# Elliptic Curves and Their Cryptographic Applications

---

A Thesis

Presented To

Eastern Washington University

Cheney, Washington

---

In Partial Fulfillment of the Requirements

for the Degree

Master of Science

---

By

Samuel L. Wenberg

Winter 2013

THESIS OF SAMUEL L. WENBERG APPROVED BY

_____ DATE:_____

FIRST MEMBER OF THE COMMITTEE, GRADUATE STUDY COMMITTEE

_____ DATE:_____

SECOND MEMBER OF THE COMMITTEE, GRADUATE STUDY COMMITTEE

_____ DATE:_____

THIRD MEMBER OF THE COMMITTEE, GRADUATE STUDY COMMITTEE

**Abstract**

This thesis is a basic overview of elliptic curves and their appilcations to Cryptography. We begin with basic definitions and a demonstration that, given an elliptic curve addition, the points of an elliptic curve form a mathematical group. We then proceed to delve further into the mathematics, discussing torsion points on the group of elliptic curves before investigating the behavior of elliptic curves over finite fields wherein is given a proof of Hasse's Theorem on elliptic curves. With these tools, we discuss the discrete log problem, and the connection between elliptic curves and the field of cryptography. Finally, we look at elliptic curves over $\mathbb{C}$ and establish a trapdoor isomorphism between elliptic curves, and a topological torus.

**Acknowledgements**

Many thanks to Dr. Ron Gentle for being a constant source of assistance in this endeavour.

# Contents

# List of Figures

# Chapter 1

# Introduction:

The first recorded appearance of elliptic curves can be traced to Diophantus in his text *Arithmetica*. Specifically, problem 24 of book IV, states: "To divide a given number into two numbers such that their product is a cube minus its side." Put in more conventional terms, the task is to take some number $a$ and split it into two values $y$ and $a - y$ such that

$$y(a - y) = x^3 - x$$

The task is thus to determine solutions to the above equation. Diophantus found that via a "secant method" any two solutions of a cubic will produce a third. Further, the "limiting case" of the secant, which is to say the "tangent" at a single point, yields similar results in producing a new solution.

## 1.1 What's So "Elliptical" About Elliptic Curves

Now, certainly, $y(a-y) = x^3 - x$ doesn't look at all like the elementary equation for an ellipse. While Diophantus may have been the first to unwittingly look at an elliptic curve type construction, he certainly did not call them as

such. The name stems from more recent mathematics, specifically the work of John Wallis during the mid 1600's. Wallis was attempting to ascertain the arc length of ellipses, a rather important notion, with many applications in the physical sciences. This led to an idea of what were dubbed elliptic integrals[4]. Looking more deeply at elliptic integrals, with some prodigious variable changes, eventually leads us back to these strange cubics that we are referring to as elliptic curves. The connection here will be looked at much deeper in a later chapter.

## 1.2 Some Examples of the Tangent and Secant Methods of Diophantus

**Example 1.1** We can see how the tangent method is employed by loosely following the methods of Diophantus, albeit with a slightly more modern bent. For our first example we will solve the problem stated at the begining of this chapter for the case of $a = 6$. Our equation to solve then becomes:

$$6y - y^2 = x^3 - x \tag{1.1}$$

Now, we note by observation that the ordered pair $(-1, 0)$ is a solution to this equation.

We create a generic line $x = ky - 1$, a line with x-intercept at $-1$. We now wish to pick $k$ such that our line is tangent to the point $(-1, 0)$. By substitution into (1.1), we get:

$$6y - y^2 = (ky - 1)^3 - (ky - 1) = k^3y^3 - 3k^2y^2 + 2ky \tag{1.2}$$

In order for our generic line to be tangent to (1.1), (1.2) must have a double root at $y = 0$ (or else $x = ky - 1$ will not be tangent). We must thus choose $k$

such that our degree-one terms are equal on either side of (1.2). In this case, $k = 3$.

(1.2) then becomes (after some simplification) $0 = y^2(27y - 26)$. Ignoring our repeated $y = 0$ solution, which we already know, the only remaining solution is $y = \frac{26}{27}$.

In terms of our problem, we find that we must split 6 into the summands $\frac{26}{27}$ and $\frac{136}{27}$, the sum of which will be 6 and the product of which will equal the difference of the perfect cube $\frac{4913}{729}$ and its side $\frac{17}{9}$. □

**Example 1.2** A second application, this time of the secant method, involves the so-called "cannonball problem." [1] Consider a square-based pyramid of cannonballs made up of $x$-many layers. Then the $x = 1$ pyramid would have just the one cannonball, the $x = 2$ pyramid would have 5 cannonballs, etc. The problem then is to ascertain values of $x$ for which, should the $x$-pyramid be knocked over the resulting cannonballs could be arranged into a square grid of cannonballs. Specifically, we desire the following:

$$y^2 = 1^2 + 2^2 + ... + x^2 \tag{1.3}$$

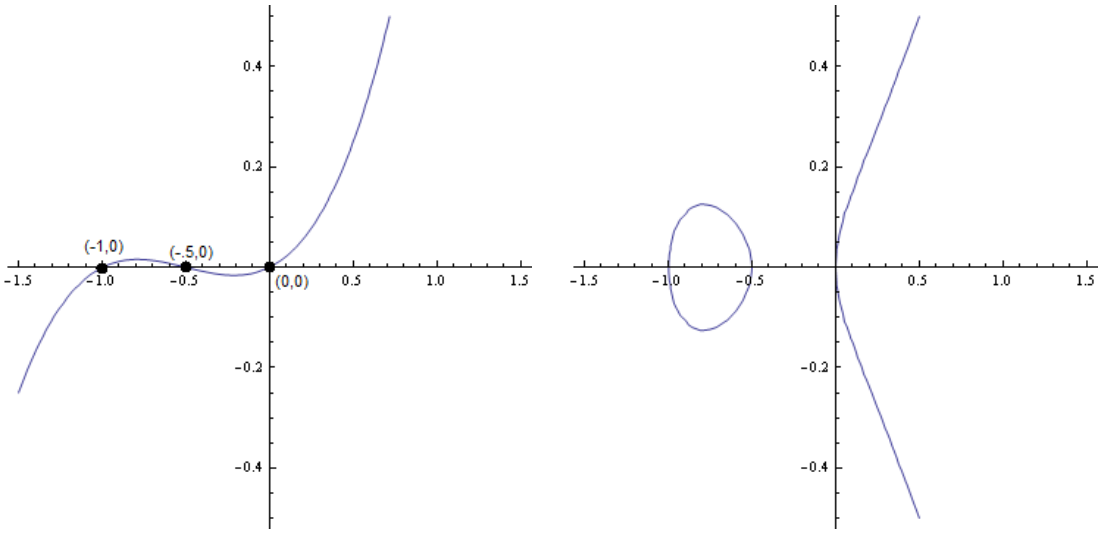
Via induction we may easily show that the sum $\sum_{i=1}^{x} i^2 = \frac{x(x+1)(2x+1)}{6}$. We may thus rewrite (1.3) as:

$$y^2 = \frac{1}{3}x^3 + \frac{1}{2}x^2 + \frac{1}{6}x \tag{1.4}$$

Trivially we know by observation that the $x = 0$ and $x = 1$ pyramids will work, resulting in the points (0,0) and (1,1) respectively. We will construct a line through these two points, resulting in (with elementary algebra) the line $y = x$. Substituting this into (1.4) yields:

$$0 = x^3 - \frac{3}{2}x^2 + \frac{1}{2}x \tag{1.5}$$

Figure 1.1: Graphical Representation of (1.4)




(a) $y = \frac{x(x+1)(2x+1)}{6}$ with the roots marked.

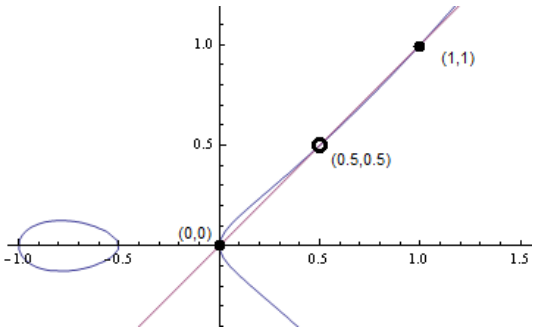
(b) $y^2 = \frac{x(x+1)(2x+1)}{6}$. Note how the roots remain the same.

Recall that a monic cubic polynomial with three roots, $x_1$, $x_2$, and $x_3$ will look like: $(x - x_1)(x - x_2)(x - x_3) = x^3 - (x_1 + x_2 + x_3)x^2 + ...$

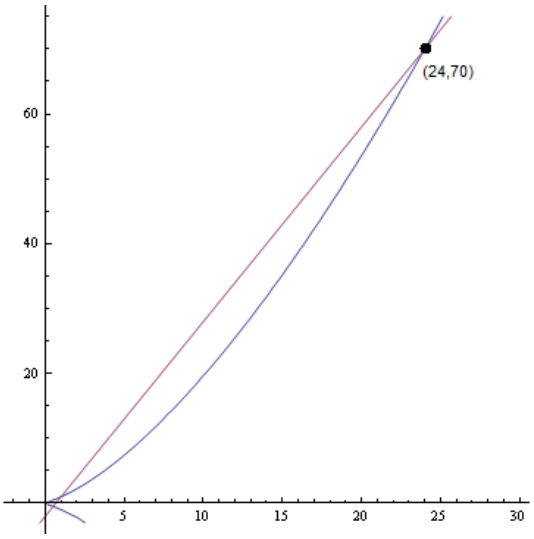
The point here being that given two known roots of a monic cubic polynomial, we may ascertain the third by using the coefficient on the $x^2$ term. Since we know two solutions of (1.5) already, namely 0 and 1, we may find the third: $0 + 1 + x_3 = \frac{3}{2}$. Thus $x_3$ here is $\frac{1}{2}$.

This naturally doesn't present itself as a valid solution to the problem, since half of a cannonball makes no sense, however we can certainly use this result to reapply the secant method, and find more solutions. We can see that the solution that we now have really gives us two distinct solutions to (1.4), specifically $(\frac{1}{2}, \frac{1}{2})$ and $(\frac{1}{2}, -\frac{1}{2})$ We will repeat the secant method with the points $(1, 1)$ and $(\frac{1}{2}, -\frac{1}{2})$. We are picking these points specifically because we wish to establish our new solution somewhere in the first quadrant. Using these two

Figure 1.2: The secant lines




(a) Our first secant line, with our two "starting points," as well as the new point at $(\frac{1}{2}, \frac{1}{2})$.




(b) The second secant line, with our final solution

points, one obtains $0 = x^3 - \frac{51}{2}x^2 + \frac{72}{2}x - 12$, so $\frac{51}{2} = 1 + \frac{1}{2} + x_3$, so $x_3 = 24$. Evaluating (1.4) at x=24, we get the point $(24, 70)$ or more specifically a 24-layered pyramid is made up of $70^2$ cannonballs. □

## 1.3 Other Applications

While the focus of this paper is on cryptography, elliptic curves appear all over mathematics. In mathematics, elliptic curves have applications in number theory, topology and analysis. Additionally, there are methods involving elliptic curves for testing primality of numbers as well as factorization of numbers. Outside of theoretical mathematics, elliptic curves come up in physics, notably in relation to the pendulum equation, as well as uses in modern physics. Perhaps most famously, elliptic curves were crucial in the proof of Fermat's Last Theorem by Wiles in 1994.

# Chapter 2

# Basics

## 2.1 Notation and Definitions

**Definition 2.1** An *Elliptic Curve* over a given field $K$ is the set of points $(x, y)$ on the non-singular curve $y^2 + axy + by = x^3 + cx^2 + dx + e$ where $x$, $y$, $a$, $b$, $c$, $d$, and $e$ are all elements of $K$, along with a point at infinity that we will refer to as $\infty$. Notationally we will refer to this elliptic curve as $E(K)$.

For now we will treat this $\infty$ as a formal symbol with some useful properties. We will investigate it further in a later section. Of importance is the fact that the curve is non-singular, which is to say it has no singular points (points where both partial derivatives are zero).

**Example 2.2** The equation $y^2 + axy + by = x^3 + cx^2 + dx + e$ will be referred to as the *generalized Weierstrass equation.*

What's more given a field $K$ that is neither characteristic 2 or 3, we may do the following:

Starting with the generalized Weierstrass equation, we have

$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

Since K is not characteristic 2, we may complete the square on the left, yielding:

$$\begin{aligned} y^2 + (ax+b)y &= x^3 + cx^2 + dx + e \\ y^2 + (ax+b)y + \left(\frac{ax+b}{2}\right)^2 &= x^3 + cx^2 + dx + e + \left(\frac{ax+b}{2}\right)^2 \\ \left(y + \frac{ax+b}{2}\right)^2 &= x^3 + \left(c + \frac{a^2}{4}\right)x^2 + \left(d + \frac{ab}{2}\right)x + \left(\frac{b^2}{4} + e\right) \end{aligned}$$

Making the following substitutions,

$$\begin{aligned} a' &= c + \frac{a^2}{4} & b' &= d + \frac{ab}{2} \\ c' &= \frac{b^2}{4} + e & y' &= y + \frac{ax+b}{2} \end{aligned}$$

we have: $y'^2 = x^3 + a'x^2 + b'x + c'$

Since K is not characteristic 3, let $x' = x + \frac{a'}{3}$.

This yields $y'^2 = (x'^3 - a'x'^2 + ....) + a'x'^2 - ... + ...$ The point here being that the $x^2$ terms disappear, and our equation can be written as: $y'^2 = x'^3 + Ax' + B$ for some constants A and B in our field $K$. □

**Definition 2.3** For an elliptic curve $E(K)$ if the field is neither characteristic 2 or characteristic 3, we may rewrite the generalize Weierstrass equation as $y^2 = x^3 + Ax + B$ for $A$ and $B$ constants in $K$. This is referred to as the *Weierstrass Equation*. What's more, for the equation to represent an elliptic curve the roots of the right-hand side of the Weierstrass equation must be distinct.

**Theorem 2.4** *The right side of the Weierstrass equation has a double root if and only if* $4A^3 + 27B^2 = 0$.

**Proof:** Recall first that for a given polynomial $P$ with coefficients in a field $F$, $P$ has a double root if and only if $P$ and $P'$ share a root, $r$. The shared double root $r$ implies that $P$ and $P'$ share a linear factor $(x-r)$. This means that $P$ has no multiple roots if and only if the greatest common divisor of $P$ and $P'$ is 1 in the ring $K[x]$. In this case, our polynomial $P$ is $x^3+Ax+B$, so $P'=3x^2+A$. Our goal is to determine the greatest common divisor of $P$ and $P'$, which we will do by way of the Euclidean algorithm.

First we compute $(x^3+Ax+B)/(3x^2+A)$ in the typical way:

$$\begin{array}{r} \frac{1}{3}x \\ 3x^2+A \,\overline{)\, x^3+Ax+B} \\ \underline{x^3+\frac{Ax}{3}} \\ \frac{2A}{3}x+B \end{array}$$

So our first remainder is $\frac{2A}{3}x+B$. Continuing to the next step of the algorithm:

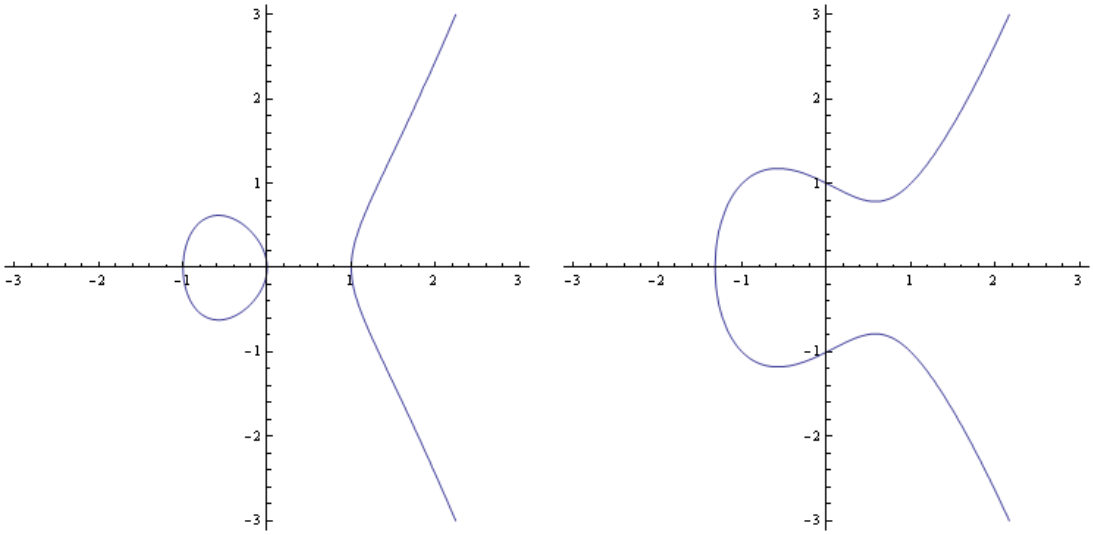
$$\begin{array}{r} \frac{9}{2A}x-\frac{27B}{4A^2} \\ \frac{2A}{3}x+B \,\overline{)\, 3x^2+A} \\ \underline{3x^2+\frac{9B}{2A}x} \\ \frac{-9B}{2A}x+A \\ \underline{\frac{-9B}{2A}x-\frac{27B^2}{4A^2}} \\ A+\frac{27B^2}{4A^2} \end{array}$$

Now, if the second remainder $A+\frac{27B^2}{4A^2}$ is non-zero, then $P$ and $P'$ share no linear factors, and thus have no common roots. Since $A+\frac{27B^2}{4A^2}=\frac{4A^3+27B^2}{4A^2}$, we have no shared linear factors (and thus no double roots) if and only if $4A^3+27B^2\neq 0$. Therefore, $x^3+Ax+B$ has a double root if and only if $4A^3+27B^2=0$. ∎

In general we will use the much simpler Weierstrass equation, only resurrecting the generalized Weierstrass equation for specific cases of characteristic 2 or characteristic 3 fields.

While in most cases pictures of elliptic curves would be relatively meaningless, we will begin our exploration with Elliptic curves over $\mathbb{R}$ which yield two general shapes, based on the number of real roots of the right hand side of the Weierstrass equation (See Figure 2.1 for two examples).

Figure 2.1: Some Elliptic Curves




(a) $y^2 = x^3 - x$. Note the three real roots at $x = -1$, $x = 0$, and $x = 1$.

(b) $y^2 = x^3 - x + 1$. Note the one real root at $x \approx -1.32472$

## 2.2 Point Addition on Elliptic Curves

Earlier, we established a basic method for finding new points given already existing points on cubics. We will now expand upon those ideas to create a

clearly defined operation by which we will add points.

As we saw earlier we can start with two relatively generic points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ on some elliptic curve $E(K)$. We can define a new operation $+_E$ as follows. First construct a line $L$ connecting $P_1$ and $P_2$. We then find the third point of intersection between $L$ and $E(K)$, calling this $P_3'$ (similar to what we found in earlier examples). Finally, in order to allow for certain behavioral properties of the operation, we change the sign of the $y$-coordinate of $P_3'$ to obtain $P_3$. Notationally we write $P_1 +_E P_2 = P_3$.

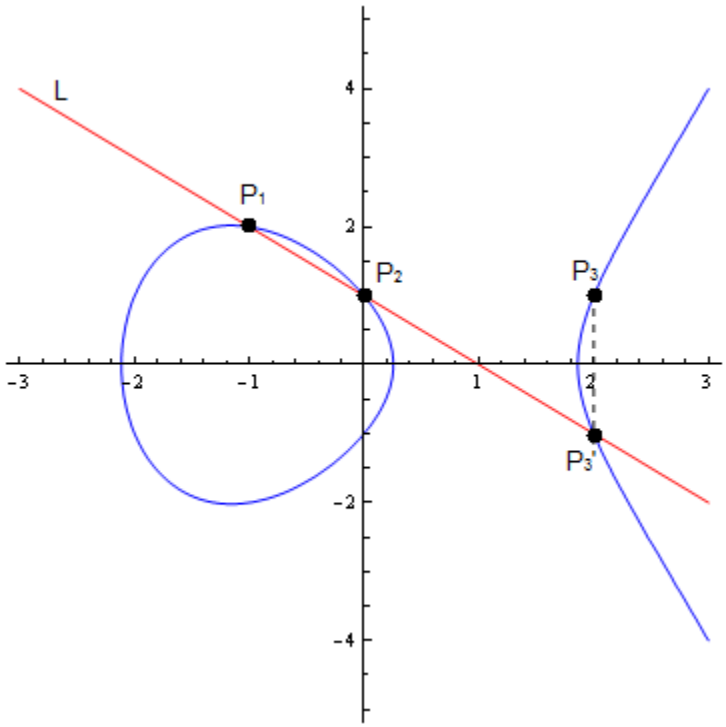



Figure 2.2: Elliptic Curve Point Addition Case (i)

**Example 2.5** Let $E(\mathbb{R})$ be an elliptic curve with the following Weierstrass equation: $y^2 = x^3 + 73$. Let $P_1 = (2, 9)$ and $P_2 = (3, 10)$. The line connecting $P_1$ and $P_2$ is clearly $y - 10 = x - 3$ or $y = x + 7$. So combining with our Weierstrass equation we get the following:

$$\begin{aligned}(x+7)^2 &= x^3 + 73\\ x^2 + 14x + 49 &= x^3 + 73\\ 0 &= x^3 - x^2 - 14x - 49\end{aligned}$$

As before, the sum of our three roots will equal the opposite of our $x^2$ coefficient, so we have $2 + 3 + x_3 = 1$ resulting in our third root being $-4$. The point $(-4, 3)$ thus lies both on the line $y = x + 7$ and the curve $y^2 = x^3 + 73$. Thus $P_1 + P_2 = (-4, -3)$ since we need to "flip" our point across the x-axis. □

More generally, let's consider two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ on some elliptic curve $E(K)$ defined by the Weierstrass equation $y^2 = x^3 + Ax + B$.

For the first case, let's assume that $P_1$ and $P_2$ are distinct points and further let's assume that $x_1 \neq x_2$. Finally, let's assume neither $P_1$ nor $P_2$ are the point at infinity. The slope of the line which passes through $P_1$ and $P_2$ we can define as: $m = \frac{y_2 - y_1}{x_2 - x_1}$. So the line can be written as $y = m(x - x_1) + y_1$, and combining with the equation of our elliptic curve yields:

$$\begin{aligned}(m(x - x_1) + y_1)^2 &= x^3 + Ax + B\\ 0 &= x^3 - m^2x^2 + ...\end{aligned}$$

Recall, we only need to worry about the coefficient on the $x^2$ term, and so $x_3 = m^2 - x_1 - x_2$. Plugging back into our linear equation, we get

$-y_3 = m(x_3 - x_1) + y_1$ (recall that this gives us the opposite of $y_3$), and thus our ordered pair for $P_3 = (x_3, y_3)$ is:

$$(m^2 - x_1 - x_2, m(x_1 - m^2 + x_1 + x_2) - y_1)$$

For the second case, let's assume that again $P_1$ and $P_2$ are distinct but $x_1 = x_2$. The line through these points is a vertical one, and this is where the aforementioned point at $\infty$ comes into play. For now we will formally say that $P_1 +_E P_2 = \infty$. From a pictorial sense think of this $\infty$ as living simultaneously along the top and the bottom of the coordinate plane. We will make more sense of what this means in a later section.

For our third case, let's assume $P_1 = P_2$. Then, instead of creating a secant line, we will use the tangent line at $P_1$. We can derive this formally via implicit differentiation.

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

$$2y\,dy = (3x^2 + A)\,dx$$

$$\frac{dy}{dx} = \frac{3x^2 + A}{2y}$$

So at the point in question the slope is $m = \frac{3x_1^2 + A}{2y_1}$. If $y_1$ is zero, then we will have a vertical tangent line at $(x_1, y_1)$, so $P_1 +_E P_1 = \infty$. We show below that when $y_1$ is zero, the numerator is not also zero (thus circumventing an indeterminate slope).

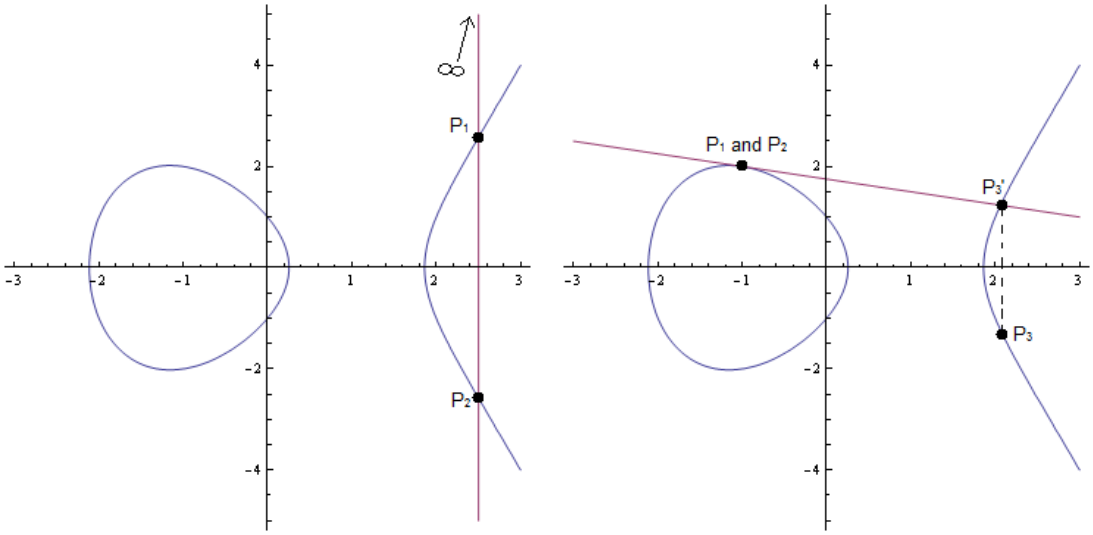
**Theorem 2.6** *Let $(x_1, y_1)$ be a point on an elliptic curve $E(K)$ given by $y^2 = x^3 + Ax + B$. Then if $y_1 = 0$, $3x_1^2 + A \neq 0$.*

**Proof:** Let $y_1 = 0$. Further, assume that $3x_1^2 + A = 0$. Then, $(x_1, y_1)$ is a critical point of $y = x^3 + Ax + B$ and thus a critical point on the elliptic curve.

What's more, since $x_1^3 + Ax_1 + B = 0$, $x_1$ is also a root of $y^2 = x^3 + Ax + B$. Since $(x_1, y_1)$ is simultaneously a critical point and a root, for our elliptic curve, then $x_1$ must be a double root, meaning $x^3 + Ax + B$ is of the form $(x - x_1)^2(x - x_2)$. This is a contradiction since we require by definition that the right hand side of the Weierstrass equation not have double roots. ∎

**Remark:** The above really ends up being a consequence of the non-singular nature of our elliptic curve. Let $f(x, y) = y^2 - (x^3 + Ax + B)$, then $f_x = -(3x^2 + A)$ and $f_y = 2y$. This gives us that $y_1 = 0$ and $3x_1^2 + A = 0$ if and only if $f_x = 0$ and $f_y = 0$, which would indicate that the point $(x_1, y_1)$ was a singular point. Given $y_1 \neq 0$ we will have as our line $y = m(x - x_1) + y_1$

Figure 2.3: Cases (ii) and (iii) for elliptic curve point addition



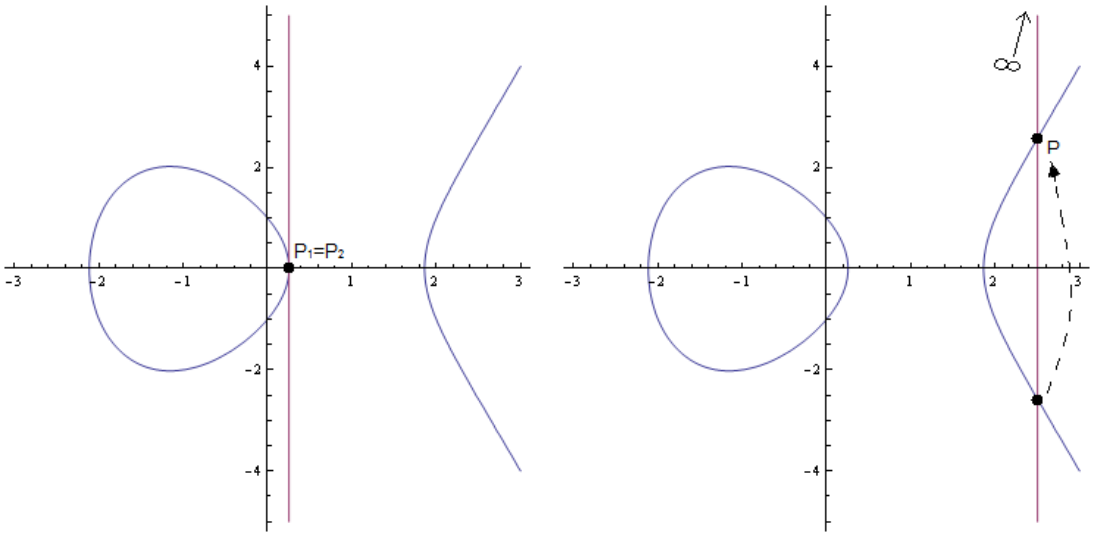

(a) Case (ii) (b) Case (iii)

and as before we will be able to find our third point by looking at roots of $(m(x - x_1) + y_1)^2 = x^3 + Ax + B$. We get $0 = x^3 - m^2x^2 + ... \Rightarrow x_3 = m^2 - 2x_1$. Further, we see that $y_3 = m(x_1 - x_3) - y_1$. For the case of $P_1 = P_2$ then we

find that $P_1 +_E P_2 = (m^2 - 2x_1, m(x_1 - m^2 + 2x_1) - y_1)$

For our final case, we will look at $P_1 +_E \infty$. Again we will treat this formally with a more in depth analysis later. For now, we will say $P_1 +_E \infty = P_1$, and what's more we will extend this notion to $\infty +_E \infty = \infty$. The definition below summarizes point addition.

