# ELLIPTIC CURVES AND THE MORDELL-WEIL THEOREM

DANIEL BROUS

Abstract. Elliptic curves are non-singular cubic curves, and they present a use to number theorists because they are intimately connected with a lot of important mathematical objects. Surprisingly, if one looks at an elliptic curve and considers only the rational points on this curve, then it can be shown that this set forms an abelian group under a particularly defined operation. In this paper, using the techniques of algebraic number theory, we will prove the Mordell-Weil Theorem, which says that this group is finitely generated.

## Contents

## 1. Introduction to Projective Space and Elliptic Curves

**Definition 1.1.** Given a field $K$ and some $(x, y, z), (a, b, c) \in K^3 \setminus \{(0, 0, 0)\}$, we write that $(x, y, z) \sim (a, b, c)$ if there exists some $k \in K$ such that $(x, y, z) = (ka, kb, kc)$.

**Lemma 1.2.** *As defined, $\sim$ is an equivalence relation on $K^3$.*

*Proof.* **Reflexive:**
Since $K$ is a field, there exists some element $1 \in K$ such that for all $k \in K$,

*Date*: DEADLINES: Draft AUGUST 14 and Final version AUGUST 28, 2021.

$1 \cdot k = k$, so if $(x, y, z) \in K^3$, then $(x, y, z) = (1 \cdot x, 1 \cdot y, 1 \cdot z)$, which means that $(x, y, z) \sim (x, y, z)$.

**Symmetric:**
If $(x, y, z) \sim (a, b, c)$, then $(x, y, z) = (ka, kb, kc)$ for some $k \in K$. We know that $k \neq 0$ because otherwise $(x, y, z) = (0, 0, 0)$, and we are excluding this element from our equivalence classes. Since $K$ is a field and $k \neq 0$, there exists some $k^{-1} \in K$ such that $k^{-1}k = 1$. Thus, $(k^{-1}x, k^{-1}y, k^{-1}z) = (a, b, c)$, and so $(a, b, c) \sim (x, y, z)$.

**Transitive:**
If $(x, y, z) \sim (a, b, c)$ and $(a, b, c) \sim (d, e, f)$, then there exists some $k_1, k_2 \in K$ such that $(x, y, z) = (k_1a, k_1b, k_1c)$ and $(a, b, c) = (k_2d, k_2e, k_2f)$. Thus, $(x, y, z) = (k_1k_2d, k_1k_2e, k_1k_2f)$. Since $K$ is a field, $k_1k_2 \in K$, so $(x, y, z) \sim (d, e, f)$. □

**Note:** We exclude $(0, 0, 0)$ from being equivalent to anything else under the equivalence relation for a couple reasons. For one, if we allow it to be included, then the proof that $\sim$ is symmetric will not hold. Also, if we defined $\sim$ in such a way that symmetry did hold and so it was an equivalence relation, then everything in $K^3$ would be in the same equivalence class because any point $(x, y, z) \sim (0, 0, 0)$.

**Definition 1.3.** Given a field $K$, we define the equivalence class

$$[x, y, z] := \{(a, b, c) \in K^3 \mid (a, b, c) \sim (x, y, z) \text{ and } (a, b, c) \neq (0, 0, 0)\}.$$

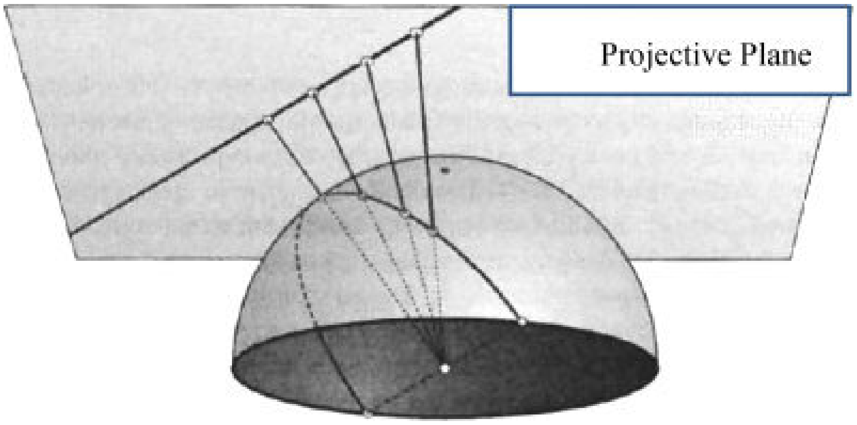
**Definition 1.4.** Given a field $K$, the **projective plane over** $K$ is the set of all these equivalence classes:

$$\mathbb{P}^2(K) := \{[x, y, z] \mid (x, y, z) \in K^3\}.$$

**Note:** Using the definitions, we can see that

$$\mathbb{P}^2(K) = \{[x, y, 1] \mid x, y \in K\} \cup \{[x, y, 0] \mid x, y \in K \text{ and } (x, y) \neq (0, 0)\}.$$

The set $\{[x, y, 1] \mid x, y \in K\}$ is bijective to $K^2$, which we will call the **affine plane**. We call the additional points $\{[x, y, 0] \mid x, y \in K \text{ and } (x, y) \neq (0, 0)\}$ the **points at infinity** because it can be shown that each of these points intersects all lines of a particular slope in the affine plane, but since they don't lie on the affine plane, we can think of them as points that are "infinitely far out" on the line. Here is a useful illustration of the projective plane, which is originally used in [4]:



It can be seen in this image that a line in the affine plane is projective down onto the semi-sphere via radial lines, and this is equivalent to what happens when a line in the affine plane is taken to its equivalent in the projective plane. Notice how the points on the bottom circle of the semi-sphere will never be mapped to by points in the affine plane. These are exactly the points at infinity, and if one draws a parallel line in the affine plane to the one drawn in the picture, then one can see that by projecting it down, it will intersect on the semi-sphere at those two points at infinity. Technically, those points on opposite sides of the circle are considered to be the same point at infinity because they represent the same equivalence class.

The solution set of a polynomial equation $p(x, y) = 0$ defined in the affine plane can be extended to the solution set of a polynomial equation in the projective plane which can obtain by multiplying each term by a coefficient of $z^d$ where $d$ is the minimal degree for each term to make the sum of the degrees of $x$, $y$ and $z$ in each term the same. For example, if $g(x, y) = x^6 + xy + 1$, then the equation in the projective plane which extends the solution set is given by $g(x, y, z) = x^6 + xyz^4 + z^6 = 0$. This equation is called the **homogeneous form** of $g$. This works because if $(x, y, z)$ is a solution to the homogeneous equation, then $(kx, ky, kz)$ is also a solution to the homogeneous equation for any $k \in K$. This follows precisely from the fact that all homogeneous equations have the same sum of degrees of each variable in every term, so if every term has a total degree of $d$, then we will always be able multiply everything by $k^d$ and distribute one $k$ to each $x$, $y$ and $z$. As an example, we can see that if $g(x, y, z) = 0$, then

$$\begin{aligned} 0 &= k^6 g(x, y, z) \\ &= k^6 x^6 + k^6 xyz^4 + k^6 z^6 \\ &= (kx)^6 + (kx)(ky)(kz)^4 + (kz)^6 \\ &= g(kx, ky, kz). \end{aligned}$$

Thus, homogeneous equations are "well-defined" as having solutions in the projective plane. Also, setting $z = 1$, we return our original affine equation, so the homogeneous equation solution set "contains" the affine equation solution set (in the sense that there is an isomorphism between the points in the solution set of the homogeneous equation where $z = 1$ and the entire solution set of the affine equation).

**Definition 1.5** (Elliptic Curve)**.** Given a field $K$ with characteristic zero, then an **elliptic curve** $E(K)$ is the subset of $\mathbb{P}^2(K)$ which satisfies a homogeneous equation

$$F(x, y, z) := y^2 z - x^3 - axz^2 - bz^3 = 0,$$

where $a, b \in K$ and the tangent vector to the curve never vanishes; that is, $\left(\frac{\partial F}{\partial x}(P), \frac{\partial F}{\partial y}(P), \frac{\partial F}{\partial z}(P)\right) \neq (0, 0, 0)$ for all $P \in E(K)$.

**Note:** While Elliptic curves can be defined with fields of characteristic other than zero, since we will only prove the Mordell-Weil Theorem for the field of rational numbers, $\mathbb{Q}$, and $\mathbb{Q}$ has characteristic zero, in order to avoid running into case work, we will assume that $K$ from now on is an arbitrary field of characteristic zero.

**Note:** If we take some elliptic curve $E(K)$ given by homogeneous equation $F(x, y, z) = 0$ and let $z = 0$, then we can see that the only way to satisfy the equation is to set $x = 0$. Thus, the only possible point in $\mathbb{P}^2(K) \cap E(K)$ which has $z = 0$ is $[0, 1, 0]$.

Thus, every elliptic curve $E(K)$ only has this one unique point at infinity, and so we will use a shorthand for this point:

$$\mathcal{O} := [0,1,0] \in \mathbb{P}^2(K).$$

**Note:** If we set $z = 1$, then the affine form of $E(K)$ is given by

$$y^2 = f(x) := x^3 + ax + b.$$

This $f(x)$ notation will be used for every elliptic curve $E(K)$ throughout the remainder of this paper, and $\theta_1, \theta_2, \theta_3 \in \overline{K}$ will be used to denote the roots of $f(x)$, where $\overline{K}$ is the algebraic closure of $K$. The equation for $E(K)$ is also called a "Weierstrass equation". This is because one can define an elliptic curve as a general cubic curve in the projective plane for which the tangent vector does not vanish, and one can show that every elliptic curve defined in this more general way has a unique corresponding elliptic curve defined by a Weierstrass equation such that there exists an invertible change of variables between the two curves (note that this invertible change of variables does not exist in fields of characteristic 2 or 3, but we will ignore this since we are only working with fields of characteristic zero). For more information on this, see chapter 2 of [3]. In this paper, we will only consider elliptic curves given by Weierstrass equations. We end this section with two important Lemmas.

