6-2015

Elliptic Curves

Trinity Mecklenburg

Elliptic Curves

A Thesis

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts

in

Mathematics

---

by

Trinity Leaire Mecklenburg

June 2015

Elliptic Curves

A Thesis

Presented to the

Faculty of

California State University,

San Bernardino

---

by

Trinity Leaire Mecklenburg

June 2015

Approved by:

Ilseop Han, Committee Chair	Date
Zahid Hasan, Committee Member	
John Sarli, Committee Member	
Charles Stanton, Chair, Department of Mathematics	Corey Dunn Graduate Coordinator, Department of Mathematics

Abstract

The main focus of this paper is the study of elliptic curves, non-singular projective curves of genus 1. Under a geometric operation, the rational points $E(\mathbb{Q})$ of an elliptic curve E form a group, which is a finitely-generated abelian group by Mordell's theorem. Thus, this group can be expressed as the finite direct sum of copies of $\mathbb{Z}$ and finite cyclic groups. The number of finite copies of $\mathbb{Z}$ is called the rank of $E(\mathbb{Q})$.

From John Tate and Joseph Silverman [ST92], we have a formula to compute the rank of curves of the form $E : y^2 = x^3 + ax^2 + bx$. In this thesis, we generalize this formula, using a purely group theoretic approach, and utilize this generalization to find the rank of curves of the form $E : y^2 = x^3 + c$. To do this, we review a few well-known homomorphisms on the curve $E : y^2 = x^3 + ax^2 + bx$ as in Tate and Silverman's *Elliptic Curves* [ST92], and study analogous homomorphisms on $E : y^2 = x^3 + c$ and relevant facts.

Acknowledgements

I would like to thank all of the wonderful professors I have had at CSUSB. I am grateful for all they have taught me. I would like to thank Professor Chavez for always having an enjoyable class and making so much sense. I know he deserves to retire someday, but part of me hopes he never does. I would also like to thank Professor Trapp for having an enjoyable class, his personality and his one-of-a-kind laugh. He patiently gave me countless office hours and stayed after every test to go over the problems that would have caused me insomnia if they were left unanswered. I would like to thank Professor Ventura for convincing me that I was competent enough to do the MA program. I would also like to thank Professor McMurran for going above and beyond her job duties. I could not possibly list all of the things I would like to thank her for. She is a mentor to me and has a vested interest in her students, like no other. Thank you to my committee members, Professor Hasan and Professor Sarli. I appreciate all the time they have given me. A special thanks to Professor Han for introducing me to this topic and for his excitement for it. He is an excellent teacher. I have learned so much from him, not just about elliptic curves, but about how to write mathematics and about life. He has given me so much of his time, unpaid. If I ever happen upon a large sum of money, I will definitely send it his way.

I would like to thank John Tate and Joseph Siverman for writing a book that really simplified elliptic curves. Their ability to bring an advanced topic down to an undergraduate level really shows their mastery of the topic. Without their book, I really wouldn't have had an entry point to this topic.

I would like to thank all of the exceptional people I met throughout the program, my study budies Jeff, Joe, Leonard, Matt and Stephanie. Our talks usually led to solutions, and if they didn't it was comforting to have someone to be lost with. I would really like to thank Joe for pushing me to be better. I have so much admiration for him. I would also like to thank Stephanie for teaching me so much. I went into this program hoping to get a master's degree, but I came out with something better, her friendship.

Finally, I would like to thank my husband. He never once harrassed me for taking way too long to complete this program. He believed in me even when I didn't believe in me.

Table of Contents

Abstract **iii**

Acknowledgements **iv**

List of Figures **vi**

1 Quadratic Polynomials **1**
1.1 Review of the Projective Plane 1
1.2 Rational Points on Quadratic Polynomials 5
1.3 Rational Points on Cubic Polynomials 16
1.4 Formulas for the Group Law 26
1.5 Properties of Points of Finite Order 28

2 Curves of the Form $y^2 = x^3 + ax^2 + bx + c$ **34**
2.1 Mordell's Theorem 34
2.2 Some Useful Homomorphisms 35
2.3 Modules and Exact Sequences 43
2.4 The Rank of $E(\mathbb{Q})$ 49