Figure 2.4: Cases (iv) and (v) for elliptic curve point addition




(a) Case (iv) (b) Case (v)

**Definition 2.7** *Addition on Elliptic Curves:*

For an elliptic curve $E(K)$ defined by the equation $y^2 = x^3 + Ax + B$ ($K$ is neither characteristic 2 or characteristic 3), and for the points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ on $E$, we have the following as definitions for $P_1 +_E P_2 = P_3 = (x_3, y_3)$:

i) If $x_1 \neq x_2$, then

$m = \frac{y_2 - y_1}{x_2 - x_1}$,

$x_3 = m^2 - x_1 - x_2$,

and $y_3 = m(2x_1 - m^2 + x_2) - y_1$

ii) If $x_1 = x_2$ and $y_1 \neq y_2$, then

$P_1 +_E P_2 = \infty$

iii) If $P_1 = P_2$ and $y_1 \neq 0$, then

$m = \frac{3x_1^2 + A}{2y_1}$

$x_3 = m^2 - 2x_1$

$y_3 = m(3x_1 - m^2) - y_1$

iv) If $P_1 = P_2$ and $y_1 = 0$, then

$P_1 +_E P_2 = \infty$

v) Further, define $P +_E \infty = P$ for all points $P$ on $E(K)$.

## 2.3 Some Words on Infinity

In order to get an idea of what exactly this point $\infty$ is, we will need some ideas using 2-dimensional projective space over our field $K$.

**Definition 2.8** Two-dimensional *projective space over* $K$ notated as $\mathbf{P_K^2}$ is given by the equivalence classes of ordered triples $(x, y, z)$ where $x, y, z \in K$ and $x, y, z$ not all zero. We say that $(x_1, y_1, z_1)$ is equivalent to $(x_2, y_2, z_2)$ if $(x_1, y_1, z_1) = (\lambda x_2, \lambda y_2, \lambda z_2)$ for some $\lambda \in K$, $\lambda \neq 0$. Denote the equivalence with $\sim$. What's more, since equivalence is only determined by the ratios of $x, y$, and $z$, we will denote the equivalence class of $(x, y, z)$ as $(x : y : z)$

When $z \neq 0$, any point $(x, y, z) \sim (x/z, y/z, 1)$. We can thus interpret equivalence classes of the form $(x : y : 1)$ as being the finite points in $\mathbf{P_K^2}$. If $z = 0$, when we divide by $z$ we interpret the resulting $x$ or $y$ coordinate as infinity. As a result, we can consider the equivalence classes $(x : y : 0)$ as being points

at infinity.

We will shortly be showing that $\infty$ from our definition for elliptic curves will be one of these $(x : y : 0)$'s.

Using the map $(x, y) \to (x : y : 1)$ we get that the points in the 2-dimensional affine plane, defined as $\mathbf{A_K^2} = \{(x, y) : (x, y) \in K \times K\}$, map in a 1-1 and onto fashion to the finite points in $\mathbf{P_K^2}$. 2-dimensional projective space over K thus contains the 2-dimensional affine plane over K as well as a bunch of points at infinity.

**Definition 2.9** A polynomial in three variables $x, y, z$, is *homogeneous of degree* $n$ when it is the sum of terms of the form $ax^iy^jz^k$ where $i + j + k = n$ and $a \in K$. Note: the coefficient need not be the same on each term.

**Theorem 2.10** If $f(x, y, z)$ is a homogeneous polynomial of degree $n$ and $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$, then $f(x_1, y_1, z_1) = 0$ iff $f(x_2, y_2, z_2) = 0$.

**Proof:** Let $f(x_1, y_1, z_1) = 0$.

Since $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$, then $(x_1, y_1, z_1) = (\lambda x_2, \lambda y_2, \lambda z_2)$. So:

$0 = f(x_1, y_1, z_1) = f(\lambda x_2, \lambda y_2, \lambda z_2)$.

Now, each term of $f(\lambda x_2, \lambda y_2, \lambda z_2)$ looks like:

$a\lambda^i x^i \lambda^j y^j \lambda^k z^k = \lambda^{i+k+j} a x^i y^j z^k = \lambda^n a x^i y^j z^k$

Factoring out $\lambda^n$ (recall that $\lambda$ is not zero) results in:

$f(\lambda x_2, \lambda y_2, \lambda z_2) = \lambda^n f(x_2, y_2, z_2) = 0 \Rightarrow f(x_2, y_2, z_2) = 0$

By symmetry, $f(x_2, y_2, z_2) = 0 \Rightarrow f(x_1, y_1, z_1) = 0$ ∎

Thus zeroes on homogeneous polynomials are well defined over $P_K^2$.

It is worth noting at this point that Theorem 2.10 requires homogeneous polynomials. Consider the function $f(x, y, z) = x^2 + 2y - 5z$. Certainly at the

point $(1:2:1)$ it appears this function is zero, using the member $(1,2,1)$ of the equivalence class as our check, however $(2,4,2)$ is also a member of this equivalence class, and $f(2,4,2) \neq 0$.

Given any polynomial $f(x,y)$ we can create a homogeneous polynomial of the form $F(x,y,z)$ by multiplying in necessary powers of $z$ onto each term. For example, given $f(x,y) = xy^2 + 2xy + 2$ we can rewrite it as the homogeneous polynomial $F(x,y,z) = xy^2 + 2xyz + 2z^3$. In this way we get the following relationships:

$$F(x,y,z) = z^n f(x/z, y/z)$$

$$f(x,y) = F(x,y,1)$$

Consider now two parallel lines with linear equations: $y = mx + b_1$ and $y = mx + b_2$. We can write them as homogeneous equations and then ascertain points of intersection in $\mathbf{P^2_K}$ as follows. First the homogeneous forms of the equations are $y = mx + b_1 z$ and $y = mx + b_2 z$. So $y - y = mx + b_1 z - mx - b_2 z$, which results in: $0 = (b_1 - b_2)z$. Thus $z = 0$ and $y = mx$. From this we get that these two parallel lines intersect at $(x : mx : 0)$. Notice that, $x \neq 0$ since if $x = 0$ then $x, y$, and $z$ would all equal zero which we asserted could not occur, so dividing by x to clean up our representation yields the intersection of these two lines to be the point $(1 : m : 0)$. Note that this is one of the points at infinity on $\mathbf{P^2_K}$

Repeating this process with the two vertical lines $x = c_1$ and $x = c_2$ yields the following:

Homogeneous versions of these equations are $x = c_1 z$ and $x = c_2 z$.

Thus, $0 = (c_1 - c_2)z \Rightarrow z = 0 \Rightarrow x = 0$.

Therefore any two vertical lines will intersect at $(0 : y : 0) \sim (0 : 1 : 0)$. Again this is a point at infinity on $\mathbf{P^2_K}$.

Consider an elliptic curve defined by the Weierstrass equation $y^2 = x^3+Ax+B$. If we want to consider points at infinity on this curve, we must first look at the homogeneous version of this equation: $y^2z = x^3 + Axz^2 + Bz^3$. Recall that points at infinity will have a z-coordinate of zero, thus substituting zero in for $z$ yields: $0 = x^3$, so points at infinity on our elliptic curve must be in the equivalence class $(0 : 1 : 0)$, and this is in fact the only point at infinity on our elliptic curve. Note that this is the point where two vertical lines intersect. It is this point that we call $\infty$.

We can now interpret points ii), iv), and v) in definition 2.7. For ii), the line passing through $P_1$ and $P_2$ will be a vertical one, and thus the only other place where it can intersect $E(K)$ is at $\infty$. Since $(0, 1, 0) \sim (0, -1, 0)$, when we "flip" $\infty$ over the x-axis we still get $\infty$. For iv), the tangent line is again vertical and so as per the previous description, $P_1 +_E P_2 = \infty$. For v), start by assuming $P \neq \infty$. Then the line between $P$ and $\infty$ will be vertical, and thus intersect E again on the opposite side of the x-axis. Flipping over the x-axis will recover $P$.

## 2.4 Group Law for Elliptic Curves

**Theorem 2.11** *Addition over elliptic curves as defined above is an abelian group:*

*i) Closure: For all* $P_1, P_2 \in E(K)$, $(P_1 +_E P_2) \in E(K)$

*ii) Associativity: For all* $P_1, P_2, P_3 \in E(K)$, $P_1+_E(P_2+_E P_3) = (P_1+_E P_2)+_E P_3$

*iii) Existence of Additive Identity: There is some* $I \in E(K)$ *such that* $P +_E I = P$ *for all* $P \in E(K)$.

*iv) Existence of Additive Inverse: For each* $P \in E(K)$ *there exists some* $-P \in E(K)$ *such that* $P +_E -P = I$ *where* $I$ *is the aforementioned additive identity.*

*v) Commutivity:* $P_1 +_E P_2 = P_2 +_E P_1$ *for all* $P_1$, $P_2 \in E(K)$.

**Proof:** i) Since the coordinates of $P_1$ and $P_2$ are elements of $K$, and $K$ is a field, clearly as defined in definition 2.9, $x_3$ and $y_3$ are elements of $K$. Thus addition of two points on an elliptic curve either yields a further point on $E(K)$: $(x_3, y_3)$ with $x_3, y_3 \in K$, or the addition yields $\infty$ which we defined as being also an element of $E(K)$, thus this point addition is closed over $E(K)$.

ii) The proof for associativity is involved, and as such will be approached in the next section.

iii) Let $I = \infty$. We then have, by definition, the desired property.

iv) Let $P \neq \infty$. Then $P = (x, y)$ for some $x, y \in K$. Let $-P = (x, -y)$. Then, as per definition 2.9, we have that $P +_E -P = \infty$. Now, if $P = \infty$, let $-P = \infty$. As defined above, $\infty +_E \infty = \infty$.

v) Clearly this is true in the cases where $P_1 = P_2$. What's more, when $P_1 \neq P_2$, the line between these points will be the same regardless of the order in which we consider our points. This means the third point of intersection between the created line and the curve itself will not change, thus resulting in the same $P_3$. ∎

Now, it is worth noting that for our elliptic curve $E(K)$, since all of our point addition can be looked at in terms of addition and multiplication on $K$, we get that sub-fields of $K$ will yield subgroups of $E(K)$. By example, the group $E(\mathbb{Q})$ is a subgroup of $E(\mathbb{R})$ which is in turn a subgroup of $E(\mathbb{C})$. We

call $E(\mathbb{Q})$ the subgroup of rational points. In a more general sense, if $K$ is a field and $\bar{K}$ is its algebraic closure, the subgroup $E(K)$ are the rational points of $E(\bar{K})$.

## 2.5 Some Words on the General Cubic

As some partial intuition into associativity, we can look at some properties of the general cubic. We will start by establishing the set of cubics forms a vector space. We will look at a special case of Bezout's theorem and use this to help establish associativity on the general cubic. This will give us associativity on elliptic curves.

**Definition 2.12** We will define the general cubic in two variables as the polynomial:

$$C(x, y) = ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j$$

for constants, $a, b, c, ..., j$.

We may also think of this projectively as:

$$C(x, y, z) = ax^3 + bx^2y + cxy^2 + dy^3 + ex^2z + fxyz + gy^2z + hxz^2 + iyz^2 + jz^3$$

It is worth noting that for $a = b = c = d = 0$, $C(x, y)$ reduces to a quadratic, however we may think of this as a degenerate cubic. Similarly, the cubic might degenerate into a line or constant depending on the values of the coefficients. This is not a problem for the projective version since all terms are cubic.

Additionally, since the important points of the generalized cubic are uneffected by scaling, really we can think of $C$ as a polynomial in 9 coefficients (divide everything by $a$ assuming $a \neq 0$.

**Theorem 2.13** *The set of cubics $C(x, y)$ forms a vector space of dimension 10.*

**Proof:** We will define our vector addition as polynomial addition, and scalar multiplication as traditional multiplication of a scalar and a multivariable polynomial. Given $C_1$ and $C_2$ being cubics, then $C_1 + C_2$ will certainly result in another cubic. Similarly, for a given scalar $\lambda$, then $\lambda C_1$ will be also be a cubic. In order to account for all possible cubics, our basis would have to be size 10, one for each of the 10 coefficients of $C(x, y)$. ∎

What's more, this vector space becomes dimension 9 once we specify the actual curves by setting each $C(x, y) = 0$, or by ignoring scaling in the projective version.

**Definition 2.14** If the coefficients of $C(x, y)$ are rational numbers and $P = (x, y)$ lies on $C$, and $x$ and $y$ are rational, then $P$ is called a *rational point* of $C$.

**Theorem 2.15** *Assume that $C$ is actually a cubic (it has at least one non-zero cubic term in $x$ and $y$). Given two rational rational points $P$ and $Q$ on $C$, then the line through $P$ and $Q$ intersects $C$ at a 3rd rational point.*

**Proof:** Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be rational points. Let $C(x, y) = ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$. Further, by the a linear substitution $(x, y)$ to $M(x, y)$ where $M$ is an invertible 2x2 matrix with rational entries, we can assume that $a \neq 0$. The line through $P$ and $Q$ is

$$y = \frac{y_2 - y_1}{x_2 - x_1}(x - x_1) + y_1 = mx + B$$

where $m$ and $B$ are rational numbers, since $x_1, x_2, y_1$, and $y_2$ are all rational. Substituting into $C$ in order to find the points of intersection yields:

$$ax^3 + bx^2(mx + B) + cx(mx + B)^2 + d(mx + B)^3 + ex^2 +$$
$$fx(mx + B) + g(mx + B)^2 + hx + i(mx + B) + j = 0.$$

We rewrite this as a monic cubic, and focus on the $x^2$ coefficient as before. This yields as the $x^2$ coefficient:

$$\frac{bB + 2cBm + 3dm^2B + e + fm + gm^2}{a + bm + cm^2 + dm^3} = V$$

$V$ is thus rational. This then requires that the third point of intersection will have $x$-coordinate of $-V - x_1 - x_2 = x_3$, which will also be rational. Then $mx_3 + B = y_3$, which is also rational. The third point on $C$ is then $(x_3, y_3)$ which is a rational point. ∎

Define $P * Q$ to be the third intersection point found above. This gives us a binary operation $P * Q$ on the set of rational points, provided it is a non-empty set.

Theorem 2.15 is a special case of Bezout's Theorem, which states that a curve of degree $m$ and a curve of degree $n$ will intersect $nm$ times taking into account multiplicities [10]. The cubic is clearly degree 3, and the connecting line through $P$ and $Q$ is degree 1. This would give us that the line and cubic intersect in three places. For two cubics $C_1$ and $C_2$ then, we get by Bezout's Theorem that these two cubics will intersect at 9 places.

**Theorem 2.16** *Let $C$, $C_1$, and $C_2$ be 3 different cubics, with $C$ passing through 8 of the 9 intersection points of $C_1$ and $C_2$. Then $C$ also intersects the 9th point of intersection.*

**Proof:** As previously stated, the set of cubics is 10-dimensional. The set of cubics passing through a designated point $P_1$ is thus 9-dimensional. Requiring our cubic to pass through 2 designated points will yield an 8-dimensional set of cubics. We can continue in this way and find that the set of cubics which pass through 8 designated points $P_1, ...P_8$ will be 2-dimensional. $C$ must then belong to this 2-dimensional subspace. What's more, any $\lambda_1 C_1 + \lambda_2 C_2$ will also belong to this subspace for any given $\lambda_1$ and $\lambda_2$. We thus have that $C_1$ and $C_2$ form a basis for this 2-dimensional subspace. This gives us that $C = \lambda_1 C_1 + \lambda_2 C_2$ for some specific $\lambda_1$ and $\lambda_2$. Since both $C_1$ and $C_2$ equal zero at the 9th point of intersection, $P_9$, then so too will $C$, thus $P_9$ lies on $C$. ∎

We now make the connection between $*$ and elliptic curve addition. We will assume that for a cubic $C$ with a rational point $O$, if $P$ and $Q$ are also rational points on $C$ we will define $P+Q$ to be $O*(P*Q)$. This operation first creates a line through $P$ and $Q$ to intersect $C$ at a third point, giving $P*Q$. We then intersect $C$ with the line through $O$ and $P*Q$ thus getting $P+Q$. Note that this is essentially elliptic curve point addition if we allow the point $O$ to be $\infty$.

**Theorem 2.17** *Let $C$ be a given cubic where we have at least one rational point. Let $P$, $Q$, and $R$ be rational points on $C$. Then $(P+Q)+R=P+(Q+R)$.*

**Proof:** Since $A + B = O * A * B$ for rational points $A$ and $B$, then it will suffice to show $(P + Q) * R = P * (Q + R)$.

Consider, when we evaluate $P * Q$ we find the line through $P$ and $Q$ and determine the third point of intersection on $C$. Call this line $l_1$. Likewise, we

create the following lines:

$$l_2 = \text{the line through } Q * R \text{ and } O$$

$$l_3 = \text{the line through } P + Q \text{ and } R$$

$$m_1 = \text{the line through } P \text{ and } Q + R$$

$$m_2 = \text{the line through } Q \text{ and } R$$

$$m_3 = \text{the line through } P * Q \text{ and } O$$

Note now that these points, $P, Q, P * Q$, etc are all intersections of the above lines, and they all lie on $C$. Further we will define the point where $m_1$ and $l_3$ intersect as a point $Z$.

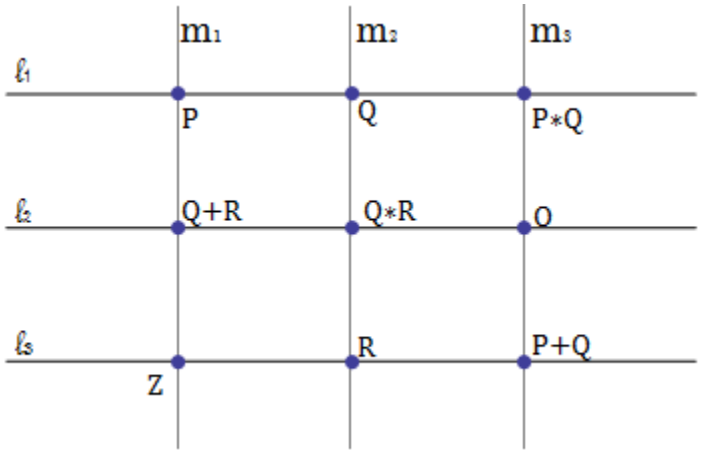



Figure 2.5: An artificial diagram of the 9 points and six lines.

Now, recall these lines will be of the form $0 = l = ax + by + c$, where $a$, $b$, and $c$ are constants. Thus the nine points on $m_1, m_2$, and $m_3$ will also be on the product of these lines: $0 = m_1 m_2 m_3 = C_1$. $C_1$ is a cubic. Likewise, the nine indicated points on $l_1$, $l_2$, and $l_3$ will be on their product, call it $C_2$ and $C_2$ will also be a cubic. Consider that $C_1$ and $C_2$ now intersect at the nine

aformentioned points, and we know that our original cubic $C$ intersects at 8 of those points, specifically, $P$, $Q$, $P * Q$, $Q + R$, $Q * R$, $O$, $R$, and $P + Q$. By theorem 2.16, the ninth point of intersection $Z$ must then be a point on $C$. Since $Z$ is on $C$ and on $m_1$, we get that $Z = (Q + R) * Z$ (the third point of intersection on the line created by $(Q+R)$ and $P$ with $C$. By similar reasoning $Z$ is on $l_3$ and $C$ thus $Z = (P + Q) * R$. ∎

Elliptic curves are a special case of the above, with rational point corresponding to $\infty$. This then establishes the associative law for elliptic curves and hence completes the proof that $E(K)$ is an abelian group.

## 2.6 Point Multiplication

Another rather basic idea that is worth mentioning at this point is the idea of elliptic curve point multiplication. It's important to note that here we are not referring to multiplying two points in the conventional sense, but rather scaling points by integer values.

**Definition 2.18** For a given integer $n$ and point $P$ from the elliptic curve $E(K)$, *elliptic curve point multiplication* will be defined as

$$nP = P +_E P +_E P +_E ... +_E P \ n \text{ times}$$

This notion will be highly useful when we look at cryptographic applications.

**Example 2.19** Consider some elliptic curve $E(\mathbb{R})$ defined by the equation $y^2 = x^3 + x + 2$. For a given point $P = (1, 2)$ on $E(\mathbb{R})$ we may find $5P$ as follows:
$(1, 2) +_E (1, 2)$ using definition 2.7 part (iii) will yield $(-1, 0)$. $(-1, 0) +_E (1, 2)$

yields $(1, -2)$. We can continue to use definition 2.7 to find that $(1, -2) +_E (1, 2) = \infty$, and $\infty +_E (1, 2)$ is $(1, 2)$. So it turns out that in this case, $5(1, 2)$ is in fact just $(1, 2)$. Note that this process required five point additions, and should we use a similar process to ascertain, say, $10P$ or $50P$, you can see that the number of point additions can quickly become quite laborious. In this case, we have the convenient fact that $4P$ happens to be $\infty$, meaning (1,2) has order 4 in $E(K)$. This fact, while highly convenient, is not always the case for any given point on an elliptic curve. □

We may use the following algorithm to more speedily compute a point multiplication.

Let $n$ be a positive integer and $P$ be a point on an elliptic curve. We may compute $nP$ as follows:
i) Define $A = n$, $B = \infty$, and $C = P$. For this algorithm, $A$ is an integer value, while $B$ and $C$ are points on our elliptic curve.
ii) If $A$ is even, redefine $A = A/2$, $B = B$, and $C = 2C$.
iii) If $A$ is odd, redefine $A = A - 1$, $B = B +_E C$, and $C = C$.
iv) If $A \neq 0$, go back to step ii).
v) If $A = 0$, then $B = nP$

The primary notion at work here is the fact that point addition is an abelian group operation, and as such we can break down $n$ via binary expansion. We may rewrite $n$ as:

$$n = 2^{k_1} + 2^{k_2} + ... + 2^{k_r} \text{ with } k_1 < k_2 < ... < k_r$$
$$\Rightarrow n = 2^{k_1} + 2^{k_2 - k_1} 2^{k_1} + 2^{k_3 - k_2} 2^{k_3} + ... + 2^{k_r - k_{r-1}} 2^{k_r}$$

Doubling $P$ $k_1$ times will then yield $2^{k_1}P$.

We can then double $2^{k_1}P$, $k_2 - k_1$ times to get $2^{k_2}P$, etc.

While doubling, we effectively add up each required piece to eventually end up with the desired result.

**Example 2.20** Using the previous example we want $5P$. We define $A = 5$, $B = \infty$ and $C = (1, 2)$.

1) $A$ is odd, so we redefine as follows: $A = 4$, $B = \infty +_E P = P$, $C = P$.

2) $A$ is now even so redefine as follows: $A = 2$, $B = P$, $C = P +_E P = 2P$.

3) $A$ is still even so redefine as follows: $A = 1$, $B = P$, $C = 2P +_E 2P = 4P$.

4) $A$ is odd, so redefine as follows: $A = 0$, $B = P +_E 4P$, $C = 4P$.

5) $A = 0$ so $B$ is our desired result. □

Now, while the algorithm does not expedite the process much in this case, let us consider a more difficult case.

**Example 2.21** Let $P$ be some point on an elliptic curve, such that for all $m \leq 30$, $mP \neq \infty$ Conventionally computing $30P$ would require 30 point additions. Instead we use the algorithm:

Since $30 = 2+4+8+16$, then $30P = 2P+4P+8P+16P$. With the notation of the algorithm:

1) $A = 30$, $B = \infty$, $C = P$

2) $A = 15$, $B = \infty$, $C = 2P$

3) $A = 14$, $B = 2P$, $C = 2P$

4) $A = 7$, $B = 2P$, $C = 4P$

5) $A = 6$, $B = 6P$, $C = 4P$

6) $A = 3$, $B = 6P$, $C = 8P$

7) $A = 2$, $B = 14P$, $C = 8P$

8) $A = 1$, $B = 14P$, $C = 16P$

9) $A = 0$, $B = 30P$, $C = 16P$

By way of the algorithm, we required only 4 doublings, and 4 point additions, one of which was a point plus $\infty$. □

Algorithms like this are especially important since in cryptographic applications, $n$ will very often take on extremely large values. The key to the algorithm is the notion of point doubling, so at this point it is worth relooking at the idea of doubling points as described earlier. Recall, for $P = (x, y)$ with $y \neq 0$,

$$m = \frac{3x^2 + A}{2y}$$

$$x_3 = m^2 - 2x$$

$$y_3 = m(3x - m^2) - y$$

It is worth noting that if we let $y^2 = F(x) = x^3 + Ax + B$, we get that $m = \frac{F'(x)}{2y}$. This implies

$$m^2 = \frac{F'(x)^2}{4y^2} = \frac{F'(x)^2}{4F(x)}$$

so

$$x_3 = \frac{F'(x)^2}{4F(x)} - 2x$$

We can thus think of doubling points in terms of this notion of derivatives.

## 2.7 Elliptic Curves Over Characteristic 2

While for the most part we can show most of the theory of elliptic curves in non-characteristic 2 or 3 fields, there are specific cases where we will need to work with these sorts of fields. It will thus be handy to have a few facts concerning elliptic curves over these fields. The Weierstrass equation will be

insufficient in these cases, so we will need to re-look at the generalized Weierstrass equation.

Consider the case of an elliptic curve over a characteristic 2 field. Recall the generalized Weierstrass equation from earlier, and assume first for simplicity that $a = 0$. The generalized Weierstrass equation then becomes:

$$y^2 + by = x^3 + cx^2 + dx + e$$

Using the same substitution for $x$ as before: $x = x + \frac{c}{3} = x + c$ (since we are in a characteristic 2 field).
This results in $y^2 + Ay = x^3 + Bx + C$. Again, since we are in a characteristic 2 field rearrange to get

$$y^2 + Ay + x^3 + Bx + C = 0 \tag{2.1}$$

For future reference, let

$$f(x, y) = y^2 + Ay + x^3 + Bx + C \tag{2.2}$$

for some coefficients $A$, $B$, and $C$.

Of course, this substitution won't work if $a \neq 0$. Instead, we will create a simpler version of the generalized Weierstrass equation by picking a substitution that will yield the following:
i) $y^2$ coefficient equals the coefficients on the $xy$ and $x^3$ terms, and that these coefficients are non-zero so we may divide through by them.
ii) $x$ coefficients on either side of the equation are equal, so that when we set one side of the equation equal to zero, we will have the $x$-terms cancel out.
iii) $y$ coefficient is zero.

Consider the generalized Weierstrass equation for an elliptic curve, with the following linear substitution:

$$y \to a'y + b' \qquad x \to c'x + d' \qquad a' \neq 0,\ c' \neq 0$$

We get

$$(a'y + b')^2 + a(c'x + d)(a'y + b') + b(a'y + b') = (c'x + d')^3 + c(c'x + d')^2 + d(c'x + d') + e$$

After some computation we get the following coefficients:

$$a'^2 \text{ is the coefficient for } y^2$$

$$c'^3 \text{ is the coefficient for } x^3$$

$$aa'c' \text{ is the coefficient for } xy$$

Now, letting $a'^2 = c'^3 = aa'c'$ yields the following:

$$a' = ac' \qquad c'^2 = aa' = a^2c'$$

$$\Rightarrow c' = a^2$$

$$\Rightarrow a' = a^3$$

The $y$ coefficient will be $(2a'b' + aa'd + ba') = aa'd + ba'$ since we are in a characteristic 2 field. Allowing for this coefficient to equal zero yields:

$$aa'd + ba' = 0 \Rightarrow d' = -a^{-1}b$$

For our $x$ coefficients, we get:

$ac'b'$ on the left and $3c'd'^2 + 2cc'd' + dc' = c'd'^2 + dc'$ on the right.

Setting these equal yields:

$$ac'b' = c'd'^2 + dc' \Rightarrow ab' = d'^2 + d \Rightarrow ab' = a^{-2}b^2 + d$$

$$\Rightarrow b' = a^{-3}(b^2 + a^2d)$$

In summary when $a \neq 0$ we have:

$$a' = a^3 \qquad b' = a^{-3}(b^2 + a^2 d)$$
$$c' = a^2 \qquad d' = a^{-1} b$$
$$x = c'x + d' \qquad y = a'y + b'$$

which will allow us the following modification of the generalized Weierstrass equation:

$$y^2 + xy + x^3 + Ax^2 + B = 0 \tag{2.3}$$

for some coefficients A and B.