**Lemma 1.6.** *If $E(K)$ is given in affine form by $y^2 = f(x) = x^3 + ax + b$, then $E(K)$ is an elliptic curve if and only if $4a^3 + 27b^2 \neq 0$.*

*Proof.* We can calculate that the tangent vector to the curve at $P = [x, y, z]$ is given by

$$(-3x^2 - az^2, 2yz, y^2 - 2axz - 3bz^2).$$

Note that if this is nonzero for $(x, y, z) \in K^3$, then it is nonzero for $(kx, ky, kz) \in K^3$ for any $k \in K \setminus \{0\}$. Therefore, whether this vector vanishes or not does not depend on the representation of $P$. If $z = 0$, then as was just shown earlier, the only possible point is $P = [0,1,0]$, and in the case, the tangent vector becomes $(0,0,1)$, and so it does not vanish. If $z = 1$, then the tangent vector becomes

$$(-3x^2 - a, 2y, y^2 - 2ax - 3b).$$

If $y \neq 0$, then the tangent vector doesn't vanish. It may vanish if $y = 0$, in which case the vector becomes

$$(-3x^2 - a, 0, -2ax - 3b).$$

In order for this to vanish, we must have that $-3x^2 = a$ and $4a^2x^2 = 9b^2$. Plugging one into the other, we get that

$$4a^3 + 27b^2 = 0.$$

Therefore, if $4a^3 + 27b^2 \neq 0$, then it is impossible for the tangent vector to vanish, and so $E(K)$ is an elliptic curve. Conversely, if $4a^3 + 27b^2 = 0$, then there are two cases. If $a = 0$, then it must be that $b = 0$, in which case the tangent vector vanishes at $P = [0,0,1]$. If $a \neq 0$, then the tangent vector vanishes at $P = [-3b/2a, 0, 1]$. Therefore, if $4a^3 + 27b^2 = 0$, then $E(K)$ is not an elliptic curve, and so by the contrapositive, if $E(K)$ is an elliptic curve, then $4a^3 + 27b^2 \neq 0$. □

**Lemma 1.7.** *If an elliptic curve $E(K)$ is given in affine form by $y^2 = f(x) = x^3 + ax + b$ and $\theta_1, \theta_2, \theta_3 \in \overline{K}$ are the roots, then*

$$[(\theta_1 - \theta_2)(\theta_2 - \theta_3)(\theta_1 - \theta_3)]^2 = -(4a^3 + 27b^2).$$

*Proof.* Since $\theta_1, \theta_2, \theta_3 \in \overline{K}$ are the roots, $f(x) = (x-\theta_1)(x-\theta_2)(x-\theta_3)$. We can calculate that

$$f'(x) = (x-\theta_1)(x-\theta_2) + (x-\theta_2)(x-\theta_3) + (x-\theta_1)(x-\theta_3).$$

But also,

$$f'(x) = 3x^2 + a.$$

Thus, plugging in each $\theta_i$ to each of these formulas, we see that

$$3\theta_i^2 + a = (\theta_i - \theta_j)(\theta_i - \theta_k)$$

where $(i, j, k)$ is a permutation of $(1, 2, 3)$. We can also see that

$$f(x) = (x-\theta_1)(x-\theta_2)(x-\theta_3) = x^3 - (\theta_1+\theta_2+\theta_3)x^2 + (\theta_1\theta_2+\theta_2\theta_3+\theta_1\theta_3)x - \theta_1\theta_2\theta_3.$$

Comparing this with $f(x) = x^3 + ax + b$, we can see that $\theta_1 + \theta_2 + \theta_3 = 0$, $\theta_1\theta_2 + \theta_2\theta_3 + \theta_1\theta_3 = a$, and $\theta_1\theta_2\theta_3 = -b$. Using the identity $(x+y+z)^2 = x^2 + y^2 + z^2 + 2(xy + yz + xz)$ with $x = \theta_1\theta_2$, $y = \theta_2\theta_3$ and $z = \theta_1\theta_3$, we can see that

$$\begin{aligned}\theta_1^2\theta_2^2 + \theta_2^2\theta_3^2 + \theta_1^2\theta_3^2 &= (\theta_1\theta_2 + \theta_2\theta_3 + \theta_1\theta_3)^2 - 2(\theta_1^2\theta_2\theta_3 + \theta_1\theta_2^2\theta_3 + \theta_1\theta_2\theta_3^2)\\ &= a^2 - 2\theta_1\theta_2\theta_3(\theta_1 + \theta_2 + \theta_3)\\ &= a^2.\end{aligned}$$

Using the same identity again but with $x = \theta_1$, $y = \theta_2$ and $z = \theta_3$, we can see that

$$\theta_1^2 + \theta_2^2 + \theta_3^2 = (\theta_1 + \theta_2 + \theta_3)^2 - 2(\theta_1\theta_2 + \theta_2\theta_3 + \theta_1\theta_3) = -2a.$$

Using many of these formulas, we can calculate that

$$\begin{aligned}&-[(\theta_1-\theta_2)(\theta_2-\theta_3)(\theta_1-\theta_3)]^2\\ &= [(\theta_1-\theta_2)(\theta_1-\theta_3)][(\theta_2-\theta_3)(\theta_2-\theta_1)][(\theta_3-\theta_1)(\theta_3-\theta_2)]\\ &= [3\theta_1^2 + a][3\theta_2^2 + a][3\theta_3^2 + a]\\ &= 27(\theta_1\theta_2\theta_3)^2 + 9a(\theta_1^2\theta_2^2 + \theta_2^2\theta_3^2 + \theta_1^2\theta_3^2) + 3a^2(\theta_1^2 + \theta_2^2 + \theta_3^2) + a^3\\ &= 27(-b)^2 + 9a(a^2) + 3a^2(-2a) + a^3\\ &= 4a^3 + 27b^2.\end{aligned}$$

Negating both sides gives the result. □

**Lemma 1.8.** *If an elliptic curve $E(K)$ is given in affine form by $y^2 = f(x) = x^3 + ax + b$, then $f(x)$ cannot have any repeated roots in $\overline{K}$.*

*Proof.* If $\theta_1, \theta_2, \theta_3 \in \overline{K}$ are the roots of $f(x)$, then suppose that $\theta_i = \theta_j$ for some $i \neq j$. Using Lemma 1.7,

$$4a^3 + 27b^2 = -[(\theta_1-\theta_2)(\theta_2-\theta_3)(\theta_1-\theta_3)]^2 = 0.$$

But since $E(K)$ is an elliptic curve, according to Lemma 1.6, this is a contradiction. Therefore, $f(x)$ has no repeated roots. □

## 2. Group Structure of $E(K)$

In this section, we will prove that $E(K)$ is a abelian group under a particularly defined operation.

2.1. **Defining Addition on affine points of $E(K)$.** Define addition on $E(K)$ implicitly by saying that $A, B, C \in E(K)$ are colinear in the projective plane if and only if $A + B + C = \mathcal{O}$, where we take $\mathcal{O}$ to be the identity of addition. In this section, aside from the associativity of addition, we will show that $E(K)$ forms a group under this operation. One condition that must be added is that if two of the points are identical, say $A = B$, then the line must not only intersect $A = B$ but also be tangent to the curve at that point. This allows for the uniqueness of inverses and the uniqueness of the sum $A + A$. To see a proof of associativity, see [1]. We can also see that addition defined in this way is commutative, because, assuming that the sum is unique, which will be proved, we have that the sum of $A$ and $B$ is defined to be the point $C$ such that $-C$ is colinear with $A$ and $B$, and if there is a unique point which is colinear with $A$ and $B$, then we will find the same point when trying to add $B$ and $A$.

2.2. **Finding the additive inverse.** We can see that if $C = \mathcal{O}$, then since $\mathcal{O}$ is defined to be the identity, we have that $A + B = \mathcal{O}$, so $B = -A$ is the additive inverse of $A$. A line in the projective plane looks like $0 = x + dy + ez$ for some $d, e \in K$. Plugging in $\mathcal{O}$ to this equation, we can see that $d = 0$, so the only lines in the projective plane that intersect $\mathcal{O}$ are those of the form $x = kz$ for some $k \in K$. Setting $z = 1$, we can see that the affine form of this line is a vertical line in the $xy$-plane. If $A = \mathcal{O}$, then $B = \mathcal{O}$ as well, and this is consistent with the idea that $B$ is the inverse of $A$ because the additive identity should be its own inverse. If $A = (x_1, y_1)$ is affine, then the line which $B$ must lie on is $x = x_1$. If $y_1 = 0$, then we can see that since $f(x_1) = 0$, the only affine point on the curve with $x$-value $x_1$ is $(x_1, y_1)$, and so $B = A$. We can see that this is consistent with the tangent condition because if $y_1 = 0$, then the tangent line in the affine plane is vertical. If $y_1 \neq 0$, then we can see that it cannot be that $B = A$, because if this is the case, then the tangent condition requires that the vertical line $x = x_1$ must be tangent to the curve at $A$, but it is not, since the tangent line is not vertical at $(x_1, y_1)$ when $y_1 \neq 0$. If $B = (x_1, -y_1)$, then this point is still on the curve because $(-y_1)^2 = y_1^2 = f(x_1)$. Thus, $(x_1, -y_1)$ is the additive inverse of $(x_1, y_1)$.

2.3. **Proving that $E(K)$ is closed under addition.**

*Proof.* Since we define $\mathcal{O}$ to be the identity, we only need to consider cases with affine points. Thus, let $A = (x_1, y_1)$ and $B = (x_2, y_2)$. We aim to show that $A + B$ is unique and $A + B \in E(K)$.

**Case 1:** $x_1 = x_2$.
If $y_1 \neq y_2$, then since there are only two possible affine points with $x$-value $x_1 = x_2$, we must have that $y_2 = -y_1$, so $B = -A$. Therefore, as shown in the previous section, $A + B = \mathcal{O}$. If $y_1 = y_2 = 0$, then again, as shown in the previous section, $A + B = \mathcal{O}$. If $y_1 = y_2 \neq 0$, then we must use the tangent condition to find the sum. Since $A = B$, by our definition, $-(A + B)$ must lie on the tangent line to the curve at $A$. Since $y_1 \neq 0$, we can calculate that the slope of the tangent line is

$$\frac{dy}{dx} = \frac{3x_1^2 + a}{2y_1}.$$

The tangent line is thus given by the equation

$$y = g(x) := y_1 + \frac{3x_1^2 + a}{2y_1}(x - x_1).$$

Since the tangent line is not vertical, $\mathcal{O}$ cannot lie on the line, so the only possible points in $E(K)$ which can lie on the tangent line must be affine and of the form $(x, g(x))$, and thus it suffices to focus on points of this form. Define the polynomial

$$P(x) := f(x) - g(x)^2.$$

By definition, $r \in K$ is a root of $P(x)$ if and only if $(r, g(r)) \in E(K)$. We know that $(x_1, g(x_1)) = A \in E(K)$, and we can verify that

$$P(x_1) = f(x_1) - g(x_1)^2 = y_1^2 - y_1^2 = 0.$$

If we want $-(A+B)$ to be unique, then there must be one and only one other root of $P(x)$, $x_3 \in K$. Factored in $\overline{K}$, $P(x)$ will have three roots. We can expand out $P(x)$ to get that the degree two term's coefficient is

$$-\frac{9x_1^4 + 6ax_1^2 + a^2}{4y_1^2}.$$

Thus, since $P(x)$ is monic, the sum of the roots must be the additive inverse of this number. This number is also in $K$, so since two of the roots should be in $K$, the last should also be in $K$. Thus, the last root would have to be a repeated root of one of the other two. Since the line is tangent to the curve at $A$, we can guess that $x_1$ is the double root and check to see that the third root is in fact in $K$ and is indeed a root. Since we must have that

$$x_1 + x_1 + x_3 = \frac{9x_1^4 + 6ax_1^2 + a^2}{4y_1^2},$$

We can see that

$$x_3 = \frac{x_1^4 - 2ax_1^2 - 8bx_1 + a^2}{4y_1^2} \in K,$$

and one can verify that $P(x_3) = 0$. Therefore, our guess was correct and $P(x)$ has a double root $x_1$ and a single root $x_3$. Therefore $(x_3, g(x_3))$ is in fact the unique other point in $E(K)$ which lies on this tangent line. This means that $-(A+B)$ is unique, and so $A+B = (x_3, -g(x_3))$ is also unique. Also, since $-(A+B) \in E(K)$, so is $A+B$.

