\mathbb{F}_q) = q^2 + q + 1$. One of the basic results is on the order of the group.

Theorem 3.3.1. *Let E be an elliptic curve defined over a finite field of $q = p^n$ elements. Then*

$$\#E(\mathbb{F}_q) = 1 + q - a_q,$$

where a_q is an integer in the range $-2\sqrt{q} \leq a_q \leq 2\sqrt{q}$.

Proof. See [6, Section 5.2]. \square

The following lemma allows us to compute the order of $E(\mathbb{F}_{p^2})$ as a function of p and a_p , thus eliminating the need to know a_{p^2} .

Lemma 3.3.2. *Let E be an elliptic curve defined over \mathbb{F}_p with a_p as given in Theorem 3.3.1. Then, $\#E(\mathbb{F}_{p^2}) = (1 + p + a_p)(1 + p - a_p)$.*

Proof. From the discussion following [6, Proposition 5.2.3], we know that there exist some complex conjugates $\alpha, \beta \in \mathbb{C}$ of \sqrt{q} such that

$$q = (\alpha\beta)^n \quad \text{and}$$

$$a_q = \alpha^n + \beta^n.$$

From here we compute

$$(\alpha + \beta)^2 = 2\alpha\beta + \alpha^2 + \beta^2 \quad \text{which is equivalent to}$$

$$a_p^2 = 2p + a_{p^2}$$

so that

$$a_{p^2} = a_p^2 - 2p.$$

By Theorem 3.3.1, $\#E(\mathbb{F}_q) = 1 - q + a_q$ which gives us the desired result with $q = p^2$:

$$\begin{aligned} \#E(\mathbb{F}_{p^2}) &= 1 + (\alpha\beta)^2 - (\alpha^2 + \beta^2) \\ &= 1 + p^2 + 2p - a_p^2 \\ &= (1 + p + a_p)(1 + p - a_p). \end{aligned}$$

□

We can classify the group structure of elliptic curves based on their order.

Theorem 3.3.3. *Let \mathbb{F}_q be a finite field with $q = p^n$ elements. Then one of the following conditions is satisfied:*

- (i) $(a_q, q) = 1$,
- (ii) $a_q = 0, n$ odd or $p \not\equiv 1(4)$,
- (iii) $a_q = \pm\sqrt{q}, n$ even or $p \not\equiv 1(3)$,
- (iv) $a_q = \pm 2\sqrt{q}, n$ even,

(v) $a_q = \pm\sqrt{2q}$, n odd and $p = 2$,

(vi) $a_q = \pm\sqrt{3q}$, n odd and $p = 3$.

Proof. See [9]. □

Note that we have allowed for $p = 2, 3$ and that all elliptic curves belong to one of the six types. Types (ii) through (vi) are known as the **supersingular** elliptic curves. Supersingular curves are not singular, because then they wouldn't be elliptic curves at all. Their group structure has been determined.

Theorem 3.3.4. *The possible group structures for curves in cases (ii) through (vi) from Theorem 3.3.3 are*

(ii) $\mathbb{Z}/2 \oplus \mathbb{Z}/(q+1)/2$ or cyclic if $q \equiv 3(4)$, cyclic otherwise,

(iii) Cyclic,

(iv) $(\mathbb{Z}/(\sqrt{q} \pm 1))^2$,

(v) Cyclic,

(vi) Cyclic.

Proof. See [5]. □

Finally, curves of type (i) satisfy $a_q \not\equiv 0 \pmod{p}$ and the group structure of these non-supersingular curves is restricted by the following result due to Voloch. Let $V_\ell(N)$ be the ℓ -adic valuation of N , i.e., the largest integer k such that $\ell^k \mid N$.

Theorem 3.3.5 (Voloch's Theorem). *The possible group structures for a non-supersingular elliptic curve E defined over a finite field are*

$$E(\mathbb{F}_q) = \mathbb{Z}/p^{v_p(N)} \oplus \bigoplus_{\substack{\ell \mid N \\ \ell \neq p}} (\mathbb{Z}/\ell^{r_\ell} \oplus \mathbb{Z}/\ell^{s_\ell})$$

where each ℓ is prime, $N = \#E(\mathbb{F}_q)$, $r_\ell + s_\ell = V_\ell(N)$, and $\min(r_\ell, s_\ell) \leq V_\ell(q-1)$.