For both (2.2) and (2.3) we must place some restrictions on the coefficients, such that the curve described is non-singular. Recall, a given point is a singular point when the partial derivatives at that point are zero [2]. We are using the formal derivative for polynomials here, since the concept of limits does not really apply to our characteristic 2 field.

Assume that $(x_1, y_1)$ is a singular point. Then for (2.2) we get:

$$f_y(x_1, y_1) = 2y_1 + A \qquad \text{and} \qquad f_x(x_1, y_1) = x_1^2 + B$$

Since we are in a characteristic 2 field though, everything with a multiple of 2 for a coefficient is really just zero, therefore:

$$f_y(x_1, y_1) = A \qquad \text{and} \qquad f_x(x_1, y_1) = x_1^2 + B$$

Thus, we can ensure that (2.2) is non-singular if we restrict $A \neq 0$.

For (2.3) we get:

$$f_y(x_1, y_1) = 2y_1 + x_1 \qquad \text{and} \qquad f_x(x_1, y_1) = y_1 + 3x_1^2 + 2Ax_1$$

Since we are in a characteristic 2 field though, everything with a multiple of 2 for a coefficient is really just zero, so we get:

$$f_y(x_1, y_1) = x_1 \qquad \text{and} \qquad f_x(x_1, y_1) = y_1 + 3x_1^2$$

Thus, for $(x_1, y_1)$ to be a singular point, $x_1$ must equal 0, and so too must $y_1$. The point $(0, 0)$ is valid for (2.3) when $B = 0$, and so to ensure (2.3) is non-singular, we will restrict $B \neq 0$.

**Proposition 2.22** *In summary: for a characteristic 2 field we have two modifications of the generalized Weierstrass equation:*

$$y^2 + Ay + x^3 + Bx + C = 0 \quad \text{with } A \neq 0 \tag{2.4}$$

$$y^2 + xy + x^3 + Ax^2 + B = 0 \quad \text{with } B \neq 0 \tag{2.5}$$

Now that we have some equations, we will need to establish how points add, specifically case (iii) from definition 2.7.

Certainly, we will still say that $P +_E \infty = P$. In general we will add in the same manner as previous (from a geometric sense at least), allowing for certain changes due to the different nature of the equations. Specifically, we need to establish what negating a point means in our two cases.

Case 1: Let $P = (x_0, y_0)$ be a point that satisfies (2.4). For $-P$, we want a point with the same $x$-coordinate of $P$, but a (possibly) different $y$-coordinate. Now if we evaluate equation (2.4) at $x = x_0$, we have a monic quadratic equation in the one variable $y$. Recall at this point that for monic-quadratic equations, the sum of the roots is the negation of the linear coefficient. Armed with this, and knowing already that $y_0$ is one of our roots, the other root must then be $-y_0 - A$. Since we are in characteristic 2, this is in fact just $y_0 + A$. Thus, for $P = (x_0, y_0)$, $-P = (x_0, y_0 + A)$.

Case 2: Let $P = (x_0, y_0)$ be a point that satisfies (2.5). If we mimic the technique as before we find that $-P = (x_0, y_0 + x_0)$.

We will now look more in depth at the notion of doubling a point (specifically case (iii) of definition 2.7). We will have two cases to look at:

Case 1: Consider the elliptic curve $E(K)$, where $K$ is characteristic 2, described by $y^2 + Ay + x^3 + Bx + C = 0$ and a point $P = (x_0, y_0)$ on $E$. Like before we would like to understand what it means to have a slope at a point $P$, and to do this we will use the formal derivative (keeping in mind that 2=0):

$$2yy' + Ay' + 3x^2 + B = 0 \Rightarrow Ay' + x^2 + B = 0 \Rightarrow y' = \frac{x^2 + B}{A}$$

Recall that $A \neq 0$ for this case, so our slope is defined.
We thus get that at $P$ our tangent line is:

$$y = \frac{x_0^2 + B}{A}(x - x_0) + y_0$$

Substitute into (2.8):

$$\left(\frac{x_0^2 + B}{A}(x - x_0) + y_0\right)^2 + A\left(\frac{x_0^2 + B}{A}(x - x_0) + y_0\right) + x^3 + Bx + C = 0$$

Simplifying yields:

$$0 = x^3 + \left(\frac{x_0^2 + B}{A}\right)^2 x^2 + ...$$

So, the $x$-coordinate of our point of intersection is $-\left(\frac{x_0^2+B}{A}\right)^2 - 2x_0$ but since we are in a characteristic 2 field, we may simplify this to $\left(\frac{x_0^2+B}{A}\right)^2$. The corresponding $y$-coordinate is $\left(\frac{x_0^2+B}{A}\right)\left(\frac{x_0^4+B^2}{A^2} - x_0\right)$. Now, we must flip this, so we may use the above and get that:

$$P +_E P = \left(\frac{x_0^4 + B^2}{A^2}, \left[\frac{x_0^2 + B}{A}\right]\left[\frac{x_0^4 + B^2}{A^2} - x_0\right] + A\right)$$

Case 2: The setup here will be the same as in the previous case, except that this time we will use the equation $y^2 + xy + x^3 + Ax^2 + B = 0$. We can mimic the techniques used in the previous case and get the following:

$$m = \frac{y_0 + x_0^2}{x_0} \text{ which yields } 0 = x^3 + (m^2 + m + A)x^2 + ....$$

Note:

$$m^2 + m + A = \frac{y_0^2 + x_0^4}{x_0^2} + \frac{y_0 + x_0^2}{x_0} + A$$

using (2.5) and the fact that we are in a characteristic 2 field yields:

$$= \frac{x_0 y_0 + x_0^3 + Ax_0^2 + B + x_0^4 + y_0 x_0 + x_0^3 + Ax_0^2}{x_0^2} = \frac{x_0^4 + B}{x_0^2}$$

Thus, using the above as well as the previous work negating a point in our second case, we get:

$$P +_E P = \left( \frac{x_0^4 + B}{x_0^2}, \left[ \frac{y_0 + x_0^2}{x_0} \right] \left[ \frac{x_0^4 + B}{x_0^2} - x_0 \right] + \frac{x_0^4 + B}{x_0^2} \right)$$

In summary:

**Proposition 2.23** For an elliptic curve $E$ defined over a characteristic 2 field $K$, we get the following for $2P$ given that $P = (x, y)$.

1) If $E$ is described by the equation $y^2 + Ay + x^3 + Bx + C = 0$, then

$$2P = \left( \frac{x^4 + B^2}{A^2}, \left[ \frac{x^2 + B}{A} \right] \left[ \frac{x^4 + B^2}{A^2} - x \right] + A \right)$$

2) If $E$ is described by the equation $y^2 + xy + x^3 + Ax^2 + B = 0$, then

$$2P = \left( \frac{x^4 + B}{x^2}, \left[ \frac{y + x^2}{x} \right] \left[ \frac{x^4 + B}{x^2} - x \right] + \frac{x^4 + B}{x^2} \right)$$

## 2.8 Endomorphisms

For later work we will need to establish some results concerning endomorphisms of $E$.

**Definition 2.24** A homomorphism $\alpha : E(\bar{K}) \to E(\bar{K})$ for $E(\bar{K})$ an elliptic curve over the closure of a field $K$, is called an *endomorphism of* $E$ if there are rational functions (quotients of polynomials) $R_1(x, y)$ and $R_2(x, y)$ with coefficients in $\bar{K}$ such that

$$\alpha(x, y) = (R_1(x, y), R_2(x, y))$$

for all $(x, y) \in E(\bar{K})$. We will notate the trivial endomorphism that maps every point to $\infty$ as 0.

**Example 2.25** For an elliptic curve $E$ given by the Weierstrass equation, let $\alpha(P) = 2P$.

$\alpha$ is certainly a homomorphism, since $\alpha(P +_E Q) = 2(P +_E Q) = P +_E Q +_E P +_E Q = 2P +_E 2Q$ since $E$ is abelian. Therefore, $\alpha(P +_E Q) = \alpha(P) +_E \alpha(Q)$. From our rules of point addition, we have (for characteristic not equal to 2 or 3)

$$\begin{aligned} \text{Given } \alpha(x, y) &= (R_1(x, y), R_2(x, y)) \\ R_1 &= \left(\frac{3x^2 + A}{2y}\right)^2 - 2x \\ R_2 &= \frac{3x^2 + A}{2y}\left(3x - \left(\frac{3x^2 + A}{2y}\right)^2\right) - y \end{aligned}$$

Thus $\alpha$ is a homomorphism given by rational functions, so $\alpha$ is an endomorphism of $E$. □

We will need to account for the cases where $R_1$ or $R_2$ might not be defined. To do this, we will first consider a general rational function $R(x, y)$. Given that $y^2 = x^3 + Ax + B$, we may replace all even powers of $y$ with a polynomial exclusively in $x$, and all odd powers of $y$ by $y$ times a polynomial in $x$. We

may thus express $R(x, y)$ as

$$R(x, y) = \frac{p_1(x) + yp_2(x)}{p_3(x) + yp_4(x)}$$

Multiplying by the conjugate of the denominator and substituting for $y^2$ yields

$$R(x, y) = \frac{q_1(x) + yq_2(x)}{q_3(x)}, \text{ for some } q_1, q_2, q_3$$

Recall now that $\alpha(x, y) = (R_1(x, y), R_2(x, y))$, and $(x, y) \in E(\bar{K})$.

$$\alpha(x, -y) = \alpha(-(x, y)) = -\alpha(x, y) \text{ since } \alpha \text{ is a homomorphism}$$

Hence: $(R_1(x, -y), R_2(x, -y)) = -(R_1(x, y), R_2(x, y)) = (R_1(x, y), -R_2(x, y))$

So, $R_1(x, -y) = R_1(x, y)$ and $R_2(x, -y) = -R_2(x, y)$.

From the general equation for $R(x, y)$ above, we thus have that for $R_1$, $q_2(x) = 0$ since the sign of $y$ cannot affect the value of $R_1$, and likewise for $R_2$, $q_1 = 0$, since the change in sign of $y$ must change the sign of $R_2$. So

$$\alpha(x, y) = (r_1(x), r_2(x)y)$$

where $r_1$ and $r_2$ are rational functions.

**Example 2.26** Continuing example 2.25, we may rewrite $R_1$ as follows:

$$R_1 = \frac{9x^4 + 6Ax^2 + A^2}{4(x^3 + Ax + B)} - 2x$$

For $R_2$:

$$\begin{aligned}
R_2 &= \frac{9x^3 + 3Ax}{2y} - \frac{(3x^2 + A)^3}{8y^3} - y \\
&= \frac{36x^3y^2 + 12Axy^2}{8y^3} - \frac{(3x^2 + A)^3}{8y^3} - \frac{8y^4}{8y^3} \\
&= \frac{36x^3(x^3 + Ax + B) + 12Ax(x^3 + Ax + B) - (3x^2 + A)^3 - 8(x^3 + Ax + B)^2}{8(x^3 + Ax + B)y} \\
&= \frac{36x^3(x^3 + Ax + B) + 12Ax(x^3 + Ax + B) - (3x^2 + A)^3 - 8(x^3 + Ax + B)^2}{8(x^3 + Ax + B)^2} y
\end{aligned}$$

We thus have that $\alpha(x,y) = (r_1(x), r_2(x)y)$ where

$$r_1 = \frac{x^4 - 2Ax^2 + A^2 - 8Bx}{4(x^3 + Ax + B)}$$

and

$$\begin{aligned} r_2 &= \frac{36x^3(x^3 + Ax + B) + 12Ax(x^3 + Ax + B) - (3x^2 + A)^3 - 8(x^3 + Ax + B)^2}{8(x^3 + Ax + B)^2} \\ &= \frac{x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - (A^3 + 8B^2)}{8(x^3 + Ax + B)^2} \end{aligned}$$

Of future interest will also be the derivative of $r_1$. With some straightforward calculation, we see that

$$\begin{aligned} r_1' &= \frac{4(4x^3 - 4Ax - 8B)(x^3 + Ax + B) - 4(3x^2 + A)(x^4 - 2Ax^2 - 8Bx + A^2)}{16(x^3 + Ax + B)^2} \\ &= \frac{x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - (A^3 + 8B^2)}{4(x^3 + Ax + B)^2} \\ &= 2r_2 \end{aligned}$$

Hence, $2(x,y) = \left(r(x), \frac{r'(x)}{2}y\right)$ where $r = r_1$. □

We may now consider the case where one of these rational functions is undefined. Let

$$r_1(x) = \frac{p(x)}{q(x)}$$

where $p(x)$ and $q(x)$ are polynomials with no common roots. For the case of $q(x) = 0$ for some $(x,y)$, we say that $\alpha(x,y) = \infty$.

**Theorem 2.27** *Let*

$$\alpha(x,y) = \left(\frac{p(x)}{q(x)}, \frac{y \cdot s(x)}{t(x)}\right)$$

*be an endomorphism of the elliptic curve $E$ given by $y^2 = x^3 + Ax + B$, with $p, q, s,$ and $t$ polynomials such that $p$ and $q$ do not share roots, and $s$ and $t$ do*

*not share any roots. If $q(x_0) \neq 0$ for some $x_0$, then $r_2(x_0)$ is defined, which is to say, $t(x_0) \neq 0$.*

**Proof:** We first use the fact that $\alpha(x, y)$ is a point on $E$ therefore,

$$\left(\frac{y \cdot s(x)}{t(x)}\right)^2 = \left(\frac{p(x)}{q(x)}\right)^3 + A\frac{p(x)}{q(x)} + B$$

$$\Rightarrow \frac{(x^3 + Ax + B)s^2(x)}{t^2(x)} = \frac{p^3(x) + Ap(x)q^2(x) + Bq^3(x)}{q^3(x)} = \frac{u(x)}{q^3(x)} \qquad (2.6)$$

where $u(x) = p^3(x) + Ap(x)q^2(x) + Bq^3(x)$. We now show that $q(x)$ and $u(x)$ share no roots.

Assume that they share a root, $x_0$. Then

$$0 = q(x_0) = u(x_0) = p^3(x_0) + Ap(x_0)q^2(x_0) + Bq^3(x_0)$$
$$\Rightarrow p^3(x_0) = 0 \Rightarrow p(x_0) = 0$$

Which contradicts the initial assertion that $p$ and $q$ do not share roots.

We will finish the proof by way of the contrapositive. Assume that $x_0$ is a root of $t(x)$. From (2.6) we know that

$$(x^3 + Ax + B)s^2(x)q^3(x) = u(x)t^2(x)$$
$$\Rightarrow (x_0^3 + Ax_0 + B)s^2(x_0)q^3(x_0) = u(x_0)t^2(x_0)$$

Since $t$ and $s$ share no roots, $s(x_0) \neq 0$. Further, since $t(x_0) = 0$, we have that

$$(x_0^3 + Ax_0 + B)q^3(x_0) = 0$$

If $q^3(x_0) = 0$, then $q(x_0) = 0$ and we are done via the contrapositive.
Instead assume that $(x_0^3 + Ax_0 + B) = 0$. Since $x_0$ is a root of $x^3 + Ax + B$ and $t(x)$ we may rewrite as follows:

$$(x^3 + Ax + B) = (x - x_0)Q(x) \text{ and } t(x) = (x - x_0)T(x)$$

where $Q(x)$ and $T(x)$ are polynomials. Via substitution,

$$(x - x_0)Q(x)s^2(x)q^3(x) = u(x)[(x - x_0)T(x)]^2$$
$$\Rightarrow Q(x)s^2(x)q^3(x) = u(x)(x - x_0)T^2(x)$$

Evaluating both sides at $x = x_0$ yields

$$Q(x_0)s^2(x_0)q^3(x_0) = 0$$

Recall that since $x^3 + Ax + B$ has no multiple roots, $Q(x_0) \neq 0$. As stated before, $s(x_0) \neq 0$, so again we have the conclusion that $q(x_0) = 0$. Therefore by contraposition, if $q(x_0) \neq 0$ for some $x_0$, then $t(x_0) \neq 0$ and thus $r_2$ is defined when $r_1$ is defined. ∎

**Definition 2.28** Let $\alpha$ be an endomorphism. The *degree* of $\alpha$ is defined as

$$\deg(\alpha) = \text{Max}\{\deg p(x), \deg q(x)\}$$

when $\alpha \neq 0$. When $\alpha = 0$, $\deg(0) = 0$.

**Definition 2.29** We say that an endomorphism $\alpha \neq 0$ is *separable* if the derivative $r_1'(x)$ is not identically zero, which is to say $r_1'(x) \neq 0$ for all $x$.

While the derivative $r_1'(x)$ may not be apparent, we use the following:

**Theorem 2.30** *For $r_1(x) = \frac{p(x)}{q(x)}$ where $p$ and $q$ do not share any roots*

*$r_1'(x)$ is identically zero $\iff$ $p'(x)$ is identically zero and $q'(x)$is identically zero.*

**Proof:** Assume $p'(x) = q'(x) = 0$, for all $x$. Then via the quotient rule,

$$r_1'(x) = \frac{p'(x)q(x) - q'(x)p(x)}{q^2(x)} \Rightarrow r_1'(x) = 0$$

Now, assume $r_1' = 0$. Then, we have that

$$\begin{aligned} r_1'(x) &= \frac{p'(x)q(x) - q'(x)p(x)}{q^2(x)} = 0 \\ &\Rightarrow p'(x)q(x) - q'(x)p(x) = 0 \end{aligned}$$

$$\Rightarrow p'(x)q(x) = q'(x)p(x) \tag{2.7}$$

Suppose $q'$ isn't identically zero, in particular, $q$ is a polynomial of degree at least 1. Let $x_0$ be a root of $q(x)$. This means $p(x_0) \neq 0$. We have two cases to look at.

Case 1: $q'(x_0) \neq 0$.

Then evaluating 2.7 for $x_0$ yields:

$$0 = q'(x_0)p(x_0) \Rightarrow p(x_0) = 0 \Rightarrow x_0 \text{ is a root of } p(x)$$

which is a contradiction.

Case 2: $q'(x_0) = 0$

Now, since $x_0$ is a root of both $q'(x)$ and $q(x)$, we may rewrite these polynomials as

$$q(x) = (x - x_0)^m Q(x) \quad \text{and} \quad q'(x) = (x - x_0)^n \hat{Q}(x)$$

where $Q(x)$ and $\hat{Q}(x)$ are polynomials for which $x_0$ is not a root, and $m > n$. From (2.7) we have

$$\begin{aligned} p'(x)(x - x_0)^m Q(x) &= (x - x_0)^n \hat{Q}(x)p(x) \\ &\Rightarrow p'(x)(x - x_0)^l Q(x) = \hat{Q}(x)p(x) \end{aligned}$$

where $l > 0$. Again, evaluating at $x = x_0$ yields

$$0 = \hat{Q}(x_0)p(x_0) \Rightarrow p(x_0) = 0$$

which again is a contradiction, since $x_0$ cannot also be a root of $p$.
We thus have that $q'(x) = 0$, and by a symmetrical argument, $p'(x) = 0$.
Therefore, $r_1'(x)$ is identically zero if and only if $p'(x)$ and $q'(x)$ are both identically zero. ∎

For some results in the next chapter we will need the following theorem.

**Theorem 2.31** *Let $\alpha \neq 0$ be a separable endomorphism of an elliptic curve $E$. Then*

$$\deg \alpha = N$$

*where $N$ is the size of the kernel of $\alpha : E(\bar{K}) \to E(\bar{K})$.*
*If $\alpha$ is not separable, then*

$$\deg \alpha > N$$

**Proof:** Let $\alpha(x, y) = (r_1(x), yr_2(x))$ with $r_1(x) = p(x)/q(x)$, with $p$ and $q$ polynomials. Assume first that $\alpha$ is a separable endomorphism. By definition, $r'(x) \neq 0$. By the quotient rule,

$$r' = \frac{p'q - q'p}{q^2} \neq 0$$

So $p'q - q'p$ is not the zero polynomial. Let $S$ be the set of $x \in E(\bar{K})$ such that $(pq' - p'q)(x)q(x) = 0$. It is worth noting that $S$ is finite, since neither $pq' - p'q$ nor $q$ are the zero polynomial. Let $(a, b) \in E(\bar{K})$. Note the following:
1.) $\bar{K}$ is algebraically closed, so not finite, and thus we have infinitely many $(a, b)$ to choose from. We may thus require that $a \neq 0, b \neq 0, (a, b) \neq \infty$, and be assured such a point exists.
2.) Let $p$ have degree $d$ and $q$ have degree $d'$. Then the degree of $p - aq$ will coincide with the maximum of $d$ and $d'$. This may not work if $d = d'$, but if

this is the case, we can specifically choose our $a$ to ensure their leading terms do not cancel out. Recalling the definition for the degree of $\alpha$ gives us that $\deg(p(x) - aq(x)) = \text{Max}\{\deg(p), \deg(q)\} = \deg(\alpha)$.

3.) Since $S$ is finite, and we have an infinite number of $a$'s to choose from, we may pick an $a$ such that $a$ is not in $r_1(S)$.

4.) $r_1(x)$ will take on infinitely many values as $x$ runs over $\bar{K}$ (remember $\bar{K}$ itself is not finite), so for each $x \in \bar{K}$ there will be a corresponding point $(x, y) \in E(\bar{K})$. $\alpha(E(\bar{K}))$ is thus an infinite set. It follows that we may find an $(a, b)$ in $\alpha(E(\bar{K}))$.

In summary, we have a point $(a, b)$ such that the following hold:

$$1.)a \neq 0, b \neq 0, (a, b) \neq \infty$$

$$2.)\deg(p(x) - aq(x)) = \text{Max}\{\deg(p), \deg(q)\} = \deg(\alpha)$$

$$3.)a \notin r_1(S)$$

$$4.)(a, b) \in \alpha(E(\bar{K}))$$

Since we are looking at an algebraically closed field, this gives us that $p(x) - aq(x) = 0$ has $\deg(\alpha)$ roots, counting multiplicities. If we can show $p - aq$ has no multiple roots then we are done.

We will show that there are exactly $deg(\alpha)$ points $(x_1, y_1) \in E(\bar{K})$ such that $\alpha(x_1, y_1) = (a, b)$. By our definitions above, we have that

$$\frac{p(x_1)}{q(x_1)} = a, \qquad y_1 r_2(x_1) = b$$

Since we definied $(a, b) \neq \infty$, we have that $q(x_1) \neq 0$. Further, since $b \neq 0$, then $r_2(x) \neq 0$, so we can write $y_1 = \frac{b}{r_2(x_1)}$, implying that $y_1$ is really just determined by $x_1$. As such, it will suffice to count the number of $x_1$'s for which $\alpha(x_1, y_1) = (a, b)$ holds. From assumption 2, we know that the degree of $p(x) - aq(x)$ is equal to $\deg(\alpha)$.

Assume that $x$ is a multiple root of $p - aq$. Then

$$p(x) - aq(x) = 0 \qquad p'(x) - aq'(x) = 0$$

Multiplying $p = aq$ and $aq' = p'$ gives us:

$$ap(x)q'(x) = ap'(x)q(x)$$

Recall, we required $a \neq 0$, so $x$ is a root of $pq' - qp'$, and thus $x \in S$, and so $a = r_1(x) \in r_1(S)$, which contradicts our third restriction above. Thus $p - aq$ has $\deg(\alpha)$ distinct roots, and thus there are $\deg(\alpha)$ many points $(x_1, y_1)$ that satisfy $\frac{p(x_1)}{q(x_1)} = a$. This gives us that the size of the kernel is equal to the degree of $\alpha$

If $\alpha$ is separable, the same logic as above holds, except that $p' - aq'$ is the zero polynomial and so $p - aq$ will have multiple roots, resulting in the size of the kernel being smaller than the degree of $\alpha$. ∎

Finally, before moving on there is one last result that we will need. In chapter 3 we will be looking at an endomorphism for multiplication by an integer $n$, that is to say, for a point $P \in E(\bar{K})$ we will want to identify some $\alpha$ such that $\alpha(P) = nP$. In order to create some sort of condition on the separability of this endomorphism, the following two lemmas will prove useful:

**Lemma 2.32** *Let $E$ be an elliptic curve $y^2 = x^3 + Ax + B$. For a fixed point $(u, v)$ on $E$, as $(x, y)$ varies over $E$ write*

$$(x, y) + (u, v) = (f(x, y), g(x, y))$$

*where $f$ and $g$ are rational functions of $x$ and $y$.*

*Then*

$$\frac{\frac{d}{dx}f(x,y)}{g(x,y)} = \frac{1}{y}$$

**Proof:** From the addition formulas for points on an elliptic curve, we get that:

$$\begin{aligned}
f(x,y) &= \left(\frac{y-v}{x-u}\right)^2 - x - u \\
g(x,y) &= \frac{2u(y-v)}{x-u} - \frac{(y-v)^3}{(x-u)^3} + \frac{x(y-v)}{x-u}) - v \\
&= \frac{2u(y-v)(x-u)^2 - (y-v)^3 + x(y-v)(x-u)^2 - v(x-u)^3}{(x-u)^3} \\
&= \frac{-vu^3 + 2u^3y - 3u^2xy + 3uvx^2 + v^3 - 3v^2y - 2vx^3 + 3vy^2 + x^3y - y^3}{(x-u)^3} \\
\frac{d}{dx}f(x,y) &= 2\left(\frac{y-v}{x-u}\right)\left(\frac{y'(x-u) - (y-v)}{(x-u)^2}\right) - 1 \\
&= \frac{2y'(y-v)(x-u) - 2(y-v)^2 - (x-u)^3}{(x-u)^3}
\end{aligned}$$

Recall that from earlier we know $2yy' = 3x^2 + A$, so by substitution:

$$\begin{aligned}
\frac{d}{dx}f(x,y) &= \frac{\frac{3x^2+A}{y}(y-v)(x-u) - 2(y-v)^2 - (x-u)^3}{(x-u)^3} \\
&= \frac{(3x^2+A)(y-v)(x-u) - 2y(y-v)^2 - y(x-u)^3}{y(x-u)^3} \\
&= \frac{Auv - Auy - Avx + Axy + u^3y - 3u^2xy + 3uvx^2 - 2v^2y - 3vx^3 + 4vy^2 + 2x^3y - 2y^3}{y(x-u)^3}
\end{aligned}$$

This implies that

$$y\frac{d}{dx}f(x,y) - g(x,y) = \frac{y(-u^3 - Au + v^2 + x^3 + Ax - y^2) + v(u^3 + Au - v^2 - x^3 - Ax + y^2)}{(x-u)^3}$$

Recall that both $(u,v)$ and $(x,y)$ are on $E$, so we get the relations:

$v^2 = u^3 + Au + B$ and $y^2 = x^3 + Ax + B$.

Rearranging and substituting yields:

$$y\frac{d}{dx}f(x,y) - g(x,y) = \frac{y(B-B) + v(-B+B)}{(x-u)^3} = 0$$

Thus $y\frac{d}{dx}f(x,y) - g(x,y) = 0$ which we may rearrange to get the desired result.

∎

**Lemma 2.33** *Let $\alpha_1$, $\alpha_2$, and $\alpha_3$ be nonzero endomorphisms of an elliptic curve $E$ with $\alpha_1 + \alpha_2 = \alpha_3$. Write*

$$\alpha_j(x,y) = (R_j(x), yS_j(x))$$

*Suppose there are constants $c_1$ and $c_2$ such that*

$$\frac{R_1'(x)}{S_1(x)} = c_1 \qquad \frac{R_2'(x)}{S_2(x)} = c_2$$

*Then*

$$\frac{R_3'(x)}{S_3(x)} = c_1 + c_2$$

**Proof:** Let $(x_1, y_1)$ and $(x_2, y_2)$ be variable points on $E$. Let $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ where $(x_1, y_1) = \alpha_1(x, y)$ and $(x_2, y_2) = \alpha_2(x, y)$. Then $x_3$ and $y_3$ are rational functions of $x_1, x_2, y_1$, and $y_2$, which in turn are rational functions of $x$ and $y$. By Lemma 2.32 and allowing $(u, v) = (x_2, y_2)$, we have

$$\frac{\partial x_3}{\partial x_1} = \frac{y_3}{y_1}$$

Similarly:

$$\frac{\partial x_3}{\partial x_2} = \frac{y_3}{y_2}$$

By the preamble, $\frac{dx_j}{dx} = c_j \frac{y_j}{y}$ for $j = 1, 2$. Using the chain rule:

$$\begin{aligned}\frac{dx_3}{dx} &= \frac{\partial x_3}{\partial x_1}\frac{dx_1}{dx} + \frac{\partial x_3}{\partial x_2}\frac{dx_2}{dx} \\ &= \frac{y_3}{y_1}\frac{dx_1}{dx} + \frac{y_3}{y_2}\frac{dx_2}{dx} = c_1\frac{y_3}{y_1}\frac{y_1}{y} + c_2\frac{y_3}{y_2}\frac{y_2}{y} = (c_1 + c_2)\frac{y_3}{y}\end{aligned}$$

Dividing by $y_3/y$ yields the desired result. ∎

**Proposition 2.34** *Let $E$ be an elliptic curve defined over a field $K$, and let $n$ be a nonzero integer. Suppose that multiplication by $n$ is given by:*

$$n(x, y) = (R_n(x), yS_n(x))$$

*Where $R_n$ and $S_n$ are rational functions that are indexed in terms of the multiplier $n$. Then*

$$\frac{R_n'(x)}{S_n(x)} = n$$

**Proof:** We will proceed by induction on $n$. First note that for $n = 1$, we have $R_1(x) = x$ and $S_1(x) = 1$ for all $x$. Thus fo $n = 1$, the proposition holds, and this gives us a base case. Assume then that the proposition holds for some $n \in \mathbb{Z}$. Then by lemma 2.33:

$$\frac{R_{n+1}'(x)}{S_{n+1}(x)} = \frac{R_n'(x)}{S_n(x)} + \frac{R_1'(x)}{S_1(x)} = n + 1$$

∎

Looking back to Example 2.26 we see that for the case of $n = 2$, $r_1' = 2r_2 \Rightarrow \frac{r_1'}{r_2} = 2$.

