EXPLORING THE EXISTENCE OF RATIONAL POINTS ON ELLIPTIC CURVES: WHAT IS THE POINT?

by

SALVADOR GARCIA PEREZ

A THESIS

Presented to the Department of Mathematics
and the Robert D. Clark Honors College
in partial fulfillment of the requirements for the degree of
Bachelor of Science

May 2023

An Abstract of the Thesis of

Salvador Garcia Pere for the degree of Bachelor of Science
in the Department of Mathematics to be taken June 2023

Title: Exploring the Existence of Rational Points on Elliptic Curves: What is the Point?

Approved: *Victor Ostrik, Ph.D.*
Primary Thesis Advisor

When introduced with any equation, whether it is given by a polynomial or cubic polynomial, the first question we typically ask ourselves is, what is the solution? In many cases, like in the equation $x + 2 = 5$, we can easily determine that the solution is $x = 3$. But, in other scenarios, like finding rational or integer solutions to certain cubic equations, the answer may be difficult to find, or, in some cases, there may not be a definitive way to find an answer at all. It is especially the case for elliptic curves. Elliptic curves of the Weierstrass form are equations of the form $y^2 = f(x) = x^3 + Ax + B$, where $A, B \in \mathbb{Z}$. Although solutions to cubic equations are well-understood with real numbers, the challenge appears when we try to find integers and rational solutions in cubic equations, which are not yet well understood. Independent rational solutions on elliptic curves, defined by the rank of a curve, have proven difficult to uncover. This thesis is interested in developing a better understanding of how to find rational solutions and understanding the ranks of elliptic curves.

Acknowledgements

First, I would like to thank Dr. Victor Ostrik for his continuous encouragement and support throughout the past year with the investigation of this thesis. With his guidance, I have developed and explored a topic I otherwise would not have encountered. Also, I would like to extend my gratitude to every mathematics professor and Clark Honors College professor and faculty who taught me during my four years at the University of Oregon. Their inspiring and creative thinking provided an engaging environment in which to learn.

I would also like to thank my family and friends for providing unconditional support. Their continuous words of encouragement kept me motivated through the highs and lows of this journey. Thank you for listening and enduring my ongoing talks about mathematics. I cannot express my appreciation for everyone's support!

Table of Contents

List of Figures

List of Tables

1 Introduction and Background

Most individuals indirectly interact with elliptic curves daily without even knowing. While many aspects of elliptic curves are still not well-understood, many contemporary applications and developments have influenced humans' everyday lives. Whether conducting online transactions or using secure messaging apps, elliptic curves manage to keep data secure and information private. In these situations, the applications of elliptic curves are in the form of elliptic curve cryptography (EEC). Cryptography focuses on encryption and decryption, where communicating private information is done securely. While there are many forms of public key cryptography, ECC has proven to be one of the most effective in recent years.

Although ECC is the most common application for elliptic curves, there are other applications in which elliptic curves have been beneficial: factoring large integers, primality proving, and proof of Fermat's Last Theorem. ECC has become the newest and most relevant form of cryptography because it has successfully defended against a plethora of attacks and is more efficient than previous forms of asymmetric cryptographic security, most notably RSA [4]. While the applications of elliptic curves are interesting, there are still many unknowns regarding the topic. This thesis will focus on developing concepts in the mathematical fields of algebra and number theory to construct a better understanding of elliptic curves.

This section will focus on developing a basic understanding of the concepts necessary to understand the elliptic curves: groups, fields, conics, and cubics. Ultimately, these concepts will develop the essential tools to understand Mordell's Theorem, which is the leading theorem for understanding rational points on elliptic curves.

1.1 Groups and Fields

Definition 1.1. *A group is a nonempty set G with a binary operation $*$ that satisfies the following axioms:*

(a) Associativity: For all elements $a, b, c \in G$ it holds that $a * (b * c) = (a * b) * c$.

(b) Identity: There exists an identity element $e \in G$ such that for every element $a \in G$ it holds that $a * e = a = e * a$.

(c) Inverse: For all elements $a \in G$, there exists an inverse element $d \in G$ such that $a * d = e$ and $d * a = e$.

A group G is also called an Abelian Group if it satisfies the following axiom:

(d) Commutativity: For every element $a, b \in G$ it holds that $a * b = b * a$ [3].

This discussion is an introduction to a concept in algebra known as groups. To better understand elliptic curves, it is necessary to comprehend the characteristics and properties of a group. A group is a nonempty set with a binary operation, such as addition or multiplication. The operation must be associative, contain an identity and inverse element, and can be commutative.

Example 1.1. *Show that the set $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ under the operation $+$ forms a group.*

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1

3	3	0	1	2

Table 1.1. Cayley Table for $(\mathbb{Z}_4, +)$

Solution. First, consider the definition of a group: associative, inverse element, and identity element. The identity element for the set is $e = 0_1$, such that,

$$0 + 0_1 = 0 = 0_1 + 0 \qquad 1 + 0_1 = 1 = 0_1 + 1$$

$$2 + 0_1 = 2 = 0_1 + 2 \qquad 3 + 0_1 = 3 = 0_1 + 3.$$

Additionally, every element of the set contains an inverse element, which is denoted by the subscript i,

$$0 + 0_i = 0 = 0_i + 0 \qquad 1 + 3_i = 0 = 3_i + 1$$

$$2 + 2_i = 0 = 2_i + 2 \qquad 3 + 1_i = 0 = 1_i + 3.$$

Lastly, the associative property holds for all combinations of $a, b, c \in \mathbb{Z}_4$, where the following are just a few cases that illustrate the associative property holds,

$$0 + (1 + 2) = 3 = (0 + 1) + 2 \qquad 1 + (2 + 3) = 6 = (1 + 2) + 3.$$

Thus, this proves that the $(\mathbb{Z}_4, +)$ is a group. Furthermore, to show that the group is also commutative, it must be that for all combinations of $a, b \in \mathbb{Z}_4$, the property holds, where the following are just a few cases that illustrate the commutative property holds,

$$2 + 3 = 1 = 3 + 2 \qquad 1 + 3 = 0 = 3 + 1,$$

because $1 \equiv 5\ (mod\ 4)$ and $0 \equiv 4\ (mod\ 4)$. Generally, this would be sufficient to indicate $(\mathbb{Z}_4, +)$ is an abelian group.

Another concept from algebra that is important for understanding elliptic curves and that builds on groups is fields. Like a group, a field has different properties that must be satisfied to maintain its structure such as distributivity, commutativity, and associativity.

Definition 1.2. *A field is a nonempty set F with the operations $+$ and $\times$ that satisfies the following axioms:*

(a) Associativity: For all elements $a, b, c \in F$ it holds that $a + (b + c) = (a + b) + c$ and $a \times (b \times c) = (a \times b) \times c$.

(b) Identity: There exist identity elements $0_F, 1_F \in F$, where $1_F \neq 0_F$, such that for every element $a \in F$ it holds that $a + 0 = a = 0 + a$ and $a \times 1 = a = 1 \times a$.

(c) Inverse: For every element $a \in F$, where $a \neq 0_F$ for multiplication, there exists an element $-a, a^{-1} \in F$ such that $a + (-a) = 0 = (-a) + a$ and $a^{-1} \times a = 1 = a \times a^{-1}$.

(d) Commutativity: For every element $a, b \in F$ it holds that $a + b = b + a$ and $a \times b = b \times a$.

(e) Distributivity: For all elements $a, b, c \in F$ it holds that $a \times (b + c) = (a \times b) + (a \times c)$ and $(b + c) \times a = (b \times a) + (c \times a)$.