Proof. See [8]. □

Notice that this is very restrictive, and that not every finite abelian group can occur as the group of \mathbb{F}_q -rational points of an elliptic curve. However, Voloch's result in general gives multiple possible group structures, the number of which depends on $\min(r_\ell, s_\ell)$ for the curve in question. We give one final result about the structure of points of an elliptic curve E having order m .

Theorem 3.3.6. *Let E be an elliptic curve defined over a finite field and let $E[m]$ denote the set of points of E having order m . Then*

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

Proof. See [6, Corollary 3.6.4]. □

4

Behavior of Elliptic Curves Under Field Extensions

Throughout this project, we will consider elliptic curves E given by a Weierstrass equation in the particularly simplified form of Lemma 3.1.3:

$$E: y^2 = x^3 + ax + b.$$

This means that we omit curves defined over fields of characteristic 2 or 3 from consideration, since their inclusion in the project would greatly complicate our equations and since the central problem of this project is easily solved by direct computation for such small fields.

Let E be an elliptic curve defined over a finite field \mathbb{F}_p , where $p \neq 2, 3$. In this chapter we prove that $E(\mathbb{F}_{p^2})$ is completely determined by $E(\mathbb{F}_p)$ for supersingular curves and curves with $a_p = -1$. For curves with $a_p = 1$, we give the necessary conditions and a method to determine $E(\mathbb{F}_{p^2})$ given $E(\mathbb{F}_p)$.

4.1 Statement of the Problem

Let E be an elliptic curve defined over the finite field \mathbb{F}_p . The question we are trying to answer is the following. Given $E(\mathbb{F}_p)$, to what extent does the group structure change

upon a degree two extension of the base field \mathbb{F}_p ? In particular, to what extent does $E(\mathbb{F}_p)$ determine $E(\mathbb{F}_{p^2})$? We are interested in the answer because if $E(\mathbb{F}_{p^2})$ is determined by $E(\mathbb{F}_p)$, in order to find the bigger group we only need to compute $E(\mathbb{F}_p)$. Even when $E(\mathbb{F}_{p^2})$ is not completely determined, it is useful to know to what extent it depends on $E(\mathbb{F}_p)$ since we might be able to reduce the amount of work necessary to find $E(\mathbb{F}_{p^2})$.

4.2 The Supersingular Case

Since Theorem 3.3.4 allows for fields of characteristic 2 and 3 we lift this restriction and allow for such fields when working with supersingular curves.

Theorem 4.2.1. *Let E be a supersingular elliptic curve defined over \mathbb{F}_p . Then $E(\mathbb{F}_{p^2})$ is uniquely determined by $E(\mathbb{F}_p)$.*

Proof. By Theorem 3.3.3, we have five cases to consider. Let $q = p^2$.

Suppose that $a_p = 0$ so that our curve is of type (ii) as in Theorem 3.3.3. Using Lemma 3.3.2 we know that $a_q = (a_p)^2 - 2p = -2p = -2\sqrt{q}$. Since we are considering $q = p^2$, the power of p is even and the a_q term characterizes our group structure to be $(\mathbb{Z}/(p \pm 1))^2$ by Theorem 3.3.4.

Suppose that our curve is of type (iii) in Theorem 3.3.3. This means that $a_p = \pm\sqrt{p}$ and that $p \not\equiv 1 \pmod{3}$. Computing as above, $a_q = -p = -\sqrt{q}$ with q an even power of p . By Theorem 3.3.4, we conclude that $E(\mathbb{F}_{p^2})$ is cyclic.

Suppose that our curve is of type (iv) in Theorem 3.3.3. Then $a_p = \pm 2\sqrt{p}$ and as before we compute $a_q = 2\sqrt{q}$ with n even. Again, the group structure of $E(\mathbb{F}_{p^2})$ is determined to be $(\mathbb{Z}/(p \pm 1))^2$.

Suppose that our curve is of type (v) in Theorem 3.3.3. Then we have $a_p = \pm\sqrt{2p}$ and $p = 2$. Now, $a_q = 0$ and note that $2 \not\equiv 1 \pmod{4}$ is satisfied. It follows that the group structure of $E(\mathbb{F}_{p^2})$ is given by Theorem 3.3.4, case (ii).