**Corollary 2.35** *Multiplication by $n$ is separable if and only if $n$ is not a multiple of the characteristic $p$ of the field.*

**Proof:** This follows directly from the above proposition. Recall that for $n(x, y) = (R_n(x), yS_n(x))$ to be separable, $R'_n$ must not be identically zero. Let $n \neq kp$ for any $k$. So $0 \neq n = \frac{R'_n}{S_n}$ which implies that $R'_n \neq 0$. Going the other direction: Assume $n(x, y)$ is separable. Then $R'_n \neq 0$ which implies that $n \neq 0$. This is equivalent to $n$ is not a multiple of the characteristic $p$. ∎

# Chapter 3

# Torsion

Before we can look at some applications of elliptic curves as they apply to cryptography, we must first investigate some properties concerning some specific types of points, called Torsion Points.

**Definition 3.1** A given point $P$ on an elliptic curve $E(K)$ is called a *torsion point of order* $n$ if for some integer $n$, $nP = \infty$.

Recall that $\infty$ is our group identity element, and as such, we may generalize this definition to any group. It should be noted we are using the term 'order' in a slightly different manner to which traditional algebra texts use it. Here, $n$ need not be the least integer for which $nP = \infty$ for $P$ to be considered a torsion point of order $n$.

It is often useful to look at the set of all torsion points of a specific order, and to facilitate this we will use the following notation for the elliptic curve $E(K)$, with $\bar{K}$ the algebraic closure of the field $K$.

$$E[n] = \{P \in E(\bar{K}) | nP = \infty\} \tag{3.1}$$

It is worth noting at this point that $E[n]$ forms a subgroup of our group $E(\bar{K})$. This stems from a more general result in modern algebra in which for any abelian group $A$, the set of $n$-torsion elements, which we will call $A[n]$, forms a subgroup of $A$. Certainly $A[n]$ inherits associativity, identity and inverses from the parent group, and so really the only sticking point is closure. Given $a, b \in A[n]$ though, then $a + b$ is certainly in $A[n]$, as $n(a + b) = na + nb$.

## 3.1 The Case of E[2]

**Example 3.2** Consider an elliptic curve $E(K)$, where $K$ is not characteristic 2. We will describe $E[2]$. From section 2.2, we found that the generalized Weierstrass equation may be rewritten as $y^2 =$ some monic cubic. Factoring over the algebraic closure of K, we may then write our equation as $y^2 = (x - x_1)(x - x_2)(x - x_3)$. Now, we are looking for the points that have the property $2P = \infty$. From Definition 2.7, $P +_E P = \infty$ if and only if $y = 0$. This means that aside from the point $\infty$ itself, we have three other 2-torsion points: $(x_1, 0), (x_2, 0)$, and $(x_3, 0)$. Geometrically this will require the tangent line at $P$ to be vertical.

What's more, with relatively little work, we can get that $E[2] = \{\infty, (x_1, 0), (x_2, 0), (x_3, 0)\} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$, when the field for $E(K)$ is not characteristic 2. Recall first that up to isomorphism there are two groups of order 4, both of which are abelian. The first is $\mathbb{Z}_4$, and the second is the $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. Now, $E[2]$ is itself a group, and further, $E[2]$ has no element of order 4. This means that $E[2]$ cannot be isomorphic to $\mathbb{Z}_4$, and thus must be isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. □

We will now look at $E[2]$ for an elliptic curve over a characteristic 2 field. Just like above, we will require $P = -P$, and just like in earlier sections we will have 2 cases to deal with.

Case 1: Let $E$ be an elliptic curve over a characteristic 2 field with the equation $y^2 + Ay + x^3 + Bx + C = 0$. Recall for this case, if $P = (x, y)$ then $-P = (x, y + A)$. Thus, for a point to be torsion of order 2, we require that $y = y + A$. This would require $A = 0$ but as we established earlier $A \neq 0$. So aside from $\infty$ there are no torsion points of order 2 in this case, and $E[2] \simeq I$ where $I$ is the trivial group.

Case 2: Let $E$ be an elliptic curve over a characteristic 2 field with the equation $y^2 + xy + x^3 + Ax^2 + B = 0$. Recall that for this case, if $P = (x, y)$ then $-P = (x, y+x)$. If $P$ is torsion of order 2, $y = y+x$ so $x = 0$. Evaluating our equation at $x = 0$ gives $y^2 + B = 0$, so $y^2 = B$, and $y = \sqrt{B}$. We know that such a square root exists because $y$ is an element of the closure of our field $K$. Furthermore, square roots are unique for characteristic 2 fields, since $a = -a$ in these fields. This means that aside from $\infty$ we have one distinct torsion point of order 2. In this case, $E[2] \simeq \mathbb{Z}_2$.

In summary, for a given elliptic curve, we have the following for $E[2]$:

1) $E[2] \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$, if $K$ is not characteristic 2.

2) $E[2] \simeq \mathbb{Z}_2$ or $E[2] \simeq I$, if $K$ is characteristic 2, where $I$ is the trivial group.

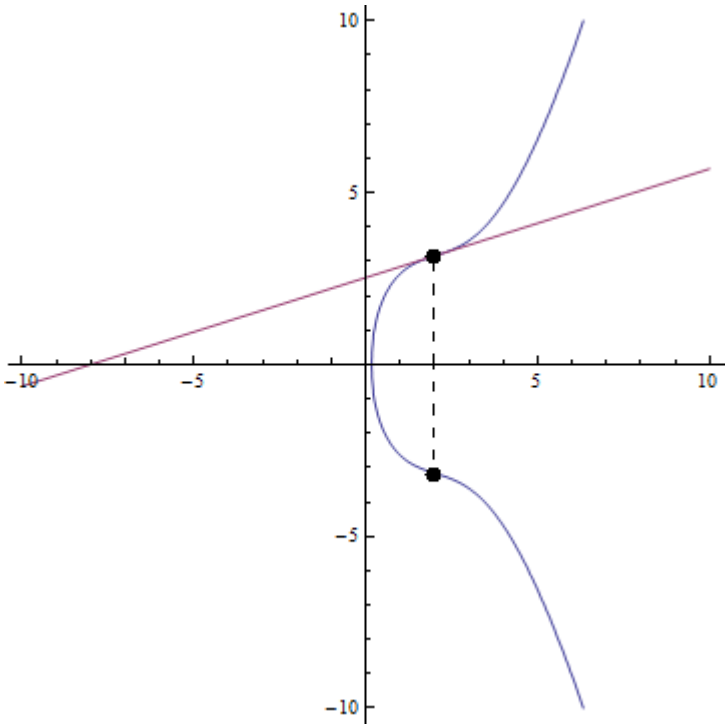
## 3.2 E[3] and Beyond

We start by assuming the characteristic of our field is not 2 or 3. If $P$ is a 3-torsion point, then $3P = \infty$, or more specifically, $2P = -P$.

From our figure, we infer that $P$ must be an inflection point.

Computationally, the picture requires that the $x$-coordinates of $P$ and $2P$ must

Figure 3.1: Graphically: $2P = -P$




It is worth noting that for $P +_E P = -P$, we need the "third point of intersection" for our tangent line to also be $P$ so that when we flip over the $x$-axis we get $-P$.

be the same, and their $y$-coordinates must differ by a sign. From definition 2.7,

$$x = m^2 - 2x, \text{ where } m = \frac{3x^2 + A}{2y}$$

This gives us:

$$x = \left(\frac{3x^2 + A}{2y}\right)^2 - 2x \Rightarrow 3x^4 + 6Ax^2 + 12Bx - A^2 = 0$$

**Proposition 3.3** *There are four distinct $x$-values that satisfy* $3x^4 + 6Ax^2 + 12Bx - A^2 = 0$.

**Proof:** Let $F(x) = x^3 + Ax + B$ as before. Let $g(x) = 3x^4 + 6Ax^2 + 12Bx - A^2$. Now recall from earlier, $m^2 = \frac{F'(x)^2}{4F(x)}$, and since $x = m^2 - 2x$, we get

$$\begin{aligned} x &= \frac{F'(x)^2}{4F(x)} - 2x \\ \Rightarrow 0 &= 12xF(x) - F'(x)^2 \\ \Rightarrow 0 &= 2F''(x)F(x) - F'(x)^2 \\ &\text{since } F'' = 6x \end{aligned}$$

So we can redefine $g(x)$ in terms of $F$:

$$g(x) = 2F''(x)F(x) - F'(x)^2$$

For $r$ a root of $g(x)$, if $r$ is a multiple root, $g(r) = 0$ and $g'(r) = 0$.
Thus, let's assume $r$ is a double root of $g$. We then get the following (note that $F''' = 6$):

$$\begin{aligned} g'(x) &= 2F''' \cdot F + 2F'' \cdot F' - 2F' \cdot F'' \\ g'(x) &= 2F''' \cdot F \\ g'(x) &= 12F(x) \end{aligned}$$

Since $r$ is a double root of $g$,

$$\begin{aligned} 0 =& g'(r) = 12F(r) \Rightarrow F(r) = 0 \\ &\text{and} \\ 0 =& 2F''(r)F(r) - F'(r)^2 \\ \Rightarrow 0 =& F'(r) \end{aligned}$$

Thus $r$ is also at least a double root of $F$. But by definition of an elliptic curve, $F(x)$ in this context cannot have a double root.

Therefore, $r$ cannot be a multiple root of $g(x)$, and thus the roots of $g$ must be distinct. ∎

Each of these roots will have 2 possible corresponding $y$-values which will yield 8 distinct points on our elliptic curve that have the desired property, aside from $\infty$. Therefore $E[3]$ is an abelian group of 9 elements. Now, $E[3]$ is not cyclic, so cannot be isomorphic to $\mathbb{Z}_9$, and thus must be isomorphic to $\mathbb{Z}_3 \oplus \mathbb{Z}_3$.

Now let's say that our field has characteristic 2. From the previous section, we know there are 2 cases to look at:
i) $y^2 + Ay + x^3 + Bx + C = 0$ with $A \neq 0$
ii) $y^2 + xy + x^3 + Ax^2 + B = 0$ with $B \neq 0$
In order to use the previous logic regarding our criterion for 3-torsion points, we will use the formulas for doubling points we found earlier:

For a given point $P = (x, y)$, for $2P = (x_1, y_1)$

$$\text{i) } x_1 = \frac{x^4 + B}{A^2}$$
$$\text{ii) } x_1 = \frac{x^4 + B}{x^2}$$

As before, $2P = -P$, so for $P = (x, y)$ we have the following for case i):

$$x = \frac{x^4 + B}{A^2} \Rightarrow A^2x = x^4 + B \Rightarrow x^4 - A^2x + B = 0$$

Now, letting $h(x) = x^4 - A^2x + B$, we get $h'(x) = 4x^3 - A^2 = A^2$, since we are in characteristic 2. Now, as we've mentioned before for this case, $A \neq 0$, and thus our roots must be distinct. Therefore there exist 4 distinct $x$-value solutions to the equation, which as we saw before implies 8 distinct non-identity

3-torsion elements. This gives us that, $E[3] \simeq \mathbb{Z}_3 \oplus \mathbb{Z}_3$.

For case ii):

$$x^3 = x^4 + B \Rightarrow x^4 - x^3 + B = 0$$

We set $h(x) = x^4 - x^3 + B$ and get that $h'(x) = 4x^3 - 3x^2 = x^2$ (characteristic 2), thus the only root of $h'(x)$ is 0, which is not itself a root of $h(x)$, and therefore we have no multiple roots. Following the previous logic, for this case $E[3]$ also has nine elements.
So, for a field of characteristic 2, $E[3] \simeq \mathbb{Z}_3 \oplus \mathbb{Z}_3$.

Now, let's say that our field is characteristic 3. As we saw in chapter 2, we can simplify the generalized Weierstrass equation to the form $y^2 = x^3 + Ax^2 + Bx + C$ for constants A, B, and C. Like previously, we may discern the following about doubling points:

For a given point $P = (x, y)$ with $2P = (x_1, y_1)$, we have:

$$m = \frac{2Ax + B}{2y}$$
$$x_1 = m^2 - A - 2x$$

As before, we may use this coupled with the fact that we require the $x$-coordinates of $P$ and $2P$ to be the same to obtain the following:

$$\left(\frac{2Ax + B}{2y}\right)^2 - A = 3x = 0$$
$$\Rightarrow \frac{4A^2x^2 + 4ABx + B^2}{4y^2} - A = 0$$

Recall that we are in a characteristic 3 field and $y^2 = x^3 + Ax^2 + Bx + C$, so:

$$\begin{aligned} \frac{A^2x^2 + ABx + B^2}{x^3 + Ax^2 + Bx + C} - \frac{A(x^3 + Ax^2 + Bx + C)}{x^3 + Ax^2 + Bx + C} &= 0 \\ \Rightarrow \frac{A^2x^2 + ABx + B^2 - Ax^3 - A^2x^2 - ABx - AC}{x^3 + Ax^2 + Bx + C} &= 0 \\ \Rightarrow \frac{-Ax^3 + B^2 - AC}{x^3 + Ax^2 + Bx + C} &= 0 \end{aligned}$$

$$\Rightarrow Ax^3 - B^2 + AC = 0 \tag{3.2}$$

If both $A$ and $B$ are zero, then the equation $y^2 = x^3 + Ax^2 + Bx + C$ becomes $y^2 = x^3 + C$, which has multiple roots in our characteristic 3 field. As such, either $A$ or $B$ must be non-zero.

If $A = 0$, then (3.2) gives us that $-B^2 = 0 \Rightarrow B = 0$, but we just said $B$ cannot equal zero if $A$ also equals zero. This implies that there are no values of $x$ for which the criteria is satisfied and $E[3] \simeq I$ in this case, where $I$ is the trivial group.

If $A \neq 0$, then we may rewrite (3.2) as $A(x^3 + D) = 0$ for some constant $D$. This gives us one value for $x$ that satisfies the criteria, and this value of $x$ has two corresponding $y$-values. As such, once we include $\infty$, $E[3]$ becomes a group of order 3, and as such must be isomorphic to $\mathbb{Z}_3$.

In summary, we have the following for $E[3]$:

1) $E[3] \simeq \mathbb{Z}_3 \oplus \mathbb{Z}_3$, if K is not characteristic 3.

2) $E[3] \simeq \mathbb{Z}_3$ or $E[3] \simeq I$, if K is characteristic 3.

**Example 3.4** Consider the elliptic curve $E$ over $\mathbb{C}$ defined by the equation

$y^2 = x^3 + x$. To find the points of $E[2]$, we set $y$ to zero and solve:

$$\begin{aligned} 0 =& x^3 + x \\ 0 =& x(x^2 + 1) \\ 0 =& x(x + i)(x - i) \end{aligned}$$

giving distinct points (aside from the point at $\infty$): $(0, 0), (i, 0), (-i, 0)$, hence $E[2] \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$

For $E[3]$. As previously stated, the $x$-coordinate of $2P$ must be the same as the $x$-coordinate of $P$. For $P = (x, y)$, using our addition rules we get

$$\begin{aligned} 2P &= \left( \left( \frac{3x^2 + 1}{2y} \right)^2 - 2x, \left( \frac{3x^2 + 1}{2y} \right) \left( 3x - \left( \frac{3x^2 + 1}{2y} \right)^2 \right) - y \right) \\ 2P &= \left( \frac{9x^4 + 6x^2 + 1}{4y^2} - \frac{8xy^2}{4y^2}, \left( \frac{3x^2 + 1}{2y} \right) \left( \frac{12xy^2}{4y^2} - \frac{9x^4 + 6x^2 + 1}{4y^2} \right) - y \right) \\ 2P &= \left( \frac{9x^4 + 6x^2 + 1 - 8x(x^3 + x)}{4y^2}, \left( \frac{3x^2 + 1}{2y} \right) \left( \frac{12x(x^3 + x) - 9x^4 - 6x^2 - 1}{4y^2} \right) - y \right) \\ 2P &= \left( \frac{x^4 - 2x^2 + 1}{4y^2}, \left( \frac{3x^2 + 1}{2y} \right) \left( \frac{3x^4 + 6x^2 - 1}{4y^2} \right) - y \right) \\ 2P &= \left( \frac{x^4 - 2x^2 + 1}{4y^2}, \left( \frac{9x^6 + 18x^4 - 3x^2 + 3x^4 + 6x^2 - 1}{8y^3} \right) - \frac{8y^4}{8y^3} \right) \\ 2P &= \left( \frac{x^4 - 2x^2 + 1}{4y^2}, \frac{9x^6 + 21x^4 + 3x^2 - 1}{8y^3} - \frac{8(x^3 + x)^2}{8y^3} \right) \\ 2P &= \left( \frac{x^4 - 2x^2 + 1}{4y^2}, \frac{9x^6 + 21x^4 + 3x^2 - 1}{8y^3} - \frac{8(x^6 + 2x^4 + x^2)}{8y^3} \right) \\ 2P &= \left( \frac{x^4 - 2x^2 + 1}{4y^2}, \frac{x^6 + 5x^4 - 5x^2 - 1}{8y^3} \right) \end{aligned}$$

and so

$$\begin{aligned} x =& \frac{x^4 - 2x^2 + 1}{4y^2} \\ \Rightarrow & 4x(x^3 + x) = x^4 - 2x^2 + 1 \\ \Rightarrow & 4x^4 + 4x^2 - x^4 + 2x^2 - 1 = 0 \\ \Rightarrow & 3x^4 + 6x^2 - 1 = 0 \end{aligned}$$

Using basic algebra, we get four distinct solutions:

$$x = \alpha, \quad -\alpha, \quad (i\sqrt{3}\alpha)^{-1}, \quad -(i\sqrt{3}\alpha)^{-1}$$

where $\alpha = \sqrt{\frac{2\sqrt{3}-3}{3}}$

We can easily determine the 8 distinct points by solving for $y$ with the different values of $x$.

Letting $\beta = \sqrt{\frac{2\alpha}{\sqrt{3}}}$, our 8 points are:

$$(\alpha, \beta), \quad (\alpha, -\beta), \quad (-\alpha, i\beta), \quad (-\alpha, -i\beta)$$

$$\left(\frac{-i}{\sqrt{3}\alpha}, \frac{2\sqrt{i}}{4\sqrt{27}\beta}\right), \quad \left(\frac{-i}{\sqrt{3}\alpha}, -\frac{2\sqrt{i}}{\sqrt[4]{27}\beta}\right), \left(-\frac{-i}{\sqrt{3}\alpha}, \frac{2\sqrt{-i}}{\sqrt[4]{27}\beta}\right), \quad \left(-\frac{-i}{\sqrt{3}\alpha}, -\frac{2\sqrt{-i}}{\sqrt[4]{27}\beta}\right)$$

These 8, along with $\infty$ form $E[3]$.

We can also determine the points in $E[4]$. Now, certainly, any point in $E[2]$ is also in $E[4]$, giving us those four points. For the others we consider that for any point $P$ in $E[4]$, $2P +_E 2P = \infty$, which requires that the $y$-coordinate of

$2P$ is 0. From our point addition definition:

$$\begin{aligned}
0 =& \frac{3x^2+1}{2y}\left(3x - \frac{9x^4+6x^2+1}{4y^2}\right) - y \\
0 =& \frac{3x^2+1}{2y}\left(\frac{12x(x^3+x) - 9x^4 - 6x^2 - 1}{4y^2}\right) - y \\
0 =& \frac{(3x^2+1)(3x^4+6x^2-1)}{8y^3} - \frac{8y^4}{8y^3} \\
0 =& 9x^6 + 18x^4 - 3x^2 + 3x^4 + 6x^2 - 1 - 8(x^3+x)^2 \\
0 =& 9x^6 + 21x^4 + 3x^2 - 1 - 8x^6 - 16x^4 - 8x^2 \\
0 =& x^6 + 5x^4 - 5x^2 - 1
\end{aligned}$$

Factoring:

$$0 = (x-1)(x+1)(x^4+6x^2+1)$$

Clearly, $x = \pm 1$ are solutions. We can easily determine the others:

$$\begin{aligned}
&\text{let:} x^2 = t \\
&\Rightarrow t^2 + 6t + 1 = 0 \\
&\Rightarrow t = \frac{-6 \pm \sqrt{32}}{2} = -3 \pm 2\sqrt{2}
\end{aligned}$$

So:

$$x = \pm i\sqrt{3 \pm 2\sqrt{2}} = \pm i(1 \pm \sqrt{2})$$

Letting $\gamma = i(1 \pm \sqrt{2})$, we have as our 6 x-values:

$$1, -1, \gamma, -\gamma, \gamma^{-1}, -\gamma^{-1}$$

At this point it is worth noting that these 6 x-values will yield 2 distinct points each, and once we include the four points from $E[2]$, we will have 16 distinct points in $E[4]$. We can find these points explicitly by solving for $y$ in the usual way.

□

This all leads up to the more general result:

**Theorem 3.5** *Let $E(K)$ be an elliptic curve defined over a field $K$ and let $n \in \mathbb{Z}^+$. If the characteristic of $K$ does not divide $n$, or the characteristic of $K$ is zero, then*

$$E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$$

*If the characteristic of $K$ equals some $p > 0$ such that $p|n$, write $n = p^r n'$ with $p \nmid n'$. Then*

$$E[n] \simeq \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'} \quad or \quad \mathbb{Z}_n \oplus \mathbb{Z}_{n'}$$

The proof for this theorem will be in the next section.

## 3.3 Division Polynomials and a Proof for Theorem 3.5

In order to go about proving theorem 3.5 we will first need an idea of division polynomial. The goal here will be to create an endomorphism as described earlier to account for multiplication of a point by an integer. Now, from earlier, we know that $\alpha(P) = 2P$ is an endomorphism, where:

$$\alpha(x, y) = \left( \left( \frac{3x^2 + A}{2y} \right)^2 - 2x, ... \right)$$

Note, that the $x$-coordinate has denominator $4y^2$, which suggests the x-coordinate of the more general $P \to nP$ endomorphism might be of the form $\frac{\phi_n}{\psi_n^2}$, for appropriately chosen polynomials $\phi_n$ and $\psi_n$.

**Definition 3.6** The set of *division polynomials*, $\psi_m \in \mathbb{Z}[x, y, A, B]$, is defined as follows:

$$\begin{aligned}
\psi_0 &= 0 \\
\psi_1 &= 1 \\
\psi_2 &= 2y \\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2 \\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) \\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \text{ for } m \geq 2 \\
\psi_{2m} &= (2y)^{-1}(\psi_m)(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \text{ for } m \geq 3
\end{aligned}$$

We will use these division polynomials to explicitely construct the endomorphism for $nP$.

**Lemma 3.7** *When $n$ is odd, $\psi_n$ is a polynomial in $\mathbb{Z}[x, y^2, A, B]$, and when $n$ is even, $\psi_n$ is a polynomial in $2y\mathbb{Z}[x, y^2, A, B]$.*

**Proof:** By definition, this is true for $n \leq 4$. We will thus first look at the even case, proceeding by induction:
Let $n > 4$ and $n = 2m$ for some $m \in \mathbb{Z}$. We will assume by induction that the lemma holds for all $\psi_i$ with $i < n$. Since $n = 2m > 4$, we have that $m > 2$, and thus $2m > m + 2$. Referring back to definition 3.6 we see that all $\psi$'s present in the definition for $\psi_{2m}$ fall under our induction assumption. If $m$ is even, we get that $\psi_m$, $\psi_{m+2}$ and $\psi_{m-2}$ are all in $2y\mathbb{Z}[x, y^2, A, B]$ by the induction hypothesis. Further, $\psi_{m+1}$ and $\psi_{m-2}$ are both polynomials in $\mathbb{Z}[x, y^2, A, B]$, and by observation $\psi_{2m}$ must be a polynomial in $2y\mathbb{Z}[x, y^2, A, B]$. If $m$ is odd, $m - 1$ and $m + 1$ are even, which still results in $\psi_{2m}$ being a polynomial in $2y\mathbb{Z}[x, y^2, A, B]$, since the $\psi_{m-1}$ and $\psi_{m+1}$ are squared.

We now let $n = 2m + 1$, $n > 4$. By the recursive formula for $\phi_{2m+1}$ and the induction hypothesis $\psi_{2m+1}$ must be a polynomial in $\mathbb{Z}[x, y^2, A, B]$, regardless of whether $m$ is even or odd. ∎

We will use the following polynomials in the next lemma:

$$\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1}$$
$$\omega_m = (4y)^{-1}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)$$

**Lemma 3.8** *$\phi_n \in \mathbb{Z}[x, y^2, A, B]$ for all $n$. $\omega_n \in y\mathbb{Z}[x, y^2, A, B]$, when $n$ is odd, and $\omega_n \in \mathbb{Z}[x, y^2, A, B]$ when $n$ is even.*

**Proof:** We will first look at the case of $n$ being odd. When $n$ is odd, we get from Lemma 3.7 that $\psi_{n+1}$ and $\psi_{n-1}$ are both polynomials in $2y\mathbb{Z}[x, y^2, A, B]$. They are thus both polynomials in $y\mathbb{Z}[x, y^2, A, B]$, and so their product will be a polynomial in $\mathbb{Z}[x, y^2, A, B]$. By observation for odd $n$, $x\psi_n^2 \in \mathbb{Z}[x, y^2, A, B]$, and thus for an odd $n$, $\phi_n \in \mathbb{Z}[x, y^2, A, B]$. Now, for $n$ odd, we get that $\psi_{n+2}\psi_{n-1}^2$ is a polynomial in $4y^2\mathbb{Z}[x, y^2, A, B]$ as is $\psi_{n-2}\psi_{n+1}^2$ and thus $\omega_n$ is a polynomial in $y\mathbb{Z}[x, y^2, A, B]$.

For the case of $n$ an even number. When $n$ is even, we get that $\psi_{n+1}$ and $\psi_{n-1}$ are both polynomials in $\mathbb{Z}[x, y^2, A, B]$ and thus their product will be as well. $\psi_n$ is a polynomial in $2y\mathbb{Z}[x, y^2, A, B]$, which upon being squared really just becomes a polynomial in $\mathbb{Z}[x, y^2, A, B]$, thus for even $n$, $\phi_n \in \mathbb{Z}[x, y^2, A, B]$. Now for $\omega_n$ when $n$ is even:

We can pretty easily see that $\omega_n \in \frac{1}{2}\mathbb{Z}[x, y^2, A, B]$, using Lemma 3.7. While this is enough for any application of this lemma that we will use, we still need to resolve the extra multiple of $\frac{1}{2}$ which we will do by first confirming the

following from [1].

$$\psi_n \equiv (x^2+A)^{(n^2-1)/4} \mod 2, \text{ when } n \text{ is odd}$$
$$(2y)^{-1}\psi_n \equiv \left(\frac{n}{2}\right)(x^2+A)^{(n^2-4)/4} \mod 2, \text{ when } n \text{ is even}$$

The mod 2 in this case means that the coefficients of the resulting polynomials are taken mod 2.