Example 1.2. *Show that the set $\mathbb{Z}_3 = \{0, 1, 2\}$ under the operation $+$ and $\times$ forms a group.*

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Table 1.2. Cayley Table for $(\mathbb{Z}_3, +)$

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Table 1.3. Cayley Table for $(\mathbb{Z}_3, \times)$

Solution. To show that the set $\mathbb{Z}_3$ is a group under the operation $+$ and $\times$, considering the previous axioms. It is determined that the identity elements for the set are $e_1 = 0_1$ and $e_2 = 1_1$, such that:

$$0 + 0_1 = 0 = 0_1 + 0 \qquad 0 \times 1_1 = 0 = 1_1 \times 0$$

$$1 + 0_1 = 1 = 0_1 + 1 \qquad 1 \times 1_1 = 1 = 1_1 \times 1$$

$$2 + 0_1 = 2 = 0_1 + 2 \qquad 2 \times 1_1 = 2 = 1_1 \times 2.$$

Every element of the set contains an inverse element:

$$0 + 0 = 0 = 0 + 0 \qquad 1 \times 1 = 1 = 1 \times 1$$

$$1 + 2 = 0 = 2 + 1 \qquad 2 \times 2 = 1 = 2 \times 2.$$

In the last case, $2 \times 2 = 1 = 2 \times 2$ because $1 \equiv 4\ (mod\ 3)$. Also, the associative property holds for all combinations of $a, b, c \in \mathbb{Z}_3$, where the following are just a few cases that illustrate the associative property holds:

$$1 + (1 + 2) = 1 = (1 + 1) + 2 \qquad 1 \times (1 \times 2) = 0 = (1 \times 1) \times 2.$$

To show that the set is commutative, it follows that for all combinations of $a, b \in \mathbb{Z}_3$, the property holds, where the following are just a few cases that illustrate the commutative property holds:

$$2 + 3 = 2 = 3 + 2 \qquad 2 \times 3 = 0 = 3 \times 2.$$

Lastly, the distributive property must hold for all combinations of $a, b, c \in \mathbb{Z}_3$, where the following are just a few cases that illustrate the distributive property holds:

$$1 \times (2 + 3) = 2 = (1 \times 2) + (1 \times 3) \qquad (1 + 2) \times 3 = 0 = (1 \times 3) + (2 \times 3).$$

Thus, this would be sufficient to indicate $(\mathbb{Z}_3, +, \times)$ is a field.

Ultimately, elliptic curves are defined over fields, which represent the plane with points of that specified field. For the purposes of this thesis, it is essential to look at elliptic curves over the rational field, $\mathbb{Q}$.

1.2 Projective Plane

To better understand elliptic curves, it is also necessary to understand the projective plane. The following will define the projective plane from both an algebraic and geometric perspective. It is essential to begin the discussion of the algebraic projective plane with an understanding of the following Fermat's equation

$$x^N + y^N = 1, \tag{1.1}$$

where $x, y \in \mathbb{Q}$. Now, suppose there is a solution such that $x = \frac{a}{c}$ and $y = \frac{b}{d}$ are in the lowest terms with a positive denominator. This substitution will result in

$$a^N d^N + b^N c^N = c^N d^N.$$

Now, it can be determined that

$$c^N | a^N d^N, \text{ where } \gcd(a, d) = 1 \text{ and } d^N | b^N c^N, \text{ where } \gcd(b, d) = 1.$$

So, it must be that $c|d$ and $d|c$. Thus, $c = d$ and any solution to (1.1) in rational numbers, $\left(\frac{a}{c}, \frac{b}{c}\right)$, gives a solution in the integers of the form (a, b, c) for the following homogeneous Fermat equation

$$X^N + Y^N = Z^N. \tag{1.2}$$

It is possible to find rational and integer solutions given that you have the solution to either of the previous equations.

Definition 1.3. *(Projective Plane $\mathbb{P}^2$; Algebraic definition). A projective plane is a set of triplets of the form $[a, b, c]$ with a, b, c not all zero, and consider two triples $[a, b, c]$ and $[a', b', c']$ the same point if there exists a non-zero t such that*

$$a = ta', b = tb', c = tc'.$$

$\mathbb{P}^2$ is the projective plane defined by the set of equivalence classes of triples $[a, b, c]$, except the triple $[0,0,0]$.

Now, for the geometric projective plane, a line is defined as a set of points $[a, b, c] \in \mathbb{P}^2$ whose coordinates satisfy the equation

$$\alpha X + \beta Y + \gamma Z = 0,$$

for constants α, β, γ not all zero, where the homogenous points are also solutions.

Since parallel lines in the geometric plane do not intersect, there needs to be an additional point defined where they intersect. We define $\mathbb{A}^2 = \{(x, y) | x \text{ and } y \text{ are numbers}\}$ as the Euclidean plane. Thus, each line in the projective plane $\mathbb{P}^2$ consists of a line in $\mathbb{A}^2$ and the set of directions of the line: the point at infinity.

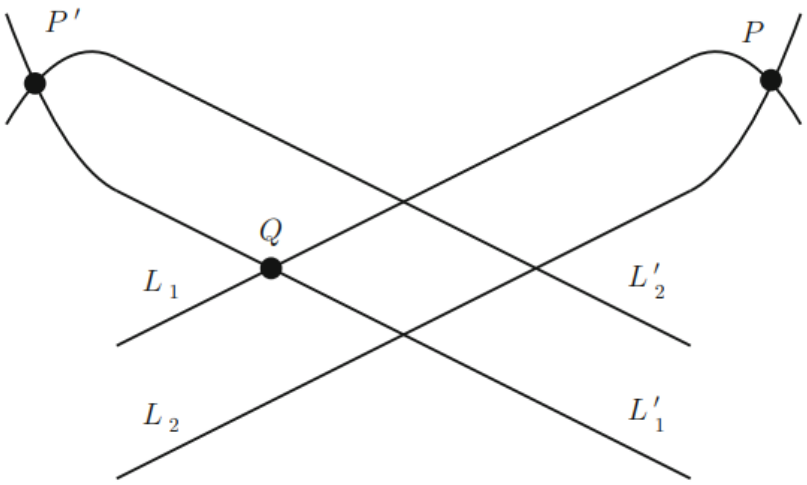

Figure 1.1. Parallel lines intersect at points "at infinity"

Definition 1.4. *(Projective Plane $\mathbb{P}^2$; Geometric Definition). The projective plane is*

$$\mathbb{P}^2 = \mathbb{A}^2 \cup \{\textit{the set of directions in } \mathbb{A}^2\}$$

where the additional points are associated with direction.

Two lines are said to have the same direction if and only if they are parallel. Thus, the geometric definition eliminates the need to distinguish between parallel and non-parallel lines: it has no parallel lines [1].

1.3 Conics

To better understand the proceeding discussion on finding rational points on cubics, this discussion begins by finding rational points on conics. As mentioned earlier, finding rational points on cubics can be more difficult than finding points on conics. To find rational points, first, let $P = (x, y)$, where $x, y \in \mathbb{Q}$, on a conic. A conic refers to a curve, of degree 2, that is generated from the intersection of a circular surface with a plane.

In this case, the conic must be rational, which implies that the coefficients of our equation will need to be rational numbers. A number is said to be rational if it is of the form $\frac{p}{q}$, where p and

q are integers, and $q \neq 0$. Some examples of conics are circles, ellipses, parabolas, and hyperbolas (Figure 1.2). As a disclaimer, ellipse and elliptic curves do not represent the same concept. An ellipse is a set of points whose distance to two fixed points on a plane adds up to a constant. Meanwhile, an elliptic curve is defined by the equation $y^2 = f(x) = x^3 + Ax^2 + Bx + C$.

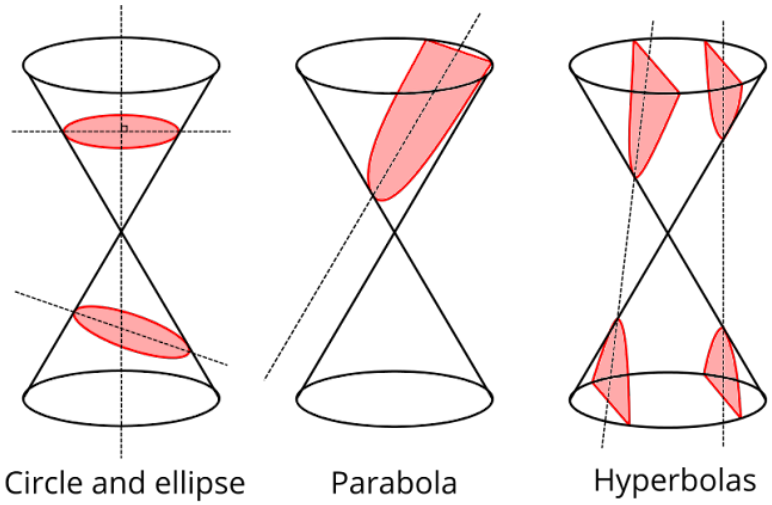

Figure 1.2. Example of Conics

Now, assume that there is a rational point $\mathcal{O}$ on a conic (Figure 1.3). To find the other rational point on the conic, there needs to be a projection of the point $\mathcal{O}$ onto an arbitrary rational line ℓ_1. As a result, there will be a projection from $\mathcal{O}$ onto a rational point Q of our arbitrary rational line ℓ_1. This will result in there being a new rational point on the conic, P. Thus, rational points on conics have a one-to-one correspondence to rational points on a line. Additionally, we determined that a line ℓ_2 and conic intersect at exactly two points. Furthermore, the two points of intersection are rational if and only if the roots of the quadratic equation (for the x-coordinates of the intersection points) are also rational.

