Elliptic Curves over Arithmetic Fields

Benjamin Keigwin

Contents

Introduction

Elliptic curves have been studied by mathematicians since the time of Diophantus. Their flexibility and versatility have allowed them to be examined from a variety of vantage points, yielding insight into complex analysis, algebraic geometry, and number theory. Indeed, the study of elliptic curves has contributed substantially to the accumulation of mathematical knowledge overall, and elliptic curves have been used in the proofs of extremely deep results. For example, building upon the work of Ribet et al., Taylor and Wiles proved Fermat's Last Theorem by showing that semistable elliptic curves are modular.

In this text, we discuss certain results on elliptic curves over arithmetically important fields such as $\mathbb{C}, \mathbb{F}_q$, and $\mathbb{Q}$. In the first chapter, we prove that for a complex elliptic curve E, the group of $\mathbb{C}$-rational points $E(\mathbb{C})$ as an abelian group is a torus (Theorem 1.3.3). To do this, we introduce some background on elliptic functions, and then define an explicit elliptic function known as the Weierstrass $\wp$ function that is then used to construct an isomorphism between $E(\mathbb{C})$ and $\mathbb{C}/\Lambda$ for a given lattice Λ. We will then restrict our study to conjugation-invariant lattices in order to show that for an elliptic curve over $\mathbb{R}$, that $E(\mathbb{R})$ is isomorphic to either S^1 or $\mathbb{Z}_2 \times S^1$ (Theorems 1.4.5 and 1.4.6).

In the second chapter, we turn our attention to elliptic curves over finite fields and provide a bound for the number of $\mathbb{F}_q$-rational points an elliptic curve may have. This bound, known as Hasse's inequality (Theorem 2.2.6), can be quite strict as we will demonstrate with a couple of examples. To prove Hasse's inequality, we will introduce the notion of the degree map and prove in Proposition 2.2.5 that $\#E(\mathbb{F}_q)$ is equal to the $\deg(\varphi_q - 1)$, where φ_q is the Frobenius endomorphism.

Lastly, we explore elliptic curves over $\mathbb{Q}$. We will begin with a discussion on the theory of heights, and then show that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite (Theorem 3.2.3). Using this result, known as the Weak Mordell-Weil theorem, and the theory of heights, we will prove the full Mordell-Weil theorem (Theorem 3.3.1), which states that $E(\mathbb{Q})$ is a finitely generated abelian group. We then close with a discussion on some extensions of Mordell-Weil, including the Birch and Swinnerton-Dyer conjecture, which relates the rank of an elliptic curve E over $\mathbb{Q}$ to the order of vanishing at $s = 1$ of the L-function $L(E, s)$ of E. This conjecture, if true, would lend a lot of insight into the theory of elliptic curves, and would provide an effective means of finding generators for $E(\mathbb{Q})$.

Background Information

We start by recalling some information on elliptic curves that will be necessary for the remainder of the paper.

We first recall the definition of an elliptic curve:

Definition. Let K be a field, then an *elliptic curve* E over K is a curve $E \subset \mathbb{P}^2$ defined by the homogenization of smooth plane cubic

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{0.1}$$

We call equation (0.1) and its homogenization

$$Y^2Z + a_1XYZ + a_3XZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

the *Weierstrass equation* of E.

In the previous definition, we identify the affine plane $\mathbb{A}^2$ with

$$\{[X : Y : Z] \in \mathbb{P}^2 | Z \neq 0\},$$

and we call the unique point $\mathcal{O} := [0 : 1 : 0]$ on E not in $\mathbb{A}^2$ the *point at infinity*. In the case that the field K is also of characteristic $\neq 2, 3$, then after a linear change of variables we may assume the smooth plane cubic defining an elliptic curve E is of the form $y^2 = x^3 + ax + b$, where $a, b \in K$ and $x^3 + ax + b$ does not have multiple roots.

Example.

1. Let $K = \mathbb{C}$, then the projective curve defined by the homogenization of $y^2 = x^3 - 7x - 6$ is an elliptic curve.

2. Let $K = \mathbb{C}$, then the projective curve defined by $y^2 = x^3 + 4x^2 + 5x + 2 = (x+1)^2(x+2)$ is not an elliptic curve, as the cubic in x has multiple roots.

3. Let $K = \overline{\mathbb{F}_{97}}$ where $\overline{\mathbb{F}_{97}}$ denotes the algebraic closure of $\mathbb{F}_{97}$. Then the projective curve defined by the homogenization of $y^2 = x^3 + 2$ is an elliptic curve.

On the points of an elliptic curve E over a field K, we may define a group law as follows:

1. Let P, Q be distinct points on E. Then by Bezout's theorem [7, Theorem 1], the line PQ intersects E at precisely three points: P, Q, and one additional point that we will denote $P * Q$.

2. If $P = Q$, the line PQ is defined as the tangent line to E at P, and we still denote the additional point of intersection $P * Q$

3. The point $\mathcal{O}$ on E is an inflection point [2, page 10], so in particular, $\mathcal{O} * \mathcal{O} = \mathcal{O}$.

4. For a point P on E, denote by $-P$ the third point of intersection of the line $P\mathcal{O}$ with E.

5. For two points P, Q on E, define $P + Q := \mathcal{O} * (P * Q)$

Proposition. The operation $+$ makes E into an abelian group with identity element $\mathcal{O}$

Proof. Associativity requires some work (see [2, Theorem 6]), but the other axioms are a bit easier to establish.
For points P, Q on E, the lines PQ and QP are the same, so the operation is commutative. Next, for P on E,

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

so $\mathcal{O}$ is the identity. For a point P, the point $-P$ as defined in item 4 is its inverse:

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

In particular, for an affine point P on an elliptic curve E, the point $-P$ is the reflection of P about the x-axis. Hence, E is an abelian group under $+$. $\square$

We can actually say a bit more than just that the points of E form an abelian group. In fact, the group law is also given by everywhere defined rational functions [4, page 54]. That is for affine points, we have the following formulas:

$$P_1, P_2, P_3 \in E \text{ with } P_1 + P_2 = P_3 \text{ and } P_i = (x_i, y_i)$$
$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$$
$$y_3 = -(\lambda + a_1)x_3 - \nu - a_3,$$

Then

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$$
$$y_3 = -(\lambda + a_1)x_3 - \nu - a_3,$$

	λ	ν
$x_1 \neq x_2$	$\dfrac{y_2 - y_1}{x_2 - x_1}$	$\dfrac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$
$x_1 = x_2$	$\dfrac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3}$	$\dfrac{-x_1^3 + a_4 x_1 + 2a_6 - a_3 y_1}{2y_1 + a_1 x_1 + a_3}$

In particular, the group law yields a group structure on rational points over any field that contains the field K of definition of an elliptic curve E, as the above functions all have coefficients in K. The formula for x_3 when $x_1 = x_2$ is also called the *duplication formula*

If L contains the field of definition K, we denote by $E(L)$ the set of L-rational points of E, that is the points on E where each coordinate of the point is in L. Then $E(L)$ is also an abelian group by the proposition, and if $L|M$ is a field extension where both contain K, then $E(M)$ is a subgroup of $E(L)$.
It is worth mentioning also what the points of order 2 on an elliptic curve are. We also have the following result that can sometimes be useful:

Proposition. Let E be an elliptic curve over a field K, and let $P, Q, R \in E$ be colinear. Then $P + Q + R = \mathcal{O}$.

Proof. We have

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

$$= \mathcal{O} * \mathcal{O} = \mathcal{O},$$

which proves the result. □

This concludes the background information.

Chapter 1

Elliptic Curves over $\mathbb{C}$ and $\mathbb{R}$

The aim of this chapter is to show for an elliptic curve E over $\mathbb{C}$, that as an abelian group, $E(\mathbb{C})$ is isomorphic to a torus $\mathbb{C}/\Lambda$, for a lattice $\Lambda \subset \mathbb{C}$. We begin by discussing some necessary facts from the theory of elliptic functions and then focus on a specific elliptic function, the Weierstrass $\wp$ function, in the second section. In the third section, we construct our explicit isomorphism between $E(\mathbb{C})$ and $\mathbb{C}/\Lambda$. In the final section, we turn our attention to real elliptic curves, and show that for an elliptic curve E over $\mathbb{R}$, $E(\mathbb{R})$ is isomorphic to either the circle S^1 or $\mathbb{Z}_2 \times S^1$.

1.1 Background on Elliptic Functions

We begin with the following definition:

Definition 1.1.1. Let $\omega_1, \omega_2 \in \mathbb{C}$ be two elements that are linearly independent over $\mathbb{R}$. A function $f : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$ is called *elliptic* with respect to the periods ω_1 and ω_2, if f is meromorphic and $f(z + \omega_1) = f(z + \omega_2) = f(z)$ for all $z \in \mathbb{C}$.

To any such ω_1, ω_2 that are linearly independent over $\mathbb{R}$, we associate the set $\Pi := \{t_1\omega_1 + t_2\omega_2 \mid t_1, t_2 \in [0, 1)\}$, known as the *fundamental parallelogram.* Given $\alpha \in \mathbb{C}$, we denote by Π_α the set $\{\alpha + x \mid x \in \Pi\}$, called the *period parallelogram* corresponding to α.

Proposition 1.1.2. *If f is an entire elliptic function, then f is constant.*

Proof. Let Π be the fundamental parallelogram for the periods corresponding to f. Then as f is entire, f is holomorphic on the closure $\overline{\Pi}$ of Π. As $\overline{\Pi}$ is compact, f is thus bounded on $\overline{\Pi}$, and hence f is bounded on all of $\mathbb{C}$ since f is elliptic. Therefore by Liousville's theorem, f is a constant function. $\square$

Proposition 1.1.3. *Let f be an elliptic function, and $\alpha \in \mathbb{C}$ such that the boundary $\partial\Pi_\alpha$ of Π_α contains no poles of f. Then the sum of the residues of f inside Π_α is zero.*

Proof. Let $\operatorname{res}_z f$ denote the residue of f at a point $z \in \mathbb{C}$. Then by the residue theorem, we have

$$\frac{1}{2\pi i} \int\limits_{\partial\Pi_\alpha} f(z)\, dz = \sum_{z \in \Pi_\alpha} res_z f, \tag{1.1.1}$$

thus it suffices to show that the integral on the left-hand side is zero. Next, observe

$$\int\limits_{\alpha}^{\alpha+\omega_1} f(z)\, dz + \int\limits_{\alpha+\omega_1+\omega_2}^{\alpha+\omega_2} f(z)\, dz = \int\limits_{\alpha}^{\alpha+\omega_1} f(z)\, dz + \int\limits_{\alpha+\omega_1}^{\alpha} f(z+\omega_2)\, dz,$$

as f is elliptic, the integrand in the second integral on the right side is $f(z)$. Hence, the entire right side is zero as the two integrals cancel. Similarly,

$$\int\limits_{\alpha+\omega_1}^{\alpha+\omega_1+\omega_2} f(z)\, dz + \int\limits_{\alpha+\omega_2}^{\alpha} f(z)\, dz = 0,$$

and therefore since

$$\int\limits_{\partial\Pi_\alpha} f(z) = \int\limits_{\alpha}^{\alpha+\omega_1} f(z)\, dz + \int\limits_{\alpha+\omega_1}^{\alpha+\omega_1+\omega_2} f(z)\, dz + \int\limits_{\alpha+\omega_1+\omega_2}^{\alpha+\omega_2} f(z)\, dz + \int\limits_{\alpha+\omega_2}^{\alpha} f(z)\, dz,$$

we have that the left-hand side of (1.1.1) is zero, and so the proposition follows.

□

Proposition 1.1.4. *Let f be an elliptic function, and $\alpha \in \mathbb{C}$ such that the boundary $\partial\Pi_\alpha$ of Π_α contains no poles of f. Let $\{m_i\}$ and $\{n_j\}$ denote the orders of the zeros and poles respectively inside Π_α. Then $\sum_i m_i = \sum_j n_j$.*

Proof. Let $g(z) = f'(z)/f(z)$, then as f is elliptic so too is f' and hence g is also an elliptic function. We claim that if f has order m at z_0, then $res_{z_0} g = m$. To begin, if $m = 0$, then $f(z_0) \neq 0$, and thus g is holomorphic at z_0, so $res_{z_0} g = 0$. Next, suppose $m \neq 0$, then we may write $f(z) = (z - z_0)^m h_1(z)$, where h_1 is a holomorphic function that does not vanish at z_0. By differentiating, this equality, we obtain $f'(z) = m(z - z_0)^{m-1} h_1(z) + (z - z_0)^m h_1'(z)$. Thus,

$$g(z) = \frac{m(z - z_0)^{m-1} h_1(z) + (z - z_0)^m h_1'(z)}{(z - z_0)^m h_1(z)} = \frac{m}{z - z_0} + \frac{h_1'(z)}{h_1(z)}.$$

Therefore, $res_{z_0} g = m$. By the previous proposition, as g has no poles or zeros on $\partial\Pi_\alpha$, we have

$$\sum_i m_i - \sum_j n_j = \sum_{z_0 \in \Pi_\alpha} res_{z_0} g = 0.$$

Hence, $\sum_i m_i = \sum_j n_j$. □

We now introduce the Weierstrass $\wp$ function, which we will use to calculate $E(\mathbb{C})$ as an abelian group for a complex elliptic curve.

1.2 Weierstrass $\wp$ function

We start with the following definition:

Definition 1.2.1. Let f be an elliptic function. The *order* of f is the number of zeros of f inside of Π_α for an $\alpha \in \mathbb{C}$ such that $\partial\Pi_\alpha$ contains no poles of f.