Finally, suppose that our curve is of type (vi) in Theorem 3.3.3. Hence $a_p = \pm\sqrt{3p}$ and $a_q = \sqrt{q}$ with $3 \not\equiv 1 \pmod{3}$ and the group structure of $E(\mathbb{F}_{p^2})$ is cyclic.

With this, we have determined the group structure of $E(\mathbb{F}_{p^2})$ completely, knowing only the order of $E(\mathbb{F}_p)$ for all possible supersingular curves over \mathbb{F}_p . \square

By generalizing the process from the proof of Lemma 3.3.2 one can compute $\#E(\mathbb{F}_q)$ as a function of p and a_p for any $q = p^n$. It is reasonable to conjecture that raising a_p to various powers in the resulting polynomials wouldn't change the way our proof of Theorem 4.2.1 works and that in fact $E(\mathbb{F}_p)$ determines $E(\mathbb{F}_q)$ for all $q = p^n$!

Conjecture 4.2.2. *Let E be a supersingular elliptic curve defined over \mathbb{F}_p and let $q = p^n$. Then $E(\mathbb{F}_q)$ is uniquely determined by $E(\mathbb{F}_p)$ for all positive integers n .*

4.3 The $a_p = -1$ Case

Proposition 4.3.1. *Let E be an elliptic curve defined over \mathbb{F}_p . If $a_p = -1$, then $E(\mathbb{F}_{p^2})$ is uniquely determined by $E(\mathbb{F}_p)$.*

Proof. Suppose that $a_p = -1$. Note that by Theorem 3.3.1 $\#E(\mathbb{F}_p) = p + 2$ and by Lemma 3.3.2 $\#E(\mathbb{F}_{p^2}) = p(p + 2)$. This means that $E(\mathbb{F}_{p^2}) = \mathbb{Z}/p \times E(\mathbb{F}_p)$ since the groups are abelian and $E(\mathbb{F}_p) \leq E(\mathbb{F}_{p^2})$. This completes the proof! \square

The $a_p = -1$ case is thus very simple. Note that we didn't have to use Voloch's structure theorem (Theorem 3.3.5) for this proof at all. In fact, all we needed was the fact that $a_p = -1$, that is, the number of points in the group. Voloch's Theorem alone couldn't solve this problem since it in general gives many possible groups for a particular curve. For the $a_p = 1$ case, however, we will use it to narrow the group choices down enough to be able to solve our problem!

Example 4.3.2. Let E be an elliptic curve defined over \mathbb{F}_{13} given by

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

It is easy to count the number of points on E , and this gives us $a_{13} = -1$. By Theorem 3.3.1, $N_1 = \#E(\mathbb{F}_p) = p + 2$ so in this case $N_1 = 15$. For all primes $\ell \mid (p + 2)$ the group $E(\mathbb{F}_p)$ is determined by the equations

$$\begin{aligned} r_\ell + s_\ell &= V_\ell(p + 2) \text{ and} \\ \min\{r_\ell, s_\ell\} &\leq V_\ell(p - 1) \end{aligned}$$

by Voloch's result. Computing the possible groups for $E(\mathbb{F}_{p^2})$ gives us a similar set of equations. In particular, note that $\#E(\mathbb{F}_{p^2}) = p(p + 2)$ by Lemma 3.3.2. Then, for any prime $\ell \mid N_2$ it is necessarily true that $\ell \mid p + 2$. This means that the group structure of $E(\mathbb{F}_{p^2})$ is *also* determined by the equations

$$\begin{aligned} r_\ell + s_\ell &= V_\ell(p + 2) \text{ and} \\ \min\{r_\ell, s_\ell\} &\leq V_\ell((p - 1)(p + 1)) = V_\ell(p - 1) \end{aligned}$$

as used in Voloch's result. The only reason we know that r_ℓ and s_ℓ are guaranteed to be the same for both groups is because of Proposition 4.3.1.

Computing the coefficients for the curve in question, however, gives only one possible group structure. Since $\#E(\mathbb{F}_p) = 15$, the possible values for ℓ are 3 and 5. In both cases, $r_\ell + s_\ell = 1$ and so $r_3 = r_5 = 1$ while $s_3 = s_5 = 0$. Hence,

$$E(\mathbb{F}_p) = \mathbb{Z}/3 \times \mathbb{Z}/5 \quad \text{and consequently} \quad E(\mathbb{F}_{p^2}) = \mathbb{Z}/13 \times \mathbb{Z}/15.$$

◇

4.4 The $a_p = 1$ Case

In this section, Theorem 4.4.5 gives the necessary conditions to determine $E(\mathbb{F}_{p^2})$ given $E(\mathbb{F}_p)$. First we prove two lemmas.