**Case 2:** $x_1 \neq x_2$.
In this case, we can see that the line going through $(x_1, y_1)$ and $(x_2, y_2)$ is given by the equation

$$y = g(x) := y_1 + \frac{y_2 - y_1}{x_2 - x_1}(x - x_1).$$

Since the line is not vertical, $\mathcal{O}$ cannot lie on the line, so the only possible points in $E(K)$ which can lie on the line must be affine and of the form $(x, g(x))$, and thus it suffices to focus on points of this form. Define the polynomial

$$P(x) := f(x) - g(x)^2.$$

By definition, $r \in K$ is a root of $P(x)$ if and only if $(r, g(r)) \in E(K)$. We know that $(x_1, g(x_1)) = A \in E(K)$ and $(x_2, g(x_2)) = B \in E(K)$, and we can verify that

$$P(x_1) = f(x_1) - g(x_1)^2 = y_1^2 - y_1^2 = 0.$$

and

$$P(x_2) = f(x_2) - g(x_2)^2 = y_2^2 - y_2^2 = 0.$$

If we want $-(A+B)$ to be unique, then there must be one and only one other root of $P(x)$, $x_3 \in K$. We already have two roots of $P(x)$, so there is definitely only one other root $x_3 \in \overline{K}$. We can expand out $P(x)$ to get that the degree two term's coefficient is

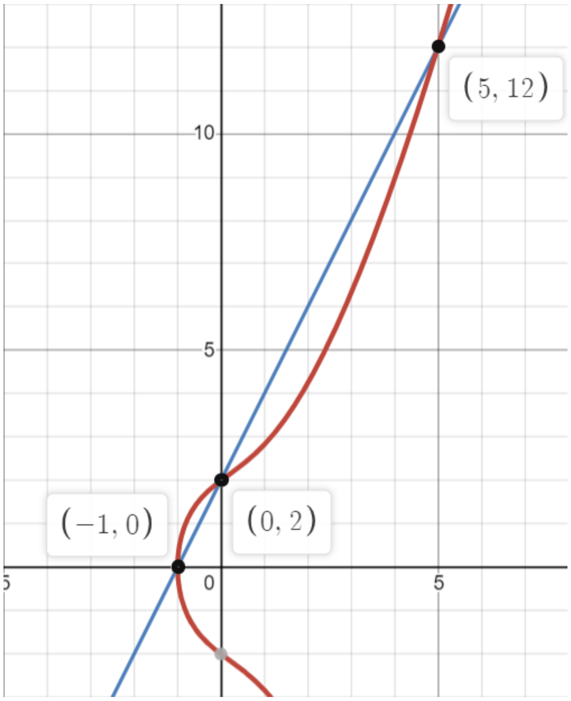
$$-\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2.$$

Since $P(x)$ is monic, the sum of the roots must be the additive inverse of this number. This number is also in $K$, so since $x_1, x_2 \in K$,

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \in K, \tag{2.1}$$

and one can verify that $P(x_3) = 0$. Therefore, $(x_3, g(x_3))$ is in fact the unique other point in $E(K)$ which lies on this line. This means that $-(A+B)$ is unique, and so $A + B = (x_3, -g(x_3))$ is also unique. Also, since $-(A+B) \in E(K)$, so is $A + B$. □

As described, the group addition has a nice visual interpretation. We can see in the following picture the elliptic curve $y^2 = x^3 + 3x + 4$ and the line going through three rational points:



The elliptic curve is the red curve, and for the part which is shown, it is clear that it is symmetric across the $x$-axis. This line is not tangent at any of the intersection points, which is consistent with the fact that these points are all different points. The sum of two points is the inverse of the third point for which they are colinear with, so in this picture, the we would have that $(-1,0) + (0,2) = (5,-12)$.

2.4. **Proving some useful identities.** In this subsection we will prove some identities that will be used in the proof of the Mordell-Weil Theorem. Suppose that $A, B \in E(K)$ and $A = (x_1, y_1)$, and $B = (x_2, y_2)$, and $x_1 \neq x_2$. Then if $C = (x_3, -y_3) := A + B$, as shown in the previous subsection, $x_1$, $x_2$ and $x_3$ are the roots of

$$P(x) = [x^3 + ax + b] - \left[y_1 + \frac{y_2 - y_1}{x_2 - x_1}(x - x_1)\right]^2.$$

Let $\theta = \theta_i$ for some $i \in \{1, 2, 3\}$ (recall that $\theta_i \in \overline{K}$ are the roots of $f(x)$), and let $\theta'$ and $\theta''$ be the other two roots of $f(x)$. Replacing $x$ by $t + \theta$, we can see that $x_1 - \theta, x_2 - \theta$ and $x_3 - \theta$ must be the roots of

$$P(t + \theta) = t(t + \theta - \theta')(t + \theta - \theta'') - \left[y_1 + \frac{y_2 - y_1}{x_2 - x_1}(t + \theta - x_1)\right]^2.$$

We can see that the second degree term of this polynomial has coefficient

$$-\left[y_1 + (\theta - x_1)\left(\frac{y_2 - y_1}{x_2 - x_1}\right)\right]^2 = \left[\frac{y_1(x_2 - \theta) - y_2(x_1 - \theta)}{x_2 - x_1}\right]^2,$$

so since $P(t + \theta)$ is monic, the additive inverse of this term is equal to the product of the roots. Thus,

$$(x_1 - \theta)(x_2 - \theta)(x_3 - \theta) = \left[\frac{y_1(x_2 - \theta) - y_2(x_1 - \theta)}{x_2 - x_1}\right]^2. \tag{2.2}$$

If $y_1 \neq 0$ and $C = (x_3, -y_3) := 2A$, then, as shown in the previous subsection, $x_1$ is a double root and $x_3$ is a single root of

$$Q(x) = (x - \theta_1)(x - \theta_2)(x - \theta_3) - \left[y_1 + \frac{3x_1^2 + a}{2y_1}(x - x_1)\right]^2.$$

Doing the same process as with the previous polynomial, setting $x = t + \theta$ and comparing the coefficient of the second degree term to the product of the roots of this new polynomial, we can see that

$$(x_1 - \theta)^2(x_3 - \theta) = \left[\frac{2y_1^2 + (3x_1^2 + a)(\theta - x_1)}{2y_1}\right]^2. \tag{2.3}$$

We can also see that

$$\begin{aligned} y_1^2 &= f(x_1) \\ &= f(x_1) - f(\theta) \\ &= x_1^3 + ax_1 + b - \theta^3 - a\theta - b \\ &= (x_1 - \theta)(x_1^2 + x_1\theta + \theta^2 + a). \end{aligned}$$

Plugging this back into (2.3) and rearranging gives us

$$x_3 - \theta = \left[\frac{-x_1^2 + 2\theta^2 + 2\theta x_1 + a}{2y_1}\right]^2. \tag{2.4}$$

Rearranging (2.1), we can see that

$$\begin{aligned}
x_3 &= \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_2 - x_1 \\
&= \frac{-(x_1 + x_2)(x_2 - x_1)^2 + (y_2 - y_1)^2}{(x_2 - x_1)^2} \\
&= \frac{-(x_1^2 - x_2^2)(x_1 - x_2) + y_2^2 - 2y_1y_2 + y_1^2}{(x_2 - x_1)^2} \\
&= \frac{-(x_1^2 - x_2^2)(x_1 - x_2) + (x_2^3 + ax_2 + b) - 2y_1y_2 + (x_1^3 + ax_1 + b)}{(x_2 - x_1)^2} \\
&= \frac{-x_1^3 - x_2^3 + x_1x_2^2 + x_1^2x_2 + x_2^3 + ax_2 - 2y_1y_2 + x_1^3 + ax_1}{(x_2 - x_1)^2} \\
&= \frac{x_1x_2^2 + x_1^2x_2 + ax_2 - 2y_1y_2 + ax_1 + 2b}{(x_2 - x_1)^2} \\
&= \frac{(x_1x_2 + a)(x_1 + x_2) + 2b - 2y_1y_2}{(x_2 - x_1)^2}
\end{aligned}$$

This gives us our final useful relation,

$$x_3 = \frac{(x_1x_2 + a)(x_1 + x_2) + 2b - 2y_1y_2}{(x_2 - x_1)^2}. \tag{2.5}$$

## 3. A Useful Group Homomorphism

In this section, we will define a homomorphism $\phi$ which will be used in subsequent sections of the paper, and we will show that it is a homomorphism and find its kernel.

### 3.1. Defining $\phi$.

**Definition 3.1.** If $R$ is a ring then $R[x_1, \ldots, x_n]$ is defined to be the smallest ring containing $R$ and $\{x_1, \ldots, x_n\}$.

**Note:** Equivalently, it is the ring of formal polynomials in $\{x_1, \ldots, x_n\}$ with coefficients in $R$, where formal here means that $\{x_1, \ldots, x_n\}$ are not necessarily variables but can signify anything. Anywhere in this paper, if we write $R[x]$, then we will take it to mean the ring of actual polynomials in $x$–that is, an element in $f(x) \in R[x]$ can be evaluated at some point $x_0 \in R$ to take some value $f(x_0) \in R$.