For a function f that is elliptic with respect to two periods ω_1, ω_2 that are linearly independent over $\mathbb{R}$, we can define a certain lattice $\Lambda \subset \mathbb{C}$ depending on these periods:

Definition 1.2.2. Let $\omega_1, \omega_2 \in \mathbb{C}$ be linearly independent over $\mathbb{R}$. Define $\Lambda(\omega_1, \omega_2) := \{m\omega_1 + n\omega_2 \mid m, n \in \mathbb{Z}\}$, then Λ is called the *period lattice* of ω_1 and ω_2.

When it is clear from context, often times we will omit the ω_1 and ω_2 and simply write Λ for $\Lambda(\omega_1, \omega_2)$. Similarly, when referring to a period lattice $\Lambda(\omega_1, \omega_2)$, we assume that ω_1 and ω_2 are linearly independent over $\mathbb{R}$. Note that if f is elliptic with respect to ω_1 and ω_2, then

$$f(z + \omega) = f(z) \text{ for all } \omega \in \Lambda(\omega_1, \omega_2).$$

Hence, if f is elliptic with respect to two periods ω_1 and ω_2, we will also write that f is elliptic with respect to $\Lambda = \Lambda(\omega_1, \omega_2)$.

The goal of the first part of this section is to prove that the following function is an elliptic function of order 2:

Definition 1.2.3. Let $\omega_1, \omega_2 \in \mathbb{C}$ be linearly independent over $\mathbb{R}$ with period lattice Λ. The *Weierstrass* $\wp$ function corresponding to Λ is

$$\wp(z) := \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left[\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right]$$

We begin with the following result:

Proposition 1.2.4. *Let $\Lambda := \Lambda(\omega_1, \omega_2)$ be a period lattice. For any real number $s > 2$,*

$$\sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{|\omega|^s}$$

converges.

Proof. Let

$$\widetilde{\Pi} := \Pi \cup (\Pi_{-\omega_1}) \cup (\Pi_{-\omega_2}) \cup (\Pi_{-\omega_1 - \omega_2})$$

be the union of the four translates of Π which surround the origin, and let $\partial\widetilde{\Pi}$ be the boundary of $\widetilde{\Pi}$. Then $\partial\widetilde{\Pi}$ is compact and does not contain 0, so there exists $c > 0$ such that for all $z \in \partial\widetilde{\Pi}$, $|z| \geq c$. Let $\omega = m\omega_1 + n\omega_2 \in \Lambda$ be such that $|m| \geq |n| > 0$, then we have

$$|\omega| = |m\omega_1 + n\omega_2| \geq |m| \cdot \left|\omega_1 + \frac{n}{m}\omega_2\right| \geq |m|c.$$

Similarly, if ω is such that $|n| \geq |m| > 0$, then $|w| \geq |n|c$. If either $m = 0$ or $n = 0$, then $|m\omega_1 + n\omega_2| \geq c\cdot \max(|m|, |n|)$, and so in general, for all $\omega = m\omega_1 + n\omega_2 \in \Lambda$, we have $|w| \geq c\cdot \max(|m|, |n|)$.

Next, observe for each $N \in \mathbb{N}$, the number of $(m, n) \in \mathbb{Z}^2$ such that $\max(|m|, |n|) = N$ is less than or equal to $8N$, therefore

$$\sum_{\omega\in\Lambda\backslash\{0\}} \frac{1}{|\omega|^s} = \sum_{m,n\in\mathbb{Z}^2\backslash(0,0)} \frac{1}{|m\omega_1 + n\omega_2|^s} \leq \sum_{M=1}^{\infty} \frac{8M}{c^s M^s}.$$

The series on the right hand side converges since $c > 0$ is constant, and $s-1 > 1$ since $s > 2$, so the proposition follows. □

Proposition 1.2.5. *The series defining $\wp(z)$ converges absolutely and uniformly on every compact subset of $\mathbb{C}\backslash\Lambda$. Moreover, $\wp(z)$ is a meromorphic function and its poles are precisely the elements of Λ, each of which is a pole of order 2.*

Proof. Let $\omega \in \Lambda$ be such that $|\omega| > 2|z|$, then we have

$$\left|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right| = \left|\frac{2\omega z - z^2}{(z-\omega)^2\omega^2}\right| \leq \frac{2|\omega||z| + |z|^2}{(|\omega| - |z|)^2|\omega|^2} \leq \frac{10|z|}{|\omega|^3}$$

Next, for each $z \in \mathbb{C}$, there are only finitely many $\omega \in \Lambda$ such that $\omega \leq 2|z|$, thus

$$\left|\frac{1}{z^2} + \sum_{\omega\in\Lambda\backslash\{0\}} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right]\right| < \infty$$

by the previous proposition. Therefore, by the Weierstrass M-test, $\wp(z)$ converges absolutely and uniformly on every compact subset of $\mathbb{C}\backslash\Lambda$.

As each term $\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}$ is holomorphic on $\mathbb{C}\backslash\Lambda$, and the series defining $\wp(z)$ converges uniformly, we also have $\wp(z)$ is holomorphic on $\mathbb{C}\backslash\Lambda$. Hence, $\wp(z)$ is meromorphic on $\mathbb{C}$, and the poles of $\wp(z)$ are precisely the elements of Λ, with each element contributing a pole of order 2 due to the term $\frac{1}{(z-\omega)^2}$. □

We may now prove that $\wp$ is elliptic of order 2.

Proposition 1.2.6. *$\wp(z)$ is an even elliptic function of order 2, and its derivative is*

$$-2\sum_{\omega\in\Lambda} \frac{1}{(z-\omega)^3}$$

which is an odd elliptic function.

Proof. The second statement follows from the first and the fact that the series defining $\wp(z)$ converges uniformly, and hence $\wp'(z)$ is equal to the term by term differentiation of $\wp(z)$. The result of this term by term differentiation is precisely the above sum, hence $\wp'(z)$ is an elliptic function.

To see that $\wp(z)$ is even, observe that

$$\wp(-z) = \frac{1}{(-z)^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left[\frac{1}{(-z-\omega)^2} - \frac{1}{\omega^2} \right] = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right] = \wp(z),$$

where the second equality follows since the series converges absolutely and hence the order of summation does not matter.

Next, consider the function $g(z) = \wp(z+\omega_1) - \wp(z)$. Differentiating both sides, we have $g'(z) = \wp'(z+\omega_1) - \wp'(z) \equiv 0$, since $\wp'(z)$ is an elliptic function with respect to the periods ω_1, ω_2 defining Λ. Therefore, $g(z)$ is constant, and $g(\frac{-\omega_1}{2}) = \wp(\frac{\omega_1}{2}) - \wp(\frac{-\omega_1}{2}) = 0$, since $\wp$ is even and $\frac{\omega_1}{2}$ is not a pole of $\wp$. Hence, $\wp(z+\omega_1) = \wp(z)$, and similarly $\wp(z+\omega_2) = \wp(z)$, so $\wp$ is an elliptic function. Lastly, as 0 is the only pole of $\wp$ inside Π, and it is a pole of order 2, we have that the order of $\wp$ is 2. □

It is also useful to know what the zeros of $\wp'(z)$ are:

Proposition 1.2.7.

1. *For any $u \in \mathbb{C}$, $g(z) := \wp(z) - u$ has either one double zero or two simple zeros inside Π.*

2. *The zeros of $\wp'(z)$ in Π are $\omega_1/2, \omega_2/2$ and $(\omega_1+\omega_2)/2$, each of which is a simple zero.*

3. *The values $u_1 = \wp(\omega_1/2), u_2 = \wp(\omega_2/2)$ and $u_3 = \wp((\omega_1+\omega_2)/2)$ are the values for which g has a double zero, and u_1, u_2, u_3 are distinct.*

Proof.

1. As g is elliptic of order 2, by Proposition 2.4, $g(z)$ has precisely two zeros inside Π counting multiplicities.

2. We have
$$\wp'\left(\frac{\omega_1}{2}\right) = \wp'\left(\frac{\omega_1}{2} - \omega\right) = \wp'\left(\frac{-\omega_1}{2}\right) = -\wp'\left(\frac{\omega_1}{2}\right),$$
so $\omega_1/2$ is a zero of $\wp'(z)$. Similarly, $\omega_2/2$ and $(\omega_1+\omega_2)/2$ are zeroes of $\wp'(z)$. As $\wp'(z)$ has a pole of order 3 at 0 and no other poles in Π, these are all the zeros of $\wp'(z)$ in Π.

3. In order for g to have a double zero at z, we must have $g'(z) = \wp'(z) = 0$, hence z must be one of $\omega_1/2, \omega_2/2$ or $(\omega_1+\omega_2)/2$, and so u must be one of the u_i. The u_i are distinct, as if say $u_1 = u_2$, then g would have a double zero at both $\omega_1/2$ and $\omega_2/2$, which would contradict part (1). Hence, the u_i are distinct.

□

Our next goal is to show that $\wp(z)$ and its derivative $\wp'(z)$ satisfy a certain differential equation. Namely, we will show that $4\wp'(z) = 4\wp(z)^3 - g_2\wp(z) - g_3$, where g_2 and g_3 are constants that we will define shortly. We begin with the following result:

Proposition 1.2.8. *Let f be an elliptic function with respect to two periods ω_1, ω_2, then $f(z) = g(\wp(z)) + wp'(z)h(\wp(z))$ where g and h are rational functions*

Proof. We first show that every even elliptic function $f(z)$ may be written $f(z) = g(\wp(z))$, where g is a rational function. For each $a \in \Pi\backslash\{0, \frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}\}$, let a^* denote the element of Π congruent to $-a$ modulo $\Lambda(\omega_1, \omega_2)$. Then we have

$$a^* = \begin{cases} \omega_1 + \omega_2 - a & \text{if } a \text{ is interior} \\ \omega_1 - a & \text{if } a \text{ is on the side along } \omega_1 \\ \omega_2 - a & \text{if } a \text{ is on the side along } \omega_2 \end{cases}$$

Moreover, $f^k(z) = (-1)^k f^k(\omega - z)$ for all $\omega \in \Lambda$ since f is even and elliptic with respect to ω_1 and ω_2. Therefore, if a is a zero of order m, then a^* is a zero of order m. Similarly, since $\frac{1}{f(z)}$ is even and elliptic with respect to ω_1 and ω_2, if a is a pole of order m, then a^* is a pole of order m.

Next, suppose $a \in \{0, \frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}\}$, then

$$f(a - z) = f(-2a + a - z) = f(-a - z) = f(a + z),$$

where the first equality follows since $2a \in \Lambda$ and f is elliptic. Hence, the Taylor expansion of f around a is even, so the order of f at a is even. Similarly, the Taylor expansion of $\frac{1}{f(z)}$ around a is even, so the same argument holds if a is a pole.

Now, let $\widetilde{A}$ denote the set of all zeros of f in Π, and $\widetilde{B}$ the set of all poles of f in Π. From $\widetilde{A}\backslash 0$, let A be a subset such that for each pair $a, a^* \in \widetilde{A}\backslash\{\frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}\}$, A contains either a or a^*, but not both, and each of $\frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}$ is an element of A if it is an element of $\widetilde{A}$. Similarly, let B be a subset of $\widetilde{B}\backslash\{0\}$ in the form of $A \subset \widetilde{A}$. Hence, A and B are both finite since $\widetilde{A}$ and $\widetilde{B}$ are finite, and we define

$$F(z) = \frac{\prod\limits_{a \in A} [\wp(z) - \wp(a)]}{\prod\limits_{b \in B} [\wp(z) - \wp(b)]}.$$

Then the zeros and poles of $F(z)$ in $\Pi\backslash\{0\}$ are precisely the zeros and poles respectively of $f(z)$. To see this, if $a \notin \{\frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}\}$ is a zero of f, then by Proposition 1.2.7, $\wp(z) - \wp(a)$ has two distinct zeros at a and a^* and if $a \in \{\frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}\}$, then $\wp(z) - \wp(a)$ has a double zero at a. Similarly, the poles of F are precisely the poles of f of the same order, so $f(z)/F(z)$ is holomorphic on $\Pi\backslash\{0\}$. However, by Proposition 1.1.4, $f(z)/F(z)$ is also holomorphic at 0, and hence holomorphic on all of $\mathbb{C}$. Thus, $f(z)/F(z)$ is constant, establishing the claim.