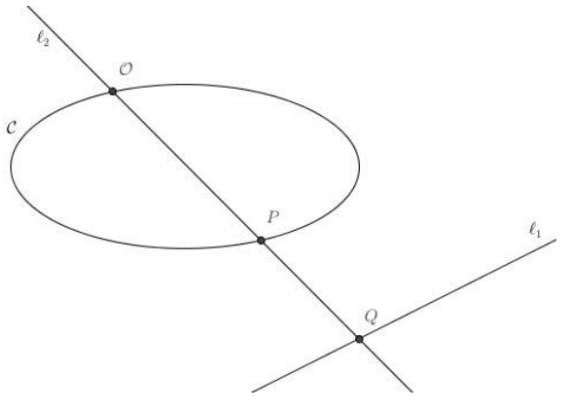

Figure 1.3. Projecting a conic onto a line

Theorem 1.1. *Let $\mathcal{C}$ be a rational conic, $\mathcal{O}$ be a rational point and ℓ_1 be a rational line. Let ℓ_2 be a line that connects $\mathcal{O}$ with ℓ_1 and that intersects the conic again at point P. Let the intersection of ℓ_1 and ℓ_2 be the point Q. The point P is a rational point if and only if Q is a rational point.*

Example 1.3. *Are there any rational solutions to the circle $y^2 = -x^2 + 4$?*

Solution. Let $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$ so that we have the homogenous form $Y^2 = -X^2 + 4Z^2$, where X, Y, and Z have no common factors. Since the equation has integers solutions, namely $(\pm 2, 0)$ and $(0, \pm 2)$, then it follows that the circle $y^2 = -x^2 + 4$ has rational solutions.

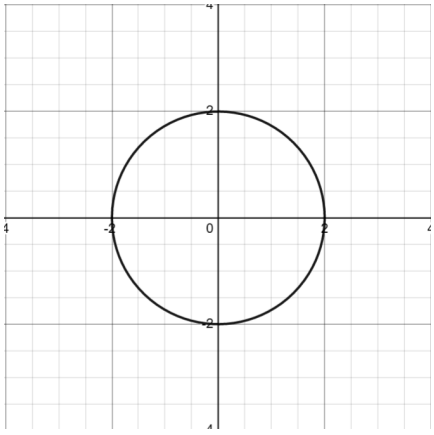

Figure 1.4. Circle: $y^2 + x^2 = 4$

Example 1.4. *Are there any rational solutions to the parabola $y^2 = x^2$?*

Solution. Given the rational point $\mathcal{O} = (0, 3)$, we can easily find another rational point P by projecting the line $L(x) = 2x - 3$ through $\mathcal{O}$, and find that $P = (2, 1)$.

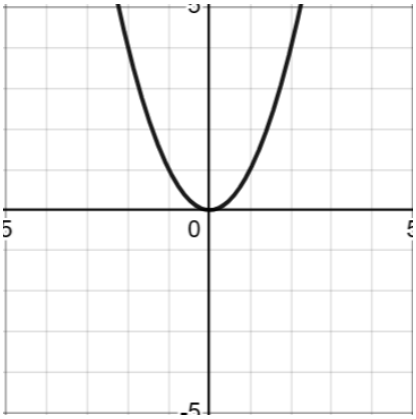

Figure 1.5. Parabolas: $y = x^2$

1.4 Cubics

Meanwhile, a cubic curve, which is of degree 3, has the general form $ax^2 + bx^2y + cxy^2 + ex^2 + fxy + gy^2 + hx + iy + j$, with coefficients $a, b, c, d, e, f, g, h, i, j$. Once again, the cubic must have rational points, so it means that the coefficients must be rational. If two rational points can be found on are given on curve C, then we can find the third point. If we can find the intersection of a rational line with a rational cubic, we can find a cubic equation. Also, if the cubic equation has two rational roots, then it must have a third rational root. So, if given two rational points, P, and Q, on a cubic curve C, then we can find a third rational point, $P * Q$ (Figure 1.6). This can be done by drawing a line through both rational points on the curve.

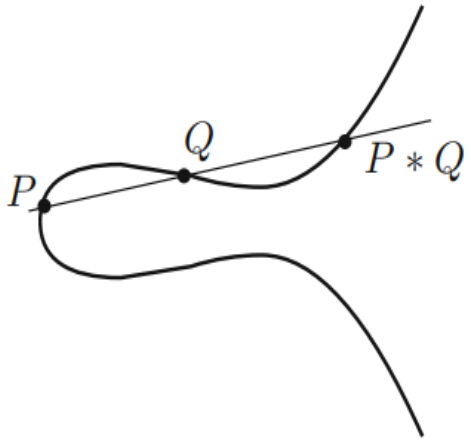

Figure 1.6. Two Distinct Points on a Cubic

However, if only one rational point is known on the curve C, then we can find one additional point (Figure 1.7). If P is the only rational point known on the curve C, we can draw a tangent line at P, so that P is a double root of the cubic equation. Thus, the last, third root, must be rational.

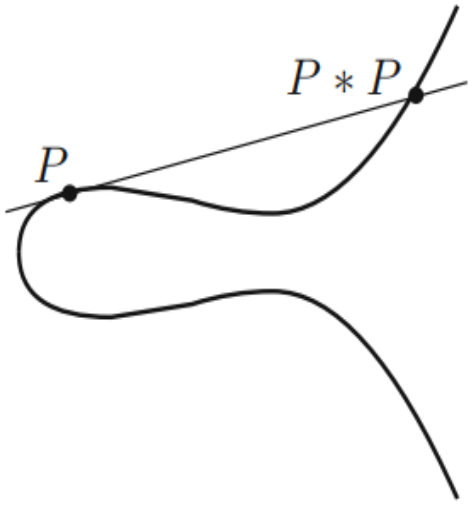

Figure 1.7. Two Non-Distinct Pints on a Cubic

Now that it is understood how to find rational points on cubics, we need to understand what we can do with this information. However, finding a third point doesn't imply a group of rational points because there may not be an identity element. A more thorough discussion on rational points forming a group and how to find these points will be in the next section. As a reminder, there is

no guaranteed way of determining whether an arbitrary rational cubic has rational points. So, what is the best method of determining a group of rational points on a curve?

2 Mordell's Theorem

Theorem 2.1 Mordell's Theorem. *If C is a non-singular rational cubic curve, then there is a finite set of rational points such that all other rational points can be obtained by repeatedly drawing lines and intersections.*

For the remainder of this section, the focus will be on developing different ideas to understand the central theorem for elliptic curves: Mordell's Theorem. This will be completed by developing the tools necessary for understanding Mordell's theorem. First, for finding a group of rational points on an elliptic curve it is necessary to use a group law under addition. This is completed by first understanding the Weierstrass normal form of a non-singular cubic curve. A cubic curve is considered non-singular if has no points at which both the partial derivatives vanish.

In addition, there is one special point that was previously discussed in the Projective Plane discussion, that is important for understanding the group law: the point "at infinity". The point at infinity is denoted by $\mathcal{O}$. Ultimately, these properties will be used to obtain a better understating of Mordell's theorem, and the interesting results of the unique properties.

2.1 Weierstrass Normal Form

Theorem 2.2 *The equation of any cubic curve with a rational point can be written in the form*

$$y^2 = 4x^3 - g_2x - g_3,$$

where a rational point is a point with rational coordinates.

The Weierstrass normal form equation is usually denoted by $y^2 = 4x^3 - g_2x - g_3$, but, with a few modifications, can be denoted by $y^2 = x^3 + ax^2 + bx + c$. To make the Weierstrass normal form equation homogeneous. suppose that $x = X/Z$ and $y = Y/Z$ to obtain $Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3$. For this cubic in Weierstrass normal form, suppose that $\mathcal{O}$ is a rational point

"at infinity" of this non-singular curve. It is a point on every vertical line. Further discussion about the point $\mathcal{O}$ will be included in the proceeding section.

2.2 Group Law

As previously mentioned, an essential theorem for understanding elliptic curves is Mordell's Theorem. It states that for non-singular rational cubic curves, then there exists a finitely generated set of rational points. Thus, we can find a set of rational points on a curve and make it into a group. To do this, we begin by denoting $\mathcal{O}$ as the rational point at infinity and denoting $+$ as the group law operation, which will be commutative. The point at infinity is a special point on the curve because it serves as the identity point for the additive group law. As a disclaimer, point addition on a curve is not related to arithmetic addition. Although both arithmetic addition and point addition on elliptic curves represent the same properties, they do not represent the same ideas. We recall that we can obtain a third point on the curve by drawing a line between two established points over the curve C in Weierstrass normal form, namely P and Q, and obtain $P * Q$ (Figure 1.8). Now, to add P and Q, take the third intersection point we found, $P * Q$, and join it to $\mathcal{O}$ with a line, and we find that the point $P + Q$ is the addition of points P and Q. Since all elliptic curves are symmetric over the x-axis, then it can be thought of as reflecting the point $P * Q$ over the x-axis to obtain $P + Q$. To define the $+$ commutative group law, it must be that the operation is associative, verify that $\mathcal{O}$ is the identity element, that every point contains an inverse (a negative of the point), and that it is commutative.