Lemma 4.4.1. *Let E be an elliptic curve defined over \mathbb{F}_p and suppose that $a_p = 1$. Then the possible structure of $E(\mathbb{F}_{p^2})$ is*

$$E(\mathbb{F}_{p^2}) \cong \mathbb{Z}/p \oplus \bigoplus_{\ell \neq p, 3} \mathbb{Z}/\ell^{V_\ell(p+2)} \oplus \begin{cases} \mathbb{Z}/3^t, & \text{if } \min(r_3, s_3) = 0; \\ \mathbb{Z}/3 \oplus \mathbb{Z}/3^{t-1}, & \text{if } \min(r_3, s_3) = 1, \end{cases}$$

where r_3 and s_3 are as defined in Theorem 3.3.5 and $t = V_3(p+2)$.

Proof. By Theorem 3.3.1 and Lemma 3.3.2 we see that

$$\#E(\mathbb{F}_p) = p \quad \text{and} \quad \#E(\mathbb{F}_{p^2}) = p(p+2).$$

Since p is prime, this forces $E(\mathbb{F}_p) \cong \mathbb{Z}/p$. We can now use Voloch's result (Theorem 3.3.5) to help us determine the structure of $E(\mathbb{F}_{p^2})$. We know that:

$$E(\mathbb{F}_{p^2}) \cong \mathbb{Z}/p \oplus \bigoplus_{\ell \neq p} (\mathbb{Z}/\ell^{r_\ell} \oplus \mathbb{Z}/\ell^{s_\ell}) \tag{4.4.1}$$

where each ℓ is a prime and $N = \#E(\mathbb{F}_q)$. The theorem also states that we can limit the possibilities for r_ℓ and s_ℓ because

$$r_\ell + s_\ell = V_\ell(N) = V_\ell(p(p+2))$$

and more crucially

$$\min(r_\ell, s_\ell) \leq V_\ell(q-1) = V_\ell((p-1)(p+1)).$$

We are only interested in the cases when $V_\ell(N) \neq 0$. So we can suppose that $\ell \mid N$ and so $V_\ell(p(p+2)) \neq 0$. Since p is prime, $V_\ell(N) = V_\ell(p+2)$. If $\ell \neq 3$ then $\ell \nmid (p-1), (p+1)$ and because $V_\ell(AB) = V_\ell(A) + V_\ell(B)$ (which is easy to verify and is one of the axioms for a valuation) then $V_\ell((p+1)(p-1)) = 0$ and so $\min(r_\ell, s_\ell) = 0$. Without loss of generality, take $r_\ell = 0$. Since $r_\ell + s_\ell = V_\ell(p+2)$ we have $s_\ell = V_\ell(p+2)$. The ℓ -term for $\ell \neq 3$ therefore looks like

$$\mathbb{Z}/\ell^{V_\ell(p+2)}. \tag{4.4.2}$$

In other words, the Sylow- ℓ subgroup of $E(\mathbb{F}_{p^2})$ is completely determined for primes $\ell \neq 3$. However, if $\ell = 3$ we still have $3 \mid p + 2$. So for distinct primes $p_1, \dots, p_r, 3$, write

$$p + 2 = p_1^{t_1} \dots p_r^{t_r} 3^t$$

as well as

$$p - 1 = p_1^{t_1} \dots p_r^{t_r} 3^t - 3 = (p_1^{t_1} \dots p_r^{t_r} 3^{t-1} - 1)3.$$

We see that $V_3(N) = V_3(p + 2) = t$.

(Case 1) If $t = 1$, we are done because the 3-term in $E(\mathbb{F}_{p^2})$ has to be $\mathbb{Z}/3$ according to Sylow's First Theorem.