We can see that these equivalencies holds by definition for $n \leq 4$, establishing some base cases. As our induction assumption, let us assume that the above equivalencies hold for all $n \leq 2m$ where $2m \geq 4$. This implies that $m \geq 2$. Recall our definitions of $\psi_{2m}$ and $\psi_{2m+1}$:

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \text{ for } m \geq 2$$
$$\psi_{2m} = (2y)^{-1}(\psi_m)(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \text{ for } m \geq 3$$

Since $m \geq 2$, the induction hypothesis is valid for all $\psi$'s in the above. First we will look at $\psi_{2m+1}$ with an odd $m$.

$$\psi_{2m+1} \equiv (x^2+A)^{((m+2)^2+3m^2-4)/4} -$$
$$(m-1)(x^2+A)^{((m-1)^2-4)/4}y^4(m+1)^3(x^2+A)^{3((m+1)^2-4)/4}$$

Since $m$ is odd, $(m+1)$ and $(m-1)$ are even, thus the second term is even, and congruent to 0 mod 2. Thus:

$$\psi_{2m+1} \equiv (x^2+A)^{((m+2)^2+3m^2-4)/4} + 0 \mod 2$$
$$\equiv (x^2+A)^{(4m^2+4m)/4}$$
$$\equiv (x^2+A)^{((2m+1)^2-1)/4}$$

For an even $m$, we get:

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3$$
$$\psi_{2m+1} \equiv y(m+2)(x^2+A)^{((m+2)^2-4)/4} y^3 m^3 (x^2+A)^{3(m^2-4)/4} - (x^2+A)^{((m-1)^2-1)/4+3((m+1)^2-1)/4}$$

Since $m$ is even, so too is $m+2$ and thus the first term is equivalent to 0, mod 2:

$$\begin{aligned}\psi_{2m+1} &\equiv 0 + (x^2+A)^{((m-1)^2-1)/4+3((m+1)^2-1)/4} \\ &\equiv 0 + (x^2+A)^{(4m^2+4m)/4} \\ &\equiv (x^2+A)^{((2m+1)^2-1)/4} \mod 2\end{aligned}$$

As desired. For $\psi_{2m}$ with $m$ odd.

$$\begin{aligned}\psi_{2m} &= (2y)^{-1}(\psi_m)(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \\ &\equiv \frac{1}{2y}(x^2+A)^{\frac{m^2-1}{4}} \Big[(x^2+A)^{((m+2)^2-1)/4} y^2 (m-1)^2 (x^2+A)^{2((m-1)^2-4)/4} \\ &\qquad -(x^2+A)^{((m-2)^2-1)/4} y^2 (m+1)^2 (x^2+A)^{2((m+1)^2-4)/4}\Big] \\ &= \frac{y}{2}(x^2+A)^{\frac{m^2-1}{4}} \Big[(m-1)^2(x^2+A)^{(3m^2-3)/4} - (m+1)^2(x^2+A)^{(3m^2-3)/4}\Big] \\ &= (x^2+A)^{(4m^2-4)/4}\frac{-4m}{2}y \\ &\equiv (2m)y(x^2+A)^{((2m)^2-4)/4} \mod 2\end{aligned}$$

Finally, we will look at $\psi_{2m}$ for an even $m$.

$$\begin{aligned}
\psi_{2m} &= (2y)^{-1}(\psi_m)(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \\
&\equiv \frac{1}{2y}\,(ym)\,(x^2+A)^{\frac{m^2-4}{4}} \Big[y(m+2)(x^2+A)^{(m^2+4m)/4}(x^2+A)^{2((m-1)^2-1)/4} \\
&\qquad - y(m-2)(x^2+A)^{(m^2-4m)/4}(x^2+A)^{2((m+1)^2-1)/4}\Big] \mod 2 \\
&= \frac{my}{2}(x^2+A)^{(m^2-4)/4}\left[(m+2)(x^2+A)^{3m^2} - (m-2)(x^2+A)^{3m^2}\right] \\
&= \frac{my}{2}(x^2+A)^{(4m^2-4)/4}(m+2-m+2) \\
&= (2m)y(x^2+A)^{((2m)^2-4)/4}
\end{aligned}$$

Thus, by induction, we get the desired result.

Armed with this knowledge, we get that for an even $n$,

$$\begin{aligned}
\omega_n &= (4y)^{-1}(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2) \\
&\equiv (4y)^{-1}\left[2y\left(\frac{n+2}{2}\right)(x^2+A)^{((n+2)^2-4)/4}(x^2+A)^{2((n-1)^2-1)/4}\right] \\
&\quad - (4y)^{-1}\left[2y\left(\frac{n-2}{2}\right)(x^2+A)^{((n-2)^2-4)/4}(x^2+A)^{2((n+1)^2-1)/4}\right] \mod 2 \\
&= \frac{1}{4}\left[(n+2)(x^2+A)^{3n^2/4} - (n-2)(x^2+A)^{3n^2/4}\right] \\
&= \frac{n+2-n+2}{4}(x^2+A)^{3n^2/4} \\
&= (x^2+A)^{3n^2/4}
\end{aligned}$$

We may thus say that for even $n$, $\omega_n \in \mathbb{Z}[x, y^2, A, B]$. ∎

For a given elliptic curve defined by $y^2 = x^3 + Ax + B$, we can replace all instances of $y^2$ with $x^3 + Ax + B$, and all polynomials in $\mathbb{Z}[x, y^2, A, B]$ may be written as polynomials in $\mathbb{Z}[x, A, B]$. For this given elliptic curve then (where $A$ and $B$ are now fixed values), we may write $\phi_n(x)$ and $\psi_n^2(x)$.

**Lemma 3.9**

$$\psi_n = y(nx^{(n^2-4)/2} + ... \qquad \text{For n even}$$

$$\psi_n = nx^{(n^2-1)/2} + ... \qquad \text{For n odd}$$

**Proof:** We will have multiple cases to look at here. This proof will require induction so first we need to establish a few base cases.

Let $n = 0$. Then $\psi_0 = 0 = y(0x^{(0^2-4)/2})$.

Let $n = 1$. Then $\psi_1 = 1 = 1x^{(1^2-1)/2}$.

Let $n = 2$. Then $\psi_2 = 2y = y(2x^{(2^2-4)/2})$.

Let $n = 3$. Then $\psi_3 = 3x^4 + ... = 3x^{(3^2-1)/2} + ...$

Let $n = 4$. Then $\psi_4 = 4yx^6 + ... = y(4x^{(4^2-4)/2})$

Let $n = 5$. Then $\psi_5 = 5x^{12} = 5x^{(5^2-1)/2}$.

We can now induct, and there will be multiple cases to look at. In all cases, we will assume that the lemma holds for all values less than or equal to $n$.

Case 1: $n = 2m$ for $m$ an even number.

Consider, $\psi_{n+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3$ by definition 3.6. By the induction hypothesis, we have that the leading term for $\psi_{n+1}$ is:

$$\begin{aligned}
&[y(m+2)x^{((m+2)^2-4)/2}][ymx^{(m^2-4)/2}]^3 - \\
&\qquad\qquad (m-1)x^{((m-1)^2-1)/2}[(m+1)x^{((m+1)^2-1)/2}]^3 \\
&= x^6(m^4+2m^3)x^{(4m^2+4m-12)/2} - (m-1)(m+1)^3x^{(4m^2+4m)/2} \\
&= (m^4+2m^3-m^4-2m^3+2m+1)x^{(4m^2+4m+1-1)/2} \\
&= (2m+1)x^{((2m+1)^2-1)/2}
\end{aligned}$$

Case 2: $n = 2m$ for $m$ an odd number.

As before $\psi_{n+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3$. By the induction hypothesis the

leading term of $\psi_{n+1}$ is:

$$(m+2)x^{(m^2+4m+4-1)/2}m^3x^{(3m^2-3)/2}-$$
$$y(m-1)x^{(m^2-2m+1-4)/2}y^3(m+1)^3x^{3(m^2+2m+1-4)/2}$$
$$=(m^4+2m^3)x^{(4m^2+4m)/2}-y^4(m^4+2m^3-2m-1)x^{(4m^2+4m-12)/2}$$
$$=(m^4+2m^3)x^{(4m^2+4m)/2}-(m^4+2m^3-2m-1)x^{(4m^2+4m)/2}$$
$$=(2m+1)x^{((2m+1)^2-1)/2}$$

Case 3: $n=2m-1$ for $m$ an even number.

From definition 3.6 we get that: $\psi_{n+1}=(2y)^{-1}(\psi_m)(\psi_{m+2}\psi_{m-1}^2-\psi_{m-2}\psi_{m+1}^2)$. By the induction hypothesis the leading coefficient will be:

$$2^{-1}mx^{(m^2-4)/2}\{[y(m+2)x^{(m^2+4m)/2}](m-1)^2x^{(m^2-2m)}-$$
$$[y(m-2)x^{(m^2-4m)/2}](m+1)^2x^{(m^2+2m)}\}$$
$$=2^{-1}myx^{(m^2-4)/2}\{(m^3-3m+2)x^{3m^2/2}-(m^3-3m-2)x^{3m^2/2}\}$$
$$=2myx^{(m^2-4)/2}x^{3m^2/2}$$
$$=y(2m)x^{((2m)^2-4)/2}$$

Case 4: $n=2m-1$ for $m$ an odd number.

As before, $\psi_{n+1}=(2y)^{-1}(\psi_m)(\psi_{m+2}\psi_{m-1}^2-\psi_{m-2}\psi_{m+1}^2)$. By the induction hypothesis the leading coefficient will be:

$$(2y)^{-1}mx^{(m^2-1)/2}\{(m+2)x^{(m^2+4m+3)/2}y^2(m-1)^2x^{(m^2-2m-3)}$$
$$-(m-2)x^{(m^2-4m+3)/2}y^2(m+1)^2x^{(m^2+2m-3)}\}$$
$$=2^{-1}ymx^{(m^2-1)/2}\{(m^3-3m+2)x^{(3m^2-3)/2}-(m^3-3m-2)x^{(3m^2-3)/2}\}$$
$$=2ymx^{(m^2-1)/2}x^{(3m^2-3)/2}$$
$$=y(2m)x^{((2m)^2-4)/2}$$

∎

Lemma 3.9 leads to the following:

**Corollary 3.10**

$$\phi_n(x) = x^{n^2} + ...$$
$$\psi_n^2(x) = n^2 x^{n^2-1} + ...$$

**Proof:** If $n$ is odd, then the corollary clearly holds for $\psi_n^2$. Recall that we defined $\phi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1}$, so for an odd $n$, the leading term of $\phi_n$ will be

$$\begin{aligned} & xn^2(x^{(n^2-1)/2})^2 - y(n+1)x^{((n+1)^2-4)/2}y(n-1)x^{((n-1)^2-4)/2} \\ &= n^2x^{n^2} - x^3(n^2-1)x^{n^2-3} \\ &= x^{n^2} \end{aligned}$$

Now, if $n$ is even, the leading term of $\psi_n^2$ is

$$y^2n^2x^{n^2-4} \to x^3n^2x^{n^2-4} = n^2x^{n^2-1} \text{ (since } y^2 = x^3 + ...)$$

The leading term for $\phi_n$ for an even $n$ will be (keeping in mind that $y^2 = x^3$+...)

$$\begin{aligned} & x^4n^2x^{n^2-4} - (n+1)x^{(n^2+2n)/2}(n-1)x^{(n^2-2n)/2} \\ &= n^2x^{n^2} - (n^2-1)x^{n^2} \\ &= x^{n^2} \end{aligned}$$

∎

The previous lemmas lead us to the following theorem, the proof for which is outside the scope of this thesis. A rigorous proof may be found in section 9.5 of [1].

**Theorem 3.11** *For $P = (x, y)$ on $y^2 = x^3 + Ax + B$ (assuming not characteristic 2 field),*

$$nP = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x,y)}{\psi_n^3(x,y)}\right) \tag{3.3}$$

This endomorphism in hand, we can further investigate the operation of point multiplication, allowing us to address questions of degree, and ultimately provide a proof for Theorem 3.5.

Of further interest is the following which will lay the groundwork for future theorems:

**Theorem 3.12** *Let $E$ be an elliptic curve defined over a field $K$. Let $\alpha \neq 0$ be the multiplication by $n$ endomorphism. Then $\alpha : E(\bar{K}) \to E(\bar{K})$ is surjective.*

**Proof:** Let $(a, b) \in E(\bar{K})$. Since $\alpha(\infty) = \infty$, we will assume $(a, b) \neq \infty$. Notationally, let $\alpha(x, y) = (r_1(x), r_2(x)y)$, and let $r_1(x) = p(x)/q(x)$, where $p$ and $q$ share no common roots. We want to show that there exists some $(x_0, y_0) \in E(\bar{K})$ with $\alpha(x_0, y_0) = (a, b)$.

Now, in our case, $p(x) = \phi_n(x)$ and $q(x) = \psi_n^2(x)$. We are looking at the instances where $a = p/q$. Now, from corollary 3.10, we have that the polynomial $\phi_n(x) - a\psi_n^2(x)$ will never be constant. We may thus consider the case where $p - aq$ is a nonconstant polynomial and identify the instances where $p(x) - aq(x) = 0$.

Consider: if $p(x) - aq(x)$ is not a constant polynomial, then there exists some $x_0$ such that $p(x_0) - aq(x_0) = 0$, since $\bar{K}$ is algebraically closed. Since $p$ and $q$ have no common roots, $q(x_0)$ cannot be 0, since if it were, this would require $p(x_0) = 0$. Now, let $y_0$ be a square root of $x_0^3 + Ax_0 + B$. We then get that $\alpha(x_0, y_0) = (a, b')$ for some $b'$. Now, since $b'^2 = a^3 + Aa + B = b^2$, then we have that $b = \pm b'$. We're done if $b' = b$. If $b' = -b$, then we simply will look at $\alpha(x_0, -y_0) = (a, -b') = (a, b)$, and again we're done. ∎

**Theorem 3.13** *The endomorphism for $nP$ has degree $n^2$.*

**Proof:** Recall that we define the degree of an endomorphism to be the the maximum of the degrees of the numerator and denominator of the first coordinate. By Corollary 3.10 we get that the degree of both polynomials is $n^2$, so the degree of the endomorphism is also $n^2$ so long as $\phi_n(x)$ and $\psi_n^2(x)$ share no common roots. We will proceed via contradiction to show this is the case.

Assume that $\phi_n(x)$ and $\psi_n^2(x)$ share a common root, and let $n'$ be the smallest index for which this occurs, and first suppose that this $n' = 2m$ for some $m$. Using our definitions for $\phi$ and $\psi$ yield:

$$\begin{aligned}\phi_2(x) &= x\psi_2^2 - \psi_3\psi_1 = x4y^2 - 3x^4 - 6Ax^2 - 12Bx + A^2 \\ &= 4x^4 + 4Ax^2 + 4Bx - 3x^4 - 6Ax^2 - 12Bx + A^2 \\ &= x^4 - 2Ax^2 - 8Bx + A^2 \end{aligned} \tag{3.4}$$

$$\begin{aligned}\psi_2^2(x) &= 4y^2 = 4(x^3 + Ax + B) \\ &= 4x^3 + 4Ax + 4B \end{aligned} \tag{3.5}$$

Since $m$ is an integer value, as is 2, we may utilize (3.3) to get:

$$n'P = 2mP = 2(mP) = 2\left(\frac{\phi_m(x)}{\psi_m^2(x)}, \frac{\omega_m(x,y)}{\psi_m^3(x,y)}\right) = \left(\frac{\phi_2(\phi_m/\psi_m^2)}{\psi_n^2(\phi_m/\psi_m^2)}, \frac{\omega_2(mP)}{\psi_2^3(mP)}\right)$$

Using (3.4) and (3.5) in conjunction with the above, while looking at just the first coordinate yields:

$$\begin{aligned}\frac{\phi_{2m}}{\psi_{2m}^2} &= \left(\frac{\phi_2(\phi_m/\psi_m^2)}{\psi_n^2(\phi_m/\psi_m^2)}\right) \\ &= \left(\frac{(\phi_m/\psi_m^2)^4 - 2A(\phi_m/\psi_m^2)^2 - 8B(\phi_m/\psi_m^2) + A^2}{4(\phi_m/\psi_m^2)^3 + 4A(\phi_m/\psi_m^2) + 4B}\right) \\ &= \frac{\phi_m^4 - 2A\phi_m^2\psi_m^4 - 8B\phi_m\psi_m^6 + A^2\psi_m^8}{(4\psi_m^2)(\phi_m^3 + A\phi_m\psi_m^4 + B\psi_m^6)} \end{aligned} \tag{3.6}$$

Define the numerator of (3.6) to be $U$ and the denominator to be $V$. Note: $\frac{U}{V}$ might be a reduced form of $\frac{\phi_{2m}}{\psi_{2m}^2}$.
In order to continue, we need the following:

**Lemma 3.14** *Let* $\Delta = 4A^3 + 27B^2$ *and*

$$F(x,z) = x^4 - 2Ax^2z^2 - 8Bxz^3 + A^2z^4$$

$$G(x,z) = 4z(x^3 + Axz^2 + Bz^3)$$

$$f_1(x,z) = 12x^2z + 16Az^3$$

$$g_1(x,z) = 3x^3 - 5Axz^2 - 27Bz^3$$

$$f_2(x,z) = 4\Delta x^3 - 4A^2Bx^2z + 4A(3A^3 + 22B^2)xz^2 + 12B(A^3 + 8B^2)z^3$$

$$g_2(x,z) = A^2Bx^3 + A(5A^3 + 32B^2)x^2z + 2B(13A^3 + 96B^2)xz^2 - 3A^2(A^3 + 8B^2)z^3$$

*We then get that*

$$Ff_1 - Gg_1 = 4\Delta z^7 \quad \textit{and} \quad Ff_2 + Gg_2 = 4\Delta x^7$$

**Proof:** It should be noted that while $F$ and $G$ mimic $U$ and $V$ the remaining polynomials come from the extended Euclidean Algorithm. These identities can be confirmed through straightforward computation. $F(x,1)$ and $G(x,1)$ have no shared roots, and so we find the polynomials $f_1$ and $g_1$ by the extended Euclidean algorithm such that $F(x,1)f_1(x) - G(x,1)g_1(x) = 4\Delta$. With a change of variables $x \to x/z$ and multiplication by $z^7$, we get the first result. Switching the roles of $x$ and $z$ yields the second. ∎

Utilizing lemma 3.14 gives us

$$U \cdot f_1(\phi_m, \psi_m^2) - V \cdot g_1(\phi_m, \psi_m^2) = 4\psi_m^{14}\Delta$$

$$U \cdot f_2(\phi_m, \psi_m^2) - V \cdot g_2(\phi_m, \psi_m^2) = 4\phi_m^7\Delta$$

From this we may deduce that if $U$ and $V$ have a common root, then so too must $\psi_m^2$ and $\phi_m$. This contradicts our assumption that $n' = 2m$ is the smallest index for which $\phi_n$ and $\psi_n^2$ share a common root.

We now must ensure that in fact $U = \phi_{2m}$ and $V = \psi_{2m}^2$. Since $U$ and $V$ share no common roots and $U/V = \phi_{2m}/\psi_{2m}^2$, we have that $\phi_{2m}$ is a multiple of $U$ and $\psi_{2m}^2$ is a multiple of $V$. Using Corollary 3.10, we can (after some computation) discern the leading term of $U$ is $x^{4m^2}$. Again using the corollary, we know that $\phi_{2m} = x^{(2m)^2}$ and since $\phi_{2m}$ is a multiple of $U$, we get the desired equality. Further, since $U = \phi_{2m}$, then $V = \psi_{2m}^2$.

Assume the smallest index where $\phi_n$ and $\psi_n^2$ have a common root is odd, so $n' = 2m + 1$ for some $m$. Let $r$ be a common root of $\phi_{n'}$ and $\psi_{n'}^2$. By definition, we have that $\phi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1}$. Evaluating at $r$ yields:

$$0 = \psi_{n'-1}(r)\psi_{n'+1}(r)$$

Consider that $\phi_{n'+1}^2$ and $\phi_{n'-1}^2$ are both polynomials, and from above, we know that their product is zero when evaluated at $r$. We can thus say that for $\delta$ equals either 1 or $-1$, $\psi_{n'+\delta}^2(r) = 0$. Now, note that $(\psi_n\psi_{n+2\delta})^2 = \psi_n^2\psi_{n+2\delta}^2$, so since $\psi_{n'}(r) = 0$, $(\psi_n\psi_{n+2\delta})(r) = 0$.

By definition, we know that $\phi_{n'+\delta} = x\psi_{n'+\delta}^2 - \psi_{n'}\psi_{n'+2\delta}$, and evaluating at $r$ gives us that $\phi_{n'+\delta}(r) = 0$. Thus $\phi_{n'+\delta}$ and $\psi_{n'+\delta}^2$ have a common root of $r$. Recall at this point that $n'$ is odd, so $n' + \delta$ must be even. Previously in this proof, we showed that if $\phi_{2m}$ and $\psi_{2m}^2$ share a root, then so too does $\phi_m$ and $\psi_m^2$. We will replicate this idea with $n' + \delta$. Specifically, we now have that $\phi_{(n'+\delta)/2}$ shares a root with $\psi_{(n'+\delta)/2}^2$. Since we previously established that $n'$ is the smallest index for which this occurs, then

$$\frac{n' + \delta}{2} \geq n' \Rightarrow \delta \geq n'$$

If $\delta$ is $-1$ this clearly will not work, and if $\delta$ is 1, then $n'$ must be 1 ($n'$ is odd). This implies that $\phi_1$ and $\psi_1^2$ share a common root, but recall that $\phi_1 = x$ and $\psi_1^2 = 1$, which clearly do not share any roots. This gives us that for any case, $\phi_n$ and $\psi_n^2$ share no common roots, and thus the degree of the endomorphism for a point multiplied by $n$ is in fact $n^2$. ∎

For the proof of theorem 3.5 we will also need the Fundamental Theorem of Finite Abelian Groups, a result from algebraic group theory. The proof for this result (or an equivalent variation) may be found in almost any algebra textbook.

**Theorem 3.15** *A finite abelian group $G$ is isomorphic to a group of the form*

$$\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus ... \oplus \mathbb{Z}_{n_s}$$

*with $n_i | n_{i+1}$ for $1 \leq i \leq s-1$. The integers $i$ are uniquely determined by $G$.*

We may now go about proving theorem 3.5. Recall:

**Theorem 3.5** *Let $E(K)$ be an elliptic curve defined over a field $K$ and let $n \in \mathbb{Z}^+$. If the characteristic of $K$ does not divide $n$, or the characteristic of $K$ is zero, then*

$$E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$$

*If the characteristic of $K$ equals some $p > 0$ such that $p | n$, write $n = p^r n'$ with $p \nmid n'$. Then*

$$E[n] \simeq \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'} \quad or \quad \mathbb{Z}_n \oplus \mathbb{Z}_{n'}$$

**Proof:** Let $p$ be the characteristic of the field $K$. Assume first that $n$ is not a multiple of $p$. Let the endomorphism for a point times an integer $n$ be denoted as $\alpha$. Then by Corollary 2.35, $\alpha$ is separable. By definition, the kernel of $\alpha$ is $E[n]$. From Theorem 3.13, $\alpha$ has degree $n^2$, and from Theorem 2.31, $E[n]$ has order $n^2$.

By Theorem 3.15, we know that $E[n] \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus ... \oplus \mathbb{Z}_{n_s}$, with $n_i | n_{i+1}$ for $1 \leq i \leq s-1$. Let $l$ be a prime dividing $n_1$. Then, it must be that $l | n_i$ for all $i$. Combining this with the fact that each $n_i$ divides $n$ since every element has order dividing $n$, we get that if $P \in E[l]$, then $P \in E[n]$ since $l|n$, so $E[l] \subseteq E[n]$. From algebra, we know that for a given cyclic group $G$ of order $n$, if $d|n$, then G has $\phi(d)$ many elements of order $d$, where $\phi$ is the Euler-Phi function [9]. Since we may apply this to each $n_i$ for $l$, and since $\phi(l) = l - 1$, we get by including the identity of each summand that $E[l]$ has order $l^s$.

From the first part of the proof though, we know that $E[l]$ is of order $l^2$, so $s = 2$. This results in $E[n] \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ for some $n_1, n_2$. Since, $E[n]$ is of order $n^2$, $n^2 = n_1 n_2$, and since $n_1 | n_2 | n$, it follows that $n_1 = n_2 = n$, and thus when $p \not| n$, $E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$.

Now, let $p|n$. First we will consider the case where $n = p^k$ where $k$ is an integer. From corollary 2.35, we know that multiplication by $p$ is not a separable endomorphism. By theorem 3.13 and theorem 2.31 we have that the size of the kernel of this endomorphism ($E[p]$) is less than $p^2$. Now, each element of $E[p]$ has either order 1 or order $p$, the size of $E[p]$ must be some power of $p$, which forces either 1 or $p$. Supposing first that $E[p]$ is of size one (trivial),

then $E[p^k]$ must also be trivial for all $k$, by definition. Now, suppose that $E[p]$ is cyclic of order $p$.

Claim: $E[p^k] \simeq \mathbb{Z}_{p^k}$ for all $k$.
We will begin here by showing the size of $E[p^k]$ is not smaller than $p^k$. Let $P \in E[p^k]$ be an element of order $p^j$, with $j < k$. By theorem 3.12, we have that multiplication by $p$ is surjective so there exists some point $Q$ such that $pQ = P$. This gives us that

$$p^j Q = p^{j-1} P \neq \infty \text{ and } p^{j+1} Q = p^j P = \infty$$

So $Q$ has order $p^{j+1}$. Since $j$ was arbitrary, and we have an element of order 1 (the identity), then via induction we can find an element of order $p^k$. This gives us that $E[p^k]$ is cyclic of order $p^k$.

We may combine this claim with our previous work to establish the remainder of the proof. Write $n = p^k n'$ where $p \not| n'$. First note that $E[n] \simeq E[n'] \oplus E[p^r]$. From above, we know that $E[p^k] \simeq 0$ or $\simeq \mathbb{Z}_{p^k}$. The Chinese Remainder Theorem gives us that $\mathbb{Z}_{n'} \oplus \mathbb{Z}_{p^k} \simeq \mathbb{Z}_{n'p^k} \simeq \mathbb{Z}_n$, and from the first part of the theorem, we know that $E[n'] \simeq \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'}$.We thus get the desired result:

$$E[n] \simeq \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'} \quad \text{or} \quad \mathbb{Z}_n \oplus \mathbb{Z}_{n'}$$

∎

Theorem 3.5 gives us a very very useful general notion of the nature of torsion subgroups on elliptic curves. We can certainly see that the results from the examples of $E[2]$ and $E[3]$ are supported by the theorem. the torsion subgroups form the basis for many higher level mathematics on elliptic curves, specifi-

cally the Weil Pairing, which proves to be very useful for future applications when looking at elliptic curves over finite fields.

# Chapter 4

# Elliptic Curves over Finite Fields

While previous examples of elliptic curves have been over relatively arbitrary fields, often in cryptography we care about fields of finite size. Consider the elliptic curve $E$ taken over some finite field of size $n$, $\mathbb{F}_n$. Since $\mathbb{F}_n$ is finite, so too will be the size of the resulting group $E(\mathbb{F}_n)$.

One method of determining $E(\mathbb{F}_n)$ is via brute force. First we construct a list of quadratic residues (the non-zero squares) in $\mathbb{F}_n$, denoted $Q(\mathbb{F}_n)$. It is worth noting that exactly half of the non-zero elements of a non-characteristic 2 finite field are quadratic residues. This results from the properties of the mapping $\mathbf{Q} : \mathbb{F} \to \mathbb{F}$ given by $\mathbf{Q}(a) = a^2$. Specifically, $\mathbf{Q}$ is a group homomorphism whose kernel is $\{-1, 1\}$. By the first isomorphism theorem then, $Q = \text{im}\mathbf{Q} \simeq \mathbb{F}/\ker \mathbf{Q} \Rightarrow |Q| = \frac{|\mathbb{F}|}{|\ker \mathbf{Q}|} = \frac{|\mathbb{F}|}{2}$.

Once we have a collection of residues, we proceed by computing $f(x)$ for each $x \in \mathbb{F}_n$ where $f(x) = x^3 + Ax + B$. Each $f(x) \in Q$ then yields a $\pm y$ satisfying $y^2 = f(x)$.

## 4.1 Examples

**Example 4.1** Let $E$ be an elliptic curve with $y^2 = x^3 + x + 1$ as the corresponding Weierstrass equation. We first will establish a list of quadratic residues (the non-zero squares) of $\mathbb{F}_{19}$, which we will denote $Q(\mathbb{F}_{19})$. With relatively little calculation these are:

$$Q(\mathbb{F}_{19}) = \{1, 4, 5, 6, 7, 9, 11, 16, 17\}$$

We now list possible values of $x$, computing $x^3 + x + 1 \mod 19$ for each $x$, picking out only the ones which yield values from $Q(\mathbb{F}_{19})$.

| $x$ | $x^3 + x + 1 \mod 19$ | $y$ | Points |
|---|---|---|---|
| 0 | 1 | 1, 18 | (0,1), (0,18) |
| 2 | 11 | 7, 12 | (2,7), (2,12) |
| 5 | 17 | 6, 13 | (5,6), (5,13) |
| 7 | 9 | 3, 16 | (7,3), (7,16) |
| 9 | 17 | 6, 13 | (9,6), (9,13) |
| 10 | 4 | 2, 17 | (10,2), (10,17) |
| 13 | 7 | 8, 11 | (13,8), (13,11) |
| 14 | 4 | 2, 17 | (14,2), (14,17) |
| 15 | 9 | 3, 16 | (15,3), (15,16) |
| 16 | 9 | 3, 16 | (16,3), (16,16) |

Our table gives us 20 distinct points, and along with the point at $\infty$, we then get that $E(\mathbb{F}_{19})$ is of size 21. □

Note in the previous example, how 19 was fairly close to 21. This hints at a more general notion. Consider for some $y^2 = f(x) = x^3 + ...$, if we assume roughly half of the values of $f(x)$ are residues, each such residue gives

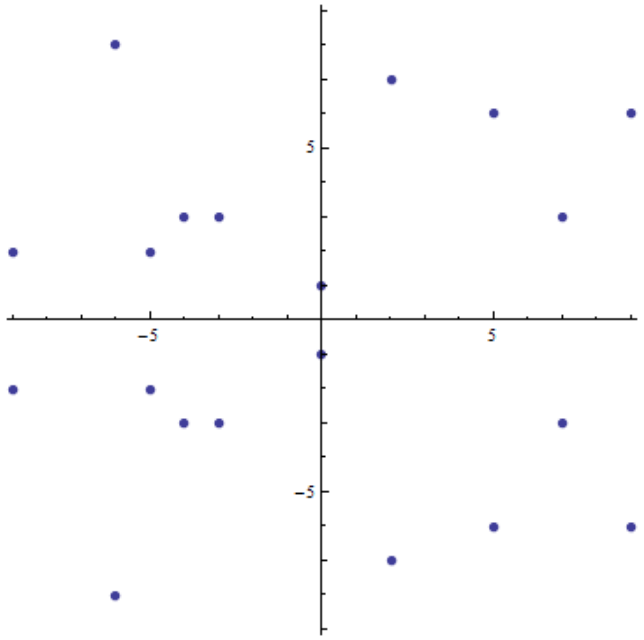



Figure 4.1: Graphical representation of $E(\mathbb{F}_{19})$. Note how it is still symmetrical about the $x$-axis.