Now consider the polynomial ring $K[x]$. We know that $f(x) \in K[x]$, so the principle ideal $(f(x)) \subseteq K[x]$. Consider the quotient space $K[x]/(f(x))$. If we define $\xi := x \mod f(x)$, then we can see that $K[x]/(f(x)) = K[\xi]$, the ring of polynomials of $\xi$ with coefficients in $K$. Consider the set of units $U \subseteq K[x]/(f(x))$. We will now prove an important Lemma:

**Lemma 3.2.** *Suppose that $R$ is a ring and $U$ is the set of units of $R$. Then $U$ forms a group under multiplication in $R$.*

*Proof.* If $u, v \in U$, then by the definition of being a unit, there exists a multiplicative inverse for each of these elements. In other words, there exists some $p, q \in R$ such that $pu = up = 1$ and $qv = vq = 1$. We can also calculate that

$$uvqp = up = 1 = qv = qpuv,$$

so since $qp \in R$ it is the multiplicative inverse of $uv$, and so $uv \in U$. Therefore, $U$ is closed under multiplication in $R$. Since $R$ is a ring with identity element 1 and our operation in $U$ is the same as the operation in $R$, multiplication in $U$ is associative. Since $1 \cdot 1 = 1$, $1|1$ and so $1 \in U$, so since $1 \in R$ is the identity element, 1 is also the identity element in $U$. Therefore, $U$ is a group under multiplication in $R$. □

**Lemma 3.3.** *If $R$ is a principal ideal domain, $(r)$ is an ideal generated by $r \in R$, and $U$ is the group of units of $R/(r)$, then $U$ is exactly the set of elements in $R$ which are coprime with $r$, projected into $R/(r)$.*

*Proof.* **Part 1:** If $q \in R$ is coprime with $r$, then $q \mod r \in U$.
Suppose $q \in R$ is coprime with $r$. By Bezout's Lemma for principal ideal domains, there exists some $p, n \in R$ such that $qp - nr = 1 \in R$. Therefore, $qp = 1 \mod r$. Therefore, $q|1 \mod r$, so by definition, $q \mod r \in U$.

**Part 2:** If $u \in U$, then $u = q \mod r$ for some $q \in R$ which is coprime with $r$.
Since $u \in U$, $u = q \mod r$ for some $q \in R$. Since $u$ is a unit, there exists some $p \in R$ such that $qp = 1 \mod r$. Thus, there exists some $n \in R$ such that $qp = 1 + nr$, so $qp - nr = 1 \in R$. If $q$ and $r$ had some common factor which is not a unit, we could pull it out of the left hand side, but not out the right hand side because only units will divide 1. Thus, $q$ and $r$ are coprime. □

From these two Lemmas, we now know that $U$ is a group and that elements in $U$ are the projection of polynomials that are coprime with $f(x)$ into $K[\xi]$. Now let's define a function $\phi : E(K) \to U/U^2$ as follows: Let $\phi(\mathcal{O}) = 1 \in U/U^2$. If $P = (\alpha, \beta) \in E(K)$ and $\beta \neq 0$, then $f(\alpha) = \beta^2 \neq 0$, so $\alpha - x$ is coprime with $f(x)$. Thus, by Lemma 3.3, since $K[x]$ is a principal ideal domain, $\alpha - \xi \in U$. Therefore, we can define $\phi(P)$ to be the projection of $\alpha - \xi$ from $U$ into $U/U^2$. If $P = (\alpha, 0)$, then $\alpha$ is a root of $f$, so

$$f(x) = (x - \alpha)g(x)$$

for some $g(x) \in K[x]$. By the Chinese remainder theorem,

$$K[\xi] \cong K[x]/(x - \alpha) \oplus K[x]/(g(x)). \tag{3.4}$$

We know by Lemma 1.8 that $g(\alpha) \neq 0$, because otherwise $f$ would have a repeated root in $K$. Thus, using the product rule,

$$f'(x) = (x - \alpha)g'(x) + g(x),$$

so when we plug in $\alpha$, we get that

$$f'(\alpha) = g(\alpha) \neq 0.$$

Therefore, $f'(\alpha)|1 \mod (x - \alpha)$, and so $f'(\alpha)$ is a unit of $K[x]/(x - \alpha)$. Also, since $g(\alpha) \neq 0$, $\alpha - x$ is coprime with $g(x)$, and thus, by Lemma 3.3, $\alpha - x$ is a unit in $K[x]/(g(x))$. Using the fact that these are units in their respective rings, there exists some $u \in K[x]/(x - \alpha)$ and some $v \in K[x]/(g(x))$ such that

$$f'(\alpha)u = 1 \mod (x - \alpha)$$

and

$$(\alpha - x)v = 1 \mod g(x).$$

By the Chinese remainder theorem, there exists a ring isomorphism $\rho : K[x]/(x-\alpha) \oplus K[x]/(g(x)) \to K[x]/(f(x))$, and so by the properties of ring isomorphisms,

$$\rho(f'(\alpha), \alpha - x)\rho(u, v) = \rho(f'(\alpha)u, (\alpha - x)v) = \rho(1, 1) = 1 \mod f(x).$$

Therefore,

$$\rho(f'(a), \alpha - x) \in U.$$

We define $\phi(P)$ in this case to be the projection of this element into $U/U^2$.

### 3.2. **Proving $\phi$ is a Group Homomorphism.**

*Proof.* We want to show that for any points $P, Q \in E(K)$, $\phi(P+Q) = \phi(P)\phi(Q)$. For any affine point $P = (\alpha, \beta)$, since $\phi(P)$ only depends on $\alpha$ and $-P = (\alpha, -\beta)$, $\phi(P) = \phi(-P)$. Since $\mathcal{O} = -\mathcal{O}$, $\phi(P) = \phi(-P)$ for all $P \in E(K)$. Also, since $\phi(P) \in U/U^2$, $\phi(P)^2 = 1 \in U/U^2$. Therefore, it suffices to prove that $\phi(P+Q)\phi(-P)\phi(-Q) = 1 \in U/U^2$ because this would imply that

$$\phi(P)\phi(Q) = \phi(P+Q)\phi(-P)\phi(-Q)\phi(P)\phi(Q) = \phi(P+Q)\phi(P)^2\phi(Q)^2 = \phi(P+Q).$$

Even further, it suffices to prove that if $A+B+C = \mathcal{O}$ on $E(K)$, then $\phi(A)\phi(B)\phi(C) = 1 \in U/U^2$. This is because if $A + B + C = \mathcal{O}$, then $C = -A - B$. The condition that $A + B + C = \mathcal{O}$ implies that $A, B$ and $C$ are colinear. Suppose that one of the points is not affine, say $A = \mathcal{O}$. Then $C = -B$, so

$$\phi(A)\phi(B)\phi(C) = 1 \cdot \phi(B)\phi(-B) = 1 \cdot \phi(B)^2 = 1 \in U/U^2.$$

In the other case, let's suppose that all three points are affine, so $A = (x_1, y_1)$, $B = (x_2, y_2)$ and $C = (x_3, y_3)$. Suppose two $x$-values are the same, say $x_1 = x_2$. If $y_1 = -y_2$, it would have to be the case that $C = \mathcal{O}$, which is a case we already covered. If $y_1 = y_2 = 0$, then again, $C = \mathcal{O}$, which is a case we already covered. If $y_1 = y_2 \neq 0$, then, as seen in the previous section of this paper, since $A$, $B$ and $C$ are colinear and $A = B$, the line between them is a tangent line, and since the tangent line is not vertical, there exists some line $y = cx + d$ such that

$$f(x) - (cx + d)^2 = (x - x_1)(x - x_2)(x - x_3). \tag{3.5}$$

The same can said about the case where none of the three $x$-values are the same (except the line $y = cx + d$ will necessarily look different, but for our purposes it does not matter), so we can lump in this case as well, assuming that $y_i \neq 0$ for all $i = 1, 2, 3$. Reducing both sides modulo $f(x)$, this equation becomes

$$-(c\xi + d)^2 = (\xi - x_1)(\xi - x_2)(\xi - x_3) = -(x_1 - \xi)(x_2 - \xi)(x_3 - \xi).$$

Taking out the factor of $-1$ on both sides and then reducing both sides modulo $U^2$, the equation transforms into

$$1 = \phi(A)\phi(B)\phi(C).$$

Now suppose that $y_1 = 0$. We can see that in this case, since $f(x) = (x - x_1)g(x)$ for some $g(x) \in K[x]$, if we let $\rho$ be the ring isomorphism given by the Chinese remainder theorem,

$$\begin{aligned}&\phi(A)\phi(B)\phi(C)\\ &= \rho(f'(x_1) \mod (x-x_1), (x_1-x) \mod g(x))(x_2-\xi)(x_3-\xi)\\ &= \rho(f'(x_1)(x_2-x)(x_3-x) \mod (x-x_1), (x_1-x)(x_2-x)(x_3-x) \mod g(x))\\ &= \rho(f'(x_1)(x_2-x)(x_3-x) \mod (x-x_1), (cx+d)^2 - f(x) \mod g(x))\\ &= \rho(f'(x_1)(x_2-x)(x_3-x) \mod (x-x_1), (cx+d)^2 \mod g(x)).\end{aligned}$$

Differentiating (3.5), we see that

$$f'(x) - 2c(cx+d) = (x-x_2)(x-x_3) + (x-x_1)(x-x_2) + (x-x_1)(x-x_3).$$

Plugging in $x_1$ and both sides, we get that

$$f'(x_1) = (x_1-x_2)(x_1-x_3) + 2c(cx_1+d)^2.$$

Plugging $x_1$ into (3.5), we see that

$$cx_1 + d = 0,$$

so plugging this into the previous equation, we get that

$$f'(x_1) = (x_1-x_2)(x_1-x_3).$$

Plugging this back into the equation for $\phi(A)\phi(B)\phi(C)$ and using the fact that $x_2 - x = x_2 - x_1 \mod (x-x_1)$ and $x_3 - x = x_3 - x_1 \mod (x-x_1)$, we get that

$$\phi(A)\phi(B)\phi(C) = \rho((x_1-x_2)^2(x_1-x_3)^2 \mod (x-x_1), (cx+d)^2 \mod g(x)).$$