(Case 2) If $t > 1$, then $3 \mid p_1^{t_1} \dots p_r^{t_r} 3^{t-1}$ and so $3 \nmid (p_1^{t_1} \dots p_r^{t_r} 3^{t-1} - 1)$. Hence $\min(r_3, s_3) \leq V_3(p - 1) = 1$ and the 3-term is isomorphic to:

$$\begin{cases} \mathbb{Z}/3^t, & \text{if } \min(r_3, s_3) = 0; \\ \mathbb{Z}/3 \oplus \mathbb{Z}/3^{t-1}, & \text{if } \min(r_3, s_3) = 1. \end{cases} \quad (4.4.3)$$

Using Equations (4.4.2) and (4.4.3) with Equation (4.4.1), we get

$$E(\mathbb{F}_{p^2}) \cong \mathbb{Z}/p \oplus \bigoplus_{\ell \neq p, 3} \mathbb{Z}/\ell^{V_\ell(p+2)} \oplus \begin{cases} \mathbb{Z}/3^t, & \text{if } \min(r_3, s_3) = 0; \\ \mathbb{Z}/3 \oplus \mathbb{Z}/3^{t-1}, & \text{if } \min(r_3, s_3) = 1. \end{cases}$$

□

Let $\mathbb{F}_p(\alpha)$ and $\mathbb{F}_p(\beta)$ be isomorphic extensions of \mathbb{F}_p . We will show that $\mathbb{F}_p(\alpha) = \mathbb{F}_p(\beta)$ in Lemma 4.4.3. However, the following example shows that this is not true in general.

Example 4.4.2. By Eisenstein's Criterion ([3, Theorem 9.4.13]), the polynomial $f(x) = x^3 - 2$ is irreducible over \mathbb{Q} . Let $\rho = \zeta_3 = \frac{-1 + \sqrt{-3}}{2}$ denote a primitive cube root of unity. Then, the roots of f are $\sqrt[3]{2}, \rho\sqrt[3]{2}$ and $\rho^2\sqrt[3]{2}$. By [3, Theorem 13.1.8], we know that $\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}(\rho\sqrt[3]{2})$ but since $\rho\sqrt[3]{2} \notin \mathbb{Q}(\sqrt[3]{2})$, then $\mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q}(\rho\sqrt[3]{2})$. ◇

Lemma 4.4.3. *Any irreducible polynomial of degree $n \geq 2$ over $E(\mathbb{F}_p)$ splits in \mathbb{F}_{p^n} . Furthermore, it is separable and has no roots in \mathbb{F}_{p^m} , for $m < n$.*

Proof. Let f be an irreducible polynomial of degree $n \geq 2$ over \mathbb{F}_p . Now, every finite field is perfect, so f is separable. Let α, β be any two of its roots. Since $\mathbb{F}_p(\alpha)$ is the *smallest* extension containing α and has degree n , the polynomial f has no roots in \mathbb{F}_{p^m} , for $m < n$. By [3, Theorem 13.1.8] we know that $\mathbb{F}_p(\alpha) \cong \mathbb{F}_p(\beta)$. For a general field k , we can have $k(\alpha) \neq k(\beta)$ as in Example 4.4.2. Over a finite field, however, [3, Proposition 14.3.18] states that the polynomial $x^{p^n} - x$ is precisely the product of all distinct irreducible polynomials $f \in \mathbb{F}_p[x]$ whose degree divides n , including p . By [3, Theorem 14.3.15], we have that the splitting field of $x^{p^n} - x$ is \mathbb{F}_{p^n} . Hence, all the irreducible factors of $x^{p^n} - x$ also split in \mathbb{F}_{p^n} and $\mathbb{F}_p(\alpha) = \mathbb{F}_p(\beta) = \mathbb{F}_{p^n}$. \square

To ease notation in the proof of Theorem 4.4.5 we make the following definition.

Definition 4.4.4. We say that $\alpha \in \mathbb{F}_{p^n}$ is **elliptic over** \mathbb{F}_{p^m} for $m \geq n$ if \mathbb{F}_{p^m} is the smallest extension of \mathbb{F}_{p^n} in which $\alpha^3 + a\alpha + b$ is a square. \triangle

We will take elliptic to mean elliptic over \mathbb{F}_{p^2} unless stated otherwise throughout the proof of the following theorem.

Theorem 4.4.5. *Let $E: y^2 = x^3 + ax + b$ be an elliptic curve defined over \mathbb{F}_p and let*

$$f_3: 3x^4 + 6ax^2 + 12bx - a^2 = 0.$$

and $t = V_3(p + 2)$. Then one of the following is true:

(1) $Syl_3(E(\mathbb{F}_{p^2})) \cong \mathbb{Z}/3 \oplus \mathbb{Z}/3^{t-1}$ and f_3 has at least two elliptic roots in \mathbb{F}_{p^2} ,

(2) $Syl_3(E(\mathbb{F}_{p^2})) \cong \mathbb{Z}/3^t$ and f_3 has exactly one elliptic root in \mathbb{F}_{p^2} ,

(3) $Syl_3(E(\mathbb{F}_{p^2}))$ is trivial.