3 Curves of the Form $y^2 = x^3 + c$ **58**
3.1 Homomorphisms for the New Curve 58
3.2 A New Formula for Rank 72

4 Conclusion **78**

Bibliography **79**

List of Figures

1.1 Two Distinct Lines Intersecting at Two Points 4
1.2 Theorem 1.2.1 6
1.3 Rational Points on the Unit Circle 7
1.4 The Composition of Two Distinct Points on a Cubic 17
1.5 The Composition of Two Non-Distinct Points on a Cubic 17
1.6 Identity For a Single Point Under $*$ 18
1.7 The Group Operation $\oplus$ 19
1.8 Verification of $\mathcal{O}$ as the Identity Element 21
1.9 The Inverse of P 22
1.10 Investigating Associativity 22
1.11 A Singularity For Which $f(x)$ Has a Double Root, Forming a Node 24
1.12 A Singularity For Which $f(x)$ Has a Triple Root, Forming a Cusp 24
1.13 Projecting P Onto $x = 1$ 25
1.14 $f(x)$ with Three Real Roots 30
1.15 $f(x)$ with One Real Root 30
1.16 Finding $2P$ 32
1.17 The Collision of P and $-2P$ 32

Chapter 1

Quadratic Polynomials

1.1 Review of the Projective Plane

A major focus of this paper is the group of rational points on an elliptic curve. These elliptic curves will be embedded in the projective plane. Hence a brief review of the projective plane will be given. We will give two different descriptions of the projective plane, one algebraic and one geometric, since it will be useful in certain situations to think of one way over the other.

Algebraic Definition of the Projective Plane

Consider the Fermat equation

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

with rational solutions. Let $x = \frac{a}{c}$ and $y = \frac{b}{d}$ be solutions such that the fractions are in lowest terms and the denominators are positive. If we substitute the solutions into (1.1) and clear the denominators, we have

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

Now it is clear that $c^N \mid a^N d^N$. Since $\frac{a}{c}$ is in lowest terms, a and c are relatively prime. Thus $c^N \mid d^N$, implying $c \mid d$. By a similar argument, we can conclude that $d \mid c$. Thus $c = \pm d$. Recall that we are given that the denominators of $\frac{a}{c}$ and $\frac{b}{d}$ are positive. There-

fore, $c = d$.

Any rational solution to (1.1) has the form $\left(\frac{a}{c}, \frac{b}{c}\right)$ and will have (a, b, c) as a corresponding integer solution to

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

Notice that as long as $c \neq 0$, the converse is true as well. That is, any integer solution (a, b, c) to (1.2) will also have the corresponding rational solution $\left(\frac{a}{c}, \frac{b}{c}\right)$ to (1.1). In fact, any triple $(\lambda a, \lambda b, \lambda c)$ for $\lambda \neq 0$ will satisfy (1.2) and will correspond to $\left(\frac{a}{c}, \frac{b}{c}\right)$ as a solution for (1.1).

Let's proceed to lay the foundation of the projective plane and see how it earned its name. Imagine that the origin in $\mathbb{R}^3$ is an eye, and that there is a screen (or a plane) in $\mathbb{R}^3$. Each point on the plane is in one-to-one correspondence with a line passing through the point and the eye. We will use this line to describe *projective points*.

Definition 1.1.1. A *projective point* is a line in $\mathbb{R}^3$ that passes through the origin of $\mathbb{R}^3$.

Notice that we only need one point in $\mathbb{R}^3$ besides the origin to describe a line in $\mathbb{R}^3$, and this point is not unique. For example, the line in $\mathbb{R}^3$ passing through the origin and $(1, 2, 3)$ is the same line that passes through the origin and $(2, 4, 6)$. This leads us to the following definition.

Definition 1.1.2. The *projective plane* is the set of triples $[a, b, c]$, with a, b and c not all zero, such that two triples $[a, b, c]$ and $[a', b', c']$ are considered to be the same point if there is a non-zero λ such that $a = \lambda a'$, $b = \lambda b'$ and $c = \lambda c'$. The numbers a, b and c are called *homogeneous coordinates* for the point $[a, b, c]$.

We will denote the projective plane $\mathbb{P}^2$. Brackets will always describe a projective point, while parentheses will describe a point in $\mathbb{R}^3$.

An *algebraic curve* in the affine plane $\mathbb{A}^2$ is defined to be the set of solutions to a polynomial equation in two variables, $f(x, y) = 0$. Fermat equation (1.1) is an example of such a curve. Curves in $\mathbb{P}^2$ will be given by polynomials in three variables, $F(X, Y, Z)$ such that if $F(a, b, c) = 0$, then $F(\lambda a, \lambda b, \lambda c) = 0$ for all λ.