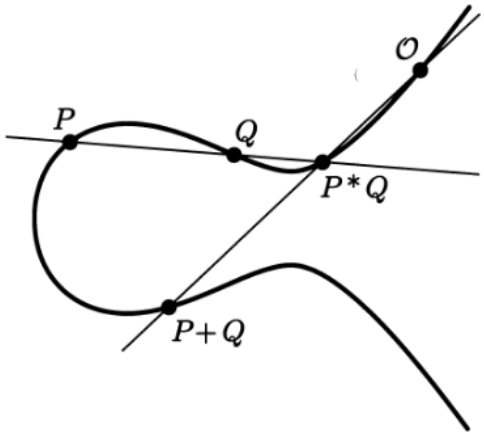

Figure 1.8. The group law on a cubic

Theorem 2.3. *The field $C(\mathbb{Q})$, where C is a non-singular curve on the projective plane, establishes a commutative group under the operation $+$ and the identity element $\mathcal{O}$.*

Proof. Since the line from P to Q is the same line from Q to P, then we determine that $P * Q = Q * P$. So, we can conclude that $P + Q = Q + P$ from the argument above. Thus, it is abelian: commutative. Since a rational line intersects the points P and Q on the rational cubic curve, then the third point must also be rational, which implies that $P * Q$ and $P + Q$ are also rational. Thus, the set of rational points is closed and well-defined under the operation $+$.

Now, to verify the point $\mathcal{O}$ is the identity element. If we draw a line through P and $\mathcal{O}$, then we find the third intersection point $P * \mathcal{O}$ (Figure 1.9). Now, if we draw a line through $\mathcal{O}$ and $P * \mathcal{O}$, then we get that the $P + \mathcal{O}$ is the addition of the points $\mathcal{O}$ and $P * \mathcal{O}$. Thus, it indicates that $P + \mathcal{O} = P = \mathcal{O} + P$ by commutativity, and that verifies that $\mathcal{O}$ is the identity element.

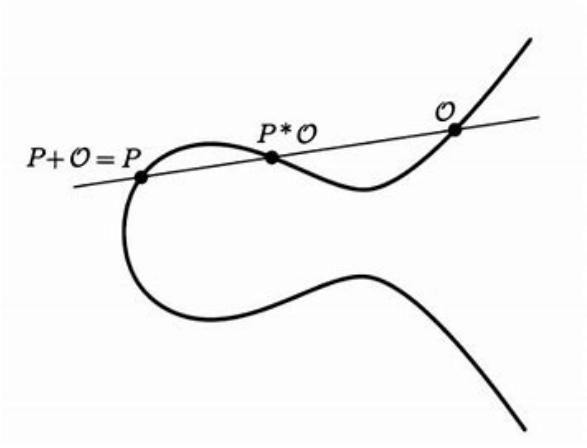

Figure 1.9. Verifying identity element

Now, it follows to demonstrate that the group law holds by showing that every point P contains an inverse. The additive inverse of the point $Q = (x, y)$ is $-Q = (x, -y)$. First, we draw the tangent through the point at $\mathcal{O}$ twice and determine that $S = \mathcal{O} * \mathcal{O}$ (Figure 1.10). It follows that given a point Q, the line through Q and S gives the point $-Q = Q * S$. Since the tangent line through the points $\mathcal{O}$ and S intersect $\mathcal{O}$ twice, then, by drawing a line through the points Q and $-Q$, we get that $Q + (-Q) = (-Q) + Q = \mathcal{O}$. As a result, we have verified that every element Q contains an inverse, namely $(-Q)$.

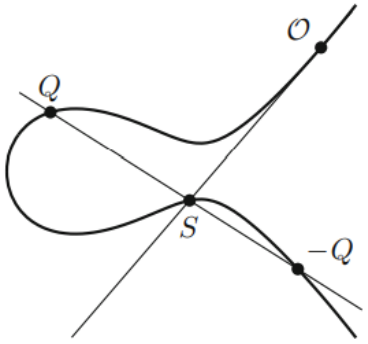

Figure 1.10. The inverse of a point

Lastly, it needs to be determined that the operation is associative. Suppose we are given the points $P, Q, R,$ and identity $\mathcal{O}$. It is known that another point can be found by drawing lines through any two known points. So, using this method we can find the points $Q * R = R * Q$ and

$P * Q = P * Q$. Now, using what we know about connecting these new points with the identity $\mathcal{O}$, we can find the points $Q + R = R + Q$ and $P + Q = Q + P$. Additionally, we need to find the point that joins all three points, which is found through a complex construction of the previous lines which produces $(P + Q) * R = P * (Q + R)$, which implies that $(P + Q) + R = P + (Q + R)$ (Figure 1.11).

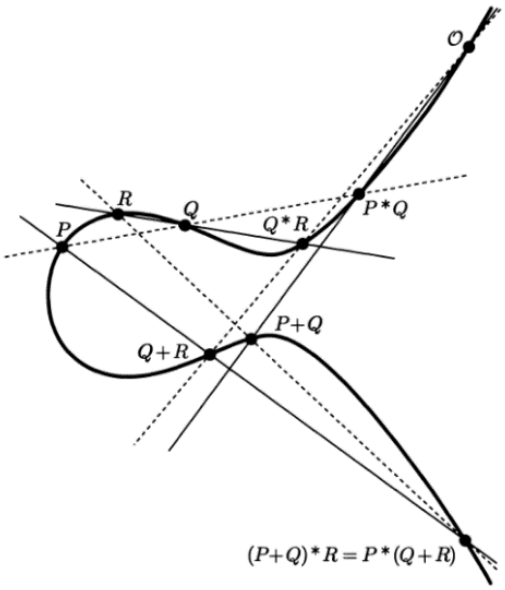

Figure 1.11. Verifying the associative law

Thus, we have roughly shown that a non-singular rational cubic curve C has points that form a commutative group under the operation $+$. ■

2.3 Group Law Explicit Formulas

Any cubic can be transformed into a special form known as Weierstrass normal form. As previously mentioned, the general Weierstrass equation takes the form $y^2 = x^3 + ax^2 + bx + c$. Now, the interest is adding two points to a cubic equation in Weierstrass form, which are explicit formulas of the group law. For that, let $P_1 = (x_1, y_1),\ P_2 = (x_2, y_2), P_1 * P_2 = (x_3, y_3)$, and $P_1 +$

$P_2 = (x_3, -y_3)$, where we have an equation that joins the points P_1 and P_2. The line connecting P_1 and P_2 is defined by the equation:

$$y = \lambda x + v, \text{ where } \lambda = \frac{y_2 - y_1}{x_2 - x_1} \text{ and } v = y_1 - \lambda x_1 = y_2 - \lambda x_2.$$

So, we determine that the third point $P_1 + P_2 = (x_3, -y_3)$ has the coordinates $x_3 = \lambda^2 - a - x_1 - x_2$ and $y_3 = \lambda x_3 + v$.

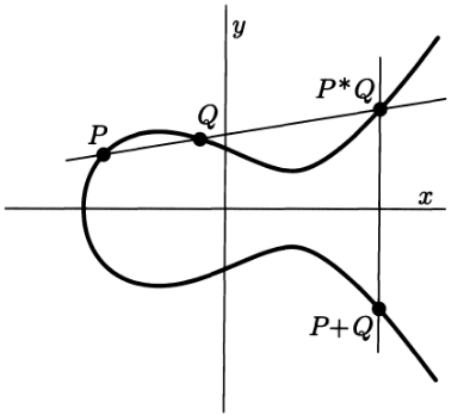

Figure 1.12. Adding points on a Weierstrass cubic

Example 2.1. *Are there any rational points on the curve* $y^2 = 3x^2 + 12$*?*

Solution*. Now, suppose that it is known that the cubic curve* $y^2 = 3x^3 + 12$ *contains the points* $P_1 = (-1, 3)$ and $P_2 = (2, -6)$. To compute $P_1 + P_2$, find the line through P_1 and P_2 to be:

$$y = (-3)x + 0, \text{ where } \lambda = \frac{-9}{3} = -3 \text{ and } v = 3 - (-3)(-1) = (-6) - (-3)(2) = 0.$$

So, we find that $x_3 = (-3)^2 - 0 - (-1) - (3) = 7$ and $y_3 = (-3)(7) + 0 = -21$. Thus, it must be that,

$$P_1 + P_2 = (x_3, -y_3) = (7, -21).$$

2.4 Points of Order 2

Definition 2.1. *The order of a point P is the smallest positive power of a point* m *which results in the identity element*

$$mP = \mathcal{O}.$$

Any point P of a group has order m if $mP = P + \cdots + P = \mathcal{O}$, where there are m sums of P, and $m'P \neq \mathcal{O}$ for all integers $1 \leq m' < m$. So, if there is such m, then the point P is of finite order. Otherwise, the point has infinite order. The Weierstrass normal form equation $y^2 = x^3 + Ax^2 + Bx + C$ and the point at infinity $\mathcal{O}$ are used for the group law. Now, when does $2P = \mathcal{O}$ or its equivalent $P = -P$?