2 solutions; $\pm y$. So recalling that our finite field is of size $n$, we would get approximately $n + 1$ solutions, the $+1$ being required due to $\infty$. We would then expect the following:

$$|E(\mathbb{F}_n)| \approx n + 1 + \epsilon(n)$$

where $\epsilon(n)$ is an error term, with $\epsilon(n)/n \approx 0$ as for large values of $n$. The precise statement of this is summed up in Hasse's Theorem for Elliptic Curves, which we will be looking at in the next section.

We would like to be able to add points, and since $\mathbb{F}_{19}$ is neither characteristic 2 nor 3, we may appeal to our formulas from chapter 2. We will need to be careful, however since all the arithmetic must be done within our field. We can also interpret this process graphically, just as we did before.

**Example 4.2** Let's add the points $(5, 6)$ and $(14, 2)$. First we will need to compute $m$, which we may do in the typical way:

$$\begin{aligned} m &= \frac{2-6}{14-5} \\ &\equiv \frac{-4}{9} \equiv \frac{15}{9} \\ &\equiv 15 \cdot 9^{-1} \equiv 15 \cdot 17 \\ &\equiv 8 \mod 19 \end{aligned}$$

So with relatively little work, we get that our connecting "line" in this case is $y = 8x + 4$.

We may then go about computing our new point:

$$\begin{aligned} x_3 &= 8^2 - 14 - 5 \\ &\equiv 7 \mod 19 \\ y_3 &= 8(2 \cdot 5 - 8^2 + 14) - 6 \\ &\equiv 8(10 - 7 + 14) + 13 \\ &\equiv 8 \cdot 17 + 13 \equiv 16 \mod 19 \end{aligned}$$

Thus, $(5, 6) +_E (14, 2) = (7, 16)$.

Simmilar to the elliptic curve over $\mathbb{R}$ we can also think of elliptic curve addition graphically. In fact, since all our coordinates are to be taken mod 19, the line we draw will end up wrapping around the coordinate axis. This behavior is similar to a line being drawn upon a torus. At this point, this notion is probably rather cryptic, but we will return to this idea in Chapter 7, where we look more closely at the relation ship between a torus and an elliptic curve.

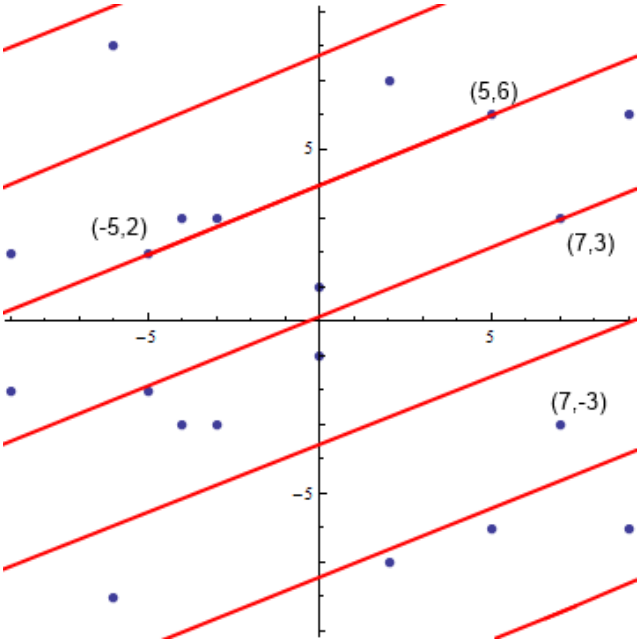



Figure 4.2: The "line," $y = 8x + 4$ connecting $(-5, 2)$ and $(5, 6)$ (seen in red) wraps around the coordinate axis. Recall also that $(14, 2)$ is the same as $(-5, 2)$ in this field. We get that $(7, 3)$ is the third point of intersection, and as we did previously, we flip over the $y$-axis to get our solution: $(7, -3) \equiv (7, 16)$.

What's more, the point $(9, 16)$ is a generator of $E(\mathbb{F}_{19})$.:

| | | | |
|---|---|---|---|
| P=(9,6), | 2P=(7,3), | 3P=(10,2) | 4P=(16,3) |
| 5P=(0,1), | 6P=(15,16), | 7P=(2,12), | 8P=(13,11) |
| 9P=(14,2), | 10P=(5,6), | 11P=(5,13) | 12P= (14,17) |
| 13P=(13,8), | 14P=(2,7), | 15P=(15,3) | 16P= (0,18) |
| 17P=(16,16), | 18P=(10,17), | 19P=(7,16) | 20P= (9,13) |
| 21P=$\infty$ | | | |

Thus, we may deduce that $E(\mathbb{F}_{19})$ is cyclic of order 21. While we will be using the point $(9, 16)$ later on (so these calculations will be handy), it is worth noting that other points will generate this group, most notably $(0, 1)$. □

Not all elliptic curves over finite fields create cyclic groups, as we will see in our next example:

**Example 4.3** Consider the elliptic curve $E$ given by $y^2 = x^3 + 2$ over $\mathbb{F}_7$. $Q(\mathbb{F}_7) = \{1, 4, 2\}$ so:

| $x$ | $x^3 + 2 \mod 7$ | $y$ | Points |
|---|---|---|---|
| 0 | 2 | 3, 4 | (0,3), (0,4) |
| 3 | 1 | 1, 6 | (3,1), (3,6) |
| 5 | 1 | 1, 6 | (5,1), (5,6) |
| 6 | 1 | 1, 6 | (6,1), (6,6) |

So along with the point $\infty$, we have that $E(\mathbb{F}_7)$ is of size 9. This means that either $E(\mathbb{F}_7) \simeq \mathbb{Z}_9$ or $E(\mathbb{F}_7) \simeq \mathbb{Z}_3 \oplus \mathbb{Z}_3$. With a little calculation we get that:

| | | |
|---|---|---|
| 1(3,1)=(3,1) | 1(5,1)=(5,1) | 1(6,6)=(6,6) |
| 2(3,1)=(3,6) | 2(5,1)=(5,6) | 2(6,6)=(6,1) |
| 3(3,1)=$\infty$ | 3(5,1)=$\infty$ | 3(6,6)= $\infty$ |

We have three elements all of which are order 3, which means that $E(\mathbb{F}_7) \not\simeq \mathbb{Z}_9$ (as $\mathbb{Z}_9$ has only two order 3 elements), and thus it must be that $E(\mathbb{F}_7) \simeq \mathbb{Z}_3 \oplus \mathbb{Z}_3$. □

## 4.2 Some Nice Theorems

There are two primary theorems that govern the size of an elliptic curve over finite fields.

**Theorem 4.4** *Let $E$ be an elliptic curve over the finite field $\mathbb{F}_n$. Then*

$$E(\mathbb{F}_n) \simeq \mathbb{Z}_k \qquad \text{or} \qquad E(\mathbb{F}_n) \simeq \mathbb{Z}_{k_1} \oplus \mathbb{Z}_{k_2}$$

*for some integer $k \geq 1$, or for some integers $k_1, k_2 \geq 1$ with $k_1$ dividing $k_2$.*

**Proof:** This theorem largely rests on the Fundamental Theorem of Finite Abelian Groups (see Theorem 3.15). Since for each $i$, the group $\mathbb{Z}_{n_i}$ has $n_1$ many elements of order dividing $n_1$, we find that for some integer power $r$, $E(\mathbb{F}_n)$ has $n_1^r$ elements of order dividing $n_1$. By Theorem 3.5 we have that there are no more than $n_1^2$ such points. Thus $r \leq 2$, and we have the desired result. ∎

**Theorem 4.5** *Let $E$ be an elliptic curve over the finite field $\mathbb{F}_n$. Then the order of $E(\mathbb{F}_n)$ satisfies:*

$$|n + 1 - ord(E(\mathbb{F}_n))| \leq 2\sqrt{n}$$

*This is referred to as Hasse's Theorem on Elliptic Curves.*

In order to prove Hasse's theorem, we will need a few extra notions. The first is the Frobenius Endomorphism.

**Definition 4.6** For a field finite field $\mathbb{F}_n$ of characteristic $p$, the *Frobenius Automorphism* notated as $\phi : \mathbb{F}_n \to \mathbb{F}_n$ is defined as

$$\phi_p(a) = a^p, \text{ for } a \in \mathbb{F}_n$$

Now, a basic result from Algebra tells us that for a prime $p$, we have $(a+b)^p = a^p + b^p \mod p$. This thus gives us that $\phi_p(a + b) = \phi_p(a) + \phi_p(b)$. Now, this holds for any characteristic $p$ field, and thus will also hold for $\overline{\mathbb{F}}_n$, where $n = p^k$ for some $k$.

We may now consider the frobenius Endomorphism on $E(\overline{\mathbb{F}}_n)$.

**Theorem 4.7** *Let $E$ be an elliptic curve over $\mathbb{F}_n$. Then the Frobenius Endomorphism $\phi : E(\overline{\mathbb{F}}_n) \to E(\overline{\mathbb{F}}_n)$ where*

$$\phi((x, y)) = (x^n, y^n)$$

*is an endomorphism of $E$ with degree $n$.*

Now, certainly, we can see that $\phi$ maps from $E(\overline{\mathbb{F}}_n)$ to $E(\overline{\mathbb{F}}_n)$, and is given by rational functions. Further, by definition, the degree is $n$, provided $\phi$ itself is a homomorphism. We must show that for $(x_1, y_1), (x_2, y_2)$, $\phi((x_1, y_1)) +_E \phi((x_2, y_2)) = \phi((x_1, y_1) +_E (x_2, y_2))$. We may then proceed by checking the elliptic curve addition rules. For this proof, we will assume $\mathbb{F}_n$ is not characteristic 2 or characteristic 3, so we may use the Weierstrass equation. The proof with the generalized Weierstrass equation is similar.

Recall for $x_1 \neq x_2$, we have for $(x_1, y_1) +_E (x_2, y_2) = (x_3, y_3)$:

$$m = \tfrac{y_2 - y_1}{x_2 - x_1}, \qquad x_3 = m^2 - x_1 - x_2, \qquad \text{and } y_3 = m(2x_1 - m^2 + x_2) - y_1$$

then, for $\phi((x_3, y_3)$ we get $(x_3^n, y_3^n)$. Now, for $x, y \in \mathbb{F}_n$, we know that $(x+y)^n = x^n + y^n$, since $\overline{\mathbb{F}}_n$ is characteristic $p$. Further, we also know that for $a \in \mathbb{F}_n$, $a^n = a$.

This gives us that the $x$-coordinate for $\phi((x_3, y_3)$ is

$$x_3^n = m'^2 - x_1^n - x_2^n, \text{ where } m' = \frac{y_2^n - y_1^n}{x_2^n - x_1^n} = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^n = m^n$$

Similarly, the $y$-coordinate of $\phi((x_3, y_3)$ is

$$y_3 = m'(2^n x_1^n - m'^2 + x_2^n) - y_1^n$$

Now, recalling that $2^n = 2$, we see that in both cases, $x_3^n$ and $y_3^n$ are really just the formulas for $x_3$ and $y_3$ with all our original coordinates $x_1, x_2, y_1$, and $y_2$ taken to the $n$th power. In essence, we have $\phi((x_1, y_1)) +_E \phi((x_2, y_2)) = \phi((x_1, y_1) +_E (x_2, y_2))$ as desired. The other cases for addition work in a similar fashion, allowing us to say $\phi$ is indeed a homomorphism, and thus an endomorphism. ∎

In addition to the Frobenius endomorphism, we also will need the following:

**Proposition 4.8** *Let $E$ be defined over $\mathbb{F}_n$, with $m \geq 1$. Then*

*1) $Ker(\phi - 1) = E(\mathbb{F}_n)$*

*2) $\phi - 1$ is a separable endomorphism.*

**Proof:** Consider that for our finite field $\mathbb{F}_n$, $a \in \mathbb{F}_n$ implies that $a^n = a$. Thus for $(x, y) \in E(\mathbb{F}_n)$, both $x$ and $y$ are in $\mathbb{F}_n$. Thus $\phi(x, y) = (x^n, y^n) = (x, y)$. More generally, for $P \in E(\mathbb{F}_n)$, $\phi(P) = P$. Since $\phi$ is an endomorphism it has the property of homomorphisms, thus we may say that:

$$\phi(P) - P = 0 \iff (\phi - 1)(P) = 0$$

So the points $P \in E(\mathbb{F}_n)$ form the kernel of $\phi - 1$.

Part 2 follows from a more general result:

**Lemma 4.9** *Let $E$ be an elliptc curve defined over $\mathbb{F}_n$, where $n$ is the power of some prime $p$. Let $r$ and $s$ be integers, not both 0. The endomorphism $r\phi + s$ is separable if and only if $p \nmid s$.*

**Proof:** Write multiplication by $r$ and multiplication by $s$ as follows:

$$r(x, y) = (R_r(x), yS_r(x))$$

$$s(x, y) = (R_s(x), yS_s(x))$$

Extending this notation, we may then describe the endomorphism $r\phi$ as

$$(r\phi)(x, y) = (R_{r\phi}(x), yS_{r\phi}(x))$$

Then we get

$$(R_{r\phi}(x), yS_{r\phi}(x)) = (\phi r)(x, y) = (R_r^n(x), y^n S_r^n(x))$$

Now, define:

$$c_{r\phi} = \frac{R'_{r\phi}}{S_{r\phi}} = \frac{(R_r^n)'}{S_{r\phi}} = \frac{nR_r^{n-1}R'_r}{S_{r\phi}} = 0, \text{ (recall we are in } \mathbb{F}_n)$$

$$c_s = \frac{R'_s}{S_s}$$

Now, by Proposition 2.34 we have that $c_s = s$. By Lemma 2.33, we have that

$$\frac{R'_{r\phi+s}}{S_{r\phi+s}} = c_{r\phi} + c_s = 0 + s = s$$

Thus, for $R'_{r\phi+s} \neq 0$, $p \nmid s$. ∎

Continuing now with Proposition 4.8, we see that by applying the above lemma with $r = 1, s = -1$, since only $\pm 1 | -1$, and $p \neq \pm 1$ since $p$ must be prime, then $\phi - 1$ must be separable. ∎

As a corollary of the above statement we have that $ord(E(\mathbb{F}_n)) = \deg(\phi - 1)$, by Theorem 2.31.

Additionally we will also need the following result

**Proposition 4.10** *Let $\alpha$ and $\beta$ be endomorphisms of $E$ and let $a$ and $b$ be integers. Define endomorphism $a\alpha + b\beta$ defined as*

$$a\alpha + b\beta(P) = a\alpha(P) + b\beta(P)$$

*where $a\alpha(P)$ means multiplication on $E$ of the point $\alpha(P)$ by the integer $a$ (likewise for $b\beta$). Then we have the following:*

$$\deg(a\alpha + b\beta) = a^2 \deg \alpha + b^2 \deg \beta + ab(\deg(\alpha + \beta) - \deg \alpha - \deg \beta)$$

The proof for this involves the use of the Weil pairing, which we will not be going into, but a complete proof may be found in 3.3 of[1].

We now have the tools needed to prove Hasse's Theorem (Theorem 4.5). Let

$$a = n + 1 - ord(E(\mathbb{F}_n))$$

By Proposition 4.8, we have that $a = n + 1 - \deg(\phi - 1)$. We must show that $|a| \leq 2\sqrt{n}$.

We now need the following lemma:

**Lemma 4.11** *Let $r, s$ be integers. Then* $\deg(r\phi - s) = r^2 n + s^2 - rsa$.

**Proof:** From Proposition 4.10, we get that

$$\deg(r\phi - s) = r^2 \deg \phi + s^2 \deg(-1) + rs(\deg(\phi - 1) - \deg(\phi) - \deg(-1))$$

Now, we know $\deg \phi = n$ from Theorem 4.7. $\deg(-1) = 1$. Substituting these values yields the desired result. ∎

Since $\deg(r\phi - s) \geq 0$, we may say that for $r, s \in \mathbb{Z}$, with $\gcd(s, n) = 1$:

$$r^2 n + s^2 - rsa \geq 0$$
$$\Rightarrow n\left(\frac{r}{s}\right)^2 - a\left(\frac{r}{s}\right) + 1 \geq 0$$

The set of rational numbers $r/s$ such that $\gcd(s, n) = 1$ is dense in $\mathbb{R}$. We may thus say that

$$nx^2 - ax + 1 \geq 0 \tag{4.1}$$

for all $x \in \mathbb{R}$.

The discriminant of (4.1) must therefore be non-positive. This means that $a^2 - 4n \leq 0$, which yields $|a| \leq 2\sqrt{n}$. ∎

Hasse's theorem becomes useful since in crypotgraphic applications of elliptic curves the size of finite field is often very large. Such a large field would make the table method far too cumbersome to employ.

# Chapter 5

# Discrete Log Problem

The discrete logarithm problem forms the cornerstone of many of the cryptographic applications we will see later. In this chapter, we will look at the classical discrete logarithm problem, as well as some basic attacks upon it as well as its use in cryptography.

## 5.1 Definition and Examples

**Definition 5.1** Let $G$ be a group. Let $a$, $b \in G$. If the group is written multiplicatively, suppose $a^k = b$ for some integer $k$ (if the group is written additively, $ka = b$). In either case the *discrete logarithm problem* is to find $k$.

This idea is perhaps most easily seen in the familiar setting the integers modulo $p$ over multiplication, where $p$ is a prime.

**Example 5.2** Consider the group $\mathbb{Z}_{19}^{\times}$. Suppose $2^k \equiv 17 \pmod{19}$. We want to find $k$. Now certainly with numbers this small, we could just guess and check, and after relatively little computation, we can find that $k = 10$. What's

more, it is trivial to check if we are correct:

$$2^{10} = 1024 = 53 \times 19 + 17 \equiv 17(\mod 19)$$

□

It is worth noting that not all formulations of this problem work out. The preamble of the discrete log problem assumes that we have $a^k = b$ is solvable for $k$, but it is worth considering the cases where such a problem cannot be solved.

**Example 5.3** As in the previous example, we will work in $\mathbb{Z}_{19}^{\times}$. Now, 2 is a generator of this field, so $2^k = b$ will have a solution for any given $b \in \mathbb{Z}_{19}^{\times}$. Consider 4, which is not a generator of $\mathbb{Z}_{19}^{\times}$. The subgroup generated by 4 is $\{1, 4, 16, 7, 9, 17, 11, 6, 5\}$. This means that while $4^k = 9$ will have a solution: $k = 4$, the equation $4^k = 8$ does not have a solution. □

Not all discrete logarithm problems are made equal. Consider the case of the group of integers modulo $n$ over addition. Let $A, B \in \mathbb{Z}$ such that $kA \equiv B \mod n$ for some $k \in \mathbb{Z}$. If $A$ is relatively prime to $n$, we can compute the multiplicative inverse of $A \mod n$ via the Extended Euclidean Algorithm, then multiply by $B$ to recover $k$.

**Example 5.4** Consider the case of the group of integers modulo 109 over addition. Let $k32 \equiv 49 \mod 109$. Via the Extended Euclidean Algorithm we can find $k$:

$$109 - 32 \cdot 3 = 13 \text{ and } 32 - 13 \cdot 2 = 6 \text{ and } 13 - 6 \cdot 2 = 1 \text{ so:}$$

$$1 = 13 - 2(32 - 13 \cdot 2) = 13(5) + 32(-2)$$

$$1 = 5(109 - 32 \cdot 3) + 32(-2)$$

$$1 = 109(5) + 32(-17)$$

Thus the inverse of 32 is congruent to -17 mod 109, or more specifically 92. Now, taking $92 \cdot 49 \mod 109$ yields 39, which we can then quite easily confirm is the desired value for $k$:

$$39 \cdot 32 = 1248 = 11 * 109 + 49 \equiv 49 \mod 109$$

□

This ease of discerning $k$ due to the Euclidean Algorithm makes the additive group of integers modulo $n$ a very poor choice for cryptographic purposes.

Finally we will briefly look at an example of the discrete log problem in the environment of elliptic curves. In this case, $a$ and $b$ will be points on the elliptic curve, with $k$ still an integer. Given $ka = b$ we will need to find $k$, if it exists.

**Example 5.5** Consider the elliptic curve $E(\mathbb{F}_{19})$, the elliptic curve defined over the finite field $\mathbb{F}_{19}$, with the Weierstrass equation $y^2 = x^3 + x + 1$. Supposing now we are given the following:

$$P = (9, 6) \qquad Q = (14, 2) \qquad kP = Q$$

where $P$, $Q \in E$ and $k \in \mathbb{Z}$.
In this case, after some calculation:

$$\begin{aligned} P = (9,6), \quad 2P = (7,3), \quad 3P = (10,2) \\ 4P = (16,3), \quad 5P = (0,1), \quad 6P = (15,16) \\ 7P = (2,12), \quad 8P = (13,11), \quad 9P = (14,2) \end{aligned}$$

So after plenty of calculation, we get that $k = 9$. □

## 5.2 Methods of Attack: Index Calculus

Now, in examples 5.2 and 5.5, we used a brute force method of tackling the discrete log problem. While this is all well and good for the multiplicative group of integers mod 19, this method becomes significantly more problematic as the size of the group increases. For the group of integers, we may instead use a technique referred to as the index calculus.

Let $p$ be a prime and let $g$ be a primitive root mod $p$ (so $g$ generates the cyclic group of integers mod $p$ over multiplication). Note that $g$ has order $p-1$. We then have that for any $h \not\equiv 0 \mod p$, we can write $h \equiv g^k$ for some integer $0 < k < p$. We will let $k = L(h)$ where $L(h)$ then denotes the discrete logarithm of $h$:

$$g^{L(h)} \equiv h \mod p$$

Now, for given $h_1$ and $h_2$, we have

$$h_1 h_2 \equiv g^{L(h_1 h_2)} \text{ and } h_1 h_2 \equiv g^{L(h_1)} g^{L(h_2)} = g^{L(h_1)+L(h_2)}$$
$$\Rightarrow L(h_1 h_2) \equiv L(h_1) + L(h_2) \mod p-1$$

Thus $L$ mimics the traditional logarithm. The index calculus offers a method for computing our function $L$. The big idea is that we compute $L(l_i)$, where each $l_i$ is a small prime. The set of $l_i$'s is called the factor base. We then use this to compute $L(h)$ for an arbitrary $h$.

**Example 5.6** We will first revist example 5.2. Recall, we needed to solve $2^k \equiv 17 \mod 19$. We will choose as our factor base $\{2, 3, 5\}$. We will now inspect some values of the form $2^x \equiv \pm$ a product of primes from our factor base, still mod 19. Unless stated otherwise, assume all equivalencies are mod

19.

$$2^1 \equiv 2$$
$$2^{15} \equiv 2^2 \cdot 3$$
$$2^{17} \equiv 2 \cdot 5$$

Now, in terms of our function $L$ this gives us:

$$2^1 \equiv 2 \mod 19 \Rightarrow 1 \equiv L(2) \mod 18$$
$$2^{15} \equiv 2^2 \cdot 3 \mod 19 \Rightarrow 15 \equiv 2L(2) + L(3) \mod 18$$
$$2^{17} \equiv 2 \cdot 5 \mod 19 \Rightarrow 17 \equiv L(2) + L(5) \mod 18$$

We may thus infer that $L(2) \equiv 1$, $L(3) \equiv 13$ and $L(5) \equiv 16$, all mod 18. Armed with all the discrete logs of our factor base, we compute $2^j \cdot 17 \mod 19$ for different values of $j$ till we find one that factors nicely using our factor base. For this example, j=1 works just fine:

$$2^1 \cdot 17 \equiv 3 \cdot 5 \mod 19$$

So,

$$1 + L(17) \equiv L(3) + L(5) \mod 18$$
$$\Rightarrow L(17) \equiv 13 + 16 - 1 \mod 18$$
$$\Rightarrow L(17) \equiv 10 \mod 18$$

And we thus have that $2^{10} \equiv 17 \mod 19$, as we saw earlier. □

Now, while this didn't really save us that much time, the index calculus can be leveraged to great effect when the size of the field is a really large prime.

**Example 5.7** Let $p = 1217$. Say now, I am given $3^k \equiv 31 \mod 1217$. Certainly, we could check all 1216 different possibilities for $k$, but that would get

dull extremely fast. Instead, we will build a factor base as before: $\{2, 3, 5, 7, 11, 13\}$. With some computation mod 1217 we find:

$$\begin{aligned} 3^1 &\equiv 3 \\ 3^{24} &\equiv -2^2 \cdot 7 \cdot 13 \\ 3^{25} &\equiv 5^3 \\ 3^{30} &\equiv -2 \cdot 5^2 \\ 3^{54} &\equiv -5 \cdot 11 \\ 3^{87} &\equiv 13 \end{aligned}$$

In order to handle the negative values above, we will need a result from number theory.

**Claim:** $3^{(p-1)/2} \equiv -1 \mod p$, for $p \neq \pm 1 \mod 12$.

**Proof:** Since $\mathbb{Z}(p)^\times$ is cyclic of order $p-1$, then for odd $p$,

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

for any $a$ in $\mathbb{Z}(p)^\times$. Thus $a^{\frac{p-1}{2}} = \pm 1$ or more specifically:

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1 \pmod p & \text{if there is an integer } x \text{ such that } a \equiv x^2 \pmod p \\ -1 \pmod p & \text{if there is no such integer.} \end{cases}$$

This is an application of Euler's Criterion.

It thus remains to show that 3 is not a square mod 1217. Using the law of quadratic reciprocity we see that 3 is a square mod $p$ when $p \equiv \pm 1 \mod 12$. For our case, we look at 1217 mod 12, and find that $1217 \not\equiv \pm 1 \mod 12$. This implies that 3 is not a residue (square) mod 1217 and thus that $3^{\frac{p-1}{2}} = -1$. ∎

Continuing on with the index calculus:

$$\begin{aligned} 1 &\equiv L(3) \\ 24 &\equiv 608 + 2L(2) + L(7) + L(13) \\ 25 &\equiv 3L(5) \\ 30 &\equiv 608 + L(2) + 2L(5) \\ 54 &\equiv 608 + L(5) + L(11) \\ 87 &\equiv L(13) \end{aligned}$$

And with just a bit of computation, we end up with $L(2) \equiv 216$, $L(3) \equiv 1$, $L(5) \equiv 819$, $L(7) \equiv 113$, $L(11) \equiv 1059$, and $L(13) \equiv 87$, all mod 1216. We now consider $3^j \cdot 31$ and after some trials with $j$ we get that:

$$\begin{aligned} 3^{26} \cdot 31 &\equiv 2^5 \cdot 3 \cdot 7 \mod 1217 \\ \Rightarrow L(31) &= 5L(2) + L(3) + L(7) - 26 \mod 1216 \end{aligned}$$

Which results in $L(31) \equiv 1168$, and so $3^{1168} \equiv 31 \mod 1217$. Again we can easily check this with any calculator that can handle modular arithmetic. □

When utilizing the index calculus, it is crucial that the factor base be chosen cleverly. Too small of a factor base will make finding values that factor into your factor base difficult, while too large of a factor base will result in problems attempting to find the values of the $L(l_i)$'s. For a practical example, A. Joux and R. Lercier used a factor base consisting of the first 1 million primes to tackle discrete logs mod a 120-digit prime in 2001 [1].

It is worth noting that the index calculus heavily relies on the fact that integers can be rewritten as products of primes. Because of this fact, we cannot easily extend this technique to any arbitrary group. While the index calculus

is often relatively quick (the runtime is subexponential) its limited area of use requires other, slower modes of attack for more general groups [1].

## 5.3 "Baby Step, Giant Step": A More General Attack

For an arbitrary additive group $G$ (we will write our groups in this section additively since that is ultimately what the group over an elliptic curve is), we will need a more general form of attack than the index calculus in the previous section. Notationally for this section, $G$ will be an additive group, $P$ and $Q$ will be elements of $G$, the order of $G$ will be $N$, and $k$ will again be an integer that we wish to find. Our discrete log problem will take the form of:

$$\text{Given } P, Q, \text{ solve } kP = Q \text{ if possible.}$$

The method we will use here is called the "Baby Step, Giant Step". While slower than the previously mentioned index calculus, it will work for any arbitrary group. The attack works as follows:

1) Fix an integer $m \geq \sqrt{N}$ and compute $mP$.

2) Make and store a list of all the elements $iP$ where $0 \leq i < m$.

3) Compute the points $Q - jmP$ for $j = 0, 1, ..., m-1$ until one matches an element from the stored list in step 2.