Definition 1.1.3. A polynomial $F(X, Y, Z)$ is a *homogeneous polynomial of degree d* if it satisfies the identity

$$F(\lambda X, \lambda Y, \lambda Z) = \lambda^d F(X, Y, Z).$$

A *projective curve* C in $\mathbb{P}^2$ is the set of solutions to a non-constant homogeneous polynomial.

Now, if we look back at the homogeneous polynomial given by Fermat equation (1.2), we can see that there are some problematic homogeneous coordinates we need to deal with. For example, $[0, 0, 0]$ is a solution to (1.2), but it has no corresponding rational point $\left(\frac{a}{c}, \frac{b}{c}\right)$. We will consider $[0, 0, 0]$ as trivial and will discard it. Notice, $[0, 0, 0]$ is not defined in Definition 1.1.2. We need a point distinct from $[0, 0, 0]$ to define a projective point. Also, if N is odd, then $[1, -1, 0]$ and $[-1, 1, 0]$ are nontrivial solutions to (1.2) that do not correspond to any rational solutions to (1.1), at least not when using the conventional method.

Consider the sequence of solutions $[a_i, b_i, c_i]$ to (1.2) where $[a_i, b_i, c_i] \to [1, -1, 0]$ as $i \to \infty$ and a_i, b_i and c_i are allowed to be real numbers. The corresponding solutions to (1.1) approach (∞, ∞). Thus we will have to extend the affine plane $\mathbb{A}^2$ to include "points at infinity," so that the homogeneous coordinates $[1, -1, 0]$ and $[-1, 1, 0]$ correspond to these points. This brings us to our second definition of the projective plane.

Geometric Derivation of the Projective Plane

Before we begin developing the projective plane geometrically, we must define what a line is in $\mathbb{P}^2$.

Definition 1.1.4. A *projective line* is a plane in $\mathbb{R}^3$ that passes through the origin.

Since a projective line is really a plane in $\mathbb{R}^3$, a line can be thought of as the set of points $[a, b, c] \in \mathbb{P}^2$ whose coordinates satisfy an equation of the form

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

for some constants α, β and γ not all zero.

Any beginning course in Euclidean geometry will include the following postulates:

(i) Two distinct points determine a unique line.

(ii) If two distinct lines intersect, then they intersect in exactly one point.

In the projective plane, we are going to add *points at infinity* so that parallel lines intersect. Then there will be no distinction between parallel and non-parallel lines. Now the question remains as to how many points at infinity we should add. What if we add one point at infinity, say P? Consider two sets of parallel lines such that $\ell_1 \parallel \ell_2$ and $\ell_3 \parallel \ell_4$, as depicted in Figure 1.1. Then ℓ_1 and ℓ_2 intersect at P, and ℓ_3 and ℓ_4 intersect at P as well. Hence, all four lines intersect at P. This creates a problem since we are trying to construct the projective plane so that postulates (i) and (ii) still hold. Property (ii) does not hold since, for example, ℓ_1 and ℓ_4 intersect at A and P.

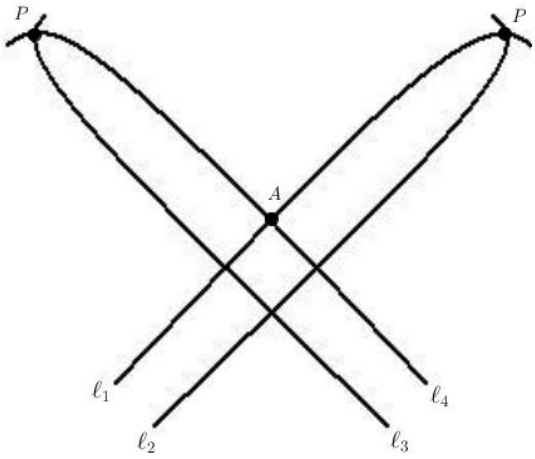


Figure 1.1: Two Distinct Lines Intersecting at Two Points

For this reason, we add points at infinity for each direction (slope), so that each line in $\mathbb{P}^2$ consists of a line in $\mathbb{A}^2$ together with a point at infinity corresponding to the line's direction. Two lines have the same direction if and only if they are parallel. This leads us to our geometric definition of the projective plane.