Proof. By Theorem 3.3.6 and Lemma 4.4.1 we have that

$$\begin{aligned} E(\mathbb{F}_{p^2})[3] &= E[3] \cap E(\mathbb{F}_{p^2}) \\ &= \begin{cases} (\mathbb{Z}/3 \oplus \mathbb{Z}/3) \cap (\mathbb{Z}/3^t), & \text{if } \min(r_3, s_3) = 0; \\ (\mathbb{Z}/3 \oplus \mathbb{Z}/3) \cap (\mathbb{Z}/3 \oplus \mathbb{Z}/3^{t-1}), & \text{if } \min(r_3, s_3) = 1, \end{cases} \\ &= \begin{cases} \mathbb{Z}/3, & \text{if } \min(r_3, s_3) = 0; \\ \mathbb{Z}/3 \oplus \mathbb{Z}/3, & \text{if } \min(r_3, s_3) = 1. \end{cases} \end{aligned}$$

This means that if we can determine the group of points on $E(\mathbb{F}_{p^2})$ of order 3, we are done. Any $P \in E(\mathbb{F}_{p^2})[3]$ has the property that $3P = \mathcal{O}$, which is equivalent to $2P = -P$. For a curve in Weierstrass form $y^2 = x^3 + ax + b$ the duplication formula (Theorem 3.2.4) gives the x coordinate of $2P$. In particular, since $x(-P) = x(P)$ we require that

$$\frac{x^4 - 2ax^2 - 8bx + a^2}{4x^3 + 4ax + 4b} = x$$

where the denominator $4(x^3 + ax + b)$ cannot equal zero since its roots are the 2-torsion points. Multiplying this equation through produces a polynomial whose zeros are exactly the x -coordinates of the points of order three:

$$f_3 : 3x^4 + 6ax^2 + 12bx - a^2 = 0. \quad (4.4.4)$$

We are interested in the splitting behavior of this polynomial. First, notice that f_3 has no roots in \mathbb{F}_p that are also elliptic over \mathbb{F}_p because then $3 \mid \#E(\mathbb{F}_p) = p$; a contradiction. In fact, f_3 can either be irreducible over \mathbb{F}_{p^2} or factor into either of the following

- (i) Four linear terms,
- (ii) One linear and one cubic term,
- (iii) Two linear and one quadratic term,
- (iv) Two quadratic terms.

In each case the nonlinear terms are irreducible over \mathbb{F}_{p^2} and thus cannot be coordinates of 3-torsion points in $E(\mathbb{F}_{p^2})$. However, each linear term produces a root x_α of f_3 and if

x_α is elliptic, the corresponding torsion points are (x_α, y_α) and its inverse $(x_\alpha, -y_\alpha)$ where $\pm y_\alpha$ are the roots of $y^2 - f(x_\alpha)$.

If f_3 has at least two linear terms producing elliptic roots, then $E[3]$ contains at least five points (including \mathcal{O}) and $\text{Syl}_3(E(\mathbb{F}_{p^2})) \cong \mathbb{Z}/3 \oplus \mathbb{Z}/3^{t-1}$ by the remark above. If f_3 has exactly one linear term producing an elliptic root x_α , then $E[3] = \{\mathcal{O}, (x_\alpha, y_\alpha), (x_\alpha, -y_\alpha)\}$ and by the same remark $\text{Syl}_3(E(\mathbb{F}_{p^2})) \cong \mathbb{Z}/3^t$. If f_3 has no elliptic roots, there are no 3-torsion points and consequently $\text{Syl}_3(E(\mathbb{F}_{p^2}))$ is trivial. \square

Theorem 4.4.5 allows us to easily determine $E(\mathbb{F}_{p^2})$ for curves with $a_p = 1$ by factoring f_3 into irreducible factors and checking which roots x_α arising from the linear terms $(x - x_\alpha)$ are elliptic. Note that if there are no linear terms we are done, since then $\text{Syl}_3(E(\mathbb{F}_{p^2}))$ is trivial. Therefore, we only need to factor f_3 and for each root x_α arising from a linear term in its factorization check whether the polynomial $y^2 - f(x_\alpha)$ is irreducible over \mathbb{F}_{p^2} since then $f(x_\alpha)$ is not a square in \mathbb{F}_{p^2} and consequently x_α is not elliptic. Both of these factorizations can be achieved by Berlekamp's algorithm (see [1]) for factoring polynomials over finite fields.