Since both of the terms inside the $\rho$ function are squares, they are equivalent to 1 in their respective unit groups reduced by the square of those groups. Using this and the fact that $\rho$ is a ring isomorphism,

$$\phi(A)\phi(B)\phi(C) = \rho(1,1) = 1 \in U/U^2.$$

Lastly, we have to consider the case where $y_1 = 0$ and $y_2 = 0$. In this case, since $A$, $B$ and $C$ are colinear, we must have that $y_3 = 0$ as well. The Chinese remainder theorem gives several ring isomorphisms,

$$\begin{aligned}\rho_1 &: K[x]/(x-x_1) \oplus K[x]/((x-x_2)(x-x_3)) \to K[x]/(f(x))\\ \rho_2 &: K[x]/(x-x_2) \oplus K[x]/((x-x_1)(x-x_3)) \to K[x]/(f(x))\\ \rho_3 &: K[x]/(x-x_3) \oplus K[x]/((x-x_1)(x-x_2)) \to K[x]/(f(x))\\ \rho_{23} &: K[x]/(x-x_2) \oplus K[x]/(x-x_3) \to K[x]/((x-x_2)(x-x_3))\\ \rho_{13} &: K[x]/(x-x_1) \oplus K[x]/(x-x_3) \to K[x]/((x-x_1)(x-x_3))\\ \rho_{12} &: K[x]/(x-x_1) \oplus K[x]/(x-x_2) \to K[x]/((x-x_1)(x-x_2))\\ \rho_{123} &: K[x]/(x-x_1) \oplus K[x]/(x-x_2) \oplus K[x]/(x-x_3) \to K[x]/(f(x)).\end{aligned}$$

It follows from the properties of ring isomorphisms that

$$\rho_1(p, \rho_{23}(q,r)) = \rho_2(q, \rho_{13}(p,r)) = \rho_3(r, \rho_{12}(p,q)) = \rho_{123}(p,q,r)$$

for all $(p,q,r) \in K[x]/(x-x_1) \oplus K[x]/(x-x_2) \oplus K[x]/(x-x_3)$. Therefore, using the definition of $\phi$, we can calculate that

$$\phi(A)\phi(B)\phi(C) = \rho_{123}(f'(x_1)(x_2-x)(x_3-x), f'(x_2)(x_1-x)(x_3-x), f'(x_3)(x_1-x)(x_2-x)).$$

Like in the previous case, we can calculate that $f'(x_i) = (x_i - x_j)(x_i - x_k)$ for any permutation $(i, j, k)$ of $(1, 2, 3)$ and $(x_i - x) \mod (x - x_j) = (x_i - x_j)$ for all $i \neq j$ where $i, j \in \{1, 2, 3\}$. Using these facts, we can see that

$$\phi(A)\phi(B)\phi(C) = \rho_{123}(f'(x_1)^2, f'(x_2)^2, f'(x_3)^2) = \rho_{123}(1, 1, 1) = 1 \in U/U^2.$$

□

### 3.3. **Proving that** $\ker \phi = 2E(K)$.

*Proof.* **Part 1:** $2E(K) \subseteq \ker \phi$.
If $P \in E(K)$, then since $\phi$ is a group homomorphism,

$$\phi(2P) = \phi(P)\phi(P) = 1 \in U/U^2.$$

Therefore, $2P \in \ker \phi$.

**Part 2:** $\ker \phi \subseteq 2E(K)$.
Suppose that $P \in \ker \phi$, so $\phi(P) = 1$. If $P = \mathcal{O}$, then $P \in 2E(K)$ because $2\mathcal{O} = \mathcal{O}$. If $P \neq \mathcal{O}$, then $P = (\alpha, \beta)$ is affine. By the definition of $\phi$, since $\phi(P) = 1$, if $\beta \neq 0$, then $\alpha - \xi$ is a square in $K[\xi]$. If $\beta = 0$, then $\alpha - \xi$ is still a square in $K[\xi]$ because the components of the decomposition will be squares. Thus, for some $\alpha_1, \alpha_2, \alpha_3 \in K$,

$$\alpha - \xi = (\alpha_1\xi^2 + \alpha_2\xi + \alpha_3)^2. \tag{3.6}$$

Using $\xi^3 = -a\xi - b$, we can rewrite this as

$$e_1\xi + f_1 = (\alpha_1\xi^2 + \alpha_2\xi + \alpha_3)(-\alpha_1\xi + \alpha_2) \tag{3.7}$$

for some $e_1, f_1 \in K$. If it were the case that $\alpha_1 = 0$, then (3.6) would imply that $1, \xi$ and $\xi^2$ are linearly dependent. However, they're linearly independent, which means that $\alpha_1 \neq 0$. Thus, we can square (3.7) and divide by $\alpha_1^2$ to get that

$$(e\xi + e')^2 = (\alpha - \xi)(h - \xi)^2$$

for some $e, e', h \in K$. This implies that $(ex + e') - (\alpha - x)(h - x)^2$ is a multiple of $f(x)$, but since they're both monic cubics, it must be that

$$f(x) = (ex + e') - (\alpha - x)(h - x)^2.$$

This equation tells us that the line $y = ex + e'$ intersects $E(K)$ at the points $(\alpha, \beta)$ or $(\alpha, -\beta)$ and two copies of $(h, t)$ where $t$ is define to be the $y$-coordinate for the point on $E(K)$ with $x$-value $h$. By the definition of the group law, this means that

$$(\alpha, (-1)^n\beta) + 2(h, t) = \mathcal{O}$$

for some $n \in \{0, 1\}$. Rearranging this equation, we have that

$$(\alpha, \beta) = 2(h, (-1)^n t),$$

which means that $P = (\alpha, \beta) \in 2E(K)$. □

## 4. The Weak Mordell-Weil Theorem

In this section, we will prove the Weak Mordell-Weil Theorem, which says that the group $E(K)/2E(K)$ is finite. We only prove this for $K = \mathbb{Q}$, though, so from now on, the only field we are working in is $\mathbb{Q}$.

**Definition 4.1.** An **algebraic number** is some complex number $\alpha$ which is a root of some non-trivial polynomial equation with rational coefficients.

**Definition 4.2.** An **algebraic integer** is some complex number $\alpha$ which is a root of some non-trivial monic polynomial equation with integer coefficients.

In the previous section, we showed that there exists a group homomorphism $\phi : E(\mathbb{Q}) \to U/U^2$, where $U$ is the group of units for $\mathbb{Q}[x]/(f(x))$. The Chinese remainder theorem tells us that

$$\mathbb{Q}[x]/(f(x)) \cong \bigoplus_{i=1}^{n} \mathbb{Q}[x]/(f_i(x))$$

where $n \in \{1, 2, 3\}$ and $f_i(x)$ are the irreducible factors of $f(x)$, factored in $\mathbb{Q}$. The following Lemma will make a useful re-characterization of $\mathbb{Q}/(f(x))$.

**Lemma 4.3.** *If $K$ is a field of characteristic zero and $\overline{K}$ is its algebraic closure, and $g(x) = \prod_{i=1}^{n}(x - r_i) \in K[x]$ where $g$ is irreducible, then $K[x]/(g(x)) \cong K[r_i]$ for all $i \in \{1, \dots, n\}$.*

*Proof.* Define a function $\phi_i : K[x]/(g(x)) \to K[r_i]$ by $1 \mod g(x) \mapsto 1 \in K$ and $x \mod g(x) \mapsto r_i$, and let it be the ring homomorphism extension of this map. Suppose that $\xi = x \mod g(x)$ and that $\sum_{j=1}^{n} a_j \xi^j = \sum_{j=1}^{m} b_j \xi^j$ for some $n, m \in \mathbb{N}$ and $a_j, b_j \in K$. Then

$$\sum_{j=1}^{n} a_j \xi^j - \sum_{j=1}^{m} b_j \xi^j = 0 = g(\xi).$$

Since $\phi_i$ is a homomorphism extension by definition,

$$\phi_i \left( \sum_{j=1}^{n} a_j \xi^j - \sum_{j=1}^{m} b_j \xi^j \right) = \phi_i(g(\xi)) = g(r_i) = 0.$$

Therefore, $\phi_i \left( \sum_{j=1}^{n} a_j \xi^j \right) = \phi_i \left( \sum_{j=1}^{m} b_j \xi^j \right)$, so $\phi_i$ is well-defined, and this shows that $\phi_i$ is indeed a ring homomorphism. Suppose that $\phi_i(h(\xi)) = 0$. This implies that $h(r_i) = 0$, so $r_i$ is a root of $h$. rearranging $g(\xi) = 0$, we can always reduce a polynomial in $\xi$ to one of degree less than $g$. In other words, $\{1, \dots, \xi^{\deg(g)-1}\}$ forms a basis for $K[x]/(g(x))$. Thus, without loss of generality, suppose that $\deg(h) < \deg(g)$. However, as proved in chapter 6 of [2], since $g$ is irreducible and has $r_i$ as a root, there is no other non-zero polynomial with $r_i$ as a root and with lower degree. Therefore, $h = 0$, and so $\ker \phi_i = \{0\}$. This means that $\phi_i$ is injective. We can also see that $\phi_i$ is surjective because if $j(r_i) \in K[r_i]$ is a polynomial in $r_i$, then $j(r_i) = \phi_i(j(\xi))$. Therefore, $\phi_i$ is a ring isomorphism, and so $K[x]/(g(x)) \cong K[r_i]$ for all $i$. □

Using this Lemma, we can see that

$$\mathbb{Q}[x]/(f(x)) \cong \bigoplus_{i=1}^{n} \mathbb{Q}[\theta_i]$$

where $n \in \{1, 2, 3\}$ and $\theta_i$ are each one root of their respective irreducible factor of $f(x)$, $f_i(x)$. Let $\mathbb{Q}[\theta_i]^*$ denote the group of units of $\mathbb{Q}[\theta_i]$. We can see that $\phi(E(\mathbb{Q}))$ is a subgroup of the direct sum of the groups $\mathbb{Q}[\theta_i]^*/(\mathbb{Q}[\theta_i]^*)^2 := G_i$. We now aim to show that if $P \in E(\mathbb{Q})$, then the $i$th component of $\phi(P)$ lies in a finite subgroup of $G_i$. If $P = \mathcal{O}$, this is true because each component of $\phi(P)$ lies in the trivial subgroup of that component's group. If $P \neq \mathcal{O}$, then $P = (\alpha/\beta, w)$, where $\alpha, \beta \in \mathbb{Z}$, $w \in \mathbb{Q}$, and $\alpha$ and $\beta$ are coprime. Let $\theta = \theta_i$ be one of the roots of $f(x)$. Then $f(x) = (x-\theta)g(x)$ for some $g(x) \in \mathbb{C}[x]$. Suppose that $g(x) = r_1x^2 + r_2x + r_3$ for some $r_1, r_2, r_3 \in \mathbb{R}$. Then

$$g(\alpha/\beta)\beta^2 = [r_1(\alpha/\beta)^2 + r_2(\alpha/\beta) + r_3]\beta^2 = r_1\alpha^2 + r_2\alpha\beta + r_3\beta^2.$$

Since the algebraic integers of any field are close under addition and multiplication, $\alpha - \beta\theta$ and $h_{\alpha,\beta} := g(\alpha/\beta)\beta^2$ are algebraic integers in $\mathbb{Q}[\theta]$. Let $I(P) := (\alpha - \beta\theta, h_{\alpha,\beta})$ be the ideal generated by these algebraic integers. In the remainder of this section, all of the algebraic integers, ideals, and units are in the ring of the algebraic integers of $\mathbb{Q}[\theta]$.