Now let f be an arbitrary function that is elliptic with respect to ω_1 and ω_2, and let $f_e(z) := \frac{1}{2}(f(z)+f(-z))$, $f_o(z) := \frac{1}{2}(f(z)-f(-z))$. Then f_e and $f_o/\wp'(z)$ are even elliptic, thus

$$f_e(z) = g(\wp(z)), \quad \frac{f_o}{\wp'(z)} = h(\wp(z))$$

for some rational functions g, h. Therefore,

$$f(z) = f_e(z) + f_o(z) = g(\wp(z)) + \wp'(z)h(\wp(z)).$$

□

We are now in a position to show that $\wp(z)$ satisfies the claimed differential equation:

Theorem 1.2.9. *Let*

$$G_m = G_m(\Lambda) := \sum_{\omega\in\Lambda\setminus\{0\}} \frac{1}{\omega^m},$$

and let $g_2 = 60G_4, g_3 = 140G_6$. *Then*

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$$

Proof. By Proposition 1.2.4, each G_m converges for $m \geq 2$, so by the Weierstrass doubles series theorem [c.f. 2, Lemma 6.13], we have

$$\wp(z) - \frac{1}{z^2} = \sum_{\omega\in\Lambda\setminus\{0\}} \left(\sum_{k=1}^{\infty} \frac{k+1}{\omega^{k+2}} z^k\right) = \sum_{k=1}^{\infty} (k+1)G_{k+2}z^k.$$

$$\wp(z) = \frac{1}{z^2} + 3G_4z^2 + 5G_6z^4 + \dots$$

and differentiating, we have

$$\wp'(z) = -2\frac{2}{z^3} + 6G_4z + 20G_6z^3 + \dots$$

Next, by direct calculation, we have

$$\wp(z)^2 = \frac{1}{z^4} + 6G_4 + 10G_6z^2 + \dots, \quad \wp(z)^3 = \frac{1}{z^6} + 9G_4\frac{1}{z^2} + 15G_6 + \dots$$

$$\wp'(z)^2 = \frac{4}{z^6} - 24G_4\frac{1}{z^2} - 80G_6 + \dots$$

Hence, we obtain $g(z) := \wp'(z)^2 - \wp(z)^3 + 60G_4\wp(z) + 140G_6$ has a zero at 0, and is an entire elliptic elliptic function. Thus, $g(z) \equiv 0$, and the theorem follows. □

1.3 Group Structure of $E(\mathbb{C})$

In this section, we will use the function $\wp(z)$ in order to construct an explicit isomorphism of groups between $\mathbb{C}/\Lambda(\omega_1, \omega_2)$ and the complex elliptic curve $Y^2Z = 4X^3 - g_2XZ^3 - g_3Z^3$. We begin with the following result:

Proposition 1.3.1. *The polynomial $4x^3 - g_2x - g_3$ has distinct roots, and hence $E : Y^2Z = 4X^3 - g_2XZ^3 - g_3Z^3$ is indeed an elliptic curve. Moreover, $E(\mathbb{C})$ is a complex manifold.*

Proof. By Theorem 1.2.9 and Proposition 1.2.7(2), the roots of $4x^3 - g_2x - g_3$ are $\wp(\frac{\omega_1}{2}), \wp(\frac{\omega_2}{2}), \wp(\frac{\omega_1+\omega_2}{2})$, which are distinct by Proposition 1.2.7(3) For the second claim, we define charts around each point $[X : Y : Z] \in E(\mathbb{C})$. Define $F(x, z) = y^2 - (4x^3 - g_2x - g_3)$, and let $[X : Y : 1] \in E(\mathbb{C})$ with affine coordinates (x, y). If $y \neq 0$, then $\frac{\partial F}{\partial y}(x, y) = 2y \neq 0$. Thus, by the Implicit Function Theorem, we can define y as analytic function of x, and hence a chart is given by $(x, y) \mapsto x$.

Similarly, if $y = 0$, then $\frac{\partial F}{\partial x}(x, y) = 12x^2 - g_2 \neq 0$, since the roots of the cubic are distinct by the first part of this proposition. Hence, by the Implicit Function Theorem, we can define x as an analytic function of y, and a chart is given by $(x, y) \mapsto y$.

It remains to consider a chart about $[0 : 1 : 0]$. Define $G(x, z) = z - (4^3 - g_2x - g_3)$, then $\frac{\partial G}{\partial z}(0, 0) \neq 0$. Hence, we can define z as an analytic function of x, and a chart is given by $(x, z) \mapsto x$. Thus, $E(\mathbb{C})$ is a complex manifold. □

Theorem 1.3.2. *Let E be the complex elliptic curve $E : Y^2Z = 4X^3 - g_2XZ^3 - g_3Z^3$, and consider the map $\varphi : \mathbb{C}/\Lambda \to E(\mathbb{C})$ given by*

$$\varphi(z) = \begin{cases} [\wp(z) : \wp'(z) : 1] & \textit{for } z \notin \Lambda \\ [0 : 1 : 0] & \textit{for } z \in \Lambda \end{cases}$$

Then φ is bijective and biholomorphic.

Proof. First observe that φ does indeed map $\mathbb{C}/\Lambda$ into $E(\mathbb{C})$ by Theorem 1.13, so φ is well defined. Next, suppose $\varphi(z_1) = \varphi(z_2)$. Then $\wp(z_1) = \wp(z_2)$, $\wp'(z_1) = \wp'(z_2)$, and $z_2 = z_1^*$ where z_1^* is the element of Π congruent to $-z_1$ modulo Λ as in Proposition 1.2.8 Thus we have,

$$\wp'(z_2) = \wp'(z_1^*) = \wp'(-z_1) = -\wp'(z_1) = -\wp'(z_2),$$

and so $\wp'(z_2) = \wp'(z_1) = 0$. Therefore, $z_1, z_2 \in \{\frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}\}$, and so $z_2 = z_1^* = z_1$. Thus, φ is injective.

Now let $\mathcal{O} \neq P \in E(\mathbb{C})$, and write P in affine coordinates as $P = (x, y)$. Then by Proposition 1.2.7(1), there exists $z \in \Pi$ such that $\wp(z) = x$, and moreover,

$$\wp'(z)^2 = 4\wp(z) - g_2\wp(z) - g_3 = 4x^3 - g_2x - g_3 = y^2.$$

Thus, $\wp'(z) = \pm y$. If $\wp'(z) = y$, then $\varphi(z) = P$, and if $\wp'(z) = -y$, then $\wp(z^*) = x$ and $\wp'(z^*) = y$, so $\varphi(z^*) = P$. As $\mathcal{O}$ is also in the image of φ by construction, φ is surjective.

We now show that φ is biholomorphic. Let $z \in \mathbb{C}\backslash\{0\}$, and write $\varphi(z)$ in affine coordinates as (x, y). Suppose $z \notin \{\frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}\}$. Then $y \neq 0$, so we have a chart given by $(x, y) \mapsto x$, hence we get a map $z \mapsto \wp(z)$. As $\wp'(z) \neq 0$, by the Inverse Function Theorem we thus have that φ is biholomorphic about z.

Next, let $z \in \{\frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}\}$. Then we have a chart given by $(x, y) \mapsto y$, and hence we get a map $z \mapsto \wp'(z)$. As $\wp''(z) \neq 0$ since $\wp'(z)$ has no double roots by Proposition 1.2.7(2), φ is biholomorphic about z.

We lastly consider the case $z = 0$. Then we have a chart given by $(x, z) \mapsto x$, and hence we get a map $z \mapsto \frac{\wp(z)}{\wp'(z)}$. As $\left(\frac{\wp(z)}{\wp'(z)}\right)' \neq 0$, since z is a simple zero, φ is also biholomorphic about $z = 0$, establishing that φ is a biholomorphic map. □

We are now in a position to prove that the group structure of $E(\mathbb{C})$ is a torus:

Theorem 1.3.3. *Let E be the complex elliptic curve $E : Y^2Z = 4X^3 - g_2XZ^3 - g_3Z^3$, and let $\varphi : \mathbb{C}/\Lambda \to E(\mathbb{C})$ be the map from the previous proposition. Then φ is a group isomorphism.*

Proof. By the previous proposition, we know that φ is bijective, so it suffices to show that φ is a homomorphism. Let $f : \mathbb{C}/\Lambda \times \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$ and $g : E(\mathbb{C}) \times E(\mathbb{C}) \to E(\mathbb{C})$ be the respective addition maps. Then we show that $g \circ (\varphi \times \varphi) = \varphi \circ f$. First, observe that both f and g are continuous, so it suffices to prove the equality of functions on a dense subset of $\mathbb{C}/\Lambda \times \mathbb{C}/\Lambda$. We claim that

$$\widetilde{X} := \{(u_1, u_2) \in \mathbb{C} \times \mathbb{C} \mid u_1, u_2, u_1 \pm u_2, 2u_1 + u_2, u_1 + 2u_2 \notin \Lambda\}$$

is dense in $\mathbb{C} \times \mathbb{C}$. To see this, observe that for any $(u_1, u_2) \in \mathbb{C} \times \mathbb{C}$, we can change u_1 and u_2 by arbitrarily small values to force (u_1, u_2) into $\widetilde{X}$, since Λ is discrete. Therefore, $\widetilde{X}$ is dense in $\mathbb{C} \times \mathbb{C}$, and hence its image X is dense in $\mathbb{C}/\Lambda \times \mathbb{C}/\Lambda$.

Now, let $(u_1 + \Lambda, u_2 + \Lambda) \in X$, $u_3 = -(u_1 + u_2)$, and $P_i := \varphi(u_i)$. Then each of the P_i are distinct, and different from $\mathcal{O}$, so we may consider each of them as an element of $\mathbb{A}^2$. Since $P_1 \neq \pm P_2$, we have that the line P_1P_2 is given by $y = ax + b$, where $a \neq 0$. As P_1 and P_2 are both on this line, we have

$$\wp'(u_1) = a\wp(u_1) + b \text{ and } \wp'(u_2) = a\wp(u_2) + b.$$

Next, define the function $h(z) := \wp'(z) - a\wp(z) - b$. Then h is an elliptic function which has a pole of order 3 at zero and no other poles in Π. It also has two zeros at u_1 and u_2, and thus has one more zero $\omega \in \Pi$ such that $u_1 + u_2 + w \equiv 0 \bmod \Lambda$. Thus, $\omega \equiv u_3 \bmod \Lambda$, so $h(u_3) = 0$ and thus u_3 lies on P_1P_2. Therefore, P_1, P_2, and P_3 lie on a line, so $P_1 + P_2 + P_3 = \mathcal{O}$ by definition of the group law on E. Hence,

$$\varphi(u_1) + \varphi(u_2) = P_1 + P_2 = -P_3 = -\varphi(-(u_1 + u_2)) = \varphi(u_1 + u_2)$$

since $\varphi(-u) = -\varphi(u)$ since $\wp$ is even and $\wp'(z)$ is odd. Thus, φ is a homomorphism and so $\mathbb{C}/\Lambda$ and $E(\mathbb{C})$ are isomorphic as groups. □

Remark 1.3.4. In fact, for each elliptic curve E over $\mathbb{C}$, there is a lattice $\Lambda \subset \mathbb{C}$ such that $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, establishing a converse to the previous theorem. For a proof of this fact, see [2, Chapter 6].

We now turn our attention to real elliptic curves.

1.4 Elliptic curves over $\mathbb{R}$

Throughout this section, we assume that we have a lattice Λ, such that $\sigma(\Lambda) = \Lambda$, where σ denotes complex conjugation. We show $E(\mathbb{R})$ is isomorphic to either S^1 or $\mathbb{Z}_2 \times S^1$, where $E : Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3$.

To begin, consider the action on the affine points of $E(\mathbb{C})$ given by $\sigma(x, y) := (\sigma(x), \sigma(y))$. Then $(x, y) \in E(\mathbb{R}) \iff \sigma(x, y) = (x, y)$. We also have a natural action on $P^2(\mathbb{C})$ given by $\sigma([x_0 : x_1 : x_2]) := [\sigma(x_0) : \sigma(x_1) : \sigma(x_2)]$.

Lemma 1.4.1. *This action of σ on $P^2(\mathbb{C})$ is well-defined, and*

$$\sigma([x_0 : x_1 : x_2]) = [x_0 : x_1 : x_2] \iff [x_0 : x_1 : x_2] \in P^2(\mathbb{R})$$

Proof. Suppose $[x_0 : x_1 : x_2] = [x'_0 : x'_1 : x'_2]$. Then there exists $\lambda \in \mathbb{C}^\times$ such that $x_i = \lambda x'_i$, for $i = 0, 1, 2$. Thus,

$$\sigma([x_0 : x_1 : x_2]) = [\sigma(x_0) : \sigma(x_1) : \sigma(x_2)] = [\sigma(\lambda x'_0) : \sigma(\lambda x'_1) : \sigma(\lambda x'_2)] =$$

$$[\sigma(\lambda)\sigma(x'_0) : \sigma(\lambda)\sigma(x'_1) : \sigma(\lambda)\sigma(x'_2)] = [\sigma(x'_0) : \sigma(x'_1) : \sigma(x'_2)] = \sigma([x'_0 : x'_1 : x'_2]).$$

Thus, the action is well-defined.

For the second statement, the backwards direction is clear, so we prove the forward direction. Suppose $\sigma([x_0 : x_1 : x_2]) = [x_0 : x_1 : x_2]$, then there exists $\lambda \in \mathbb{C}^\times$ such that $\sigma(x_i) = \lambda x_i$ for $i = 0, 1, 2$. Applying σ again, we see that $x_i = \sigma(\lambda)\sigma(x_i)$.

Adding the expressions, we have

$$2Re(x_i) = x_i + \sigma(x_i) = x_i + x_i\lambda = x_i(1 + \lambda)$$

$$\implies \frac{x_i(1 + \lambda)}{2} = Re(x_i).$$

If $\lambda = -1$, then each of the x_i are of the form iy_i, for some $y_i \in \mathbb{R}$, and hence $[x_0 : x_1 : x_2] = [iy_0 : iy_1 : iy_2] = [y_0 : y_1 : y_2] \in P^2(\mathbb{R})$. Otherwise, $(1 + \lambda)/2 \in \mathbb{C}^\times$, so $[x_0 : x_1 : x_2]$ is the same as $[z_0 : z_1 : z_2]$ for some z_i in $\mathbb{R}$. □

As a result of the previous claim, the real points of E are precisely the points that are fixed by the action of σ on $P^2(\mathbb{C})$. Since $\Lambda = \overline{\Lambda}$, we have a natural well-defined action on $\mathbb{C}/\Lambda$ given by $\sigma(z + \Lambda) := \sigma(z) + \Lambda$.