We conclude this section with an example of this process.

Example 4.4.6. Let

$$E_1: y^2 = x^3 + 5 \quad \text{and}$$

$$E_2: y^2 = x^3 + 3x + 5$$

be elliptic curves defined over \mathbb{F}_7 . Using a computer algebra program (such as Pari or Magma) it is easy to verify that $a_7 = 1$ in both cases and that $E_1(\mathbb{F}_7) \cong E_2(\mathbb{F}_7) \cong \mathbb{Z}/7$ while on the other hand

$$E_1(\mathbb{F}_{7^2}) \cong \mathbb{Z}/7 \times \mathbb{Z}/3 \times \mathbb{Z}/3 \quad \text{and}$$

$$E_2(\mathbb{F}_{7^2}) \cong \mathbb{Z}/7 \times \mathbb{Z}/9.$$

We now verify this result using the process described above. The polynomials (over \mathbb{F}_7) whose roots are the x -coordinates of the 3-torsion points for these two curves are given by

$$f_3(E_1) = 3x^4 + 4x \quad \text{and}$$

$$f_3(E_2) = 3x^4 + 4x^2 + 4x + 5.$$

Over \mathbb{F}_7 their factorizations are

$$f_3(E_1) = 3x(3+x)(5+x)(6+x) \quad \text{and}$$

$$f_3(E_2) = 3(5+x)(5+3x+2x^2+x^3).$$

It is easy to check that $y^2 - f(x_\alpha)$ is irreducible over \mathbb{F}_7 for $x_\alpha = 0, -3, -5, -6$. By Lemma 4.4.3 all the roots arising from the linear terms are elliptic for both $f_3(E_1)$ and $f_3(E_2)$. It follows that

$$E_1[3] \cong \mathbb{Z}/3 \quad \text{and}$$

$$E_2[3] \cong \mathbb{Z}/3 \times \mathbb{Z}/3$$

and by Theorem 4.4.5 also that

$$\text{Syl}_3(E_1) \cong \mathbb{Z}/3^2 \quad \text{and}$$

$$\text{Syl}_3(E_2) \cong \mathbb{Z}/3 \times \mathbb{Z}/3,$$

since $t = V_3(9) = 2$. Since $\ell \nmid 9$ for all $\ell \neq 7, 3$, by Lemma 4.4.1 we conclude that

$$E_1(\mathbb{F}_{7^2}) \cong \mathbb{Z}/7 \times \mathbb{Z}/3 \times \mathbb{Z}/3 \quad \text{and}$$

$$E_2(\mathbb{F}_{7^2}) \cong \mathbb{Z}/7 \times \mathbb{Z}/9$$

as desired. ◇

From this example it follows that both possible group structures for $E(\mathbb{F}_{p^2})$ given by Theorem 4.4.1 occur. They are *not* uniquely determined by $E(\mathbb{F}_p)$ and can be computed by the process described above. In other words, all cases of Theorem 4.4.5 can actually occur!

4.5 Further Research

The approach we have taken in this project can become substantially more difficult for a_p with large absolute value. In particular, we can have more primes ℓ for which the Sylow- ℓ subgroup of $E(\mathbb{F}_{p^2})$ is not uniquely determined and it becomes more difficult to find the possible group structure for each ℓ . This is true even if $a_p = 2$.

Example 4.5.1. Suppose that E is an elliptic curve defined over \mathbb{F}_p with $a_p = 2$. Then $N = \#E(\mathbb{F}_{p^2}) = (p-1)(p+4)$ by Lemma 3.3.2. To determine the possible group structures by using Theorem 3.3.5, we need $\ell \mid N$ and have to consider

$$\min(r_\ell, s_\ell) \leq V_\ell((p-1)(p+1)).$$

If $\ell = 3 \mid N$ and $V_3(p+4) \neq 0$, then also $3 \mid p+1$. If $\ell = 5 \mid N$, then for large enough p we have $5 \mid p-1$. So we need to specially consider $\ell = 3$ and 5 , where the methods used in Lemma 4.4.1 will have to be modified or new ones made. \diamond

Finally, a related problem is the following. Let E_1 and E_2 be elliptic curves defined over \mathbb{F}_p . Under which conditions does $E_1(\mathbb{F}_p) \cong E_2(\mathbb{F}_p)$ imply $E_1(\mathbb{F}_{p^2}) \cong E_2(\mathbb{F}_{p^2})$. We have already seen that this is not true in general in Example 4.4.6, but it is not hard to find an example in which it is true.