Definition 1.1.5. The *projective plane*

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

where the extra points in $\mathbb{P}^2$ associated to directions, that is the points in $\mathbb{P}^2$ that are not in $\mathbb{A}^2$, are called *points at infinity*, and the set of points at infinity is considered to be a line L_∞ whose intersection with any other line L is the point at infinity corresponding to the direction of L.

1.2 Rational Points on Quadratic Polynomials

Now that we have defined the projective plane, we are ready to look at some Diophantine equations and lay the foundations for the group we are going to investigate. In order to better study our group and its operation, let's start by considering the rational points that satisfy simpler polynomials that we are familiar with. We will start with quadratic polynomials, or conics, since much is known about their behavior.

Recall that a line of the form $ax + by + c = 0$ is a *rational line* if a, b and c are all rational, and a point (x, y) is a *rational point* if both its coordinates are rational numbers. If a line is drawn through two rational points, then the line will be a rational line. We can see this is true by using the point-slope formula to derive the equation of the line that passes through the given points. Since $\mathbb{Q}$ is field, all of the operations used to simplify the point-slope equation will result in rational coefficients. Also, if two rational lines intersect, their intersection is a rational point. All of the operations used to solve the system would again be closed since $\mathbb{Q}$ is a field.

When will the intersection points of a rational line with a rational conic be

rational? Upon solving the system, the resulting x-coordinates would be solutions to a quadratic equation with rational coefficients. So the points of intersection of the rational line with the rational conic will be rational if the solutions to the quadratic equation are rational. It is important to note for future reference that if one point of intersection is rational, then the other is as well. If one of the points of intersection is irrational, then the other is as well since it is its conjugate.

We might question next if we could find all of the rational points on a rational conic. To start, assume we know one rational point $\mathcal{O}$ on the given conic. We can draw a rational line ℓ_1 and project the conic onto ℓ_1 from $\mathcal{O}$. Every line connecting $\mathcal{O}$ to ℓ_1 will intersect the conic at another point. We will consider the line tangent at $\mathcal{O}$ as intersecting the conic at $\mathcal{O}$ twice. This gives a one-to-one correspondence between any point on the conic and its corresponding point on ℓ_1.

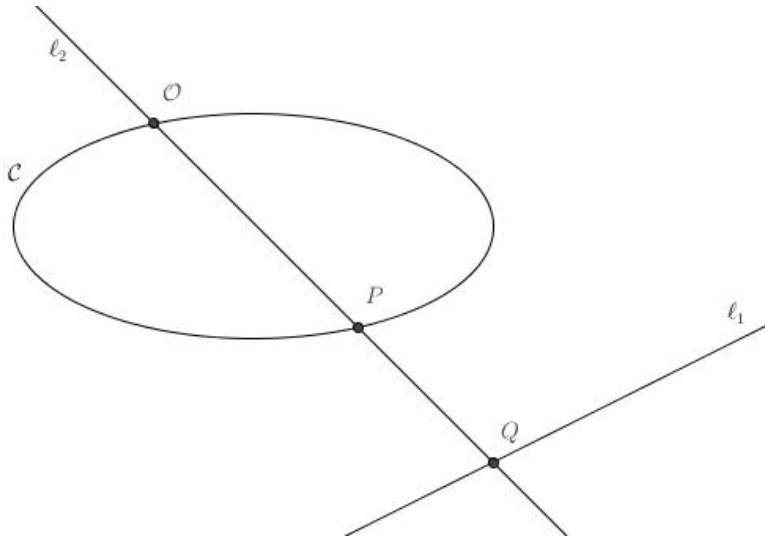


Figure 1.2: Theorem 1.2.1

Theorem 1.2.1. *Let 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.*

Proof. If P is rational, then there are two rational points on ℓ_2, making it a rational line. We are given that ℓ_1 is a rational line. We showed earlier that the intersection of two rational lines is a rational point. Therefore, Q is a rational point.

Conversely, if Q is rational, then there are two rational points on ℓ_2, so again it is a rational line. We saw earlier that the intersection of a rational line with a conic could produce rational or irrational solutions to a quadratic, but if we knew that one solution was rational, the other was as well. Since we know that $\mathcal{O}$ is rational, we have that P is rational. □

Example 1.2.1. Find all of the rational points on $x^2 + y^2 = 1$.