Lemma 1.4.2. *The action of σ commutes with the map φ from the previous section, that is, $\varphi \circ \sigma = \sigma \circ \varphi$, where first σ denotes the action on $\mathbb{C}/\Lambda$ and then on $P^2(\mathbb{C})$:*

Proof. We have

$$\wp(\overline{z}) = \frac{1}{\overline{z}^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left[\frac{1}{(\overline{z} - \omega)^2} - \frac{1}{\omega^2} \right] = \overline{\frac{1}{z^2}} + \sum_{\omega \in \Lambda \setminus \{0\}} \left[\frac{1}{(\overline{z} - \overline{\omega})^2} - \frac{1}{\overline{\omega}^2} \right]$$

$$\overline{\frac{1}{z^2}} + \sum_{\omega \in \Lambda \setminus \{0\}} \left[\overline{\frac{1}{(\overline{z} - \omega)^2}} - \overline{\frac{1}{\omega^2}} \right] = \overline{\frac{1}{\overline{z}^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left[\frac{1}{(\overline{z} - \omega)^2} - \frac{1}{\omega^2} \right]} = \overline{\wp(z)}$$

where in the second equality, we use the fact that the sum representing $\wp(z)$ is absolutely convergent. The case with $\wp'(z)$ is similar. □

As a result of this claim, we deduce that it suffices to describe the fixed points of the action of σ on $\mathbb{C}/\Lambda$, $(\mathbb{C}/\Lambda)^\sigma$.

We have that Λ is a free $\mathbb{Z}$-module of rank 2. Let $\Lambda_+ := \{a \in \Lambda \mid \sigma(a) = a\}$, and let $\Lambda_- := \{a \in \Lambda \mid \sigma(a) = -a\}$.

Proposition 1.4.3. *Λ is of the form $\Lambda = \Lambda_+ \oplus \Lambda_-$, or there is a basis for Λ such that $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, where $\sigma(\omega_1) = \omega_2$*

Proof. We claim that there exists $v_1 \in \Lambda_+$ such that v_1 generates Λ_+. To see this, let x_1, x_2 be any basis for Λ such that the x_i are linearly independent over $\mathbb{R}$. Suppose that we need two elements v_1, v_2 to form a basis for Λ_+ (note that it cannot be more than 2 since $\mathbb{Z}$ is a PID, and Λ_+ is a $\mathbb{Z}$-submodule of Λ). Then there exist $a, b, c, d \in \mathbb{Z}$ such that $v_1 = ax_1 + bx_2$, and $v_2 = cx_1 + dx_2$. Then,

$$0 = v_1 - v_1 = v_1 - \frac{v_1}{v_2} v_2 = (a - \frac{v_1}{v_2} c)x_1 + (b - \frac{v_1}{v_2} d)x_2,$$

hence $a = \frac{v_1}{v_2} c$, and $b = \frac{v_1}{v_2} d$, since $v_1, v_2 \in \mathbb{R}$. Thus, $\frac{v_1}{v_2} \in \mathbb{Q}$, so, there exist $p, q \in \mathbb{Z}$ such that $\frac{v_1}{v_2} = \frac{p}{q}$. Thus, $qv_1 + pv_2 = 0$, contradicting the assumption that v_1 and v_2 are linearly independent over $\mathbb{Z}$. The case showing Λ_- has only one element as its basis is similar.

Thus, let v_1,v_2 be a basis for Λ_+ and Λ_- respectively. Suppose there exists $\omega \in \Lambda \setminus \Lambda_+ \oplus \Lambda_-$. Then we may assume that ω is in the area of $\mathbb{C}$ enclosed by the parallelogram with vertices $0, v_1, v_2, v_1 + v_2$. To see this, observe that $\omega = x + iy$, so by subtracting multiples of v_1 and v_2 if necessary, we can force ω into this region. Next, we have $2\omega = (\omega + \overline{\omega}) + (\omega - \overline{\omega}) \in \Lambda_+ \oplus \Lambda_-$. Since ω by construction is not in Λ_+ or Λ_-, we must have that $2\omega = \omega_1 + \omega_2$. Thus, Λ is generated by ω and $\overline{\omega}$, since $\overline{\omega} = \omega - \omega_2$. □

We now have a specific form for Λ_- in the case $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, where $\sigma(\omega_1) = \omega_2$:

Proposition 1.4.4. *Suppose $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, where $\sigma(\omega_1) = \omega_2$, then*

$$\Lambda_- = (\sigma - 1)\Lambda.$$

Proof. Certainly we have the reverse inclusion. Conversely, suppose $x \in \Lambda_-$. Then $x = a\omega_1 + b\omega_2$, and applying σ, we obtain $\sigma(x) = b\omega_1 + a\omega_2$. Adding the expressions, we have $0 = x + \sigma(x) = (a+b)\omega_1 + (a+b)\omega_2$, so $a = -b$. Thus, $x = \sigma(a\omega_2) - a\omega_2 \in (\sigma - 1)\Lambda$. □

We now state and prove the first possibility for the structure of $E(\mathbb{R})$:

Theorem 1.4.5. *If $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, where $\sigma(\omega_1) = \omega_2$, then $E(\mathbb{R}) \cong S^1$*

Proof. Let $z \in (\mathbb{C}/\Lambda)^\sigma$, then $\sigma(z + \Lambda) = z + \Lambda$, so $\sigma(z) - z \in \Lambda$. Moreover, since $(\sigma - 1)\Lambda = \Lambda_-$ by the previous proposition, we actually have $\sigma(z) - z \in \Lambda_-$. Thus, $\sigma(z) - z = \sigma(\lambda) - \lambda$, for some $\lambda \in \Lambda$. Hence, $\sigma(z - \lambda) = z - \lambda$, so $z - \lambda \in \mathbb{R}$. Thus, z and $z - \lambda$ lie in the same coset mod Λ, and $z - \lambda$ is real. As z was arbitrary, we then have that the map $\mathbb{R} \mapsto (\mathbb{C}/\Lambda)^\sigma$ must then be surjective. Moreover, the kernel of this map is precisely Λ_+, so $\mathbb{R}/\Lambda_+ \cong (\mathbb{C}/\Lambda)^\sigma$, and $\mathbb{R}/\Lambda_+ \cong S^1$ from which we deduce the result. □

We now consider the case that $\Lambda = \Lambda_+ \oplus \Lambda_-$:

Theorem 1.4.6. *Suppose Λ is of the form $\Lambda = \Lambda_+ \oplus \Lambda_-$, then $E(\mathbb{R}) \cong \mathbb{Z}_2 \times S^1$*

Proof. First note that in this case, $(\sigma - 1)\Lambda$ is a proper subset of Λ_-. To see this, let ω be a basis for Λ_-, and suppose $\omega \in (\sigma - 1)\Lambda$. Then $Im(\omega) = 2Im(x)$, for some $x \in \Lambda$. Then $x = a + bi$, where a is divisible by the real part of some basis for Λ_+. Hence, subtracting by the necessary multiple of this basis, we may assume $x = bi$, where $b \in \mathbb{R}$. Thus, $x \in \Lambda_-$, and $b < \omega$, a contradiction.

Let $m \in \Lambda_- \backslash (\sigma - 1)\Lambda$, and let $q = \frac{m}{2}$. Then $\Lambda_- = (\sigma - 1)\Lambda + \langle \sigma(q) - q \rangle$ (note that $(\sigma - 1)\Lambda$ is of index 2 in Λ_-, since if ω is a basis for Λ_-, then $2\omega \in (\sigma - 1)\Lambda$). Next, let $z \in (\mathbb{C}/\Lambda)^\sigma$, then $\sigma(z + \Lambda) = z + \Lambda$, so $\sigma(z) - z \in \Lambda_-$. Thus, z is either in the same coset of $z - \lambda$, where $z - \lambda$ is real and we proceed as before, or

$$\sigma(z + q - \lambda) = z + q - \lambda \implies z + q - \lambda \in \mathbb{R},$$

so $(\mathbb{C}/\Lambda)^\sigma \cong (\mathbb{R}/\Lambda_+) + (q + \mathbb{R}/\Lambda_+) \cong \mathbb{Z}_2 \times S^1$. □

Chapter 2

Elliptic Curves over Finite Fields

We now turn our attention to elliptic curves over finite fields $\mathbb{F}_q$. The goal of the first section is to prove Hasse's inequality, which states that for an elliptic curve E over $\mathbb{F}_q$,

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

As we will see with a couple of examples, this inequality is quite strong. We first require some background on endomorphisms of elliptic curves.

2.1 Endomorphisms of Elliptic curves

In an effort to simplify our exposition, we will assume that any field we are working over has characteristic $\neq 2, 3$. The reason for doing so is that in this case, we may assume that any elliptic curve E is defined by a cubic of the form $y^2 = x^3 + ax + b$.

We begin with the following definition:

Definition 2.1.1. An *endomorphism* of an elliptic curve E over a field K is a homomorphism $\varphi : E(\overline{K}) \to E(\overline{K})$ given by rational functions.

In fact, we have the following result:

Proposition 2.1.2. *Let* $\varphi : E(\overline{K}) \to E(\overline{K})$ *be a map given by rational functions. Then* φ *is an endomorphism if and only if* $\varphi(\mathcal{O}) = \mathcal{O}$. *[2, Chapter 3, Theorem 4.8]*

With this result in hand, we have the following:

Definition 2.1.3. Let $\mathrm{End}(E)$ denote the set of endomorphisms of a given elliptic curve E over a field K. Then $\mathrm{End}(E)$ is a ring via the operations

$$(\varphi_1 + \varphi_2)(P) := \varphi_1(P) + \varphi_2(P), \text{ and } (\varphi_1\varphi_2)(P) := \varphi_1(\varphi_2(P)),$$

and taking the zero element in End(E) to be $\varphi(P) = \mathcal{O}$ for all P

Note that this definition is indeed well-defined by the previous proposition. Indeed, since $\varphi_1(\mathcal{O}) + \varphi_2(\mathcal{O}) = \mathcal{O} + \mathcal{O} = \mathcal{O}$ for all $\varphi_1, \varphi_2 \in$ End(E), the sum of two endomorphisms is again an endomorphism. Similarly the product of two elements in End(E) is again in End(E).

We will now introduce the notion of the degree of an endomorphism of an elliptic curve. We first require some preliminary remarks.

Remark 2.1.4. Let $\varphi = (f(x,y), g(x,y))$ be an endomorphism of an elliptic curve E over K. Note that since char$(K) \neq 2, 3$, we may assume E is of the form $y^2 = x^3 + ax + b$. Hence, any term in $f(x)$ or $g(x)$ with a power of y greater or equal to 2 may be replaced with some power of $x^3 + ax + b$. Thus, we may assume both f and g are of the form

$$f(x,y) = p_1(x) + yq_1(x), \quad g(x,y) = p_2(x) + yq_2(x),$$

where $p_i(x)$ and $q_i(x)$ are rational functions for $i = 1, 2$. Finally, since φ is also a homomorphism, we have that for any $\varphi(-P) = -\varphi(P)$ for any $P \in E(K)$, and hence that $\varphi(x, -y) = -\varphi(x, y)$. Therefore, both q_1 and p_2 are identically 0. Hence, we conclude that given $\varphi \in End(E)$, that $\varphi = (f(x), g(x)y)$, where f and g are rational functions.

In light of the previous remark, we now define the degree of an endomorphism:

Definition 2.1.5. Let $\varphi = (f(x), g(x)y)$ be an endomorphism of an elliptic curve E over a field K. Write $f(x) = p_1(x)/p_2(x)$, where the $p_i(x)$ are coprime polynomials. Then the *degree* of φ is $\max\{deg(p_1(x)), deg(p_2(x))\}$. If φ is the zero endomorphism, then we say the degree is zero.

We will now discuss the notion of (in)separability of an endomorphism:

Definition 2.1.6. Let $\varphi = (f(x), g(x)y)$ be an endomorphism of an elliptic curve E over a field K. Then φ is *separable* if $f'(x)$ is not identically zero, and is called *inseparable* otherwise.

The following result on relating the size of the kernel of a separable endomorphism to its degree will prove crucial in proving Hasse's inequality:

Theorem 2.1.7. *Let E be an elliptic curve over a field K, and let φ be a nonzero separable endomorphism, then*

1. *φ is surjective*
2. *For all $Q \in E(\overline{K})$, $|\varphi^{-1}(Q)| = |Ker(\varphi)|$*
3. *$|Ker(\varphi)| = deg(\varphi)$*

Proof. Suppose φ is of degree m, and write $\varphi(x, y) = (r_1(x), r_2(x)y)$, where $r_i(x) = a_i(x)/b_i(x)$ and $gcd(a_i(x), b_i(x)) = 1$. Consider the following three subsets of $E(\overline{K})$:

$$S_1 := \{Q = (u, v) \mid u = 0 \text{ or } deg(ub_1(x) - a_1(x)) < deg(\varphi)\}$$

$$S_2 := \{Q = (u, v) \mid \exists x \in \overline{K} \text{ such that } u = r_1(x) \text{ and } r_1'(x) = 0\}$$

$$S_3 := \{Q = (u, v) \mid \exists x \in \overline{K} \text{ such that } u = r_1(x) \text{ and } r_2(x) = 0\}$$

Let S denote the union of the S_i. We claim that S is finite, and for any point $Q = (u, v) \in E(\overline{K})\backslash S$, that $ub_1(x) - a_1(x)$ has m distinct roots.