**Lemma 4.4.** *The set of ideals $I(P)$ is finite.*

*Proof.* Since $\theta$ is a root of the second degree polynomial $g(x) - g(\theta)$, we can say that

$$g(x) - g(\theta) = (x - \theta)t(x)$$

for some linear polynomial $t(x) \in \mathbb{R}[x]$. Substituting in $x = \alpha/\beta$, multiplying both sides by $\beta^2$, and moving some terms around, we get that

$$g(\theta)\beta^2 = h_{\alpha,\beta} - (\alpha - \beta\theta)t(\alpha/\beta)\beta,$$

which implies that $g(\theta)\beta^2 \in I(P)$. Also, we can see that

$$\begin{aligned} g(\theta)x^2 - g(x)\theta^2 &= g(\theta)(x^2 - \theta^2) + \theta^2(g(\theta) - g(x)) \\ &= (x - \theta)[g(\theta)(x + \theta) - \theta^2 t(x)]. \end{aligned}$$

Again, plugging in $x = \alpha/\beta$, multiplying both sides by $\beta^2$, and moving some terms around, we get that

$$g(\theta)\alpha^2 = (\alpha - \beta\theta)[g(\theta)(\alpha + \beta\theta) - \theta^2 t(\alpha)] + \theta^2 h_{\alpha,\beta}.$$

This implies that $g(\theta)\alpha^2 \in I(P)$. Therefore, $(g(\theta)\alpha^2, g(\theta)\beta^2) \subseteq I(P)$, and it is proven in chapter 12 of [2] that for two ideals $I$ and $J$ in the ring of algebraic integers, $I|J$ if and only if $J \subseteq I$. Thus, $I(P)|(g(\theta)\alpha^2, g(\theta)\beta^2)$. Since $\alpha$ and $\beta$ are coprime, so are $\alpha^2$ and $\beta^2$, and so by Bezout's lemma, there exists some integers $c, d$ such that $c\alpha^2 + d\beta^2 = 1$. Therefore,

$$cg(\theta)\alpha^2 + dg(\theta)\beta^2 = g(\theta),$$

and so $(g(\theta)\alpha^2, g(\theta)\beta^2)|(g(\theta))$, which implies that $I(P)|(g(\theta))$. Since $g(\theta) \neq 0$, $(g(\theta))$ only has a finite number of ideal divisors since, according to chapter 12 in [2], ideals have a unique factorization made of prime ideals. Thus, there can only be finitely many ideals $I(P)$. □

**Lemma 4.5.** $(\alpha - \beta\theta) = I(P)C^2$ *for some ideal* $C$.

*Proof.* Suppose that some ideal $J$ is a common divisor of $(\alpha - \beta\theta)$ and $(h_{\alpha,\beta})$. Then $(\alpha - \beta\theta), (h_{\alpha,\beta}) \subseteq J$. This implies that $I(P) = (\alpha - \beta\theta, h_{\alpha,\beta}) \subseteq J$, which means that $J|I(P)$. Therefore, since $I(P)$ is also a common divisor of $(\alpha - \beta\theta)$ and $(h_{\alpha,\beta})$

and $J$ was chosen arbitrarily, $I(P)$ must be the greatest common divisor. Therefore, there exists ideals $A, B$ such that $(\alpha - \beta\theta) = I(P)A$ and $(h_{\alpha,\beta}) = I(P)B$, where $A$ and $B$ are coprime ideals. Since $P \in E(\mathbb{Q})$, there exists some rational number $r/s \in \mathbb{Q}$ such that $(r/s)^2 = f(\alpha/\beta)$. Multiplying both sides by $\beta^3 s^2$, we get that

$$r^2\beta^3 = (\alpha/\beta - \theta)g(\alpha/\beta)\beta^3 s^2 = (\alpha - \beta\theta)h_{\alpha,\beta}s^2.$$

Now suppose that $w = c/d$ for coprime integers $c, d$. Then since $P \in E(\mathbb{Q})$,

$$\beta^3 c^2 = d^2(\alpha^3 + a\alpha\beta^2 + b\beta^3).$$

Since $\beta^3$ divides the left hand side but $\alpha$ and $\beta$ are coprime, it must be the case that $\beta^3 | d^2$. This means that $d^2 = e\beta^3$ for some $e \in \mathbb{Z}$. Subbing this into the equation and removing a $\beta^3$ from both sides, we see that

$$c^2 = e(\alpha^3 + a\alpha\beta^2 + b\beta^3).$$

Therefore, $e|c^2$. If $e \neq 1$, then this is a contradiction because $c$ and $d$ are coprime, so $c^2$ and $d^2$ should also be coprime. Therefore, $e = 1$, and $\beta^3 = d^2$. Therefore, since the integers are a commutative ring,

$$(rd)(rd) = (r^2d^2) = ((\alpha - \beta\theta)h_{\alpha,\beta}s^2) = (\alpha - \beta\theta)(h_{\alpha,\beta})(s)^2 = (s)^2 I(P)^2 AB,$$

so the ideal $AB$ must be a square. Thus, since $A$ and $B$ are coprime, $A$ and $B$ are both squares. This implies that $A = C^2$ for some ideal $C$, and so $(\alpha - \beta\theta) = I(P)C^2$. □

**Definition 4.6.** Suppose that $R$ is a ring and that $I, J$ are ideals. Then we say that $I \sim J$ if there exists some non-zero $r_1, r_2 \in R$ such that $r_1 I = r_2 J$.

**Lemma 4.7.** *There is a finite set of algebraic integers $S$ such that for any $P = (\alpha, \beta) \in E(\mathbb{Q})$,*

$$\alpha - \beta\theta = u\gamma\tau^2$$

*for some unit $u$, algebraic number $\tau$, and $\gamma \in S$.*

*Proof.* Let $C$ be the ideal from Lemma 4.5. Then $C \sim C_s$ for some representative of a class of ideals, $C_s$. Thus, by Lemma 4.5, $I(P)C_s^2$ is equivalent to a principle ideal, so it is a principle ideal. Let's say that $I(P)C_s^2 = (\gamma)$. By Lemma 4.4 and the fact that there are only a finite number of ideal classes–which is proven in chapter 12 of [2]–the set $\{(\gamma)\}$ is finite and does not depend on $P$, but only on $E(\mathbb{Q})$. Since $C_s$ is the ideal class equivalent to $C$, by definition, there exists algebraic integers $\rho, \tau_1$ such that $\rho C = \tau_1 C_s$. Therefore,

$$(\rho^2(\alpha - \beta\theta)) = I(P)\tau_1^2 C_s^2 = (\tau_1^2\gamma).$$

Thus, $\rho^2(\alpha - \beta\theta) = u\tau_1^2\gamma$ for some unit $u$, and so if we let $\tau := \tau_1/\rho$, then we have our result. □

**Theorem 4.8** (Weak Mordell-Weil Theorem)**.** *The group $E/2E$ is finite.*

*Proof.* Since $\phi : E \to U/U^2$ is a group homomorphism, by the first isomorphism theorem, $\phi(E) \cong E/\ker\phi$, But, as proved in section 3.3, $\ker\phi = 2E$, so therefore, it suffices to prove that $\phi(E)$ is finite. Since there are at most 3 points of the form $(\alpha/\beta, 0)$ and 1 point which is not affine, we only have to consider points $P = (\alpha/\beta, w)$ where $w \neq 0$ and show that $\phi$ maps the set of these points to a finite set. If $P = (\alpha/\beta, w)$ and $w \neq 0$, then by definition, $\phi(P)$ is the coset modulo $U^2$ of $\alpha/\beta - x$. By Lemma 4.7, the image of $(\alpha/\beta - x)$ in $\mathbb{Q}[\theta_i]^*/(\mathbb{Q}[\theta_i]^*)^2$ is the coset of

$(1/\beta)u\gamma$. As shown in a previous lemma, $\beta^3$ is a square, which means that $\beta$ itself must be a square. By the weak Dirichlet unit theorem, which is proved in chapter 19 of [2], the group of units in the ring of algebraic integers in $\mathbb{Q}[\theta_i]$ is finitely generated with some basis $\{u_1, \dots, u_t\}$. Thus, the coset of $(1/\beta)u\gamma \mod (\mathbb{Q}[\theta_i]^*)^2$ has a representative of the form $u_1^{\varepsilon_1} \cdots u_t^{\varepsilon_t}\gamma$, where $\varepsilon_j \in \{0, 1\}$. Thus, since there are only finitely many $\gamma$, there are only finitely many representatives, and so $i$th component of the image $\phi(E)$ is finite. Therefore, the image as a whole is finite. □

## 5. The Descent Argument

In this final section, we will prove some lemmas and then use the Weak Mordell-Weil theorem to prove the Mordell-Weil Theorem.

### 5.1. A Specific Characterization of Homogeneous Coordinates.

In this section, we will show that we can write every point on $E(\mathbb{Q})$ in a particular fashion which will be used in the following subsections. Suppose that the coefficients of $f(x)$ are integers, that is, $a, b \in \mathbb{Z}$. In homogeneous form, $f(x)$ becomes

$$y^2 z = x^3 + axz^2 + bz^3. \tag{5.1}$$

Suppose $P = (x_0, y_0, z_0)$ is a point on $E(\mathbb{Q})$. Since $(x_0, y_0, z_0) = (x_0q, y_0q, z_0q)$ for any $q \in \mathbb{Q}$, without loss of generality, we may assume that $x_0$, $y_0$ and $z_0$ are coprime integers. Suppose that $P \neq \mathcal{O}$ so that $\gcd(x_0, z_0)$ is well defined. Then let $Z_0 := \gcd(x_0, z_0)$ and define $X_0 := x_0/Z_0$ and define $Y_0 := y_0$ for continuity in notation. Plugging in these definitions to (5.1), we get that

$$X_0^3 Z_0^3 = z_0(Y_0^2 - ax_0z_0 - bz_0^2). \tag{5.2}$$

Since $\gcd(Z_0, Y_0)$ must divide $x_0$, $y_0$ and $z_0$, it must be that $\gcd(Z_0, Y_0) = 1$. Looking at the second term on the right-hand side of (5.2), we can see that $Z_0|z_0$, so if it were the case that $Z_0$ divided this term, then $Z_0|Y_0$. But since $\gcd(Z_0, Y_0) = 1$, it must be that $Z_0$ does not divide this term, and so $Z_0^3|z_0$ since it divides the left hand side. Let $t$ be the integer such that $Z_0^3 t = z_0$. This simplifies the equation to