Solution. Using the logic from above, let's find the proper choice for our rational point and rational line. A good choice for the rational line is the y-axis. Let's use $(-1, 0)$ as the rational point on the circle. Then the equation of any line ℓ through $(-1, 0)$ is $y = t(1 + x)$, where t is the y-intercept.

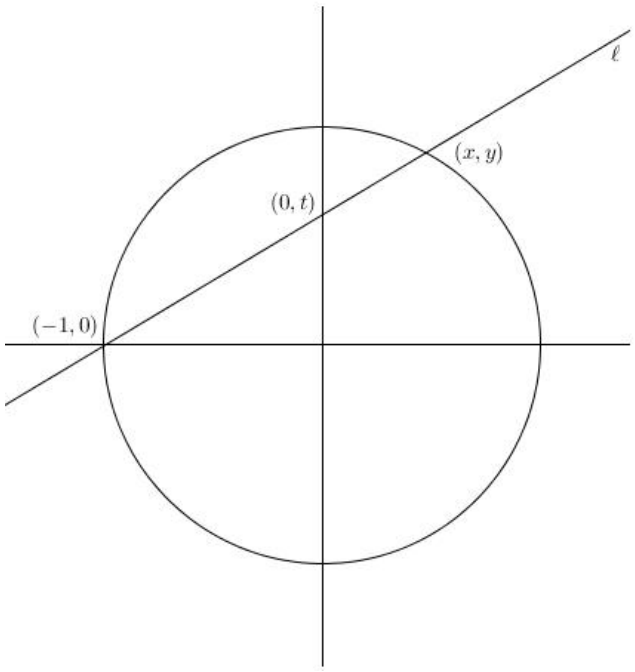


Figure 1.3: Rational Points on the Unit Circle

To find all of the rational points (x, y) on the circle, we need to find the intersection of ℓ and the circle. From the circle, we have $y^2 = 1 - x^2$. From the line, we have $y^2 = t^2(1 + x)^2$. So $1 - x^2 = t^2(1 + x)^2$. We already know $(-1, 0)$ is both on the circle and line, so $x = -1$ is obvioulsy a root of this equation. For $x \neq -1$,

$$\begin{aligned} 1 - x^2 &= t^2(1 + x)^2 \\ (1 + x)(1 - x) &= t^2(1 + x)^2 \\ 1 - x &= t^2(1 + x). \end{aligned}$$

Solving for x in terms of t, we have

$$\begin{aligned} 1 - t^2 &= t^2x + x \\ x &= \frac{1 - t^2}{1 + t^2}. \end{aligned}$$

Substituting this result into $y = t(1 + x)$ gives us

$$\begin{aligned} y &= t\left(1 + \frac{1 - t^2}{1 + t^2}\right) \\ y &= \frac{2t}{1 + t^2}. \end{aligned}$$

Thus, for any $t \in \mathbb{Q}$, the map $t \to \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$ will allow us to find all rational points on the unit circle except for $(-1, 0)$, which we get if we let $t \to \infty$. On the other hand, from $y = t(1 + x)$, we have that the map $(x, y) \to \frac{y}{1+x}$ will map any rational point (x, y) on the unit circle, aside from $(-1, 0)$, to the set of rational points $\mathbb{Q}$. The point $(-1, 0)$ would of course map to the point at infinity. To sum up, there is a one-to-one correspondence between the set of rational points on the unit circle $x^2 + y^2 = 1$ and the set $\mathbb{Q}$ of rational points by given by the maps above. □

The formulas derived above also play an integral role in finding formulas to describe the lengths of the sides of all primitive right triangles.

Definition 1.2.1. A *Pythagorean triple* is a set of positive integers, a, b and c, written as (a, b, c), such that $a^2 + b^2 = c^2$.

If (a, b, c) is a Pythagorean triple, then so is (ka, kb, kc) for any positive integer k.

Definition 1.2.2. We say that a Pythagorean triple is *primitive* if a, b and c are coprime, that is, $\gcd(a, b, c) = 1$.

The following two lemmas will be useful in the derivation of formulas that describe all primitive Pythagorean triples.