S_1 is finite since $m = \deg(\varphi)$ is by definition the larger of the degrees of a_1 and b_1, so the only way $\deg(ub_1(x) - a_1(x))$ is strictly less than m if the degrees of a_i and b_i are the same, and multiplication by u with the leading coefficient of b_1 yields the leading coefficient of a_1. This can only happen for at most one choice of u, which in turn yields only finitely many choices for v, so S_1 is finite.

The finiteness of S_2 follows since φ is separable, so r_1 is not the zero polynomial, and hence $r_1'(x)$ has finitely many roots.

Similarly, S_3 is finite since r_2 has only finitely many zeros, and so there are only finitely many choices for u with $u = r_1(x)$, where x is a zero of r_2. Thus, S is finite, and for any point $Q = (u, v) \in E(\overline{K})\backslash S$, $ub_1(x) - a_1(x)$ is of degree m. It remains to show for any choice of Q, that this polynomial has no multiple roots.

Choose, $Q = (u, v) \in E(\overline{K})\backslash S$, and suppose that x_0 is a multiple root. Then $ub_1(x_0) - a_1(x_0) = ub_1'(x_0) - a_1'(x_0) = 0$, and therefore, $u(a_1b_1' - a_1'b_1)(x_0) = 0$, but then since $u \neq 0$, that $(a_1b_1' - a_1'b_1)(x_0) = 0$, and hence that the numerator of $r_1'(x_0)$ is zero. However, then Q is an element of S_2, contradicting that $Q \in E(\overline{K})\backslash S$, so $ub_1(x) - a_1(x)$ has m distinct roots.

Next, for $Q = (u, v) \notin S$, $r_2(x) \neq 0$ for any root of $ub_1(x) - a_1(x)$, since $Q \notin S_3$, and therefore, $\varphi^{-1}(Q) = \{(x, y) \mid ub_1(x) - a_1(x) = 0, y = v/r_2(x)\}$, which has cardinality m since $ub_1(x) - a_1(x)$ is separable of degree m. Therefore, φ the complement of the image of φ is at most finite, namely the cardinality of S. However, if $P \in E(\overline{K})\backslash\text{Image}(\varphi)$, then $P + Q \in E(\overline{K})\backslash\text{Image}(\varphi)$ for all $Q \in \text{Image}(\varphi)$, so $E(\overline{K})\backslash\text{Image}(\varphi)$ is infinite as $|E(\overline{K})|$ is infinite, a contradiction. Thus, φ is surjective.

To prove the second statement, observe that since φ is surjective, $\varphi^{-1}(Q)$ is nonempty for every $Q \in E(\overline{K})$. Thus, for any $P_0 \in \varphi^{-1}(Q)$ the map $f : Ker(\varphi) \to \varphi^{-1}(Q)$ given by $P \mapsto P + P_0$ is a well-defined bijection, $|\varphi^{-1}(Q)| = |Ker(\varphi)|$.

The third statement follows from the second statement and taking $Q \in E(\overline{K})\backslash S$, where it has been established that $|\varphi^{-1}(Q)| = deg(\varphi)$ in the argument that φ is surjective. □

It is worth mentioning that a similar result holds in general, that is, for nonseparable endomorphism of elliptic curves. In fact, the first two claims of Theorem 2.1.7 are true for all endomorphisms, and in general we must replace equality with $|Ker(\varphi)| \leq deg(\varphi)$ in the third claim. To prove the result in general, one introduces the notion of *separable degree* of an endomorphism, however, we only need the version of Theorem 2.1.7 as stated.

We now have the following proposition whose proof may be found in [1, Theorem 6.2.7]:

Proposition 2.1.8. *Let $E : y^2 = x^3 + ax + b$ be an elliptic curve over K, then*

1. *Suppose $P_3 = P_1 + P_2$ for points $P_i = (x_i, y_i)$, then viewing x_3 and y_3 as rational functions in the indeterminates x_1, y_1, x_2, y_2, we have*

$$\frac{\partial x_3}{\partial x_1} = \frac{y_3}{y_1} \text{ and } \frac{\partial x_3}{\partial x_2} = \frac{y_3}{y_2}$$

2. *Suppose $Q = [m]P$, where $[m]$ is the multiplication by m map, and write $P = (x, y), Q = (x_m, y_m)$, then*

$$\frac{\partial x_m}{\partial x_1} = m\frac{y_m}{y_1}$$

3. *If $\alpha \in$End(E), $P = (x, y)$, and $\alpha(P) = (x_\alpha, y_\alpha)$, then there exists $c_\alpha \in \overline{K}$ such that*

$$\frac{\partial x_\alpha}{\partial x_1} = c_\alpha \frac{y_\alpha}{y_1},$$

and moreover the map $f : End(E) \to \overline{K}$ is a ring homomorphism.

4. *The constant c_α from part (3) is zero $\iff$ α is inseparable. In particular, for any non-zero integer m, the multiplication by m map $[m]$ is separable in characteristic $p > 0$ if and only if p does not divide m.*

We are now going to use the degree map in order to define a symmetric bilinear form on End(E). To do this, we first require a few lemmas on the degree map:

Lemma 2.1.9. *Let $\alpha, \beta \in$ End(E), then*

$$deg(\alpha + \beta) + deg(\alpha - \beta) = 2deg(\alpha) + 2deg(\beta)$$

Proof. As $deg(0) = 0, deg([-1]) = 1$, and $deg([2]) = 4$, the result holds when α or β is 0 or $\alpha = \pm\beta$. We now show the result in general by mutual inequality.

Let $P = (x, y) \in E(\overline{K})$, $\alpha, \beta \in End(E)$, and write

$$P_1 = \alpha(x, y) = (x_1, y_1),\ P_2 = \beta(x, y) = (x_2, y_2)$$

$$P_3 = (\alpha + \beta)(x, y) = (x_3, y_3),\ P_4 = (\alpha - \beta)(x, y) = (x_4, y_4),$$

where $x_i = a_i(x)/b_i(x)$ for polynomials $a_i(x), b_i(x)$ such that $gcd(a_i(x), b_i(x)) = 1$. Let $d_i = \max\{deg(a_i(x)), deg(b_i(x))\}$, then in these notations, showing $deg(\alpha + \beta) + deg(\alpha - \beta) \leq 2deg(\alpha) + 2deg(\beta)$ amounts to showing that

$$d_3 + d_4 \leq 2d_1 + 2d_2.$$

By the addition formulas, we have

$$(x_1 - x_2)^2 x_3 = (x_1 x_2 + A)(x_1 + x_2) - 2y_1 y_2 + 2B$$

$$(x_1 - x_2)^2 x_4 = (x_1 x_2 + A)(x_1 + x_2) + 2y_1 y_2 + 2B,$$

and hence, adding these two expressions and multiplying them, we have the following two equations:

$$(x_1 - x_2)^2 (x_3 + x_4) = 2(x_1 x_2 + A)(x_1 + x_2) + 4B \tag{2.1.1}$$

$$(x_1 - x_2)^4 x_3 x_4 = (x_1 x_2 - A)^2 - 4B(x_1 + x_2) \tag{2.1.2}$$

Therefore, by (2.1.1) and (2.1.2), in projective coordinates, we have the following identity in the x_i:

$$[1 : x_3 + x_4 : x_3 x_4] = [(x_1 - x_2)^2 : 2(x_1 x_2 + A)(x_1 + x_2) + 4B : (x_1 x_2 - A)^2 - 4B(x_1 + x_2)].$$

Next, homogenize each x_i via

$$X_i := \frac{Z^{d_i} a_i(X/Z)}{Z^{d_i} b_i(X/Z)} := \frac{U_i(X, Z)}{V_i(X, Z)},$$

then from the projective coordinates identity, we have the following:

$$[U_3 V_4 : U_3 V_4 + U_4 V_3 : U_3 U_4] = [F : G : H] \tag{2.1.3}$$

where

$$F = (U_1 V_2 - U_2 V_1)^2, \;\; G = 2(U_1 U_2 + 2AV_1 V_2)(U_1 V_2 + U_2 V_1) + 4BV_1^2 V_2^2$$

$$H = (U_1 U_2 - AV_1 V_2)^2 - 4B(U_1 V_1 + U_2 V_2) V_1 V_2.$$

We claim that the polynomials on the left hand side of (2.1.3) are coprime. Suppose H is an irreducible polynomial that divides both $V_3 V_4$ and $U_3 U_4$. Then without loss of generality, H divides both V_3 and U_4 as the case with V_4 and U_3 is similar. Hence, in this case H divides neither U_3 nor V_4, and so then H does not divide the middle term of the left hand side of (2.1.3).

Next, observe that the polynomials on the left hand side are all of degree $d_3 + d_4$ and all the polynomials on the right hand side are of degree $2d_1 + 2d_2$. We have just established that the polynomials on the left are coprime, hence, let $D = gcd(F, G, H)$, then we have

$$[U_3 V_4 : U_3 V_4 + U_4 V_3 : U_3 U_4] = [D\widetilde{F} : D\widetilde{G} : D\widetilde{H}] = [\widetilde{F} : \widetilde{G} : \widetilde{H}],$$

where the polynomials on the right hand side are coprime. Therefore, we have

$$d_3 + d_4 = 2d_1 + d_2 - deg(D) \leq 2d_1 + 2d_2,$$

and hence

$$deg(\alpha+\beta)+deg(\alpha-\beta)\leq 2deg(\alpha)+2deg(\beta).$$

We lastly show the other inequality to establish the lemma. Observe that we proved this first inequality for arbitrary $\alpha,\beta\in End(E)$, so applying this result to $\alpha\pm\beta$ in place of α and β respectively, we obtain

$$deg(2\alpha)+deg(2\beta)\leq 2deg(\alpha+\beta)+2deg(\alpha-\beta),$$

which by multiplicativity of degree is equal to

$$2deg(\alpha)+2deg(\beta)\leq deg(\alpha+\beta)+deg(\alpha-\beta),$$

which proves the lemma. □

As a corollary of the lemma, we have the following result on the degree of the multiplication by m map:

Corollary 2.1.10. *Let $[m]$ denote the multiplication by m map, then*

$$deg([m])=m^2$$

Proof. We first show the claim for m nonnegative by induction. The cases $m=0,1$ hold, so it suffices to consider $m>1$.

By Lemma 2.1.9, we have $deg([m+1])+deg([m-1])=2deg([m])+2deg([1])$, so by our induction hypothesis, we have

$$deg([m+1])=2deg([m])+2deg([1])-deg([m-1])=2m^2+2-(m-1)^2=(m+1)^2$$

Lastly, the result holds for m negative by the above argument and multiplicativity of degree, since $deg([-1])=1$. □

2.2 Hasse's Inequality

We begin with the following lemma on obtaining a bilinear form from maps from an abelian group into a field:

Lemma 2.2.1. *Let A be an abelian group, F a field of characteristic different from 2, and $Q:A\to F$ such that*

$$Q(x+y)+Q(x-y)=2Q(x)+2Q(y).$$

Define

$$B(x,y):=\frac{Q(x+y)-Q(x)-Q(y)}{2},$$

then B is a symmetric bilinear form.

Proof. Since $Q(0)+Q(0) = Q(0+0)+Q(0-0) = 2Q(0)+2Q(0)$, and $\mathrm{char}(F) \neq 2$, we have $Q(0) = 0$, so $B(0,0) = 0$.
Next, we have

$$B(x,y) = \frac{Q(x+y) - Q(x) - Q(y)}{2} = \frac{Q(y+x) - Q(y) - Q(x)}{2} = B(y,x).$$

Finally,

$$2B(x,y) + 2B(z,y) = Q(x+y) - Q(x) - Q(y) + Q(z+y) - Q(z) - Q(y) =$$

$$= (2Q(x) + 2Q(y) - Q(x-y)) - Q(x) - Q(y) + Q(z+y) - Q(z) - Q(y)$$

$$= Q(x) - Q(x-y) + Q(z+y) - Q(z) = \frac{Q(x+z+y) - Q(x+z-y)}{2}$$

$$= Q(x+z+y) - Q(x+z) - Q(y) = 2B(x+z,y),$$

and so linearity follows since the characteristic of F is different from 2. □

We now introduce the following map:

Definition 2.2.2. For $\alpha, \beta \in End(E)$, define

$$\langle \alpha, \beta \rangle := \frac{deg(\alpha+\beta) - deg(\alpha) - deg(\beta)}{2}$$

In light of Lemma 2.2.1, the map in Definition 2.2.2 is a symmetric bilinear form. Moreover, as the degree of an endomorphism is nonnegative, this form is also positive definite.

We now prove the Cauchy-Schwarz inequality on this bilinear form:

Proposition 2.2.3. *For any $\alpha, \beta \in End(E)$, we have*

$$\langle \alpha, \beta \rangle^2 \leq deg(\alpha) deg(\beta)$$

Proof. If either α or β is the zero endomorphism, the result certainly holds, so we may assume that both endomorphisms are nonzero.