Theorem 2.4. Points of Order Two. *Let C be a non-singular cubic curve*

$$y^2 = f(x) = x^3 + ax^2 + bx + c$$

(Recall that C is non-singular provided that $f(x)$ and $f'(x)$ have no common complex roots, or equivalently if $f(x)$ does not have a double root.)

(a) A point $P = (x, y) \neq \mathcal{O}$ on C has order two if and only if $y = 0$.

Proof. The condition $2P = \mathcal{O}$ implies that P has order 2, which is equivalent to $P = -P$. It is known that $-P = -(x, y) = (x, -y)$, so it must be that P has order 2 when $y = -y$. Thus, it must be that $y = 0$. Conversely, if $y = 0$, then $P = -P$, and P has order 2. ■

Lastly, two theorems that will be important later are the following:

Theorem 2.5. (Mazur's Theorem) *Let C be a non-singular rational cubic curve and suppose that $C(\mathbb{Q})$ contains a point of finite order m. Then either*

$$1 \leq m \leq 10 \text{ and } m = 12.$$

More precisely, the set of points of finite order in $C(\mathbb{Q})$ forms a subgroup that has one of the following forms:

(a) A cyclic group of order N with $1 \leq N \leq 10$ or $N = 12$.

(b) The product of a cyclic group of order two and a cyclic group of order $2N$ with $1 \leq N \leq 4$

Theorem 2.6. (Nagell-Lutz Theorem) *Let*

$$y^2 = f(x) = x^3 + ax^2 + bx + c$$

be a non-singular cubic curve with integer coefficients a, b, c*, and let* D *be the discriminant of the cubic polynomial*

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$$

Let $P = (x, y)$ *be a rational point of finite order. Then* x *and* y *are integers, and either* $y = 0$*, in which case* P *has order two, or else* y *divides* D*.*

2.5 Proof of Mordell's Theorem

Theorem 2.1. Mordell's Theorem. *(for curves with rational points of order two) Let* C *be a non-singular cubic curve given by an equation*

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

where A *and* B *are integers. Then the group of rational points* $C(\mathbb{Q})$ *is a finitely generated abelian group.*

To prove Mordell's Theorem, it needs to be shown that $C(\mathbb{Q})$ satisfies the conditions for the Descent Theorem.

Theorem 2.7 (Descent Theorem) *Let* Γ *be a commutative group and suppose that there is a function*

$$h: \Gamma \to [0, \infty)$$

with the following four conditions:

(a) For every real number M, the set $\{P \in C(\mathbb{Q}) \mid h(P) \leq M\}$ *is finite.*

(b) For every $P_0 \in \Gamma$ *there is a constant* κ_0 *so that*

$$h(P + P_0) \leq 2h(P) + \kappa_0 \text{ for all } P \in \Gamma.$$

(c) There is a constant κ *so that*

$$h(2P) \leq 4h(P) - \kappa \text{ for all } P \in \Gamma.$$

(d) The subgroup 2Γ has a finite index in Γ.

Then Γ is finitely generated.

Now, it needs to be shown that the group of rational points $C(\mathbb{Q})$ is finitely generated, to prove Mordell's Theorem. There are four key lemmas to define a finite generation of rational points on $C(\mathbb{Q})$. Before discussing the lemmas, it is important to know that for a non-singular cubic with integer coefficients $a, b,$ and c, and rational point $P_1 = (x_1, y_1)$, then the height of the point is

$$H(P) = H(x_1),$$

which is its complexity from a number theory perspective. The height of a point is always a positive integer $x = \frac{m}{n}$, such that it is the maximum of the absolute value of the numerator and denominator: $H(x_1) = \max\{|m|, |n|\}$. We also have the property,

$$h(P) = \log H(P),$$

which is the "small h height" and is a non-negative real number. Lastly, the Finiteness Property of the Height states that the set of all rational numbers whose height is less than some fixed number is a finite set.

Since we want to prove that the group of rational points $C(\mathbb{Q})$ is finitely generated, we will use the following four lemmas: Lemma 2.1, 2.2, 2.4, and 2.6.

Lemma 2.1. *For every real number M, the set*

$$\{P \in C(\mathbb{Q}) \mid h(P) \leq M\}$$

is finite.

Proof. First, note that the rational points on curve C fulfill the finiteness property. Thus, if M is any positive number, then

$$\{P \in C(\mathbb{Q}) \mid H(P) \leq M\}$$

is a finite set. ■

It is a finite set because there is a finite amount of x-coordinates, and each of those coordinates only has two possibilities of a y-coordinate. Additionally, it follows that we can replace $H(P)$ with $h(P)$.

Lemma 2.2. *Let P_0 be a fixed rational point of C. There is a constant κ_0 that depends on P_0 and on $a, b,$ and c, so that*

$$h(P + P_0) \leq 2h(P) + \kappa_0 \text{ for all } P \in C(\mathbb{Q}).$$

Proof. Assume that there is a fixed rational point P_0 such that $P_0 \neq \mathcal{O}$ and that $P_0 = (x_0, y_0)$. Additionally, it is sufficient to prove this lemma for $P \notin \{P_0, -P_0, \mathcal{O}\}$. Also, we define $P = (x, y)$. Next, we write $P + P_0 = (\xi, \eta)$ and we must obtain the height. To do so, we note that

$$\xi + x + x_0 = \lambda^2 - a \text{ with } \lambda = \frac{y - y_0}{x - x_0},$$

which can be expanded to

$$\xi = \frac{(y - y_0)^2}{(x - x_0)^2} - a - x - x_0$$

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

If we expand the numerator, we will obtain $y^2 - x^3$. Since we know that the point P lies on the curve we are on, then we can replace $y^2 - x^3$ with $ax^2 + bx + c$ because we know that the curves are of the form $y^2 = x^3 + ax^2 + bx + c$. Then, rearranging and replacing the previous equation we obtain

$$\xi = \frac{Ay + Bx^2 + Cx + D}{Ex^2 + Fx + G},$$

where A, B, C, D, E, F, G are integers that depend and are expressed in terms of a, b, c and (x_0, y_0).

Next, we want to substitute $x = \frac{m}{e^2}$ and $y = \frac{n}{e^2}$ and multiplying both the numerator and denominator by e^4. Then, we obtain

$$\xi = \frac{Ane + Bm^2 + Cme^2 + De^4}{Em^2 + Fme^2 + Ge^4}.$$

Now, since we know the equation has a numerator and denominator that are integers, we can find the height of ξ such that

$$H(\xi) \leq \max\{|Ane + Bm^2 + Cme^2 + De^4|, |Em^2 + Fme^2 + Ge^4|\},$$

and using the following properties

$$e \leq H(P)^{\frac{1}{2}}, n \leq KH(P)^{\frac{3}{2}}, \text{and } m \leq H(P),$$

where K depends on a, b, c, we use the triangle inequality to determine

$$\begin{aligned} |Ane + Bm^4 + Cme^2 + De^4| &\leq |Ane| + |Bm^2| + |Cme^2| + |De^4| \\ &\leq (|AK| + |B| + |C| + |D|)H(P)^2, \end{aligned}$$

and

$$\begin{aligned} |Em^2 + Fme^2 + Ge^4| &\leq |Em^2| + |Fme^2| + |Ge^4| \\ &\leq (|E| + |F| + |G|)H(P)^2. \end{aligned}$$

Thus, we find that

$$H(P + P_0) = H(\xi) \leq \max\{|AK| + |B| + |C| + |D|, |E| + |F| + |G|\}\, H(P)^2,$$

and if we take the log of both sides, we obtain

$$h(P + P_0) \leq 2h(P) + \kappa_0,$$

such that $\kappa_0 = \log \max\{|AK| + |B| + |C| + |D|, |E| + |F| + |G|\}$, which only depends on a, b, c and (x_0, y_0) and not on P. ■

Before continuing there must be an additional lemma that will help with the lemmas necessary for Mordell's Theorem. It is necessary to prove the following lemma involving heights and polynomials before continuing.