Lemma 1.2.2. *If (a, b, c) is a primitive Pythagorean triple, then a and b have opposite parity.*

Proof. Since (a, b, c) is a primitive Pythagorean triple, $a^2 + b^2 = c^2$ and $\gcd(a, b, c) = 1$. If a and b were both even, then their squares would be even. The sum of two even numbers is again even. Then c^2 is even, from which it follows that c is even. Thus, 2 divides a, b and c. This contradicts the fact that $\gcd(a, b, c) = 1$.

If a and b were both odd, then their squares would be odd. Perfect squares are congruent to either 0 or 1 modulo 4 depending on if they are even or odd, respectively. Then $a^2 \equiv b^2 \equiv 1 \pmod 4$, implying that $a^2 + b^2 \equiv 2 \pmod 4$. On the other hand, $c^2 \equiv 0$ or $1 \pmod 4$. This contradicts the fact that $a^2 + b^2 = c^2$. Hence, a and b cannot both be odd either. Therefore, a and b have opposite parity. □

Lemma 1.2.3. *A Pythagorean triple (a, b, c) is primitive if and only if any two of a, b and c are relatively prime.*

Proof. Let (a, b, c) be a primitive Pythagorean triple, that is, $a^2 + b^2 = c^2$ and $\gcd(a, b, c) = 1$. If any two of a, b and c were to have a common factor, then that factor would divide the sum or difference of their squares, and consequently, the remaining number of a, b and c. This contradicts the given that $\gcd(a, b, c) = 1$. Thus, any two of a, b and c are relatively prime.

Conversely, assume that for the Pythagorean triple (a, b, c) any two of a, b and c are relatively prime. If any two of a, b and c do not share a common factor, then it is clear that all three do not have a common factor. Thus, the Pythagorean triple (a, b, c) is primitive. □

Example 1.2.2. Derive formulas to describe all primitive Pythagorean triples.

Solution. Let's find integers X, Y, and Z such that $X^2+Y^2 = Z^2$. Assume $\gcd(X, Y, Z) = 1$ so that we have a primitive right triangle. By Lemma 1.2.2, X and Y have opposite parity. Suppose X is odd and Y is even and dehomogenize $X^2 + Y^2 = Z^2$, so that $x^2 + y^2 = 1$ where $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$. Then (x, y) is a rational point on the unit circle. From Example 1.1, we know that

$$x = \frac{1 - t^2}{1 + t^2} \quad \text{and} \quad y = \frac{2t}{1 + t^2}.$$

Letting $t = \frac{m}{n}$ for m and n relatively prime, the formulas above simplify to

$$\frac{X}{Z} = x = \frac{n^2 - m^2}{n^2 + m^2} \quad \text{and} \quad \frac{Y}{Z} = y = \frac{2mn}{n^2 + m^2}.$$

By Lemma 1.2.3, X and Z are relatively prime, as well as Y and Z. Thus, there exists a positive integer k such that $kX = n^2 - m^2$, $kY = 2nm$, and $kZ = n^2 + m^2$. Let's show that $k = 1$. Since $kX = n^2 - m^2$ and $kZ = n^2 + m^2$, it follows that $k \mid n^2 - m^2$ and $k \mid n^2 + m^2$. Thus k divides any linear combination of $n^2 - m^2$ and $n^2 + m^2$, in particular, $k \mid 2n^2$ and $k \mid 2m^2$. So $k \mid \gcd(2n^2, 2m^2) = 2\gcd(n^2, m^2)$. Since we assumed $\gcd(n, m) = 1$, it follows that $\gcd(n^2, m^2) = 1$. Thus $k \mid 2$. So either $k = 1$ or $k = 2$. If $k = 2$, then $n^2 - m^2$ is even, implying that n and m have the same parity. If n and m are both odd or both even, then $n^2 - m^2 \equiv 0 \pmod 4$ using the logic from the proof of Lemma 1.2.2. However, since X is odd, $2X \equiv 2 \pmod 4$, which reaches a contradiction. Hence, we have $k = 1$. Therefore, in order to find the side lengths X, Y and Z of any primitive right triangle, you can substitute any relatively prime integers m and n into

$$X = n^2 - m^2, \quad Y = 2mn, \quad \text{and} \quad Z = n^2 + m^2.$$

□

The findings above lead us to the theorem that follows. We used a geometric approach to develop the formulas above. Now we will take an algebraic approach to prove the theorem below.