4) If $iP = Q - jmP$ we then have with some rearranging $Q = kP$ with $k \equiv i + jm \mod N$.

Now, since $m^2 > N$, $i < m$, and $j < m$, then

$$k = i + j, \qquad m \leq (m-1) + (m-1)m = m^2 - 1 < m^2, \qquad 0 \leq k < m^2$$

We can rewrite $k$ as $k = k_0 + mk_1$ with $k_0 \equiv k \mod m$ and $0 \leq k_0 < m$ and $k_1 = (k - k_0)/m$. Thus, $0 \leq k_1 < m$, since $k < m^2$. We then have $i = k_0$ and $j = k_1$, which will yield the desired $Q - k_1 mP = kP - k_1 mP = k_0 P$.

In a more general sense, consider the set $S = \{jm + i : 0 \leq i < m, 0 \leq j < m\}$ for a fixed integer $m$. If $j_1 m + i_1 = j_2 m + i_2$, this forces $i_1 \equiv i_2 \mod m$, which then requires that $i_1 = i_2$ due to the constraints on $i$. We then get that $j_1$ must be equal to $j_2$. So $S$ has $m^2$ elements. What's more, its largest value occurs at $(m-1)m + (m-1) = m^2 - 1$, and its smallest value occurs at 0, so really $S = \{0, 1, 2, ..., m^2 - 1\}$.We can thus use the elements of this set to cover the numbers 0 to $m^2 - 1$; our baby steps being of size 1 (indexed with the $i$'s), and our giant steps of size $m$ (indexed by the $j$'s). For some value $N \leq m^2$, we will then assuredly cover the numbers 0 to $N - 1$, possibly more than once mod $N$.

For the particular set of steps outlined above, the baby step is computed at step 2, when we compute values of $iP$ by taking $P$ and adding it to $(i-1)P$. The giant step then is in step 3, when we add $-mP$ to $Q - (j-1)mP$.

This attack is better than brute force because it requires only $2m$ basic computations, plus step 4 where we extract our value for $k$. For large values of $m$, $2m$ is significantly smaller than $m^2$.

**Example 5.8** Consider example 5.5 above. We will now use the baby step giant step method to tackle this problem, instead of brute force. Recall, our discrete log problem here was:

$$k(9, 6) = (14, 2)$$

Now, as we've seen earlier the order of $E(\mathbb{F}_{19})$ is 21. We will let $m = 5$. We then get that

$$5P = (0, 1)$$

From before we also have our list of "$iP$ elements":

$$P = (9, 6), \quad 2P = (7, 3), \quad 3P = (10, 2), \quad 4P = (16, 3)$$

We need to look at $Q - j5P$ for values of $j$. This results in the following:

$$Q - 1(0, 1) = (14, 2) + (0, 18) = (16, 3)$$

So $k = 4 + 1 * 5 = 9$ just as we got before. □

## 5.4 Cryptographic Applications of Discrete Logs

But just how difficult is the discrete log problem? The problem itself is widely regarded as being just as computationally difficult as factoring integers[5]. As we saw in the previous sections, the index calculus lets us solve discrete logs in subexponential time, but only for a specific type of group. This makes the discrete log problem fantastic to build on as a cornerstone for cryptography. Before we can look at some codes of our own though, we must first establish some groundwork.

### 5.4.1 Terminonlogy and "Big Ideas"

The typical situation involving secret messages has three parties, often referred to as Alice, Bob, and Eve. We will keep this naming convention. Generally, Alice wishes to send a message to Bob. This message will be referred to as the *plaintext*. Eve wishes to know the contents of the plaintext, against the

wishes of both Alice and Bob. Alice will employ an *encryption key* to convert the plaintext into a coded form of the original, known as the *ciphertext*. This ciphertext, she will send to Bob, who will then use his *decryption key* to convert the ciphertext back into plaintext. The goal of any cryptographic system then is to create an encryption scheme that is undecipherable by Eve.

There are two main types of crypto-systems. The first is *symmetric encryption*, wherein the encryption key and decryption key are either the same, or one can be easily inferred from the other. The downside of these systems is that they require some way of initially establishing the keys ahead of time between Alice and Bob, a situation that is not always practical or possible. The advantages are that good symmetric systems are often computationally relatively quick.

The other type of crypto-system is referred to as *public key encryption*. In a public key system, Alice and Bob need no prior contact. Bob possesses both a public key, that he publishes to the world, which Alice uses to encrypt the plaintext, as well as a private decryption key. Obviously for these systems to be secure, the decryption key should be virtually unobtainable from knowledge of the public encryption key. While often more convenient, since Alice need not have met Bob to exchange keys, public key systems are often much slower to implement than symmetric systems.

### 5.4.2 Diffie-Hellman Key Exchange

So, what if Alice and Bob haven't had any prior communication, but still wish to use a symmetric encryption scheme. One way of exchanging the required

keys is via the Diffie-Hellman Key Exchange. Though the original method used multiplicative groups of finite fields, it is equally valuable in the realm of elliptic curves.

1) Alice and Bob agree between each other on a particular multiplicative group of some finite field, call this $G$. This choice is made such that the discrete log problem is nontrivial. They also publicly agree upon an element $P \in G$, such that the subgroup generated by $P$ is large (most often these are chosen so that the order of the subgroup generated by $P$ is a large prime value).
2) Alice and Bob each choose an integer that they keep to themselves. Alice will choose $a \in \mathbb{Z}$ and Bob will choose $b \in \mathbb{Z}$. They each then compute $P^a$ and $P^b$ respectively.
3) Alice will send Bob $P^a$, and likewise, Bob will send Alice $P^b$.
4) Using her secret integer, Alice will use the information sent to her by Bob to compute $(P^b)^a$ and likewise, Bob will compute $(P^a)^b$. Note now that both Alice and Bob have the same element: $P^{ab}$.
5) Alice and Bob will then employ an agreed upon method of extracting a key from the resulting $P^{ab}$.

It might seem that Eve knows quite a lot from this exchange, but the crux of the matter is that Eve does not know the values of $P^{ab}$. She only knows $G$, $P$, $P^a$, and $P^b$. If she can somehow solve the discrete log problem on $G$, she could find either $a$ or $b$, however as we previously mentioned, Alice and Bob specifically chose $G$ such that the discrete log problem was hard.

Formally, Eve's conundrum is referred to as the Diffie-Hellman Problem.

"Given $P$, $P^a$, and $P^b$ all in $G$, compute $P^{ab}$."

Provided Eve can solve discrete logs, she can leverage her knowledge of $P$ and $P^a$ to recover $a$, then compute $(P^b)^a$ just like Bob does.

Say that Eve is sent a tip from some source claiming to know $P^{ab}$. Is there a way she can determine whether the information is correct? This is a related problem to the Diffie-Hellman problem, referred to as the Decision Diffie-Hellman Problem.

"Given $P$, $P^a$, and $P^b$ all in $G$, and given $Q \in G$, determine whether $Q = P^{ab}$."

**Example 5.9** For this example we will be considering a multiplicative group over the integers modulo 113. Our element $P$ will be the number 3. Alice will choose 23 as her secret integer and Bob will choose 32. Now, Alice will send Bob $3^{23} \mod 113$ and Bob will send Alice $3^{32} \mod 113$. Alice now has 28, and Bob has the number 39. Alice now finds that $28^{23} \equiv 106 \mod 113$, and Bob finds that $39^{32} \equiv 106 \mod 113$. In this case, Alice and Bob might use the first 4 bits of the binary representation of 106 as their key, or some other previously agreed upon method. □

Now, certainly Alice and Bob would want to use a much larger value than 113 for the size of their group, otherwise Eve could (with modern computing technology) brute force the problem and discern the values of $a$ and $b$ very quickly.

### 5.4.3 Elgamal Public Key Encryption

Where Diffie-Hellman can be used to set up a symmetric system, the discrete log problem can also be used to establish public key systems. This method,

described by Taher Elgamal in 1984 [7], allows for Alice and Bob to communicate securely without the need to have any pre-established contact. For Alice to send her message, she must first obtain Bob's public key.

**Bob's Public Key**

1) Bob chooses a multiplicative group $G$ where the discrete log problem is difficult.

2) Bob chooses a element $P \in G$, customarily choosing $P$ such that the order of $P$ is a large prime.

3) Bob chooses some integer $n$, and computes $P^n$. For our purposes we will let $B = P^n$.

4) Bob makes $G$, $P$, and $B$ public. Bob keeps the integer $n$ private.

**Alice Encrypts Her Message**

1) Alice obtains all of Bob's public key.

2) Alice expresses her message as an element $M \in G$.

3) Alice chooses her own secret integer, $k$ and computes $P^k = M_1$.

4) Alice computes a new point $M_2 = MB^k$.

5) Alice sends $M_1$ and $M_2$ to Bob.

**Bob Decrypts the Message**

Bob decrypts by calculating $M_2 M_1^{-n}$. This yields $M$ as follows:

$$(MB^k)(P^k)^{-n} = MP^{nk}(P^{kn})^{-1} = M$$

**What Eve Sees**

Assuming Eve is watching, all she will see is the components of Bob's public key, as well as $M_1$ and $M_2$. Eve can only ascertain $M$ if she can somehow solve the discrete log problem on $G$.

**Example 5.10** For this example, we will use the multiplicative group of the integers modulo 2539. Bob's public key will consist of this group $G$, the integer

P=35, and the integer B=154. Bob's secret integer in this case is n=54.

Now, let's say that Alice wishes to encode the message "HELLO WORLD". She first will need a method of translating her message into numbers. One common method is to correspond letters to their numerical position in the alphabet (with $a \to 00$, $b \to 01$ and so on till $z \to 25$) and look at two-letter blocks. In this way, the message "HELLO WORLD" would be broken up into: "HE LL OW OR LD," which would then translate numerically to:

$$0704\ 1111\ 1422\ 1417\ 1103$$

She will then choose a different secret integer $k$ for each block. She could use the same integer $k$ for each block, however picking a different one for each block will better the security of the encrypted message. Looking at the first block, Alice chooses as her secret integer for this block 29. She computes her encoded message as follows:

$$M_1 = 35^{29} \equiv 2400 \mod 2539$$
$$M_2 = 704 \times 154^{29} \equiv 1832 \mod 2539$$

This first block would then be encoded as the ordered pair (2400, 1832). Alice would send this block to Bob, as well as similarly encoded versions of the four other blocks. Bob would then compute (for the first block) $1832 \times 2400^{-54}$ mod 2539, which he would find to be 704, which he would then interpret as the letters H and E. □

# Chapter 6

# Elliptic Curve Cryptography

With the ever increasing speed of computers, it is imperative that encryption keeps pace. Groups on elliptic curves provide a much more efficient ecosystem than more traditional groups. All the previously discussed techniques of encryption can be mimicked with an elliptic curve as the group. Not only that but elliptic curves can provide equivalent security at a lower cost computationally to legitimate users [1]. It is estimated that a 160-bit elliptic curve key will provide the same level of security as a more traditional RSA key of 1024-bits [6]. In this chapter, we will first reapply the earlier cryptographic methods using discrete logs in the setting of elliptic curves. We will follow this with a new method known as the Elliptic Curve Integrated Encryption Scheme.

## 6.1 Using Elliptic Curve Discrete Logs in Cryptography

Most of the applications in this section will work exactly as they did in the previous chapter, just with the group being now an elliptic curve over some

finite field.

### 6.1.1 Diffie-Hellman Key Exchange

1) Alice and Bob agree between each other on an elliptic curve $E$ over a finite field $\mathbb{F}_n$. This choice is made such that the discrete log problem on $E(\mathbb{F}_n)$ is nontrivial. They also publically agree upon a point $P \in E(\mathbb{F}_n)$, such that the subgroup generated by $P$ is large (most often these are chosen so that the order of the subgroup generated by $P$ is a large prime value).

2) Alice and Bob each choose an integer that they keep to themselves. Alice will choose $a \in \mathbb{Z}$ and Bob will choose $b \in \mathbb{Z}$. They each then compute $aP$ and $bP$ respectively.

3) Alice will send Bob $aP$, and likewise, Bob will send Alice $bP$.

4) Using her secret integer, Alice will use the information sent to her by Bob to compute $a(bP)$ and likewise, Bob will compute $b(aP)$. Note now that both Alice and Bob have the same point: $abP$.

5) Alice and Bob will then employ an agreed upon method of extracting a key from the resulting $abP$, like using information based on the $x$-coordinate of $abP$ or some similar method.

**Example 6.1** Consider the elliptic curve $E(\mathbb{F}_{19})$. We will use the point $(9, 6)$ as our point $P$. Alice and Bob will choose the integers 3 and 5, respectively. Alice will then compute $3(9, 6) = (10, 2)$, and send Bob $(10, 2)$, while Bob will compute $5(9, 6) = (0, 1)$ and send Alice $(0, 1)$. Alice will then compute $3(0, 1) = (15, 3)$, while Bob will compute $5(10, 2) = (10, 2) + (14, 17) = (15, 3)$. Alice and Bob then might use the number 15 as the key for some symmetric system of encryption like a Caesar cipher. □

### 6.1.2 Elgamal Public Key Encryption

Again, just like the Diffie-Hellman key exchange, we may conduct Elgamal public key encryption using elliptic curves over finite fields.

**Bob's Public Key**

1) Bob chooses an elliptic curve $E$ over a finite field $\mathbb{F}_n$, where the discrete log problem is difficult.

2) Bob chooses a point $P$ on $E$, customarily choosing $P$ such that the order of $P$ is a large prime.

3) Bob chooses some integer $r$, and computes $rP$. For our purposes we will let $B = rP$.

4) Bob makes $E$, $\mathbb{F}_n$, $P$, and $B$ public. Bob keeps the integer $r$ private.

**Alice Encrypts Her Message**

1) Alice obtains all of Bob's public key.

2) Alice expresses her message as a point $M \in E(\mathbb{F}_n)$.

3) Alice chooses her own secret integer, $k$ and computes $kP = M_1$.

4) Alice computes a new point $M_2 = M +_E kB$.

5) Alice sends $M_1$ and $M_2$ to Bob.

**Bob Decrypts the Message**

Bob decrypts by calculating $M_2 +_E -rM_1$.

**Example 6.2** Let's say that Bob's public key consists of the elliptic curve $E(\mathbb{F}_{19})$ with the equation $y^2 = x^3 + x + 1$. Bob will choose as his public point $(9, 16)$. Bob's private integer will be 3 so Bob's public key will be $E(\mathbb{F}_{19})$, and the points $(9, 16)$ and $(10, 2)$.

For the sake of argument, Alice wishes to send Bob the point $(5, 6)$. Alice then

must compute $M_1$ and $M_2$ with her secret integer, say 5:

$$M_1 = 5(9, 16) = (0, 1)$$

$$M_2 = (5, 6) +_E 5(10, 2) = (5, 6) +_E (15, 3) = (16, 3)$$

Alice now sends these two points to Bob, who decrypts like so:

$$(16, 3) - 3(0, 1) = (16, 3) +_E 3(0, 18) = (16, 3) +_E (15, 16) = (5, 6)$$

□

## 6.2 Elgamal Digital Signatures

With the prevalance of electronic documents in business and government, the notion of a digital signature is of high importance. A digital signature not only requires some method of assuring the signer is who she says she is, but also must somehow be intrinsically tied to the corresponding document. One scheme of digital signatures, developed by Elgamal, originally was implemented over the multiplicative group of a finite field. We can extend the algorithm easily to elliptic curves [1].

In order for Alice to sign a document she must first establish some form of public key. Her key is made up of an elliptic curve $E$ over some finite field $\mathbb{F}_n$, again choosing these so that the discrete log problem is hard on $E(\mathbb{F}_n)$. She then chooses some point $A \in E(\mathbb{F}_n)$, as well as some integer $a$. Alice then computes $aA$ and names the resulting point $B$. Alice also picks some function $f : E(\mathbb{F}_n) \to \mathbb{Z}$. The only requirements on $f$ are that its image be large, and the number of inputs that yield any given output be small. Alice's public information is then $A$, $B$, $E$, $\mathbb{F}_n$, and $f$. Alice keeps the integer $a$ to herself, and this

integer will serve to assure that the signed document is indeed signed by Alice.

Alice will then sign the document as follows:

1) Represent the item to be signed as some integer $m$. Also let $N$ be the order of the point $A$.

2) Choose $k \in \mathbb{Z}$ such that $k$ and $N$ are relatively prime. Compute $kA$ and call the result $R$.

3) Compute $s \equiv k^{-1}(m - af(R)) \mod N$.

4) The signed message to be sent then is $(m, R, s)$.

Bob can then verify that Alice sent the message as follows:

1) Compute $V_1 = f(R)B +_E sR$.

2) Compute $V_2 = mA$.

3) The signature is valid if $V_1 = V_2$.

This works since

$$V_1 = f(R)B + sR = f(R)aA + skA = f(R)aA + (m - af(R))A = mA = V_2$$

**Example 6.3** Let Alice's public key consist of the elliptic curve $E$ over the finite field of size 19, represented by the equation $y^2 = x^3 + x + 1$. Let Alice's chosen point $A = (9, 6)$. Her chosen integer $a$ will be 7 and thus, $B = (2, 12)$. Alice's function will be $f(x, y) = x$.

Alice's public key is then:

$$E(\mathbb{F}_{19}), \qquad A = (9, 6), \qquad B = (2, 12), \qquad f(x, y) = x$$

Now, say she wishes to sign off on the integer 13. Now, from previous, we know the order of $(9, 6)$ is 21, and so we will pick as our $k$ the number 2, since

$\gcd(2, 21) = 1$. $R = 2(9, 6) = (7, 3)$. For $s$ we then get:

$$s \equiv 11(13 - 7 \cdot 7) \mod 21$$
$$s \equiv 3 \mod 21$$

Alice then sends Bob the ordered triple $(13, (7, 3), 3)$.
Bob then checks the authenticity as follows:

$$V_1 = 7(2, 12) +_E 3(7, 3) \qquad V_2 = 13(9, 6)$$
$$= (2, 12) +_E (15, 16) \qquad = (13, 8)$$
$$= (13, 8)$$

Therefore, Bob knows Alice sent the message. □

It is worth noting that at no point did Alice mask the fact that she was sending Bob the integer 13. If Alice wished to keep the contents of her message a secret, she would also have to encrypt the plaintext using some other form of encryption.

When using this method it is imperative that Alice use a different value of $k$ each time she signs a document. If two signed documents by Alice have the same value $k$, Eve will immediately know it, since $R$ will be the same in both cases. If the first message is $(m, R, s)$, call the second $(m', R, s')$, Eve may proceed as follows to ascertain $a$.

$$ks \equiv m - af(R) \mod N \qquad \text{and} \qquad ks' \equiv m' - af(R) \mod N$$

$$\text{So: } k(s - s') = ks - ks' \equiv m - m' \mod N$$

Eve knows both $s$ and $s'$, and since she also knows that we are working mod $N$, there are only finitely many possible values for $k$. In fact she need only check $\gcd(s - s', N)$ many values. Eve need only try each one of them to ascertain which one satisfies $R = kA$. Once she knows $k$, Eve can narrow down the possibilities for $a$ and then use trial and error on $B = aA$ till she finds the one that works.

## 6.3 Messages as Points on Elliptic Curves

In the previous sections, Alice's plaintext was a point on an elliptic curve. Obviously, just sending a point is not relatively useful. As with most mathematical crypto-systems, we first need a way of encoding our given language as some sort of numbers. We can easily consult a convenient ASCII table, and use that to map letters and punctuation to corresponding numerical values, however in many cases this is not the most secure manner in which to encode a message [3]. The following is an alternative method courtesy of Koblitz:

1) Pick an elliptic curve $E$ over the finite field $\mathbb{F}_p$ where $p$ is prime. This method is extensible to any arbitrary finite field, but we will use a prime here for simplicity.
2) Map your characters to numbers, either with an ASCII chart, or in some other mutually agreed upon fashion.
3) Choose an integer $k$. Often used values of $k$ can range anywhere from 20 to 100 or even larger, but really any positive integer will work here. Generally speaking the larger your value of $k$ the more likely you will be able to encode your entire message properly.
4) For each character, let the plaintext value of that character be $m$. Now

assign $x = mk+1$, and solve for $y$ in the equation for the curve. Now, there is no guarantee that there will be a valid solution, but if there is, then this point is the point that will represent that character.

5) If step 4 failed to offer a valid point, re-evaluate the equation at $x = mk+2$, and attempt to solve for $y$. If this fails, try $x = mk + 3$ and so on. In general this process will yield a valid point before you reach $x = mk + (k - 1)$.

6) Repeat for each character. The entire message then becomes a sequence of points on $E$.

Now, in order to accommodate all possible characters, $p$ needs to be at least as large as the number of different characters you have times the size of your integer $k$. Further, since the method is probabilistic, there is a chance that a poorly chosen value for $k$ will yield no feasible result. This is however unlikely and the odds of not finding a valid point are $2^{-k}$ (so larger values of $k$ are more likely to yield results) [1].

Now, one potential problem is that these values can get quite large. Further, if Alice needs to sign each integer she sends Bob, this will triple the amount of information she must send. One way of reducing the burden on the system is by means of a cryptographic hash function.

**Definition 6.4** A *cryptographic hash function* $H$ is a function which takes inputs of arbitrary length (perhaps millions of bits), and outputs values of fixed lengths (128 bits for example). The Hash function $H$ must possess three qualities in order for it to be useful:

1) For a given input $m$, $H(m)$ should be very quick to calculate.

2) Given $H(m) = y$, it is infeasible to determine $m$ given the value of $y$.

3) It is computationally infeasible to find any two inputs $m_1$ and $m_2$ such that $H(m_1) = H(m_2)$.

In definition 6.4 if 2) is satisfied, we say that $H$ is *one-way* or *preimage resistant*. If 3) is satisfied, we say that $H$ is *strongly collision-free*.

## 6.4 Elliptic Curve Integrated Encryption Scheme

Another way to encode messages proposed by Bellare and Rogaway goes by the moniker Elliptic Curve Integrated Encryption Scheme, or ECIES for short. ECIES is handy because it possesses much of the security of public key systems, but the message encryption is actually predominantly handled via a symmetric encryption scheme. The setup is as follows:

Bob picks an elliptic curve $E$ over a finite field $\mathbb{F}_n$ such that the discrete log problem is hard. Also as with earlier setups, Bob will choose a point $A \in E$, customarily such that the order of $A$ (call this $N$) is a large prime. Bob will then choose some secret integer $s$ and compute $B = sA$. Bob's public key that Alice will need to encrypt her message then is $(n, E, N, A, B)$. Bob keeps the integer $s$ to himself. Further, in order for this to work, there must also be some previously agreed upon symmetric encryption function $E_k$, where $k$ is the key for this encryption. Two cryptographic hash functions $H_1$ and $H_2$ will also be required.

**Alice Encrypts Her Message**

1) Alice obtains all of Bob's public key. She wishes to encrypt the message $r$.

2) Alice chooses an integer $r$ such that $1 \leq r \leq N - 1$.

3) Alice computes $R = rA$ and $Z = rB$.

4) Alice writes the output of $H_1(R, Z)$ as two keys $k_1$ and $k_2$ that are retrieved from the result of the hash function in some predetermined manner.

5) Alice takes her message, $m$, and computes $C = E_{k_1}(m)$, using $k_1$ as the encryption key for $E$ the symmetric encryption function, and $t = H_2(C, k_2)$.

6) Alice sends Bob $(R, C, t)$.

**Bob Decrypts the Message**

1) Bob computes $Z = sR$.

2) Bob computes $H_1(R, Z)$, just as Alice did to recover the two keys $k_1$ and $k_2$.

3) Bob computes $H_2(C, k_2)$. If it does not equal $t$, Bob stops and rejects the ciphertext as not authentic.

4) Computes $m = D_{k_1}(C)$ where $D_{k_1}$ is the appropriate decryption function for $E_{k_1}$.

It is important to note here that the majority of the encryption here is being done by the symmetric encryption function $E$. Only the key for $E$ is being encrypted via the public key code method. Further, Alice's message does not need to be represented as a point on an elliptic curve, nor does Bob need to conduct repeated elliptic curve computations for each part of the ciphertext. This ultimately allows for a greater degree of speed without sacrificing security.

Additionally, the "check" step that Bob conducts during decryption can aid in defeating a common attack on these sorts of systems. An attacker might send Bob ciphertexts with the intent of attacking the system through Bob's

decryption. While an attacker might pick a random value for $k_2$, call it $k_2'$, and their own ciphertext, call this $C$, to send to Bob in the form of $H_2(C, k_2')$, the attacker will not have known $Z$ in advance, and thus this will in all likelyhood not match up with Bob's computation of $H_2(C, k_2)$. As soon as this match doesn't occur, Bob knows that the ciphertext doesn't come from a legitimate user, and can simply refuse to decrypt the message.

# Chapter 7

# Elliptic Curves and Complex Numbers

As we mentioned back at the beginning, elliptic curves derived their name from a notion of attempting to find the arc length of an ellipse. In this chapter we will make that connection in more detail as well as look at some properties of elliptic curves over the complex numbers.

## 7.1 The Arc Length of an Ellipse

From geometry, we know that the equation for a generic ellipse is

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1 \tag{7.1}$$

Further, we know we can find arc-length $L$ as:

$$L = \int ds = \int \sqrt{dx^2 + dy^2} = \int \sqrt{1 + \frac{dy}{dx}^2}\, dx$$

Now, from (7.1) we get through implicit differentiation:

$$\begin{aligned}
&\frac{2x}{a^2}dx + \frac{2y}{b^2}dy = 0 \\
\Rightarrow &\frac{dy}{dx} = \frac{(-2x)/a^2}{(2y)/b^2} = \frac{-xb^2}{ya^2} \\
\Rightarrow &1 + \frac{dy}{dx}^2 = 1 + \frac{x^2b^4}{y^2a^4} = 1 + \frac{x^2b^4}{b^2(1-x^2/a^2)a^4} \\
\Rightarrow &1 + \frac{dy}{dx}^2 = 1 + \frac{b^2x^2}{a^2(a^2-x^2)}
\end{aligned}$$

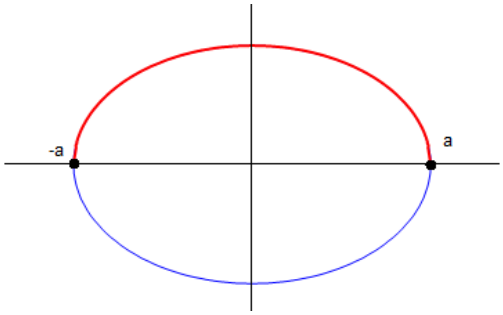



Figure 7.1: We want the arc length as indicated in red.

Thus, the arc length for the half-ellipse is:

$$\begin{aligned}
L &= \int \sqrt{1 + \frac{b^2x^2}{a^4 - a^2x^2}}\, dx \\
&= \int \sqrt{\frac{a^4 - a^2x^2 + b^2x^2}{a^4 - a^2x^2}}\, dx \\
&= \int \sqrt{\frac{a^2 - (1 - b^2/a^2)x^2}{a^2 - x^2}}\, dx
\end{aligned}$$

Now, let $k^2 = 1 - \frac{b^2}{a^2}$ and conduct the following change of variables:

$x \to ax$. We then get:

$$L = a\int_{-1}^{1} \sqrt{\frac{1-k^2x^2}{1-x^2}}\,dx$$
$$= a\int_{-1}^{1} \frac{1-k^2x^2}{\sqrt{(1-x^2)(1-k^2x^2)}}\,dx \tag{7.2}$$

Using (7.2), we can then rewrite as

$$L = a\int_{-1}^{1} \frac{1-k^2x^2}{y}\,dx \tag{7.3}$$

where $y^2 = (1-x^2)(1-k^2x^2)$. We call (7.3) an elliptic integral. Stated more formally:

**Definition 7.1** The integral $\int R(x,y)dx$ is an *elliptic integral* when $R(x,y)$ is a rational function of the coordinates $(x,y)$ on an elliptic curve. Specifically (7.3) is referred to as an *elliptic integral of the second kind.*

An *elliptic integral of the first kind* looks like

$$\int \frac{dx}{\sqrt{(1-x^2)(1-k^2x^2)}}$$

Notice now, that $y^2$ is set equal to a quartic, which still doesn't quite match up with our previously established notion of elliptic curves. This can be resolved with a change of variables courtesy of [8]:

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

Now, let

$$x_1 = \frac{2(y+1)}{x^2}$$
$$y_1 = \frac{4(y+1) + 2(k^2+1)x^2}{x^3}$$

This change of variables will satisfy the equation:

$$y_1^2 = x_1^3 - (k^2+1)x_1^2 - 4k^2x_1 + 4k^2(k^2+1)$$

Which as we know from earlier chapters may be simplified to the Weierstrass equation $y^2 = x^3 + Ax + B$ for properly chosen constants $A$ and $B$.

## 7.2 $\mathbb{C}/L$ as a Group

Before going futher, we will take some time to look further at the field of complex numbers mod some lattice $L$. First, some definitions:

**Definition 7.2** For $\omega_1, \omega_2$ linearly independent complex numbers over $\mathbb{R}$, the set $L = \{n_1\omega_1 + n_2\omega_2 | n_1, n_2 \in \mathbb{Z}\}$ is called a *lattice*.