Lemma 2.3. *Let $\phi(X)$ and $\psi(X)$ be polynomials with integer coefficients and no common complex roots. Let d be the maximum of the degrees of ϕ and ψ.*

(a) There is an integer $R \geq 1$, depending on ϕ and ψ, so that for all rational numbers $\frac{m}{n}$,

$$gcd\left(n^d\phi\left(\frac{m}{n}\right), n^d\psi\left(\frac{m}{n}\right)\right) divides\ R.$$

(b) There are constants κ_1 and κ_2, depending on ϕ and ψ, so that for all rational numbers $\frac{m}{n}$ that are not roots of ψ,

$$dh\left(\frac{m}{n}\right) - \kappa_1 \leq h\left(\frac{\phi\left(\frac{m}{n}\right)}{\psi\left(\frac{m}{n}\right)}\right) \leq dh\left(\frac{m}{n}\right) + \kappa_2.$$

Proof. *(a)* We note that $n^d\phi\left(\frac{m}{n}\right)$ and $n^d\psi\left(\frac{m}{n}\right)$ are integers and we let $deg(\phi) = d$ and $\deg(\psi) = e \leq d$, so we obtain

$$n^d\phi\left(\frac{m}{n}\right) = a_0m^d + a_1m^{d-1}n + \cdots + a_dn^d = \Phi(\mathrm{m}, \mathrm{n}),$$

$$n^d\psi\left(\frac{m}{n}\right) = b_0m^en^{d-e} + b_1m^{e-1}n^{d-e+1} + \cdots + b_en^d = \Psi(m, n).$$

Now, we must note that since $\phi(X)$ and $\psi(X)$ have no common roots, then in the Euclidean ring $\mathbb{Q}[X]$ they are relatively prime, so there exists polynomials $F(X)$ and $G(X)$ such that

$$F(X)\phi(X) + G(X)\psi(X) = 1.$$

Now, let A be an integer such that $AF(X)$ and $AG(X)$ have integer coefficients and D be the maximum degree of both F and G, which do not depend on polynomials m and n. By substituting $X = \frac{m}{n}$, we obtain

$$n^D AF\left(\frac{m}{n}\right) \cdot n^d \phi\left(\frac{m}{n}\right) + n^D AG\left(\frac{m}{n}\right) \cdot n^d \psi\left(\frac{m}{n}\right) = An^{D+d}.$$

If we let $\gamma = \gamma(m, n)$ be the $\gcd(\Phi\,(m, n), \Psi(\mathrm{m}, \mathrm{n}))$, we obtain

$$\left\{n^D AF\left(\frac{m}{n}\right)\right\} n^d \phi\left(\frac{m}{n}\right) + \left\{n^D AG\left(\frac{m}{n}\right)\right\} n^d \psi\left(\frac{m}{n}\right) = An^{D+d}$$

where γ divides An^{D+d}. Also, since γ divides $\Phi(m, n)$, then it divides

$$An^{D+d-1}\Phi(m, n) = Aa_0 m^d n^{D+d-1} + Aa_1 m^{d-1} n^{D+d} + \cdots + Aa_d n^{D+2d-1},$$

where γ divides $Aa_0 m^d n^{D+d-1}$. Therefore, we know that γ divides $\gcd(An^{D+d}, Aa_0 m^d n^{D+d-1})$. Also, since m and n are relatively prime, then we can further conclude that γ divides $Aa_0 n^{D+d-1}$. Ultimately, by continuously showing that γ is a divisor of $Aa_0^2 n^{D+d-2}\Phi(m, n)$, we can eventually find that γ divides Aa_0^{D+d}.

(b) First, we will only prove the lower bound. We assume that the rational number $\frac{m}{n}$ is not a root of ϕ. We note that if r is any non-zero rational number, then $h(r) = h\left(\frac{1}{r}\right)$. Also, assume that $deg(\phi) = d$ and $\deg(\psi) = e \leq d$. Then, we find that

$$\xi = \frac{\phi\left(\frac{m}{n}\right)}{\psi\left(\frac{m}{n}\right)} = \frac{n^d \phi\left(\frac{m}{n}\right)}{n^d \psi\left(\frac{m}{n}\right)} = \frac{\Phi(\mathrm{m}, \mathrm{n})}{\Psi(m, n)},$$

so $H(\xi) = \max(|\Phi(m, n)|, |\Psi(\mathrm{m}, \mathrm{n})|)$, where there is an $R \geq 1$ such that the greatest common divisor of $\Phi(\mathrm{m}, \mathrm{n})$ and $\Psi(\mathrm{m}, \mathrm{n})$ divides R, where we can obtain

$$H(\xi) \geq \frac{1}{R}\max\{|\Phi(\mathrm{m},\mathrm{n})|, |\Psi(m,n)|\}$$

$$= \frac{1}{R}\max\left\{\left|n^d\phi\left(\frac{m}{n}\right)\right|, \left|n^d\psi\left(\frac{m}{n}\right)\right|\right\}$$

$$= \frac{1}{2R}\left(\left|n^d\phi\left(\frac{m}{n}\right)\right| + \left|n^d\psi\left(\frac{m}{n}\right)\right|\right).$$

Next, we must observe that

$$H\left(\frac{m}{n}\right)^d = \max\{|m|^d, |n|^d\}$$

and we consider

$$\frac{H(\xi)}{H\left(\frac{m}{n}\right)^d} \geq \frac{1}{2R}\cdot\frac{\left|n^d\phi\left(\frac{m}{n}\right)\right| + \left|n^d\psi\left(\frac{m}{n}\right)\right|}{\max\{|m|^d, |n|^d\}}$$

$$= \frac{1}{2R}\cdot\frac{\left|\phi\left(\frac{m}{n}\right)\right| + \left|\psi\left(\frac{m}{n}\right)\right|}{\max\left\{\left|\frac{m}{n}\right|^d, 1\right\}}.$$

If we consider the equation $p(t) = \frac{\left|\phi\left(\frac{m}{n}\right)\right|+\left|\psi\left(\frac{m}{n}\right)\right|}{\max\left\{\left|\frac{m}{n}\right|^d,1\right\}}$, then there is a constant $C_1 > 0$ such that $p(t) \geq$ C_1. So we determine that

$$\frac{H(\xi)}{H\left(\frac{m}{n}\right)^d} \geq \frac{1}{2R}\cdot\ p\left(\frac{m}{n}\right)$$

and conclude that

$$H(\xi) \geq \frac{C_1}{2R}\cdot H\left(\frac{m}{n}\right)^d.$$

Additionally, we can derive the inequality

$$h(\xi) \geq dh\left(\frac{m}{n}\right) - \kappa_1 \text{ with } k_1 = \log(\tfrac{2R}{C_1}).$$

So, we have completed the proof for the lower bound. ■

Now, it is possible to move forward with the essential lemma for Mordell's Theorem.

Lemma 2.4. *There is a constant κ, depending on $a, b,$ and c, so that*

$$h(2P) \leq 4h(P) - \kappa \text{ for all } P \in C(\mathbb{Q}).$$

Proof. Suppose $P = (x, y)$ and $2P = (\xi, \eta)$, and because of the duplication formula, we know that

$$\xi + 2x = \lambda^2 - a \text{ with } \lambda = \frac{f'(x)}{2y}$$

and by setting $y^2 = f(x)$, we can get

$$\xi = \frac{f'(x)^2 - (8x + 4a)f(x)}{4f(x)} = \frac{x^4 + \cdots}{4x^3 + \cdots}$$

where $f(x) \neq 0$ because $2P \neq \mathcal{O}$. Also, there are no common roots between the numerator and denominator of ξ. Now, using *Lemma 2.3*, we derived the inequality

$$h(\xi) \geq dh\left(\frac{m}{n}\right) - \kappa_1 \text{ with } k_1 = \log(\tfrac{2R}{C_1}).$$

Then, can determine that

$$h(2P) \leq 4h(P) - \kappa \text{ for all } P \in C(\mathbb{Q}).$$ ■

Now, we will complete the last lemma necessary for understanding Mordell's Theorem. For this last lemma, we will only want to prove it for cubics with one rational point, which implies that there is at least one rational point $(x_0, 0)$ of order 2. Since we want the cubic $f(x)$ to contain at least one rational root x_0, then it follows that $f(x_0) = 0$. This curve is of the form $C: y^2 = f(x) = x^3 + Ax^2 + Bx$, where $A, B \in \mathbb{Z}$, with a discriminant $D = b^2(a^2 - 4b)$ that is non-zero. Additionally, there are a few tools that need to be developed before the completion of the last lemma.