Consider the map $H : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Q}$ given by $H(m,n) := \langle m\alpha + n\beta, m\alpha + n\beta \rangle$. Then in view of 2.2.2, this is a positive definite symmetric bilinear form, and the matrix representation of H is given by

$$A := \begin{pmatrix} deg(\alpha) & \langle \alpha, \beta \rangle \\ \langle \alpha, \beta \rangle & deg(\beta) \end{pmatrix}$$

Hence, the map $F : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ given by $F(x,y) = (x,y)A(x,y)^T$ is a positive definite, and so the determinant of A is positive. Thus, $\langle \alpha, \beta \rangle^2 \leq deg(\alpha) deg(\beta)$. □

We now introduce a particular endomorphism that is vital in the proof of Hasse's inequality:

Definition 2.2.4. Let E be an elliptic curve over $\mathbb{F}_q$, then the *Frobenius map* $\varphi_q : E(\overline{\mathbb{F}_q}) \to E(\overline{F}_q)$ of E is given by $\varphi_q(x, y) := (x^q, y^q)$, and $\varphi_q(\mathcal{O}) := \mathcal{O}$

It is worth mentioning that φ_q is indeed an endomorphism. The map is given by rational functions, and $\varphi_q(\mathcal{O}) := \mathcal{O}$, so assuming φ_q is even well-defined, then it is an endomorphism. For well-definedness, one uses the fact that E is defined over $\mathbb{F}_q$, so

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

and hence φ_q is a well-defined map.

We now have the following proposition:

Proposition 2.2.5. *Let E be an elliptic curve over $\mathbb{F}_q$, then*

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

Proof. The proof of this fact will be done in two stages. First, we will argue that $\varphi_q - 1$ is separable, and then we will use appeal to Theorem 2.1.7 after showing that $|E(\mathbb{F}_q)| = |Ker(\varphi_q - 1)|$.

To begin, observe that φ_q is inseparable, as the derivative of x^q is 0, so by (4) of Proposition 2.1.8, $c_{\varphi_q} = 0$. Next, by (3) of Proposition 2.1.8, we have the constant $c_{\varphi_q - 1}$ for the endomorphism $\varphi_q - 1$ is given by

$$c_{\varphi_q - 1} = c_{\varphi_q} + c_{-1} = 0 + 1 = 1,$$

and so again by (5) of 2.1.8, $\varphi_q - 1$ is separable.

Next, let $P := (x, y) \in E(\overline{F}_q)$, then we have the following chain of equivalences:

$$P \in E(\mathbb{F}_q) \iff (x^q, y^q) = (x, y) \iff \varphi_q(P) = P \iff P \in Ker(\varphi_q - 1),$$

and so $|E(\mathbb{F}_q)| = |Ker(\varphi_q - 1)|$. The result now follows by Theorem 2.1.7 since $\varphi_q - 1$ is separable. □

We are now in a positive to proof Hasse's inequality:

Theorem 2.2.6. *(Hasse)*
Let E be an elliptic curve over $\mathbb{F}_q$, then we have

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

Proof. We prove Hasse's theorem by using the bilinear form introduced in 2.2.2. Observe that the degree of the Frobenius map φ_q is q, and so we have by Proposition 2.2.3,

$$|\langle \varphi_q, 1 \rangle| \leq \sqrt{q}.$$

Thus, by Proposition 2.2.5,

$$\#E(\mathbb{F}_q) = deg(\varphi_q - 1) = deg(\varphi_q) - 2\langle \varphi_q, 1 \rangle + 1,$$

and so

$$|\#E(\mathbb{F}_q) - (q + 1)| = 2|\langle \varphi_q, 1 \rangle| \leq 2\sqrt{2}$$

□

The bound given by Hasse's inequality ends up being pretty sharp in some cases. For example, using Sage, one can compute the following:

Example 2.2.7. Let E be the elliptic curve over $\mathbb{F}_{97}$ defined by the cubic $y^2 = x^3 + 2$. Then we compute $\#E(\mathbb{F}_{97}) = 117$, and Hasse tells us

$$|\#E(\mathbb{F}_{97}) - 98| \leq \sqrt{97} \approx 19.7$$

Chapter 3

Elliptic Curves over $\mathbb{Q}$

3.1 Heights on Elliptic Curves

We begin with some remarks on general heights on $\mathbb{P}^n(\mathbb{Q})$ and then consider heights on elliptic curves.
We begin with the following definition:

Definition 3.1.1. Let $P = [a_0 : \ldots : a_n] \in \mathbb{P}^(\mathbb{Q})$. Then by clearing denominators and dividing by common factors, we may assume that the a_i are coprime integers. We define the *height* $H(P)$ to be the max of the $|a_i|$.

We now have the following lemma:

Lemma 3.1.2. *Let $c \in \mathbb{R}$ be positive, and $S := \{P \in \mathbb{P}^n(\mathbb{Q}) \mid H(P) \leq c\}$. Then $|S|$ is finite*

Proof. If $P = [a_0 : \ldots : a_n] \in S$, with a_i coprime integers, then each $a_i \in [-c, c]$. As the number of integers in $[-c, c]$ is less than $2(c + 1)$, we thus have

$$|S| < (2(c + 1))^{n+1} < \infty.$$

□

We now introduce the notion of the resultant of two polynomials:

Definition 3.1.3. Given two polynomials $f = a_m t^m + \ldots + a_0, g = b_n t^n + \ldots + b_0$ over a unique factorization domain A, we define the *resultant* of f and g to be the determinant

$$R_{f,g} := \begin{vmatrix} a_0 & a_1 & \ldots & a_m & 0 & \ldots \\ 0 & a_0 & a_1 & \ldots & a_m & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ b_0 & b_1 & \ldots & b_n & 0 & \ldots \\ 0 & b_0 & b_1 & \ldots & b_n & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \end{vmatrix}$$

This leads to the following lemma:

Lemma 3.1.4. *Let $f(X,Y), g(X,Y)$ be two homogeneous polynomials of degrees m and n respectively over $\mathbb{Q}$. Let f_1, f_2 and g_1, g_2 be the dehomogenizations of f and g with respect to X and Y respectively. Then $R_{f_1,g_1} = R_{f_2,g_2}$.*

Proof. This follows since dehomogenizing with respect to Y instead of X will just reverse the order of the coefficients as they appear in each row, which will not change the value of the determinant. Hence, the resultants are the same. □

In the situation of the previous lemma, we call $R_{f_1,g_1} = R_{f_2,g_2}$ the *resultant* of f and g. We now have the following two lemmas about general heights, before we restrict our discussion of heights to those on elliptic curves.

Lemma 3.1.5. *Let $f(X,Y), g(X,Y)$ be two homogeneous polynomials of degree m over $\mathbb{Q}$. Let $S \subset \mathbb{P}^1(\mathbb{Q})\}$ be the set of points where f and g are not both zero. Then:*

1. *The map $\varphi : S \to \mathbb{P}^1(\mathbb{Q})$ given by $\varphi(P) = (f(P), g(P))$ is well-defined.*

2. *There exists $c > 0$ such that $H(\varphi(P)) \leq cH(P)^m$ for all $P \in S$.*

3. *Let R be the resultant of f and g. If R is not identically zero, then $S = \mathbb{P}^1(\mathbb{Q})$, and there exists $c' > 0$ such that $H(\varphi(P)) \geq rH(P)^m$ for all P.*

Proof.

1. This follows since f and g are homogeneous of the same degree, and $\varphi(P) \neq [0:0]$ for all $P \in S$.

2. Clearing denominators on the coefficients, which does not change $\varphi(P)$, we may assume both f and g have integer coefficients. Let us write $f(X,Y) = \sum_{k=0}^{m} a_k X^k Y^{n-k}$ and $g(X,Y) = \sum_{k=0}^{m} b_k X^k Y^{n-k}$, then for $[x,y] \in S$ we have

$$|f(x,y)| = \left| \sum_{k=0}^{m} a_k x^k y^{n-k} \right| \leq \sum_{k=0}^{m} |a_k||x^k y^{n-k}| \leq \left(\sum_{k=0}^{m} |a_k| \right) N^m =: c_1 H(P)^m,$$

   where N is the maximum of $|x|$ and $|y|$. Similarly, we obtain that $|g(x,y)| \leq c_2 H(P)^m$, where c_2 is the sum of the magnitudes of the coefficients of g. Letting c be the larger of c_1, c_2 yields the this part of the lemma.

3. As $R \neq 0$, F and G have no common factor, and so $S = \mathbb{P}^1(\mathbb{Q})$. Next, by Lemma 3.1.4, we may write

$$V_1(X,Y)F(X,Y) + U_1(X,Y)G(X,Y) = RX^{2m-1}$$

$$V_2(X,Y)F(X,Y) + U_2(X,Y)G(X,Y) = RY^{2m-1},$$

   where the U_i and the V_i are homogeneous polynomials of degree $m-1$ over $\mathbb{Z}$.

Next, let $P := [a : b] \in \mathbb{P}^1(\mathbb{Q})$ with a and b coprime integers, and write $P' := \varphi(P) = [a' : b']$ where a', b' coprime. Then we have

$$V_1(a,b)a' + U_1(a,b)b' = \frac{Ra^{2m-1}}{d}$$

$$V_2(a,b)a' + U_2(a,b)b' = \frac{Rb^{2m-1}}{d},$$

where d is the greatest common divisor of $F(a,b)$ and $G(a,b)$. By part (ii) of this lemma, we have that there exists some $c_1 > 0$ such that $|U_i(a,b)|, |V_i(a,b)| \leq c_1 H(P)^{m-1}$ and thus we have

$$\frac{|R|}{|d|}H(P)^{2m-1} = \frac{|R|}{|d|}max\{|a|^{2m-1}, |b|^{2m-1}\} \leq 2c_1 H(P)^{m-1} H(\varphi(P)).$$

Finally, dividing everything by $2C_1 H(P)^{m-1}$, and letting $c' := 1/(2c_1)$, we have

$$H(\varphi(P)) \geq \frac{|R|}{c'|d|}H(P)^m \geq c' H(P)^m,$$

which proves the claim.

□

Lemma 3.1.6. *Let $P_i = [a_i : b_i] \in \mathbb{P}^1(\mathbb{Q})$, for $i = 1, 2$. Then $P_3 := [b_1 b_2 : a_1 b_2 + a_2 b_1 : a_1 a_2]$ is in $\mathbb{P}^2(\mathbb{Q})$, and moreover*

$$\frac{1}{2}H(P_1)H(P_2) \leq H(P_3) \leq 2H(P_1)H(P_2)$$

Proof. As usual, we may assume that a_i, b_i are coprime integers, which then implies the three components of P_3 are coprime. Hence, P_3 is a well-defined point of $\mathbb{P}^2(\mathbb{Q})$.

To prove the first inequality, observe that by symmetry, it is enough to show $|a_1 b_2| \leq 2\max\{|b_1 b_2|, |a_1 b_2 + a_2 b_1|, |a_1 a_2|\}$. Hence, assume $a_1 b_2 \neq 0$, and that $2|b_1 b_2|, 2|a_1 a_2| < |a_1 b_2|$, then we have

$$|a_1 b_2| = |a_1 b_2 + a_2 b_1 - a_2 b_1| \leq |a_1 b_2 + a_2 b_1| + |a_2 b_1| < |a_1 b_2 + a_2 b_1| + \frac{1}{4}|a_1 b_2|,$$

where the last inequality follows since $2|b_1 b_2|, 2|a_1 a_2| < |a_1 b_2|$ implies that $|b_1| < \frac{1}{2}|a_1|, |a_2| < \frac{1}{2}|b_2|$. Hence, subtracting both sides by $\frac{1}{4}|a_1 b_2|$ completes the proof. □

We now turn our attention to heights on elliptic curves.

Definition 3.1.7. Let E be an elliptic curve over $\mathbb{Q}$, define $h : E(\mathbb{Q}) \to \mathbb{R}$ by $h(P) = \log H(P)$ if $P \neq \mathcal{O}$, and $h(P) = 0$ if $P = \mathcal{O}$. The function h is called the *naive height.*

Note that in view of Lemma 3.1.2, for each $c \in \mathbb{R}^+$, the number of points on an elliptic curve E over $\mathbb{Q}$ is bounded.

Our next goal is to prove that this naive height satisfies an approximate parallelogram law. To do so, we require the following two lemmas:

Lemma 3.1.8. *Let E : be an elliptic curve over $\mathbb{Q}$ with whose defining cubic is of the form $y^2 = x^3 + ax + b$, with $a, b \in \mathbb{Z}$. Then there exists $c > 0$ such that for every pair of points $P, Q \in E(\mathbb{Q})$, $h(P+Q) + h(P-Q) \leq 2h(P) + 2h(Q) + c_2$.*

Proof. Let $P, Q \in E(\mathbb{Q})$, and let $x_i = a_i/b_i$ be the x-coordinate of $P, Q, P+Q$, and $P-Q$ respectively. By [equation reference(this is from finite fields identities], we have

$$[1 : x_3+x_4 : x_3x_4] = [(x_1-x_2)^2 : 2(x_1x_2+a)(x_1+x_2)+4b : (x_1x_2-a)^2-4b(x_1+x_2)],$$

hence, after clearing denominators, $[b_3b_4 : a_3b_4 + a_4b_3 : a_3a_4] = [z_1 : z_2 : z_3]$, where

$$z_1 = (a_1b_2 - a_2b_1)^2, \quad z_2 = 2(a_1a_2 + ab_1b_2)(a_1b_2 + a_2b_1) + 4bb_1^2b_2^2,$$
$$z_3 = (a_1a_2 - ab_1b_2)^2 - 4b(a_1b_2 + a_2b_1)b_1b_2.$$

Hence, by Lemma 3.1.6

$$H(x_3)H(x_4) \leq 2\max\{|b_3b_4|, |a_3b_4+a_4b_3|, |a_3a_4|\} \leq 2\max\{|z_1|, |z_2|, |z_3|\} \leq cH(x_1)^2H(x_2)^2,$$

where $c > 0$ is some constant obtained as in Lemma 3.1.5. Taking the log of both the left and right side completes the proof. □

Lemma 3.1.9. *Let E : be an elliptic curve over $\mathbb{Q}$ with whose defining cubic is of the form $y^2 = x^3 + ax + b$, with $a, b \in \mathbb{Z}$. Then there exists $c > 0$ such that for every $P \in E(\mathbb{Q})$, $4h(P) \leq h(2P) + c$.*

Proof. From the duplication formulas, we have the following identity:

$$x(2P) = \frac{x^4 - 2ax^2 - 8bx + a^2}{4(x^3 + ax + b)} =: \frac{f(x)}{g(x)}.$$

Let $F(X, Y)$ and $G(X, Y)$ be the homogenizations of f and g respectively with respect to a variable Y, and let $u(x)$ and $v(x)$ be given by

$$u(x) = -3x^2 - 4a, \ \ v(x) = 3x^3 - 5ax - 27b,$$

then we have $v(x)f(x) + u(x)g(x) = -4a^3 - 27b^2$. However, $-4a^3 - 27b^2$ is precisely the discriminant of E, that is, the discriminant of $x^3 + ax + b$, which is necessarily nonzero since E is an elliptic curve. As the resultant of f and g is also the discriminant of E c.f. [1, Lemma 10.2.4], we may thus apply part (3) of Lemma 3.1.4 to F and G, and so there exists $c' > 0$ such that $H(P)^4 \leq c'H(2P)$. Therefore, taking the logarithm of both sides, we obtain

$$4h(P) \leq c + h(2P),$$

where $c = log(c')$. □

We now state and prove the approximate parallelogram law for the naive height.