Theorem 1.2.4. *If (a, b, c) is a primitive Pythagorean triple (with b even), then*

$$a = n^2 - m^2, \quad b = 2nm, \quad \textit{and} \quad c = n^2 + m^2$$

where n and m are positive integers with $n > m$, gcd$(n, m) = 1$ and n and m have opposite parity. Conversely, for n and m as above, (a, b, c) yields a primitive Pythagorean triple.

Proof. Let (a, b, c) be a primitive Pythagorean triple with b even. Then $a^2 + b^2 = c^2$, or equivalently, $b^2 = c^2 - a^2$. Since b is even, b^2 is even. From which it follows that $c^2 - a^2$ is even. From Lemma 1.2, we know that a and b have opposite parity, so a must be odd. If a is odd, then a^2 is odd. Hence, c^2 must be odd as well in order for $c^2 - a^2$ to even. So we have that both a and c are odd. Then we can conclude that $c+a$ and $c-a$ are even.

Let $\gcd(c + a, c - a) = d$. Then $d \mid c + a$ and $d \mid c - a$. Thus, d divides any linear combination of $c + a$ and $c - a$, in particular, $d \mid 2a$ and $d \mid 2c$. It follows that $d \mid \gcd(2a, 2c) = 2\gcd(a, c)$. Given that (a, b, c) is a primitive Pythagorean triple, by Lemma 1.2.3, a and c are relatively prime. Hence, $d \mid 2$. So $\gcd(c + a, c - a)$ is either 1 or 2. We showed above that $c + a$ and $c - a$ are both even, so it must be the case that $\gcd(c + a, c - a) = 2$. Thus, $\gcd(\frac{c+a}{2}, \frac{c-a}{2}) = 1$.

Since $\frac{b^2}{4} = \left(\frac{c+a}{2}\right)\left(\frac{c-a}{2}\right)$ and $\frac{c+a}{2}$ and $\frac{c-a}{2}$ are relatively prime, $\frac{c+a}{2}$ and $\frac{c-a}{2}$ must be perfect squares. Let $\frac{c+a}{2} = n^2$ and $\frac{c-a}{2} = m^2$. Then $n^2 - m^2 = \frac{c+a}{2} - \frac{c-a}{2} = a$. Also, $2mn = 2\sqrt{\frac{c-a}{2}}\sqrt{\frac{c+a}{2}} = 2\sqrt{\frac{c^2-a^2}{4}} = \sqrt{c^2 - a^2} = \sqrt{b^2} = b$. Finally, $n^2 + m^2 = \frac{c+a}{2} + \frac{c-a}{2} = c$.

Now if $m, n > 0$, then $n > m$ since $a = n^2 - m^2$, and a side of a triangle can only have positive length. Additionally, $\gcd(n, m) = 1$. For if n and m shared a common

factor, any two of a, b and c would not be relatively prime, contradicting Lemma 1.2.2. From Lemma 1.2.3, since b is even, a and c are odd. Since $n^2 - m^2 = a$ and $n^2 + m^2 = c$, it follows that n and m must have opposite parity if the sum and difference of the their squares is to be odd.

Conversely, assume that m and n are positive integers such that $n > m$, $\gcd(n, m) = 1$, n and m have opposite parity and $a = n^2 - m^2$, $b = 2nm$, and $c = n^2 + m^2$. Then,

$$\begin{aligned} a^2 + b^2 &= (n^2 - m^2)^2 + (2nm)^2 \\ &= n^4 - 2n^2m^2 + m^4 + 4n^2m^2 \\ &= n^4 + 2n^2m^2 + 2m^4 \\ &= (n^2 + m^2)^2 \\ &= c^2. \end{aligned}$$

Also, we are given that $\gcd(n, m) = 1$, which implies that $\gcd(n^2, m^2) = 1$. Then $\gcd(n^2 - m^2, n^2 + m^2)$ is either 1 or 2 by the same argument above. Since n and m have opposite parity, n^2 and m^2 have opposite parity as well. Thus, their sum and difference would both be odd, giving us $\gcd(n^2 - m^2, n^2 + m^2) = 1$. Therefore, (a, b, c) is primitive by Lemma 1.2.3. □

Example 1.2.3. Find all primitive integral right triangles whose hypotenuse has length less than 30.