Proposition 2.1. *Let C and $\bar{C}$ be elliptic curves given by the equations*

$$C: y^2 = x^3 + ax^2 + bx \text{ and } \bar{C}: y^2 = x^3 + \bar{a}x^2 + \bar{b}x,$$

and let $T = (0,0) \in C$. It follows that

(a) There is a homomorphism $\phi: C \longmapsto \bar{C}$ defined by

$$\phi(P) = \begin{cases} \left(\dfrac{y^2}{x^2}, \dfrac{y(x^2-b)}{x^2}\right), & if\ P = (x,y) \neq \mathcal{O}, T, \\ \bar{\mathcal{O}}\,, & if\ P = \mathcal{O} \text{ or } P = T\,. \end{cases}$$

The kernel of ϕ is $\{\mathcal{O}, T\}$.

(b) Applying the same process $\bar{C}$ gives the map $\bar{\phi}: \bar{C} \longmapsto \bar{\bar{C}}$. The curve $\bar{\bar{C}}$ is isomorphic to C via the map $(x,y) \longmapsto \left(\frac{1}{4}x, \frac{1}{8}y\right)$. There is thus a homomorphism $\psi : \bar{C} \longmapsto C$ defined by

$$\psi(\bar{P}) = \begin{cases} \left(\dfrac{\bar{y}^2}{\bar{x}^2}, \dfrac{\bar{y}(\bar{x}^2-\bar{b})}{\bar{x}^2}\right), & if\ \bar{P} = (\bar{x},\bar{y}) \neq \bar{\mathcal{O}}, \bar{T}, \\ \mathcal{O}\,, & if\ \bar{P} = \bar{\mathcal{O}} \text{ or } \bar{P} = \bar{T}\,. \end{cases}$$

(c) The composition $\psi \circ \phi$: $C \to C$ is the multiplication by the two maps,

$$\psi \circ \phi(P) = 2P.$$

Proposition 2.2.

(a) The map $\alpha: \Gamma \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ described above is a homomorphism.

(b) The kernel of α is the image $\psi(\bar{\Gamma})$. Hence α induces a one-to-one homomorphism

$$\Gamma/\psi(\bar{\Gamma}) \hookrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}\,.$$

(c) Let $p_1, p_2, \ldots, p_t$ be the distinct primes dividing b. Then the image of α is contained in the subgroup $\mathbb{Q}^*/\mathbb{Q}^{*2}$ consisting of the elements $\{\pm p_1^{\epsilon_1}, p_2^{\epsilon_2}, \ldots, p_t^{\epsilon_t} | each\ \epsilon_i\ equal\ 0\ or\ 1\}$.

(d) The index $(\Gamma: \psi(\bar{\Gamma}))$ is at most 2^{t+1}.

Lemma 2.5. *Let A and B be abelian groups, and suppose that $\phi: A \to B$ and $\Psi: B \to A$ are homomorphisms satisfying*

$$\psi \circ \phi(a) = 2a \; for \; all \; a \in A \; and \; \phi \circ \psi(b) = 2b \; for \; all \; b \in B.$$

Suppose further that $\phi(A)$ has a finite index in B and $\psi(B)$ has a finite index in A. Then $2A$ has a finite index in A. More, precisely, the indices satisfy

$$(A: 2A) \leq \big(A: \psi(B)\big)\big(B: \phi(A)\big).$$

Proof. Since $\psi(B)$ has a finite index in A and $\phi(A)$ has a finite index in B, we state that

$$\{a_i + \psi\big(b_j\big): 1 \leq i \leq n, 1 \leq j \leq m\}$$

is a set that represents the cosets of $2A$ in A. Then, we can determine that

$$a = a_i + \psi(b) = a_i + \psi(b_j + \phi(a'))$$

$$= a_i + \psi(b_{j)} + \psi(\phi(a'))$$

$$= a_i + \psi\big(b_j\big) + 2a',$$

so it holds that

$$(A: 2A) \leq \big(A: \psi(B)\big)\big(B: \phi(A)\big). \qquad \blacksquare$$

Now, there are sufficient tools to complete the last lemma of the Descent Theorem for $C(\mathbb{Q})$.

Lemma 2.6. *The index $(C(\mathbb{Q}) \mid 2C(\mathbb{Q}))$ is finite.*

Proof. We determined that the form of the cubic is

$$C: y^2 = f(x) = x^3 + Ax^2 + Bx.$$

Since we are interested in $(\Gamma: 2\Gamma)$, we need the map from $P \longmapsto 2P$ as a composition of two maps of degree two, so need another curve

$$\bar{C}: y^2 = x^3 + \bar{a}x^2 + \bar{b}x,$$

$$\bar{\bar{C}}: y^2 = x^3 + \bar{\bar{a}}x^2 + \bar{\bar{b}}x$$

such that $\bar{a} = -2a$ and $\bar{b} = a^2 - 4b$, and $\bar{\bar{a}} = -2\bar{a} = 4$ and $\bar{\bar{b}} = \bar{a}^2 - 4\bar{b} = 16b$. Important to note that C and $\bar{\bar{C}}$ have an isomorphic group under rational numbers such that you can obtain the latter through transformation. This can be simplified into *Proposition 2.1*.

Next, we use the following claims to have an understanding of the image of the homomorphism $\phi: C \mapsto \bar{C}$ and $\psi: \bar{C} \longmapsto C$ such that the compositions are

$$\phi \circ \psi: \bar{C} \mapsto \bar{C} \text{ and } \psi \circ \phi: C \longmapsto C.$$

The claims are,

(a) $\bar{O} \in \phi(\Gamma)$

(b) $\bar{T} = (0,0) \in \phi(\Gamma)$ if and only if $\bar{b} = a^2 - 4b$ is a perfect square.

(c) Let $\bar{P} = (\bar{x}, \bar{y}) \in \bar{\Gamma}$ with $\bar{x} \neq 0$. Then $\bar{P} \in \phi(\bar{\Gamma})$ if and only if $\bar{x}$ is the square of a rational number.

It follows from *Proposition 2.2* we can find the necessary mappings. Lastly, using the previous tools and *Lemma 2.6*, we prove that

$$(C(\mathbb{Q}) \mid 2C(\mathbb{Q})) \text{ is finite.} \qquad \blacksquare$$

Thus, by satisfying the four conditions of the Descent Theorem and the proof of $C(\mathbb{Q})$ for Mordell's Theorem [2].

3 Ranks of Elliptic Curves

In the previous section, it was discussed how to find rational points on a cubic curve to form a group. It was discussed that points could be added to find additional points on a curve using group law, and how to find these points using explicit formulas. Now, these properties and tools will be used to determine the rank of a curve. These sections will focus on looking at previous achievements associated with investigating the ranks of elliptic curves. Additionally, they will investigate ranks of specific elliptic curves: $y^2 = x^3 + Ax^2 + Bx$ and $y^2 = x^3 + Bx$.

3.1 Ranks

Definition 3.1, *The rank of an elliptic curve is the number of independent points of infinite order.*

We define the group Γ of rational points on the curve $C: y^2 = x^3 + ax^2 + bx$ as a finitely generated abelian group. We denote the additive group of integers as $(\mathbb{Z}, +)$ and $\mathbb{Z}_m$ denote the cyclic group $(\mathbb{Z}/m\mathbb{Z}, +)$ of integers modulo m. Also, we can interpret this form as

$$P_1, \dots, P_r, Q_1, \dots, Q_s \in \Gamma,$$

such that every $P \in \Gamma$ is of the form $P = n_1P_1 + \cdots + n_rP_r + m_1Q_1 + \cdots + m_sQ_s$. The group Γ is finite if and only if it has rank $r = 0$. Then, Γ takes the form

$$\Gamma \cong \mathbb{Z} \oplus \mathbb{Z} \oplus \dots \oplus \mathbb{Z} \oplus \mathbb{Z}_{p_1^{v_1}} \oplus \mathbb{Z}_{p_2^{v_2}} \oplus \dots \oplus \mathbb{Z}_{p_s^{v_s}},$$

where $\mathbb{Z}_{p_1^{v_1}} \oplus \mathbb{Z}_{p_2^{v_2}} \oplus \dots \oplus \mathbb{Z}_{p_s^{v_s}}$ corresponds to the finite order in Γ, and $p_1^{v_1}p_2^{v_2} \dots p_s^{v_s}$ is the order of the torsion subgroup of Γ.