**Proposition 7.3** *The lattice* $L = \{n_1\omega_1 + n_2\omega_2 | n_1, n_2 \in \mathbb{Z}\}$ *is a normal additive subgroup of* $\mathbb{C}$.

**Proof:** First note that since $\mathbb{C}$ is an additive abelian group, then any subgroup will be normal. It thus suffices to show closure and inverses in $L$.
Let $n_1\omega_1 + n_2\omega_2, n_3\omega_1 + n_4\omega_2 \in L$. Then $(n_1\omega_1 + n_2\omega_2) + (n_3\omega_1 + n_4\omega_2) = (n_1+n_3)\omega_1 + (n_2+n_4)\omega_2 \in L$, so we have closure under addition.
Further, for a given $a = n_1\omega_1 + n_2\omega_2 \in L$, let $-a = (-n_1)\omega_1 + (-n_2)\omega_2$. We then get that $a + (-a) = 0\omega_1 + 0\omega_2 = 0$. We thus have inverses, and therefore $L$ is an additive normal subgroup of $\mathbb{C}$. ∎

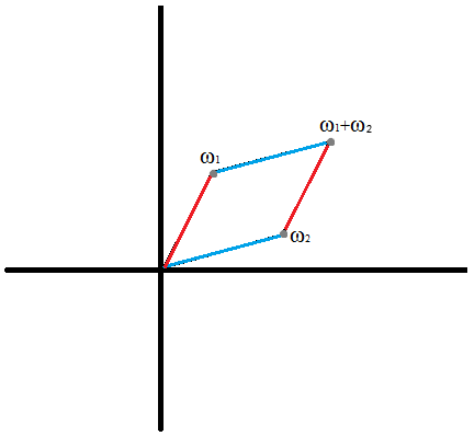
Consider now the quotient group $\mathbb{C}/L$. Elements will be of the form $z + L$ for $z \in \mathbb{C}$. For purposes of representing the cosets, we define the following set:

**Definition 7.4**

Figure 7.2

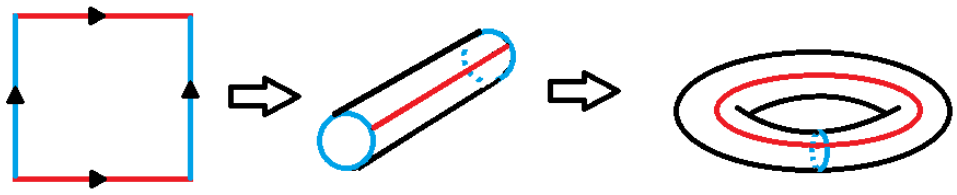
$F = \{a_1\omega_1 + a_2\omega_2 | 0 \leq a_i < 1, i = 1, 2\}$

This set is called the *fundamental parallelogram* for the given lattice $L$.




Note that opposite edges of the fundamental parallelogram are in the same equivalence class. This causes the fundamental parallelogram to appear (abstractly) as the following topological plane model which, as shown, is really just a torus:

Figure 7.3: Fundamental Parallelogram to Torus



It is worth noting that we could have constructed a similar picture with the finite field of size 19 from chapter 4. In that case, the fundamental parallelogram was really just the 19x19 square of points with integer coordinates in quadrant 1 with the lower left corner at the origin.

Consider now, the torsion subgroups in $\mathbb{C}/L$. While the previous definition of Torsion in Chapter 3 was specific to elliptic curves, the more general definition

is analgous: for a group $G$, the $n$-torsion points of $G$ denoted $G[n]$ is the set of points $P$ in $G$ such that $nP = I$ where $I$ is the identity element of $G$.
Consider then the case of $\mathbb{C}/L[2]$. This is pretty clearly

$$\{0, \omega_1/2, \omega_2/2, (\omega_1 + \omega_2)/2\}$$

. Similarly, we may find $\mathbb{C}/L[3]$ to be $\{0, \frac{\omega_1}{3}, \frac{2\omega_1}{3}, \frac{\omega_2}{3}, \frac{2\omega_2}{3}, \frac{\omega_1+\omega_2}{3}, \frac{2(\omega_1+\omega_2)}{3}, \frac{2\omega_1+\omega_2}{3}, \frac{\omega_1+2\omega_2}{3}\}$.

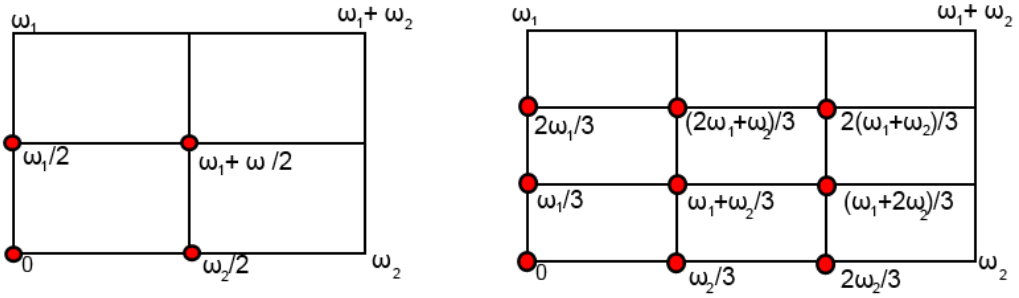



Figure 7.4: Pictorial representation of $\mathbb{C}/L[2]$ and $\mathbb{C}/L[3]$.

From these examples, we may determine a more general statement about $\mathbb{C}/L[n]$.

$$\mathbb{C}/L[n] = \left\{ \frac{l\omega_1 + m\omega_2}{n} \middle| l, m \in \mathbb{Z}, 0 \leq l, m < n \right\} \tag{7.4}$$

## 7.3 Doubly Periodic Functions and Elliptic Curves

In this section, we will begin by looking at some properties of doubly periodic functions, and then make the connection to elliptic curves To begin our discussion here first consider the result from calculus:
The circular integral $\int_0^w \frac{dx}{\sqrt{1-x^2}} = \sin^{-1}(w)$ has inverse function $w = sin(z)$, which is periodic over a period of $2\pi$.

Consider now an elliptic integral of the first kind after we transform our denominator as in the section 7.1:

$$\int_{\alpha}^{w} \frac{dx}{\sqrt{x^3 + Ax + B}}$$

This integral is a complex line integral with all variables complex numbers. The integral is along any curve from $\alpha$ to $\omega$ avoiding the zeroes of $x^3 + Ax + B$. It turns out we can do a somewhat analgous thing here as with the circular integral, where this integral has an inverse function, $\wp(z)$, but this function is doubly periodic, which is to say that it has two complex periods $\omega_1$ and $\omega_2$ such that:

$$\wp(z + \omega_1) = \wp(z) = \wp(z + \omega_2)$$

This double period lines up with our previously established notion of lattices. Further, note that by double periodicity the inputs for the $\wp$ function could be taken to be elements of $\mathbb{C}/L$.

**Definition 7.5** A meromorphic function $f : \mathbb{C} \to \mathbb{C} \cup \infty$ such that $f(z + \omega) = f(z)$ for all $z \in \mathbb{C}$ and all $\omega \in L$ is called a *doubly periodic function* or *elliptic function.*

For future use it is also worth mentioning the following facts:

**Proposition 7.6** *Let $f$ be a doubly periodic function with no poles in $\mathbb{C}$. Then $f$ is constant.*

This is really just an application of Liouville's theorem from complex analysis, which states that every bounded function, which is analytic everywhere on $\mathbb{C}$, is constant. In this case, since $f$ is bounded on the funcamental domain and $f$ is doubly periodic, we get that it is analytic and bounded on $\mathbb{C}$.

**Proposition 7.7** *If $f$ is a non-constant doubly periodic function, then $f$ must be surjective.*

**Proof:** Assume $f$ is not surjective. Then there is some $\omega$ not in the image of $f$. We thus have that $1/(f(z)-\omega)$, a doubly periodic function with no pole. By Proposition 7.6, then $1/(f(z)-\omega)$ is constant which implies that $f(z)$ is constant, hence $f$ must have been surjective. ∎

In order to make the connection to elliptic curves we will need to introduce a new doubly periodic function.

**Definition 7.8** Given a lattice, $L$, define the *Weierstrass $\wp$-function* by

$$\wp(z;L) = \frac{1}{z^2} + \sum_{\omega \in L, \omega \neq 0} \left( \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right) \tag{7.5}$$

While $\wp$ is really just a function of $z$, we include $L$ in the argument to reinforce the notion that this is defined over a specific given lattice.

For future use we will also define the following:

**Definition 7.9** For $k \geq 3$, let $G_k$ be defined as follows:

$$G_k = G_k(L) = \sum_{l \in L-0} l^{-k}$$

Note that this series is absolutely convergent since $k \geq 3$.

Further, using the notation in Definition 7.9 we get the following from [1].

**Proposition 7.10** *For $0 < |z| < \min_{l \in L-0}(|l|)$,*

$$\wp(z) = z^{-2} + \sum_{j=1}^{\infty} (2j+1) G_{2j+2} z^{2j}$$

While the Weierstrass $\wp$-function possesses many many nice properties, the primary one which we are concerned with is the following:

**Theorem 7.11** *The Weierstrass $\wp$-function satisfies:*

$$\wp'(z)^2 = 4\wp(z)^3 + A\wp(z) + B$$

*for properly chosen values of $A$ and $B$.*

**Proof:** This proof will pull heavily from some results in analysis outlined in [1]. From Proposition7.10, we get the following for $z \neq 0$ but sufficiently close to 0:

$$\wp(z) = z^{-2} + 3G_4 z^2 + 5G_6 z^4 + ...$$
$$\wp'(z) = -2z^{-3} + 6G_4 z + 20G_6 z^3 + ...$$

Cubing and squaring (respecitvely) yields:

$$\wp^3(z) = z^{-6} + 9G_4 z^{-2} + 15G_6 + ...$$
$$\wp'^2(z) = 4z^{-6} - 24G_4 z^{-2} - 80G_6 + ...$$

Now, define $f(z)$ as

$$f(z) = \wp'^2(z) - 4\wp^3(z) + 60G_4\wp(z) + 140G_6 \tag{7.6}$$

Using the results above, we find that $f(z) = c_1 z + c_2 z^2 + ...$ for constants $c_1, c_2, ....$ $f(z)$ is thus a power series, with no negative powers of $z$ nor any constant term. Since $f(z)$ is just a sum of multiples of $\wp$ and $\wp'$, the only possible poles of $f(z)$ will be the poles of $\wp(z)$ or $\wp'(z)$. We can see by the definition of $\wp$ and $\wp'$ that these poles (if they exist) will have to be elements of the lattice $L$.Since 0 is not a pole by (7.6), then $f(z)$ has no poles. Now,

from Proposition 7.6, $f(z)$ must be constant. Noting that $f(0) = 0$ then $f(z)$ must be identically 0. Thus,

$$\wp'(z)^2 = 4\wp(z)^3 + A\wp(z) + B$$

for $A = 60G_4$ and $B = 140G_6$. ∎

This in hand, we may now consider the main point of this section:

**Theorem 7.12** *For a given lattice $L = \{n_1\omega_1 + n_2\omega_2 | n_1, n_2 \in \mathbb{Z}\}$, and Weierstrass $\wp$-function on that lattice, as well as a given Elliptic Curve $E(\mathbb{C})$ described by $y^2 = 4x^3 + Ax + B$, the map $\Phi : \mathbb{C}/L \to E(\mathbb{C})$ is an isomorphism of groups, where $\Phi$ is defined by:*

$$z \to (\wp(z), \wp'(z)) \text{ for } z \neq 0$$
$$0 \to \infty$$

**Proof:** For $\Phi$ to be a homomorphism, we must have that, $\Phi(z_1 + z_2) = \Phi(z_1) +_E \Phi(z_2)$. In order to utilize the previously established notions of elliptic curve addition, we will need to eliminate the coefficient on the $x^3$ term. Via the change of variables $y \to y/2$, we get a new curve:

$$E_1(\mathbb{C}) : y^2 = x^3 + A_1x + B_1$$

where $A_1 = A/4$ and $B_1 = B/4$.
Note that $E_1$ and $E$ are isomorphic via the map $(x, y) \to (x, y/2)$. Thus, if we can show that $\mathbb{C}/L$ is isomorphic to $E_1$ we will get the desired result. To do this we need a new map $\Phi_1$:

$$z \to \left(\wp(z), \frac{\wp'(z)}{2}\right) \text{ for } z \neq 0$$
$$0 \to \infty$$

In order to show $E_1(\mathbb{C}) \simeq \mathbb{C}/L$ we will need to look at multiple cases.

Case 1: $z_1 = z_2 = 0$

$$\Phi_1(0+0) = \Phi_1(0) = \infty = \infty +_E \infty = \Phi_1(0) +_E \Phi_1(0)$$

Case 2: $z_1 = 0$ and $z_2 \neq 0$

$$\Phi_1(0+z_2) = \Phi_1(z_2) = \infty +_E \Phi_1(z_2) = \Phi_1(0) +_E \Phi_1(z_2)$$

Case 3: $z_1 = z_2 \neq 0$

Since $\Phi_1(z) = (\wp(z), \wp'(z)/2)$ and $E_1$ is defined by $y^2 = x^3 + A_1 x + B_1$, we may now use the addition formulas for the Weierstrass equation.

For the x-coordinate of $2\Phi_1(z)$, we may look at the doubling formula (part 3 of Definition 2.7) with $x_1 = \wp$ and $y_1 = \wp'/2$. We thus get that the x-coordinate for $2\Phi_1(z)$ is (with the arguments ommitted for clarity):

$$\left(\frac{3\wp^2 + A_1}{\wp'}\right)^2 - 2\wp$$

We would like to show that this is in fact the same as the $x$-coordinate of $\Phi_1(2z)$, specifically we must show that

$$\wp(2z) = \left(\frac{3\wp^2 + A_1}{\wp'}\right)^2 - 2\wp$$

From [11], we have that

$$\wp(2z) = \frac{1}{4}\frac{\wp''^2(z)}{\wp'^2(z)} - 2\wp(z) \tag{7.7}$$

Recall that $\wp'(z)^2 = 4\wp(z)^3 + A\wp(z) + B$ so differentiation gives us:

$$\frac{d}{dz}\wp'(z)^2 = \frac{d}{dz}(4\wp(z)^3 + A\wp(z) + B)$$

$$2\wp'\wp'' = 12\wp^2\wp' + A\wp'$$

$$\wp''(z) = 6\wp^2 + 2A_1 \tag{7.8}$$

Combining (7.7) with (7.8) gives:

$$\begin{aligned}\wp(2z) &= \frac{1}{4}\frac{(6\wp^2+2A_1)^2}{\wp'^2} - 2\wp \\ &= \left(\frac{3\wp^2+A_1}{\wp'}\right)^2 - 2\wp\end{aligned}$$

Thus, the $x$-coordinate of $2\Phi_1(z)$ is the same as the $x$-coordinate of $\Phi_1(2z)$.

With regards to the $y$-coordinate of $2\Phi_1(z)$, we again use our doubling formulas from Definition 2.7, which yields:

$$\left(\frac{3\wp^2+A_1}{\wp'}\right)\left(3\wp - \left(\frac{3\wp^2+A_1}{\wp'}\right)^2\right) - \frac{\wp'}{2}$$

Since the $y$-coordinate of $\Phi_1(2z) = \wp'(2z)/2$ we must show that

$$\wp'(2z)/2 = \left(\frac{3\wp^2+A_1}{\wp'}\right)\left(3\wp - \left(\frac{3\wp^2+A_1}{\wp'}\right)^2\right) - \frac{\wp'}{2}$$

To do this, we will need a grasp of $\wp'(2z)$:

$$\begin{aligned}\frac{d}{dz}\wp(2z) &= \frac{d}{dz}\left[\left(\frac{3\wp^2+A_1}{\wp'}\right)^2 - 2\wp\right] \\ 2\wp'(2z) &= 2\left(\frac{3\wp^2+A_1}{\wp'}\right)\frac{6\wp\wp'^2 - \wp''(3\wp^2+A_1)}{\wp'^2} - 2\wp' \\ \wp'(2z) &= \left(\frac{3\wp^2+A_1}{\wp'}\right)\left(6\wp - \frac{(6\wp^2+2A_1)(3\wp^2+A_1)}{\wp'^2}\right) - \wp' \\ &= \left(\frac{3\wp^2+A_1}{\wp'}\right)\left(6\wp - \frac{2(9\wp^4+6A_1\wp^2+A_1^2)}{\wp'^2}\right) - \wp' \\ &= 2\left(\frac{3\wp^2+A_1}{\wp'}\right)\left(3\wp - \frac{(3\wp^2+A_1)^2}{\wp'^2}\right) - \wp'\end{aligned}$$

We thus get that

$$\frac{\wp'(2z)}{2} = \left(\frac{3\wp^2+A_1}{\wp'}\right)\left(3\wp - \frac{(3\wp^2+A_1)^2}{\wp'^2}\right) - \frac{\wp'}{2}$$

Combining these results gives us that:

$$2\Phi_1(z) = (\wp(z), \wp'(z)/2) +_E (\wp(z), \wp'(z)/2) = (\wp(2z), \wp'(2z)/2) = \Phi_1(2z)$$

Case 4: $z_1 \neq z_2$ and neither is 0.

For this case, we want to show that the $x$ and $y$ coordinates of $\Phi_1(z_1) +_E \Phi_1(z_2)$ and $\Phi_1(z_1 + z_2)$ are the same. For the $x$-coordinates, again appealing to Definition 2.7, we get that the $x$-coordinate of $\Phi_1(z_1) +_E \Phi_1(z_2)$ is

$$\left(\frac{\wp'(z_1)/2 - \wp'(z_2)/2}{\wp(z_1) - \wp(z_2)}\right)^2 - \wp(z_1) - \wp(z_2)$$

We want this to be equal to $\wp(z_1 + z_2)$, the $x$-coordinate of $\Phi_1(z_1 + z_2)$.

A result from [11] states that:

$$\wp(z_1 + z_2) = \frac{1}{4}\left(\frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}\right)^2 - \wp(z_1) - \wp(z_2) \tag{7.9}$$

Consider then for $\Phi_1(z_1 + z_2)$, the $x$-coordinate will look like (7.9), giving us:

$$\begin{aligned}&\frac{1}{4}\left(\frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}\right)^2 - \wp(z_1) - \wp(z_2)\\ =&\left(\frac{\wp'(z_1)/2 - \wp'(z_2)/2}{\wp(z_1) - \wp(z_2)}\right)^2 - \wp(z_1) - \wp(z_2)\end{aligned}$$

which is precisely the $x$-coordinate of $\Phi_1(z_1) +_E \Phi_2(z_2)$.

The $y$-coordinate of $\Phi_1(z_1) +_E \Phi_1(z_2)$ will look like:

$$\left(\frac{\wp'(z_1)/2 - \wp'(z_2)/2}{\wp(z_1) - \wp(z_2)}\right)\left[2\wp(z_2) - \left(\frac{\wp'(z_1)/2 - \wp'(z_2)/2}{\wp(z_1) - \wp(z_2)}\right)^2 + \wp(z_1)\right] - \frac{\wp'(z_2)}{2}$$

We want to show that this is in fact equal to $\wp'(z_1 + z_2)/2$. We will proceed by starting with (7.9), and differentiating with respect to $z_2$.

$$\begin{aligned}\wp'(z_1 + z_2) &= \frac{1}{2}\left(\frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}\right)\left(\frac{-\wp''(z_2)(\wp(z_1) - \wp(z_2)) + \wp'(z_2)(\wp'(z_1) - \wp'(z_2))}{(\wp(z_1) - \wp(z_2))^2}\right) - \wp'(z_2)\\ &= \frac{1}{2}\left(\frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}\right)\left(\frac{-(6\wp^2(z_2) + 2A_1)(\wp(z_1) - \wp(z_2)) + \wp'(z_2)(\wp'(z_1) - \wp'(z_2))}{(\wp(z_1) - \wp(z_2))^2}\right) - \wp'(z_2)\\ &= \frac{1}{2}\left(\frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}\right)\left(\frac{-(6\wp^2(z_2) + 2A_1)(\wp(z_1) - \wp(z_2)) + \wp'(z_2)(\wp'(z_1) - \wp'(z_2))}{(\wp(z_1) - \wp(z_2))^2}\right) - \wp'(z_2)\end{aligned}$$

Looking at just the numerator of the middle, we get:

$$
\begin{aligned}
&6\wp^3(z_2) + 2A_1\wp(z_2) - 6\wp^2(z_2)\wp(z_1) - 2A_1\wp(z_1) + \wp'(z_2)(\wp'(z_1) - \wp'(z_2)) \\
=&6\wp^3(z_2) + 2A_1\wp(z_2) - 6\wp^2(z_2)\wp(z_1) - \frac{1}{2}(\wp'^2(z_1) - \\
&\qquad 4\wp^3(z_1) - B) + \wp'(z_2)(\wp'(z_1) - \wp'(z_2)) \\
=&2\wp^3(z_2) + 2A_1\wp(z_2) + \frac{B}{2} + 4\wp^3(z_2) - 6\wp^2(z_2)\wp(z_1) - \\
&\qquad \frac{1}{2}\wp'^2(z_1) + 2\wp^3(z_1) + \wp'(z_2)(\wp'(z_1) - \wp'(z_2)) \\
=&\frac{1}{2}\wp'^2(z_2) + 4\wp^3(z_2) - 4\wp^2(z_2)\wp(z_1) - \frac{1}{2}\wp'^2(z_1) + 2\wp^3(z_1) - \\
&\qquad 2\wp^2(z_2)\wp(z_1) + \wp'(z_2)(\wp'(z_1) - \wp'(z_2)) \\
=&\frac{1}{2}\wp'^2(z_2) + 4\wp^3(z_2) - 4\wp^2(z_2)\wp(z_1) - \frac{1}{2}\wp'^2(z_1) + 2\wp(z_1)[\wp^2(z_1) - \wp^2(z_2)] - \\
&\qquad \wp'^2(z_2) + \wp'(z_2)\wp'(z_1) \\
=&-\frac{1}{2}\wp'^2(z_2) + \wp'(z_2)\wp'(z_1) - \frac{1}{2}\wp'^2(z_1) + 4\wp^3(z_2) - \\
&\qquad 4\wp^2(z_2)\wp(z_1) + 2\wp(z_1)[\wp^2(z_1) - \wp^2(z_2)] \\
=&-\frac{1}{2}(\wp'(z_1) - \wp'(z_2))^2 + 2\wp(z_1)[\wp^2(z_1) - \wp^2(z_2)] + 4\wp^3(z_2) - 4\wp^2(z_2)\wp(z_1) \\
=&-\frac{1}{2}(\wp'(z_1) - \wp'(z_2))^2 + 2\wp^3(z_1) - 4\wp(z_2)\wp^2(z_1) + 2\wp(z_1)\wp^2(z_2) \\
&\qquad + 4\wp^3(z_2) - 8\wp^2(z_2)\wp(z_1) + 4\wp(z_2)\wp^2(z_1) \\
=&-\frac{1}{2}(\wp'(z_1) - \wp'(z_2))^2 + 2\wp(z_1)(\wp(z_1) - \wp(z_2))^2 + 4\wp(z_2)(\wp(z_1) - \wp(z_2))^2
\end{aligned}
$$

This results in

$$\wp'(z_1 + z_2) = \frac{1}{2}\left(\frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}\right)\left(2\wp(z_1) + 4\wp(z_2) - \frac{1}{2}\frac{(\wp'(z_1) - \wp'(z_2))^2}{(\wp(z_1) - \wp(z_2))^2}\right) - \wp'(z_2)$$

Dividing by 2 yields

$$\frac{\wp'(z_1 + z_2)}{2} = \left(\frac{\wp'(z_1)/2 - \wp'(z_2)/2}{\wp(z_1) - \wp(z_2)}\right)\left[2\wp(z_2) - \left(\frac{\wp'(z_1)/2 - \wp'(z_2)/2}{\wp(z_1) - \wp(z_2)}\right)^2 + \wp(z_1)\right] - \frac{\wp'(z_2)}{2}$$

Therefore $\Phi_1(z_1) +_E \Phi_1(z_2) = (\wp(z_1 + z_2), \wp'(z_1 + z_2)/2) = \Phi_1(z_1 + z_2)$.

It remains to show that $\Phi_1$ is one to one and onto.

For this we will need a Complex Analysis result from [1]:

**Proposition 7.13** *Let $f$ be a doubly periodic function for the lattice $L$, and let $F$ be a fundamental parallelogram for $L$. If $n$ is the sum of the orders of the poles of $f$ in $F$ and $z_0 \in \mathbb{C}$, then $f(z) = z_0$ has $n$ solutions counting multiplicities.*

Let $(x, y) \in E_1(\mathbb{C})$. From [1] we have that $\wp(z) - x$ has a double pole, implying it has zeroes. Thus there exists some $z \in \mathbb{C}$ such that $\wp(z) = x$. Consider that by our definition for $\wp$, we get that $\wp(z) = \wp(-z)$.

From Theorem 7.11, and our change of variables in this proof, we get that:

$$\left(\frac{\wp'(z)}{2}\right)^2 = y^2$$

We may thus say that $\wp'(z)/2 = \pm y$. If $\wp'(z)/2 = y$, we're done, and if $\wp'(z)/2 = -y$, then, $\wp'(-z)/ = y$. Recalling that $\wp(-z) = x$ in this case finishes the proof that $\Phi_1$ is onto, as we have either $z \to (x, y)$ or $-z \to (x, y)$.

Note: By the definition of $\Phi_1$, we have that the kernel of $\Phi_1$ is $\{0\}$. Since $\Phi_1$ is onto, and the kernel is 0, we have via the first isomorphism theorem that $\Phi_1$ is one to one.

Therefore, $\Phi_1$ is an isomorphism of groups, and we may thus say that $\mathbb{C}/L \simeq E(\mathbb{C})$. ∎

Of interest is the fact that while the map from $\mathbb{C}/L$ to $E(\mathbb{C})$ is realtively straightforward, the inverse bijection from $E(\mathbb{C})$ to $\mathbb{C}/L$ is non-trivial to determine. What's more, the torsion groups of $\mathbb{C}/L$ were much more straightforward to determine than their counterparts in $E$. Topologically speaking, we've

already seen that $\mathbb{C}/L$ forms a torus, however, $E$ itself is a complex algebraic curve.

At the end of the day, the ease with which one can work with the complex plane modded out by a lattice as compared to the same procedures on an elliptic curve proves to be one of the primary reasons elliptic curves can create such strong encryption. Elliptic curves inherently display properties of a classic trapdoor function (a function that is easy to do one way, but very difficult to determine its inverse without some special information). While this trapdoor isomorphism does not exist for finite fields, many of the motivating concepts for elliptic curves and their use in encryption stem from the behavior of $\mathbb{C}/L$.

# Bibliography


[1] Washington, Lawrence C. *Elliptic Curves: Number Theory and Cryptography.* 2nd ed.Boca Raton, FL: Chapman & Hall/CRC, 2008. Print.

[2] "Algebraic Curve." *Wikipedia*. Wikimedia Foundation, 07 Sept. 2012. Web. 17 July 2012. ¡http://en.wikipedia.org/wiki/Algebraic_curve¿.

[3] Bh, Padma, D. Chandravathi, and P. Prapoorna Roja. "Encoding And Decoding of a Message in the Implementation of Elliptic Curve Cryptography Using Koblitz's Method." *International Journal on Computer Science and Engineering* 02.05 (2010): 1904-907. *Google Docs*. Web. 17 July 2012.

[4] Segal, Sanford L. "Chapter 8." *Nine Introductions in Complex Analysis, Revised Edition*. Amsterdam: Elsevier, 2008. 300. Print.

[5] Rosen, Kenneth H. *Elementary Number Theory and Its Applications*. 5th ed. Boston: Pearson/Addison Wesley, 2005. Print.

[6] Hankerson, Darrel R., Scott A. Vanstone, and A. J. Menezes. *Guide to Elliptic Curve Cryptography*. New York: Springer, 2011. Print.

[7] Elgamal, T. "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms." *IEEE Transactions on Information Theory* 31.4 (1985): 469-72. Print.

[8] Connell, Ian. Elliptic Curve Handbook. N.p., Feb. 1999. Web. July 2012. ¡http://www.ucm.es/BUCM/mat/doc8354.pdf¿.

[9] Laval, Philippe B. "Cyclic Groups." N.p., 15 Mar. 2010. Web. 2 Nov.2012 ¡http://science.kennesaw.edu/ plaval/math4361/groups_cyclic.pdf¿

[10] Fulton, William. "Algebraic Curves." Math.lsa.umich.edu. N.p., 28 Jan. 2008. Web. 14 Jan. 2013. ¡http://www.math.lsa.umich.edu/ wfulton/CurveBook.pdf¿.

[11] Du Val, Patrick. "The Weierstrass Functions." Elliptic Functions and Elliptic Curves. Cambridge Eng.: University, 1973. N. Print.

Vita

Author: Samuel L. Wenberg

Place of Birth: Seoul, South Korea

Undergraduate Schools Attended: Gonzaga University

Degrees Awarded: Bachelor of Science, 2010, Gonzaga University