Lemma 3.1.10. *Let E : be an elliptic curve over $\mathbb{Q}$ with whose defining cubic is of the form $y^2 = x^3 + ax + b$, with $a, b \in \mathbb{Z}$. Then there exists $c > 0$ that only depends on E such that for every $P, Q \in E(\mathbb{Q})$,*

$$|h(P+Q) + h(P-Q) - 2h(P) - 2h(Q)| < c$$

Proof. Let $P, Q \in E(\mathbb{Q})$. By Lemmas 3.1.8 and 3.1.9, there is c_1 and c_2 both greater than zero such that

$$4h(P)+4h(Q) \leq h(2P)+h(2Q)+c_1, \text{ and } h(2P)+h(2Q) \leq 2h(P+Q)+2h(P-Q)+c_2.$$

Therefore, $2h(P) + 2h(Q) \leq h(P+Q) + h(P-Q) + c$, where c is the larger of c_1 and $\frac{c_1+c_2}{2}$, which proves the approximate parallelogram law. □

We now have the preparation to define the (canonical) height of an elliptic curve. We will then close this section with a theorem on properties of this canonical height that will be instrumental when deducing the Mordell-Weil theorem from the Weak Mordell-Weil theorem.

Definition 3.1.11. Let E be an elliptic curve over $\mathbb{Q}$. The *canonical height* $\widehat{h} : E(\mathbb{Q}) \to \mathbb{R}_{\geq 0}$ on $E(\mathbb{Q})$ is given by

$$\widehat{h}(P) := \lim_{n\to\infty} \frac{1}{4^n} h(2^n P)$$

Theorem 3.1.12. *Let E be an elliptic curve over $\mathbb{Q}$ with canonical height $\widehat{h}$, then*

1. *$\widehat{h}$ is well-defined.*

2. *There exists $c > 0$ such that for all $P \in E(\mathbb{Q})$, $|h(P) - \widehat{h}(P)| \leq c$*

3. *For all $c > 0$, $S := \{P \in E(\mathbb{Q}) \mid \widehat{h}(P) \leq c\}$ is finite.*

4. *For $m \in \mathbb{Z}$ and every $P \in E(\mathbb{Q})$, $\widehat{h}(mP) = m^2 \widehat{h}(P)$*

5. *For every $P, Q \in E(\mathbb{Q})$, $\widehat{h}(P+Q) + \widehat{h}(P-Q) = 2\widehat{h}(P) + 2\widehat{h}(Q)$*

6. *$\widehat{h}(P) = 0 \iff P$ has finite order.*

Proof.

1. By Lemma 3.1.9, there exists $c > 0$ such that for all $P \in E(\mathbb{Q})$, $|h(2P) - 4h(P)| \leq c$. Next, for $N \geq M \geq 0$ integers, we have

$$|4^{-N}h(2^N P) - 4^{-M}h(2^M P)| = \left|\sum_{n=M}^{N-1} 4^{-n-1}h(2^{n+1}P) - 4^{-n}h(2^n P)\right| \leq$$

$$\leq \sum_{n=M}^{N-1} 4^{-n-1} \left| h(2^{n+1}P) - 4h(2^n P) \right| \leq \sum_{n=M}^{N-1} 4^{-n-1} c \leq 4^{-M} c.$$

Thus, the sequence $4^{-n}h(2^nP)$ is Cauchy and hence converges.

2. This follows from the argument in part (1), taking $M = 0$ and letting $N \to \infty$ in the estimate $|4^{-N}h(2^NP) \to 4^{-M}h(2^MP)| \leq 4^{-M}c$ for some constant c.

3. This follows from part (2) and Lemma 3.1.2, as if $|S|$ is infinite, then choosing sufficient c, there would be infinitely many P with $H(P) \leq c$.

4. We first claim $h(mP) = m^2h(P) + c$ for some constant $c > 0$ that depends on P. We prove the claim by induction. The case $m = 1$ holds, and by Lemma 3.1.10, we have for some $c' > 0$

$$h([m+1]P) = -h([m-1]P) + 2h([m]P) + 2h(P) + c'.$$

By our induction hypothesis, we then have the right hand size is equal to

$$(-(m-1)^2 + 2m^2 + 2)h(P) + c'' = (m+1)^2h(P) + c'',$$

for a constant c''. Hence, the claim follows by induction.
Lastly, the result for part (4) now follows by replacing P in the just proved claim with $[2^n]P$, dividing by $\frac{1}{4^n}$ and letting $n \to \infty$.

5. By Lemma 3.1.10, we have $h(P+Q) + h(P-Q) = 2h(P) - 2h(Q) + c$ for any $P, Q \in E(\mathbb{Q})$. Replacing P and Q with $[2^n]P$ and $[2^n]Q$ respectively, dividing by 4^n and letting n go to infinity, we then have

$$\widehat{h}(P+Q) + \widehat{h}(P-Q) = 2\widehat{h}(P) + 2\widehat{h}(Q)$$

as claimed.

6. If P is a torsion point, then $[2^n]P$ takes on only finitely many values as n goes to infinity, so $4^{-n}h(2^nP) \to 0$ as $n \to \infty$. Conversely, if $\widehat{h}(P) = 0$, then for every integer m, we have $\widehat{h}([m]P) = m^2\widehat{h}(P) = 0$. By part (ii), there exists a constant $c > 0$ such that

$$h([m]P) = |\widehat{h}([m]P) - h([m]P)| \leq c.$$

As the set of points P such that $h(P) \leq c$ is finite, and all powers of P are contained in this finite set, it follows that P must be of finite order.

□

3.2 The Weak Mordell-Weil Theorem

In this section, we show that for an elliptic curve E over $\mathbb{Q}$, that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite. As $\mathrm{char}(\mathbb{Q}) \neq 2, 3$, we may assume that E is of the form

$$y^2 = x^3 + ax + b = (x-\alpha)(x-\beta)(x-\gamma), \tag{3.2.1}$$

for some $a, b \in \mathbb{Q}$. We first assume that each of the roots α, β, γ of $x^3 + ax + b$ are in $\mathbb{Z}$, and then prove the result in general. We begin with the following result, whose proof may be found in [2, Chapter 4, Theorem 4.2]:

Proposition 3.2.1. *Let K be a field of characteristic not equal to 2 or 3, and suppose E is an elliptic curve over K of the form $y^2 = (x-\alpha)(x-\beta)(x-\gamma)$, for some $\alpha, \beta, \gamma \in K$. Then a point (x, y) on E is a square in $E(K)$ if and only if $x-\alpha, x-\beta$, and $x-\gamma$ are squares in K.*

Proposition 3.2.2. *Let E be as in (4.1), and let $\varphi_\alpha : E(\mathbb{Q})/ \to \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ be the map*

$$\varphi_\alpha(P) = \begin{cases} \mathbb{Q}^{\times 2} & \textit{if } P = \mathcal{O} \\ (x-\alpha)\mathbb{Q}^{\times 2} & \textit{if } P = (x, y) \textit{ and } x \neq \alpha \\ (\alpha-\beta)(\alpha-\gamma)\mathbb{Q}^{\times 2} & \textit{if } P = (\alpha, 0) \end{cases}$$

and similarly define φ_β. Then φ_α and φ_β are group homomorphisms, and hence each descend to homomorphisms $\varphi_\alpha, \varphi_\beta : E(\mathbb{Q})/2E(\mathbb{Q})/ \to \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. Moreover,

$$\varphi = \varphi_\alpha \times \varphi_\beta : E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathbb{Q}^\times/\mathbb{Q}^{\times 2} \times \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$$

is injective.

Proof. By definition of the group law and the fact that $\varphi(-P) = \varphi(P) = \varphi(P)^{-1}$, it suffices to show that if $P_1+P_2+P_3 = \mathcal{O}$, then $\varphi_\alpha(P_1)\varphi_\alpha(P_2)\varphi_\alpha(P_3) \in \mathbb{Q}^{\times 2}$. Note that if any of the P_i are the point $\mathcal{O}$, then the claim follows, so we may write $P_i = (x_i, y_i)$ for $i = 1, 2, 3$.

First suppose that none of the P_i are the point $(\alpha, 0)$, and let $y = mx + b$ be the line on which the P_i lie. As the P_i are in $E(\mathbb{Q})$, the roots of the polynomial $(x-\alpha)(x-\beta)(x-\gamma) - (mx+b)^2$ are precisely x_1, x_2 and x_3, thus

$$(x-\alpha)(x-\beta)(x-\gamma) - (mx+b)^2 = (x-x_1)(x-x_2)(x-x_3).$$

Hence, substituting in $x = \alpha$, we get

$$(m\alpha+b)^2 = (x_1-\alpha)(x_2-\alpha)(x_3-\alpha) = \varphi_\alpha(P_1)\varphi_\alpha(P_2)\varphi_\alpha(P_3),$$

so $\varphi_\alpha(P_1)\varphi_\alpha(P_2)\varphi_\alpha(P_3) \in \mathbb{Q}^{\times 2}$.

We now consider the case that one of the P_i is equal to $(\alpha, 0)$. Observe that indeed only one of the P_i may be $(\alpha, 0)$, otherwise the third point is necessarily $\mathcal{O}$, and we have already dealt with this case. Hence, without loss of generality, suppose $P_1 = (\alpha, 0)$. Then from the previous case, we obtain

$$(x-\alpha)(x-\beta)(x-\gamma) - (mx+b)^2 = (x-\alpha)(x-x_2)(x-x_3),$$

and so $mx+b = m(x-\alpha)$, as $(x-\alpha)$ must divide $(mx+b)^2$. Substituting this into the above expression, we obtain

$$(x-\beta)(x-\gamma) - m^2(x-\alpha) = (x-x_2)(x-x_3).$$

Lastly, substituting $x=\alpha$, we obtain $\varphi_\alpha(P_1)\varphi_\alpha(P_2)\varphi_\alpha(P_3) = 1 \in \mathbb{Q}^{\times 2}$, so φ_α is indeed a homomorphism. Similarly, φ_β is a homomorphism, and so both descend to maps on $E(\mathbb{Q})/2E(\mathbb{Q})$, as thus $\varphi_\alpha(2P) = \varphi_\alpha(P)^2 \in \mathbb{Q}^{\times 2}$. It remains to show that φ is injective.

Suppose $\varphi(x,y) = 0$. We again consider two cases. First suppose that $(x,y) \neq \mathcal{O}, (\alpha,0)(\beta,0)$. Then if $\varphi(x,y)=0$, we have that both $(x-\alpha)$ and $(x-\beta)$ are squares in $\mathbb{Q}^\times$. As $y^2 = (x-\alpha)(x-\beta)(x-\gamma)$, we thus have that $(x-\gamma)$ is a square in $\mathbb{Q}^\times$ as well. Thus, by Proposition 3.2.1, there exists $(x',y') \in E(\mathbb{Q})$ such that $2(x',y') = (x,y)$, and so $(x,y) \in 2E(\mathbb{Q})$.

We now consider the case that $(x,y) = (\alpha,0)$. Then by assumption, $\varphi_\alpha(x,y) = (\alpha-\beta)(\alpha-\gamma)$ and $\varphi_\beta(x,y) = (\alpha-\beta)$ are both squares, and hence so is $(\alpha-\gamma)$. Thus, by Proposition 3.2.1, since 0 is also a square in $\mathbb{Q}$, there exists $(x',y') \in E(\mathbb{Q})$ such that $2(x',y') = (\alpha,0)$, and so $(\alpha,0) \in 2E(\mathbb{Q})$. Similarly, the argument proceeds if $(x,y) = (\beta,0)$. Thus, φ is injective. □

We can now prove the Weak-Mordell Weil theorem in the case that all the roots of the cubic defining E are integers:

Theorem 3.2.3. *Let E be as in (3.2.1) such that each of α,β,γ are in $\mathbb{Z}$. Then $E/2E(\mathbb{Q})$ is finite.*

Proof. Let P denote the set of primes in $\mathbb{Z}$ (including negatives). By unique factorization of integers, we may write

$$\mathbb{Q}^\times/\mathbb{Q}^{\times 2} = \{\pm 2^{n_1}3^{n_2}5^{n_3}7^{n_4}\cdot \ldots \mid n = (n_i) \in \{0,1\}^{\mathbb{N}}\} \cong \bigoplus_{p\in P} \mathbb{Z}_2.$$

Identifying $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ with $A := \oplus_{p\in P}\mathbb{Z}_2$, we will show that the image of φ in Proposition 3.2.2 is contained in summands of $A\times A$ such that p divides the discriminant d of $(x-\alpha)(x-\beta)(x-\gamma)$.