Now, Mordell's Theorem allowed for the determination of the quotient group $\Gamma/2\Gamma$ and can find that

$$2\Gamma \cong 2\mathbb{Z} \oplus 2\mathbb{Z} \oplus \dots \oplus 2\mathbb{Z} \oplus 2\mathbb{Z}_{p_1^{v_1}} \oplus 2\mathbb{Z}_{p_2^{v_2}} \oplus \dots \oplus 2\mathbb{Z}_{p_s^{v_s}}, \text{ and}$$

$$\Gamma/2\Gamma \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}_{p_1^{v_1}} \oplus \mathbb{Z}/2\mathbb{Z}_{p_2^{v_2}} \oplus \dots \oplus \mathbb{Z}/2\mathbb{Z}_{p_s^{v_s}}.$$

Ultimately, it can be derived that

$$(\Gamma : 2\Gamma) = 2^r \cdot \#\Gamma[2],$$

such that, for this purpose,

$$\#\Gamma[2] = \begin{cases} 2, & if\ a^2 - 4b\ is\ not\ square, \\ 4, & if\ a^2 - 4b\ is\ a\ square\ , \end{cases}$$

and serves as the formula for any finitely generated abelian groups of rank r. Along these lines, we can define another definition for Mordell's Theorem using the torsion subgroup.

Theorem 2.1. Mordell's Theorem *The group $E(\mathbb{Q})$ is a finitely generated abelian group. Thus*

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

where the torsion subgroup $E(\mathbb{Q})_{tors}$ is a finite abelian group corresponding to the elements of $E(\mathbb{Q})$ with finite order, and r is the rank of $E(\mathbb{Q})$.

Example 3.1. *What is the group $E(\mathbb{Q})$ of the curve $y^2 = x^3 - x$?*

Solution. It can be determined that $E(\mathbb{Q}) = E(\mathbb{Q})_{tors} \times \mathbb{Z}^0 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ for $y^2 = x^3 - x$, so the rank of the curve is $r = 0$. Also, the points $(0,0), (\pm 1,0)$ have order 2 in $E(\mathbb{Q})$.

Rank ≥	*Year*	*Author(s)*
3	*1938*	*Billing*
4	*1945*	*Wiman*
6	*1974*	*Penney - Pomerance*
7	*1975*	*Penney - Pomerance*
8	*1977*	*Grunewald – Zimmert*
9	*1977*	*Brumer – Kramer*
12	*1982*	*Mestre*
14	*1986*	*Mestre*
15	*1992*	*Mestre*
17	*1992*	*Nagao*
19	*1992*	*Fermigier*
20	*1993*	*Nagao*
21	*1994*	*Nagao – Kouya*
22	*1997*	*Fermigier*
23	*1998*	*Martin – McMillen*
24	*2000*	*Martin - McMillen*

28	*2006*	*Elkies*

Table 1.4. Rank Records [6]

3.2 Investigating Ranks of Elliptic Curves

Theorem 3.1. (Bhargava, Shankar) *The average rank of all elliptic curves over $\mathbb{Q}$ is less than 1.*

More precisely, the average rank is greater than 0.2 and less than 0.9. It is believed to be exactly ½: half rank 0 and half rank 1.

Now that there is a general understanding of elliptic curves and some of their properties, one recent investigation about elliptic curves is the bound of the rank of elliptic curves: the minimum number of generators. Thus, one unanswered question about the rank of elliptic curves is the Birch and Swinnerton-Dyer conjecture, a Millennium Prize Problem.

Conjecture 3.1 (Birch and Swinnerton-Dyer) *The Taylor expansion of $L(C,s)$ at $s = 1$ has the form*

$$L(C,s) = c(s-1)^r + higher\ order\ terms$$

with $c \neq 0$ and $r = rank\big(C(\mathbb{Q})\big)$ [5].

In particular, this conjecture asserts that $L(C,1) = 0 \Leftrightarrow C(\mathbb{Q})$ is infinite.

It implies that the average rank is bound. The following illustrates different forms of elliptic curves and their ranks across their coefficients.

Rank	*A = B*	*Independent Points*
0	*1, 2, 3, 5, 7, 8, 9, 10, 11, 14, 15, 16, 20, 23,25, 26, 27, 29, 30, 31, 32, 35, 37, 44, 45, 47, 50*	

1	*6, 12, 13, 17, 18, 19, 21, 24, 28, 33, 34, 36, 39, 40, 41, 43, 46, 48, 49*	*[(-3,3)], [(-6,12)], [(4,18)], [(361/144, 22211/1728)], [(-6,18)], [(729/64, 33021/512)], [(4,22)], [(1,7)], [(9,57)], [(64, 632)], [(9/4, 129/8)], [(-18, 72)], [(624, 16068)], [(1,9)], [(961/144, 84599/1728)], [(14161/2304, 5093081/110592)], [(81/4, 1341/8)], [(4,32)], [(16,132)]*
2	*22, 42*	*[(-18,30), (-11,33)], [(-27,99), (-14,70)]*

Table 1.5. Rank for the curves of the form $C: y^2 = x^3 + Ax^2 + Bx$

Rank	*B*	*Independent Points*
0	*1, 2, 4, 6, 7, 10, 11, 12, 16, 17, 22, 23, 25, 26, 27, 30, 32, 36, 38, 41,42,43, 44, 45, 50*	
1	*3, 5, 8, 9, 13, 15, 18, 19, 20, 21, 24, 28, 31, 35, 37, 40, 47, 48, 49*	*[(1,2)], [(20,90)], [(1,3)], [(4,10)], [(9/4, 51/8)], [(1,4)], [(3,9)], [(9,30)], [(4,12)], [(25/4, 155/8)], [(1,5)], [(2,8)], [(25/9, 280/27)], [(1,6)], [(22801/900, 3540799/27000)], [(9,33)], [(289/25, 5712/125)], [(4,16)], [(16/9, 260/27)]*
2	*14, 33, 34, 39, 46*	*[(2,6), (18,78)], [(4,14), (16,68)], [(8,28), (32,184)], [(3,12), (27,144)], [(2,10), (1127,37835)]*

Table 1.6. Rank for the curves of the form $C: y^2 = x^3 + Bx$

4 Conclusion

This thesis focused on informing and investigating concepts about elliptic curves that still have unanswered questions. Primarily, it focused on finding independent rational points on elliptic curves of the Weierstrass normal form. While this thesis focused on elliptic curves over the rational fields, understating elliptic curves over other number fields is essential for obtaining a holistic understanding of them.

The inclusion of the final conjectures and theorems is indicative that there is still much work that needs to be done in this field. But acknowledges some advances in the field, such as the boundedness of ranks, by Manjul Bhargava and Arul Shankar, in the last few decades. However, the understanding of ranks on elliptic curves is still limited and there is a lot of work that needs to be accomplished to further the understanding of this mathematical field. It will be interesting to see the application of elliptic curves as we continue to obtain a greater understanding of them.

Glossary

Associative: When performing an operation, the grouping in which the operation is executed is trivial

Binary Operation: An operation that uses two elements to produce another element.

Commutative: Changing the order of the operands will not change the results

Cubic Polynomial: An equation of degree 3.

Discriminant: A value that helps determine the smoothness and singularity of a curve.

Elliptic Curves: Equations of the form $y^2 = f(x) = x^3 + Ax^2 + Bx + C$, where A, B, C are coefficients on a field.

Field: An established set where addition, subtraction, multiplication, and division are well-defined according to the given operation.

Group: An established set with an operation that combines elements of a set to produce another element in that same set. The operation must be associative, the set must contain an identity, and there must be an inverse for every element in the set.

Height: Assigns a measure of complexity or size to a point on a curve.

Integers: $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$

Nonsingular curve: The curve has no cusps or intersections or where both partial derivatives simultaneously vanish.

Order: The cardinality or the number of elements that form a set or group.

Polynomial: An equation of degree 2.

Rank: The maximum number of independent points on an elliptic curve based on the group structure.

Rational Numbers: $\mathbb{Q} = \left\{ \frac{p}{q} \,\middle|\, p, q \in \mathbb{Z} \; and \; q \neq 0 \right\}$

References

[1] Sala, M., & Taufer, D. "A Survey on the Group of Points Arising from Elliptic Curves with a Weierstrass Model over a Ring." International Journal of Group Theory, vol. 12, no. 3, (2023), 177–196.

[2] Silverman, J. H., & Tate, J. T. "Rational Points on Elliptic Curves." Springer, 2015.

[3] Lauter, K. "The Advantages of Elliptic Curve Cryptography for Wireless Security." IEEE Wireless Communications, vol. 11, no. 1, (2004), 62–67. doi:10.1109/mwc.2004.1269719.

[4] Amara, M., & Siad, A. "Elliptic Curve Cryptography and its Applications." In International Workshop on Systems, Signal Processing and their Applications, WOSSPA, Tipaza, Algeria, 2011, pp. 247-250. doi:10.1109/WOSSPA.2011.5931464.

[5] Rubin, K., & Silverberg, A. "Ranks of Elliptic Curves." Bulletin of the American Mathematical Society, vol. 39, no. 4, (2002), 455–474. doi:10.1090/s0273-0979-02-00952-7.

[6] Dujella, A. "History of Elliptic Curves Rank Records." Available at: https://web.math.pmf.unizg.hr/~duje/tors/rankhist.html.