Example 4.5.2. Let

$$E_1: y^2 = x^3 + 5x + 5 \quad \text{and} \quad E_2: y^2 = x^3 + 6x + 5$$

be elliptic curves defined over \mathbb{F}_7 . It is easy to verify that

$$E_1(\mathbb{F}_7) \cong E_2(\mathbb{F}_7) \cong \mathbb{Z}/7$$

as well as that

$$E_1(\mathbb{F}_{49}) \cong E_2(\mathbb{F}_{49}) \cong \mathbb{Z}/7 \times \mathbb{Z}/9.$$

\diamond

Appendix A

Connection of Elliptic Curves to Ellipses

In this appendix we demystify the naming of elliptic curves by showing how they arise when computing the arclength of an ellipse. Special thanks to John Cullinan for this explanation.

An elliptic curve is the set of solutions (x, y) to an equation of the form:

$$y^2 = x^3 + Ax^2 + Bx + C.$$

Recall that an ellipse is the set of solutions (x, y) to an equation of the form:

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1.$$

We can compute the arclength of the graph of an ellipse using the familiar formula from elementary calculus:

$$L = 4 \int_0^a \sqrt{1 + \left(\frac{dy}{dx}\right)^2} dx.$$

Using implicit differentiation, it follows that $\frac{dy}{dx} = -\left(\frac{b^2}{a^2}\right)\frac{x}{y}$, so the resulting arclength formula becomes:

$$\begin{aligned}
L &= 4 \int_0^a \sqrt{1 + \left(\frac{b^2}{a^2}\right)^2 \frac{x^2}{a^2 - x^2}} dx \\
&= 4 \int_0^a \sqrt{\frac{1 - (1 - b^2/a^2)(x/a)^2}{1 - (x/a)^2}} dx \\
&= 4a \int_0^1 \sqrt{\frac{1 - k^2t^2}{1 - t^2}} dt, \quad \text{where } t = x/a, k = 1 - (b^2/a^2) \\
&= 4a \int_0^1 \frac{1 - k^2t^2}{\sqrt{(1 - t^2)(1 - k^2t^2)}} dt \\
&= 4a \int_0^1 \frac{1 - k^2t^2}{u} dt, \quad \text{where } u = \sqrt{(1 - t^2)(1 - k^2t^2)}.
\end{aligned}$$

Letting $x = 1/(t - 1)$ and $y = u/(t - 1)^2$ yields the relation

$$y^2 = (2k^2 - 2)x^3 + (5k^2 - 1)x^2 + 4k^2x + k^2.$$

Dividing both sides by $(2k^2 - 2)$ (we can do this since $2k^2 - 2 = 0$ if and only if $b = 0$, an impossibility), and changing variables once again produces

$$y^2 = x^3 + Ax^2 + Bx + C,$$

which is the equation of an elliptic curve!

Bibliography

- [1] E. R. Berlekamp, *Factoring polynomials over large finite fields*, Mathematics of Computation **24** (1970), no. 111, 713-735.
- [2] David Cox, John Little, and Donal O'Shea, *Ideals, Varieties, and Algorithms*, Springer-Verlag, New York, 1992.
- [3] David S. Dummit and Richard M. Foote, *Abstract Algebra*, Prentice-Hall, Englewood Cliffs, New Jersey, 1991.
- [4] Robin Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, 1977.
- [5] René Schoof, *Non-singular plane cubic curves over finite fields*, [Ph.D. Thesis], University of Amsterdam, 1985.
- [6] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.
- [7] Joseph H. Silverman and John Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, New York, 1992.
- [8] Felipe Voloch, *A note on elliptic curves over finite fields*, Bull. Soc. Math. France **116** (1988), 455-458.
- [9] William C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École. Norm. Sup. (4) **2** (1969), 521-560.