$$X_0^3 = t(Y_0^2 - ax_0z_0 - bz_0^2). \tag{5.3}$$

Since $Z_0 = \gcd(x_0, z_0)$, $1 = \gcd(x_0/Z_0, z_0/Z_0) = \gcd(X_0, Z_0^2 t)$. Using (5.3), we can see that if a prime $p|t$, then $p|X_0^3$, so since $p$ is prime, $p|X_0$. However, this would imply that $\gcd(X_0, Z_0^2 t) \geq p$. Therefore, no primes divide $t$, and so $t = 1$ (after a sign adjustment). Thus, $z_0 = Z_0^3$ and $\gcd(X_0, Z_0) = 1$. We can now see that $P = (x_0, y_0, z_0) = (X_0Z_0, Y_0, Z_0^3)$, and the corresponding affine form for $P$ is $(X_0/Z_0^2, Y_0/Z_0^3)$. Since $\gcd(X_0, Z_0) = \gcd(Y_0, Z_0) = 1$, this affine form is written in lowest terms. In the following arguments, all affine points will be written in this form. Subbing in the values for $x_0$ and $z_0$ into (5.3), we get that

$$Y_0^2 = X_0^3 + aX_0Z_0^4 + bZ_0^6. \tag{5.4}$$

### 5.2. The Height Function.

We now define the height function $H : E(\mathbb{Q}) \to \mathbb{N}$ which will become important to the proof of the Mordell-Weil Theorem. Define $H(\mathcal{O}) := 1$, and otherwise, if $P = (X_0Z_0, Y_0, Z_0^3)$, then define

$$H(P) := \max\{|X_0|, Z_0^2\}.$$

That is, $H(P)$ is the maximum of the absolute value of the numerator and denominator of the first coordinate of $P$ in affine form. Suppose that $P = (X_0 Z_0, Y_0, Z_0^3)$. If $|X_0| \geq Z_0^2$, then using (5.4) and the fact that $X_0$ and $Z_0$ are integers,

$$Y_0^2 = X_0^3 + ax_0 Z_0^4 + bZ_0^6 \leq |X_0|^3 + |a||X_0|H(P)^2 + |b|H(P)^3 = (1+|a|+|b|)H(P)^3.$$

If $Z_0^2 \geq |X_0|$, then using (5.4) and the fact that $X_0$ and $Z_0$ are integers,

$$Y_0^2 = X_0^3 + ax_0 Z_0^4 + bZ_0^6 \leq |X_0|^3 + |a||X_0|H(P)^2 + |b|H(P)^3 \leq (1+|a|+|b|)H(P)^3.$$

Thus, in either case, $|Y_0| \leq \sqrt{1+|a|+|b|}H(P)^{3/2}$. If $P = \mathcal{O}$, then $Y_0 = 1$, so since $H(P) = 1$ and $\sqrt{1+|a|+|b|} \geq 1$,

$$|Y_0| \leq \sqrt{1+|a|+|b|}H(P)^{3/2} \tag{5.5}$$

for all $P \in E(\mathbb{Q})$.

**Lemma 5.6.** *Suppose that $C \in \mathbb{R}$. Then there exists only finitely many points $P \in E(\mathbb{Q})$ such that $H(P) \leq C$.*

*Proof.* Suppose that $H(P) \leq C$ for some point $P$. Then using (5.5), we can see that there are only finitely many possible values for $Y_0$. For each value of $Y_0$, since $P = (X_0 Z_0, Y_0, Z_0^3)$ and $X_0, Z_0$ must be integers, and they must also satisfy (5.4), there can only be finitely many points with each value of $Y_0$. Thus, there can only be finitely many such points $P$ where $H(P) \leq C$. □

5.3. **Final Important Lemma.** We will now prove the following Lemma:

**Lemma 5.7.** *If $\{Q_1, \ldots, Q_{n_0}\}$ is a fixed set of points in $E(\mathbb{Q})$, then there exists some positive constant $C \in \mathbb{R}$ which only depends on $E(\mathbb{Q})$ and $\{Q_1, \ldots, Q_{n_0}\}$ such that*

$$H(P) \leq CH(2P - Q_i)^{1/2}$$

*for all $P \in E(\mathbb{Q})$ for all $i \in \{1, \ldots, n_0\}$.*

*Proof.* If suffices to only consider one point in the fixed set of points, $Q$, because if the statement holds for $n_0 = 1$, then we can take $C$ to be the maximum of the constants for each $Q$. Thus, fix some point $Q \in E(\mathbb{Q})$ such that $Q \neq \mathcal{O}$ and take some point $P \in E(\mathbb{Q})$ such that $2(P - Q) \neq \mathcal{O}$, or in other words, $2P \neq 2Q$. Using the homogeneous coordinates as above,

$$\begin{aligned} P &= (x_1 z_1, y_1, z_1^3) \\ Q &= (ce, d, e^3) \\ 2P - Q &= (x_2 z_2, y_2, z_2^3) \end{aligned}$$

for some $x_1, y_1, z_1, x_2, y_2, z_2, c, d, e \in \mathbb{Z}$. Since $2P = (2P - Q) + Q$, if it were the case that $2P - Q = Q$, then we would have that $2P = 2Q$. Since we are assuming this is not the case, $2P - Q \neq Q$, and so if we let $2P = (x_3 z_3, y_3, z_3^3)$, we can use (2.5) to say that

$$\begin{aligned} \frac{x_3}{z_3^2} &= \frac{[(x_2/z_2^2)(c/e^2) + a][(x_2/z_2^2) + (c/e^2)] + 2b - 2(y_2/z_2^3)(d/e^3)}{[(c/e^2) - (x_2/z_2^2)]^2} \\ &= \frac{[x_2 c + az_2^2 e^2][x_2 e^2 + cz_2^2] + 2bz_2^4 e^4 - 2y_2 z_2 de}{[cz_2^2 - x_2 e^2]^2}. \end{aligned}$$

Let's denote the numerator of this last expression as $A$ and the denominator as $B$. Since $\gcd(x_3, z_3) = 1$, the left hand side of the above equation is just $A/B$ but in lowest terms. Thus, $x_3|A$ and $z_3^2|B$. Since we can see that $x_3, z_3^2, A, B \in \mathbb{Z}$, we must have that $|x_3| \leq |A|$ and $z_3^2 \leq |B|$. Thus,

$$H(2P) = \max\{|x_3|, z_3^2\} \leq \max\{|A|, |B|\}. \tag{5.8}$$

By (5.5), we can see that $|y_2| \leq C_1 H(2P-Q)^{3/2}$ for some positive constant $C_1 \in \mathbb{R}$. Since $z_2^2 \leq \max\{|x_2|, z_2^2\} = H(2P-Q)$, taking the square root on both sides, we can see that $|z_2| \leq H(2P-Q)^{1/2}$. Similarly, $|x_2| \leq \max\{|x_2|, z_2^2\} = H(2P-Q)$. Using the triangle inequality and these three bounds for $|x_2|$, $|y_2|$ and $|z_2|$, we can see that

$$\begin{aligned}|A| &= |[x_2c + az_2^2e^2][x_2e^2 + cz_2^2] + 2bz_2^4e^4 - 2y_2z_2de| \\ &= |x_2^2ce^2 + x_2z_2^2c^2 + x_2z_2^2ae^4 + z_2^4ace^2 + 2bz_2^4e^4 - 2y_2z_2de| \\ &\leq |x_2^2ce^2| + |x_2z_2^2c^2| + |x_2z_2^2ae^4| + |z_2^4ace^2| + |2bz_2^4e^4| + |2y_2z_2de| \\ &\leq (|ce^2| + |c^2| + |ae^4| + |ace^2| + |2be^4| + |2de|)H(2P-Q)^2\end{aligned}$$

and

$$\begin{aligned}|B| &= |[cz_2^2 - x_2e^2]^2| \\ &= |c^2z_2^4 - 2ce^2x_2z_2^2 + e^4x_2^2| \\ &\leq |c^2z_2^4| + |2ce^2x_2z_2^2| + |e^4x_2^2| \\ &\leq (|c^2| + |2ce^2| + |e^4|)H(2P-Q)^2.\end{aligned}$$

Therefore, plugging in this inequalities to (5.8), we get that

$$H(2P) \leq \max\{|A|, |B|\} \leq C_Q H(2P-Q)^2 \tag{5.9}$$

where $C_Q \in \mathbb{N}$ is some constant which only depends on $a, b, c, d, e$, which is to say it only depends on $Q$ because $a$ and $b$ tell us which group $E(\mathbb{Q})$ we are talking about. Using $2P$ and $P$ with (2.4), we get that for each $i \in \{1, 2, 3\}$,

$$x_3/z_3^2 - \theta_i = \left[\frac{-(x_1/z_1^2)^2 + 2\theta_i^2 + 2\theta_i(x_1/z_1^2) + a}{2(y_1/z_1^3)}\right]^2.$$

Rearranging slightly, we get that

$$x_3 - \theta_i z_3^2 = z_3^2\left[\frac{-x_1^2 + 2\theta_i^2 z_1^4 + 2\theta_i x_1 z_1^2 + az_1^4}{2y_1z_1}\right]^2.$$

Since $a, b \in \mathbb{Z}$, we know that $\theta_i$ are algebraic integers, so the left hand side of the equation is an algebraic integer. Thus, if we define

$$\alpha_i := z_3\left[\frac{-x_1^2 + 2\theta_i^2 z_1^4 + 2\theta_i x_1 z_1^2 + az_1^4}{2y_1z_1}\right],$$

then $\alpha_i$ must also be an algebraic integer. Furthermore, we can simplify the expression to see that

$$\alpha_i = q_1 + q_2\theta_i + q_3\theta_i^2$$

for some numbers $q_1, q_2, q_3 \in \mathbb{Q}$. We can see that these three equations give us a linear equation

$$\begin{bmatrix}1 & \theta_1 & \theta_1^2 \\ 1 & \theta_2 & \theta_2^2 \\ 1 & \theta_3 & \theta_3^2\end{bmatrix}\begin{bmatrix}q_1 \\ q_2 \\ q_3\end{bmatrix} = \begin{bmatrix}\alpha_1 \\ \alpha_2 \\ \alpha_3\end{bmatrix}.$$