Let $(x,y) = (\frac{n_1}{m_1}, \frac{n_2}{m_2}) \in E(\mathbb{Q})\backslash\mathcal{O}$, where $x \neq \alpha,\beta,\gamma$ and let $p \in P$ be positive. Next, let $a := v_p(x-\alpha), b := v_p(x-\beta)$, and $c := v_p(x-\gamma)$, where v_p is the p-adic valuation on $\mathbb{Q}$. Suppose that $a<0$, then as $\alpha \in \mathbb{Z}$, we have $p^{|a|}|m_1$. Hence, p^a divides each of $x-\alpha, x-\beta$, and $x-\gamma$, so a, b, and c are equal. As $(x-\alpha)(x-\beta)(x-\gamma) = x^3+ax+b = y^2$, we have that each of a, b and c are even, and thus the image of (x,y) in the p-th coordinate of $A\times A$ is 0. Similarly if either either b or c is less than zero.

Now suppose that $a>0$. If p does not divide d, then necessarily p does not divide $\alpha-\beta$ and hence $b \le 0$ as $x-\beta = (x-\alpha)+(\alpha-\beta)$. By the argument in the previous paragraph, if $b<0$, then the image of (x,y) in the p-th coordinate of $A\times A$ is 0, so we may assume then that $b=0$. By symmetry, we may also assume that $c=0$, and hence as $(x-\alpha)(x-\beta)(x-\gamma) = y^2$, we then have that a is even. Therefore, the image of (x,y) in the p-th coordinate of $A\times A$ is 0.

Finally, we consider the case that $x = \alpha, \beta$, or γ. In this case, if p does not divide the discriminant d, then by definition of φ_a and φ_b, p necessarily does not divide $\varphi_a(x)$ nor $\varphi_b(x)$ and hence the p-th coordinate of $\varphi(x, y)$ is 0. As φ is injective by Proposition 3.2.2, the result follows. □

Note that in the proof of theorem 3.2.3, we used the fact that $\mathbb{Z}$ is a unique factorization ring. In the case that each of the roots of the cubic polynomial defining our elliptic curve are not all integers, we require a different approach as the ring of integers of the splitting field of the cubic may not be a UFD. The full case is addressed in Section 4 of Chapter 4 of [2], and relies on the Dirichlet Unit Theorem, the finiteness of the class number for rings of algebraic integers, and the fact that rings of algebraic integers are Dedekind domains.

One proves that if k denotes the splitting field of $(x-\alpha)(x-\beta)(x-\gamma)$, that the kernel canonical map

$$E(\mathbb{Q})/2E(\mathbb{Q}) \to E(k)/2E(k)$$

has at most $2^{2[k:\mathbb{Q}]}$, and so it suffices to then show $E(k)/2E(k)$ is finite. This then follows by the following result:

Theorem 3.2.4. *Let k be a number field with ring of integers $\mathcal{O}_k$, then there exists a ring R such that $\mathcal{O}_k \subseteq R \subseteq k$ with*

1. *R is a principal ideal domain*
2. *The groups of units in R is finitely generated*

The proof of this theorem uses the facts from algebraic number theory listed above, and may be found in Section 9 of Chapter 4 of [2].

One then interprets units and primes of $\mathcal{O}_k$ as units and primes in the ring R obtained from Theorem 3.2.4 in order to write $k^\times/(k^{\times 2})$ as we did $\mathbb{Q}/\mathbb{Q}^{\times 2}$ in the proof of Theorem 3.2.3. The argument then proceeds as in Theorem 3.2.3 to show that $E(k)/2E(k)$ is finite, which in turn proves the Weak Mordell-Weil theorem in the general case by the remark prior to Theorem 3.2.4.

3.3 The Mordell-Weil Theorem and the Rank

We are now in a position to prove that $E(\mathbb{Q})$ is finitely generated:

Theorem 3.3.1. *Let E be an elliptic curve over $\mathbb{Q}$, then $E(\mathbb{Q})$ is a finitely generated abelian group.*

Proof. By the previous section, we know that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite, hence

$$E(\mathbb{Q})/2E(\mathbb{Q}) = \{R_1 2E(\mathbb{Q}), \ldots, R_n 2E(\mathbb{Q})\}$$

for some $n \in \mathbb{N}$. Without loss of generality, take $R_1 \in 2E(\mathbb{Q})$ and n minimal. Next, let c be the maximum of the $\widehat{h}(R_i)$, and let $\{Q_1, \ldots, Q_m\}$ be the (finite) set of all points in $E(\mathbb{Q})$ such that $\widehat{h}(Q_i) \leq c$. Let A be the subgroup of $E(\mathbb{Q})$ generated by the Q_i and by way of contradiction, suppose $A \neq E(\mathbb{Q})$. Then there exists $P \in E(\mathbb{Q})\backslash A$, and taking P to be such that $\widehat{h}(P)$ is minimal, we have that there exists an R_i such that $P - R_i \in 2E(\mathbb{Q})$. Hence, there exists $Q \in E(\mathbb{Q})$ such that $P - R_i = 2Q$. Therefore, we have that

$$4\widehat{h}(Q) = \widehat{h}(2Q) = \widehat{h}(P - R_i) = 2\widehat{h}(P) + 2\widehat{h}(R_i) - \widehat{h}(P + R_i) \leq 2\widehat{h}(P) + 2\widehat{h}(R_i).$$

By construction of c, we also have

$$2\widehat{h}(P) + 2\widehat{h}(R_i) \leq 2\widehat{h}(P) + 2c < 2\widehat{h}(P) + 2\widehat{h}(P) = 4\widehat{h}(P).$$

Hence, we obtain that $\widehat{h}(Q) < \widehat{h}(P)$, and so by minimality of $\widehat{h}(P)$, we obtain $Q \in A$. Therefore, $P = R_i + 2Q \in A$, which is a contradiction.

Thus, $A = E(\mathbb{Q})$, so $E(\mathbb{Q})$ is finitely generated. □

By Theorem 3.2.4, for an elliptic curve E over $\mathbb{Q}$, $E(\mathbb{Q})$ is a finitely generated abelian group. Hence, by the fundamental theorem for finitely generated abelian groups, $E(\mathbb{Q})$ is isomorphic to $\mathbb{Z}^r \oplus T$, where T is a finite abelian group.

This motivates the following definition:

Definition 3.3.2. Let E be an elliptic curve over $\mathbb{Q}$, with $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T$. The integer r in this direct sum is known as the *rank* of E, or the *geometric rank* of the elliptic curve E.

Example.

1. Let E be the elliptic curve defined by $y^2 = x^3 + 10x + 5$, then, via Sage, one can compute $E(\mathbb{Q}) \cong \mathbb{Z}$
2. Let E be the elliptic curve defined by $y^2 = x^3 - 7x + 6$, then, via Sage, one can compute $E(\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

A natural question to ask is whether r may be arbitrarily large, and what the possibilities for the T are. The second question turns out to be much easier to answer than the first. It is a theorem of Mazur that the following are the only possibilities for T up to isomorphism:

Theorem 3.3.3. *(Mazur)*
Let E be an elliptic curve over $\mathbb{Q}$, with $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T$. Then

$$T \cong \begin{cases} \mathbb{Z}/n\mathbb{Z} & (n = 1, \ldots, 10 \textit{ or } 12); \textit{ or} \\ \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} & (n = 1, 2, 3 \textit{ or } 4) \end{cases}$$

The question on the boundedness of the rank is another matter, and in fact remains an open problem.

The largest known possibility for the rank of an elliptic curve was found by Elkies in 2006, when he found a curve of rank at least 28:

$$y^2+xy+y = x^3-x^2-20067762415575526585033208209338542750930230312178956502x$$

$+3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9$

The problem of determining if there is a bound on the rank is a well-studied problem in number theory and has motivated much research, including a conjecture of Birch and Swinnerton-Dyer.

3.4 Birch and Swinnerton-Dyer Conjecture

Before we can state this conjecture, we must introduce a bit of new machinery. Throughout this section, we assume that E is an elliptic curve over $\mathbb{Q}$, with defining cubic of the form $y^2 = x^3 + ax + b$, where a and b are integers.
We begin with the following definition:

Definition 3.4.1. Let p be prime, and let $\widetilde{E}$ denote the reduction curve of E modulo p. Then we say E has *good reduction* modulo p if $\widetilde{E}$ is an elliptic curve. If $\widetilde{E}$ is singular at a point $P \in \widetilde{E}(\mathbb{F}_p)$, then we say that E has *bad reduction* at p.

If E has bad reduction at a prime p, with $\widetilde{E}$ singular at a point $P = (x_0, y_0)$, then we may write the Taylor expansion of $y^2 - x^3 - ax - b$ around P as:

$$((y - y_0) - \alpha(x - x_0))((y - y_0) - \beta(x - x_0)) - (x - x_0)^3,$$

where $\alpha, \beta \in \overline{\mathbb{F}_p}$. In the case that $\alpha \neq \beta$, then we say P is a *node*, and if $\alpha = \beta$, we say that P is a *cusp*.

We now have the following definition:

Definition 3.4.2. Suppose E has bad reduction at a prime p, with $\widetilde{E}$ singular at a point P. Then

1. If $\widetilde{E}$ has a cusp at P, we say that E has *additive reduction.*
2. If $\widetilde{E}$ has a node at P, then we say E has *multiplicative reduction.* If both α and β are actually elements of $\mathbb{F}_p$ then the reduction is referred to as *split* multiplicative, and is called *non-split* multiplicative otherwise

If E has good reduction at a prime p, denote by N_p the cardinality $\#\widetilde{E}(\mathbb{F}_p)$, and define $a_p := p + 1 - N_p$. Note by Hasse's inequality, that $|a_p| \leq 2\sqrt{p}$.
We can now define the L-function of E:

Definition 3.4.3. Define the *local factor at p* of the L-series of E to be

$$L_p(T) := \begin{cases} 1 - a_pT + pT^2, \text{ if } E \text{ has good reduction at } p \\ 1 - T, \text{ if } E \text{ has split multiplicative reduction at } p \\ 1 + T, \text{if } E \text{ has non-split multiplicative reduction at } p \\ 1, \text{ if } E \text{ has additive reduction at } p \end{cases}$$

and define the L-function of E by

$$L(E, s) := \prod_{\substack{p \geq 2 \\ p \text{ prime}}} \frac{1}{L_p(p^{-s})}$$

It is a fact [c.f. 3, Remark 5.1.2] that $L(E, s)$ converges and is analytic whenever the real part of s is larger than $3/2$. However, $L(E, s)$ actually has an analytic continuation to all of $\mathbb{C}$ and moreover satisfies a certain functional equation. This functional equation depends on a certain quantity called the *conductor* $N_{E/\mathbb{Q}}$ of E, which we will not define, but the overall functional equation is as follows:

Theorem 3.4.4. *Let E be an elliptic curve over $\mathbb{Q}$, then $L(E, s)$ has an analytic continuation to all of $\mathbb{C}$. Define*

$$\Lambda(E, s) := (N_{E/\mathbb{Q}})^{s/2}(2\pi)^{-s}\Gamma(s)L(E, s),$$

where $\Gamma(s)$ is the Gamma function, then

$$\Lambda(E, s) := w \cdot \Lambda(E, 2 - s),$$

where w is ± 1, and is called the root number of E.

Theorem 3.4.4 actually follows from a conjecture called the Taniyama-Shimura-Weil conjecture, which Taylor and Wiles proved a special case of in proving Fermat's last theorem. The conjecture was later proved in full by Breuil et al.

We can finally state the Birch and Swinnerton-Dyer conjecture:

Conjecture 3.4.5. *(Birch and Swinnerton-Dyer)*
Let E be an elliptic curve over $\mathbb{Q}$, with $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T$. Then $L(E, s)$ has a zero at $s = 1$ of order r.

The Birch and Swinnerton-Dyer conjecture remains wide open and has only been proved in a few special cases. It is known by a theorem of Gross-Zagier and Kolyvagin that in the case $\mathrm{ord}_{s=1}L(E, s) \leq 1$, that then the Birch and Swinnerton-Dyer conjecture is true. However the full conjecture is unknown, and is one of the most famous open problems in the study of elliptic curves.

Bibliography

[1] S. Anni, *Elliptic Curves*, available at: https://wwwproxy.iwr.uni-heidelberg.de/groups/arith-geom/anni/MA426.pdf

[2] A.W. Knapp, *Elliptic Curves*, Princeton University Press, 1992.

[3] Álvaro Lozano-Robledo, *Elliptic Curves, Modular Forms, and Their L-functions*, Student Mathematical Library IAS/Park City Mathematical Subseries, 2011

[4] J.H. Silverman, *The Arithmetic of Elliptic Curves*, GTM 106, Springer, 1986.

[5] J.H. Silverman, J. Tate *Rational Points on Elliptic Curves*, Springer 1992.

[6] I. Rapinchuk, *Elliptic Curves with Complex Multiplication and Kronecker's Jugendtraum*

[7] I. Rapinchuk, *On Bezout's Theorem and Some of its Applications*