Let's define

$$M := \begin{bmatrix} 1 & \theta_1 & \theta_1^2 \\ 1 & \theta_2 & \theta_2^2 \\ 1 & \theta_3 & \theta_3^2 \end{bmatrix}$$

and $M_i$ to be the matrix $M$ but with the $i$th column being swapped out with the column vector $(\alpha_1, \alpha_2, \alpha_3)^T$. After tedious algebra, we can calculate that

$$\det(M) = (\theta_1 - \theta_2)(\theta_2 - \theta_3)(\theta_1 - \theta_3).$$

Thus, according to Lemma 1.7,

$$\det(M)^2 = -(4a^3 + 27b^2).$$

Since Lemma 1.6 tells us that $4a^3 + 27b^2 \neq 0$, we have that $\det(M) \neq 0$. Therefore, we can apply Cramer's rule to say that

$$q_i = \frac{\det(M_i)}{\det(M)} \alpha_i.$$

Let's define $\delta := -(4a^3 + 27b^2)$. We can see that

$$\delta q_i = \det(M)\det(M_i)\alpha_i.$$

Since $\det(M) \in \mathbb{Z}[\theta_1, \theta_2, \theta_3, \alpha_1, \alpha_2, \alpha_3]$ and we can calculate $\det(M_i)$ to show that $\det(M_i) \in \mathbb{Z}[\theta_1, \theta_2, \theta_3, \alpha_1, \alpha_2, \alpha_3]$, we can see that $\delta q_i \in \mathbb{Z}[\theta_1, \theta_2, \theta_3, \alpha_1, \alpha_2, \alpha_3]$ for all $i$. Therefore, since $\theta_i$ and $\alpha_i$ are algebraic integers for all $i$, $\delta q_i$ must be algebraic integers for all $i$. But since $\delta$ is an integer and $q_i$ are rational, $\delta q_i$ must also be rational for all $i$. As proven in chapter 6 of [2], a rational number is an algebraic integer if and only if it is an integer. Therefore, $\delta q_i$ are integers. Now, expanding out the definition of $\alpha_i$, we can see that

$$2q_1 - aq_3 = \frac{z_3}{z_1 y_1} x_1^2$$

and

$$q_3 = \frac{z_3}{z_1 y_1} z_1^4.$$

Therefore, since $a, \delta q_1, \delta q_3 \in \mathbb{Z}$, $\delta(2q_1 - aq_3) = \frac{z_3}{z_1 y_1} x_1^2 \in \mathbb{Z}$ and $\delta q_3 = \frac{z_3}{z_1 y_1} z_1^4 \in \mathbb{Z}$. This means that $(\delta z_3)/(z_1 y_1) = m/n$ for some $m, n \in \mathbb{Z}$ such that $\gcd(m, n) = 1$. By definition, $m x_1^2 = n\delta(2q_1 - aq_3)$ and $m z_1^4 = n\delta q_3$. Since $\gcd(m, n) = 1$, we must have that $n | x_1^2$ and $n | z_1^4$, so since $\gcd(x_1, z_1) = 1$, we must have that $n = 1$. Thus, $(\delta z_3)/(z_1 y_1)$ is an integer and so

$$x_1^2 \leq \left| \frac{\delta z_3}{z_1 y_1} \right| x_1^2 \leq \left| \frac{\delta z_3}{z_1 y_1} x_1^2 \right| = |\delta(2q_1 - aq_3)| \tag{5.10}$$

and

$$z_1^4 \leq \left| \frac{\delta z_3}{z_1 y_1} \right| z_1^4 \leq \left| \frac{\delta z_3}{z_1 y_1} z_1^4 \right| = |\delta q_3|. \tag{5.11}$$

Since the algebraic integers are a subset of the complex numbers, $\theta_i \in \mathbb{C}$, so $\theta_i = \mathrm{Re}(\theta_i) + \mathrm{Im}(\theta_i)\sqrt{-1}$. We can see that $\alpha_i^2 = x_3 - \theta_i z_3^2$, so therefore

$$\begin{aligned}
\|\alpha_i\|^2 = \|\alpha_i^2\| \\
&= \sqrt{(x_3 - \mathrm{Re}(\theta_i)z_3^2)^2 + (-\mathrm{Im}(\theta_i)z_3^2)^2} \\
&= \sqrt{x_3^2 + (\mathrm{Re}(\theta_i)^2 + \mathrm{Im}(\theta_i)^2)z_3^4 - 2\mathrm{Re}(\theta_i)x_3z_3^2} \\
&\leq \sqrt{x_3^2 + (\mathrm{Re}(\theta_i)^2 + \mathrm{Im}(\theta_i)^2)z_3^4 + 2\mathrm{Re}(\theta_i)|x_3|z_3^2} \\
&\leq \sqrt{x_3^2} + \sqrt{(\mathrm{Re}(\theta_i)^2 + \mathrm{Im}(\theta_i)^2)z_3^4} + \sqrt{2\mathrm{Re}(\theta_i)|x_3|z_3^2} \\
&= |x_3| + \|\theta_i\|z_3^2 + \sqrt{2\mathrm{Re}(\theta_i)}\sqrt{|x_3|z_3^2} \\
&\leq \max\{|x_3|, z_3^2\} + \|\theta_i\| \max\{|x_3|, z_3^2\} + \sqrt{2\mathrm{Re}(\theta_i)}\sqrt{\max\{|x_3|, z_3^2\}^2} \\
&= C_2H(2P)
\end{aligned}$$

for some constant $C_2 \in \mathbb{R}$. Thus,

$$\|\alpha_i\| \leq \sqrt{C_2}H(2P)^{1/2}.$$

One can see by the calculation of $q_1$, $q_2$ and $q_3$ that $\delta(2q_1 - aq_3)$ and $\delta q_3$ are linear combinations of $\alpha_i$. Thus, using the inequality just proved along with (5.10) and (5.11), we can see that there exists some positive constant $C_3 \in \mathbb{R}$ such that

$$H(P) \leq C_3H(2P)^{1/4}.$$

Combining this with (5.9), we get that

$$H(P) \leq C_4H(2P - Q)^{1/2} \tag{5.12}$$

for all $P$ for some positive constant $C_4 \in \mathbb{R}$ which only depends on $Q$. We only considered the cases of $P$ where $2P \neq 2Q$, but there may be such $P \in E(\mathbb{Q})$ where $2P = 2Q$. In this case, however, there are only finitely many such $P$. This is because if $2Q = \mathcal{O}$, then there are can only be at most three such $P$ because only points of the form $P = (x, 0)$ can have that $2P = \mathcal{O}$ and since these points correspond to roots of $f(x)$, there can be at most three. If $2Q = (x_q, y_q)$, then in order for a point $P$ to satisfy $2P = 2Q$, the tangent line to the curve at $P$ must intersect $-2Q = (x_q, -y_q)$. This gives us the condition that if $P = (x_p, y_p)$, then, assuming $x_p \neq x_q$,

$$2(y_q + y_p)y_p = (3x_p^2 + a)(x_p - x_q).$$

Rearranging this and plugging it into $y_p^2 = f(x_p)$, we can see that the only such points $(x_p, y_p)$ must lie on the intersection of two unequal quadratics, and thus there can be at most two solutions. Since there are finitely many cases where $2P = 2Q$, we can increase $C_4$ to make (5.12) hold for all these extra cases. Therefore, without loss of generality, (5.12) holds for all $P \in E(\mathbb{Q})$. □

### 5.4. **The Mordell-Weil Theorem.**

**Theorem 5.13** (Mordell-Weil Theorem)**.** *$E(\mathbb{Q})$ is finitely generated.*

*Proof.* By the weak Mordell-Weil Theorem (4.8), we know that $E(\mathbb{Q})/2E(\mathbb{Q})$ is a finite group. Let $\{Q_1, \ldots, Q_{n_0}\}$ be a set of representatives in $E(\mathbb{Q})$ for this group. By definition, for any point $P \in E(\mathbb{Q})$, there exists some $j \in \{1, \ldots, n_0\}$ such that $P + Q_j = 2P'$ for some point $P' \in E(\mathbb{Q})$. So take some point $P \in E(\mathbb{Q})$. There exists some $a_1 \in \{1, \ldots, n_0\}$ and $P_1 \in E(\mathbb{Q})$ such that $P + Q_{a_1} = 2P_1$. By Lemma 5.7, we have that

$$H(P_1) \leq CH(2P_1 - Q_{a_1})^{1/2} = CH(P)^{1/2}.$$

There exists some $a_2 \in \{1, \ldots, n_0\}$ and some $P_2 \in E(\mathbb{Q})$ such that $P_1 + Q_{a_2} = 2P_2$. Using the same technique but substituting in the previous inequality, we have that

$$H(P_2) \leq CH(2P_2 - Q_{a_2})^{1/2} = CH(P_1)^{1/2} \leq C^{1+1/2} H(P)^{1/4}.$$

Continuing in this fashion, by induction, it can be shown that we arrive at a sequence of points $P_r \in E(\mathbb{Q})$ such that

$$H(P_r) \leq C^{1+\frac{1}{2}+\cdots+\frac{1}{2^r}} H(P)^{1/(2^{r+1})} \tag{5.14}$$

and

$$P = 2^r P_r - 2^{r-1} Q_{a_r} - \cdots - Q_{a_1}. \tag{5.15}$$

As $r$ approaches infinity, the right-hand side of (5.14) approaches $C^2$. Thus, there exists some integer $r_0$ such that for all $r \geq r_0$,

$$H(P_r) \leq C^2 + 1.$$

According to Lemma 5.6, there can only be finitely many such points $P_r$, so let us call them $\{P'_1, \ldots, P'_{s_0}\}$. It is important to note that even though the sequence $(P_r)$ may differ for different starting points $P$, since we would always arrive at the same inequality, we must always have that $\{P_r\}_{r \geq r_0} \subseteq \{P'_1, \ldots, P'_{s_0}\}$. Thus, if we let $r = r_0$ in (5.15), then we can see that $P$ is expressible as an integer linear combination of the points in the set $\{P'_1, \ldots, P'_{s_0}\} \cup \{Q_1, \ldots, Q_{n_0}\}$. Therefore, since $P$ was chosen arbitrarily, $E(\mathbb{Q})$ is finitely generated. □

## Acknowledgments

I thank my mentor, Eric Zhu, for helping me understand the material required to understand these proofs and for being patient when ideas were hard to explain.

## References

[1] Fulton, William. ”Algebraic curves. An introduction to algebraic geometry. Notes written with the collaboration of Richard Weiss.” Mathematics Lecture Notes Series (WA Benjamin, New York, 1969). MR 313252.47 (1969).

[2] Ireland, Kenneth, and Michael Rosen. ”A classical introduction to modern number theory. 1990.” Grad. Texts in Math (1990).

[3] Lozano-Robledo, Álvaro, and Alvaro Lozano-Robledo. Elliptic curves, modular forms, and their L-functions. Providence, RI: American Mathematical Society, 2011.

[4] Mendel, M. B., and P. H. A. J. M. van Gelder. ”Visualizing and gauging collision risk.” (2017).