Solution. If the hypotenuse is to have length less than 30, then we need n^2 and m^2 such that $n^2 + m^2 < 30$. The only numbers less than 30 that are the squares of integers are 1, 4, 9, 16 and 25. The table below shows all of the possible sums of these numbers that are less than 30.

n^2+m^2	n	m
1+1=2	1	1
4+1=5	2	1
4+4=8	2	2
9+1=10	3	1
9+4=13	3	2
9+9=18	3	3
16+1=17	4	1
16+4=20	4	2
16+9=25	4	3
25+1=26	5	1
25+4=29	5	2

We know from Theorem 1.2.4 that $n > m$, $\gcd(n, m) = 1$, and n and m have opposite parity. Thus we can eliminate the following (n, m): $(1, 1)$, $(2, 2)$, $(3, 1)$, $(3, 3)$, $(4, 2)$, and $(5, 1)$. Using the formulas from Theorem 1.2.4 with the remaining (n, m), we have the following table describing the possible side lengths.

n	m	n^2-m^2	$2mn$	n^2+m^2
2	1	3	4	5
3	2	5	12	13
4	1	15	8	17
4	3	7	24	25
5	2	21	20	29

Thus, the triples $(3, 4, 5)$, $(5, 12, 13)$, $(8, 15, 17)$, $(7, 24, 25)$ and $(20, 21, 29)$ describe all primitive integral right triangles whose hypotenuse has length less than 30. □

Example 1.2.4. Are there any rational points on the ellipse $3x^2 + 4y^2 = 5$?

Solution. Let $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$ so that in homogenized form we have $3X^2+4Y^2 = 5Z^2$ with X, Y and Z having no common factors. If X, Y, and Z had a common factor, we could remove it. If this equation has solutions in the integers, then $3x^2 + 4y^2 = 5$ would have rational solutions.

We start by showing that 3 cannot divide Y or Z. If $3 \mid Y$, then $3 \mid 3X^2 + 4Y^2$ which implies that $3 \mid 5Z^2$. Then $3 \mid Z$, from which it follows that $9 \mid 5Z^2 - 4Y^2$ or equivalently $9 \mid 3X^2$. So we have that $3 \mid X$. This contradicts that fact that X, Y and Z have no common factors. A similar argument will hold if we assume that $3 \mid Z$. So 3 cannot divide Y or Z.

We know that $3X^2 \equiv 0 \pmod 3$, but is $5Z^2 - 4Y^2 \equiv 0 \pmod 3$? We have only a finite number of cases to check since $\mathbb{Z}_3 = \{0, 1, 2\} = \{0, \pm 1\}$. Also, we showed earlier that 3 cannot divide Y or Z, eliminating 0 from our choices. If Y or Z were ± 1, then Y^2 and Z^2 would be equivalent to 1 (mod 3). Since $4(1) - 3(1) = 1 \not\equiv 0 \pmod 5$, we have that $4Z^2 - 3Y^2 \not\equiv 5Y^2 \pmod 5$. Thus, there are no integers X, Y and Z such that $3X^2 + 5Y^2 = 4Z^2$, from which we can conclude that there are no rational numbers x and y such that $3x^2 + 5y^2 = 4$. □

Example 1.2.5. Does the conic $3x^2 + 4y^2 + 6x + 12y + 7 = 0$ contain any rational points?

Solution. The following simplications will take the conic from general form to transformational form:

$$\begin{aligned} 3x^2 + 4y^2 + 6x + 12y + 7 &= 0 \\ 3x^2 + 6x + 4y^2 + 12y &= -7 \\ 3\left(x^2 + 2x + 1\right) + 4\left(y^2 + 3y + \frac{9}{4}\right) &= 5 \\ 3\left(x + 1\right)^2 + 4\left(y + \frac{3}{2}\right)^2 &= 5 \\ 3a^2 + 4b^2 &= 5 \end{aligned}$$

where $a = x + 1$ and $b = y + \frac{3}{2}$. Now the problem is equivalent to Example 1.2.4. Hence, there are no rational points on the given conic. □

Note that any conic can be transformed into a quadratic of the form above. The conic from Example 1.2.5 was missing an xy term, but recall that if there is an xy term, the conic is no longer parallel to the x- or y-axis. A simple application of the formulas

$tan2\theta = \frac{B}{A-C}$, $x = x'cos\theta - y'sin\theta$ and $y = x'sin\theta + y'cos\theta$ for a conic of the form $Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0$ will rotate the conic so that it is parallel to the x- or y-axis and eliminate the xy term.

Example 1.2.6. Are there any rational points on the ellipse $3x^2 + 6y^2 = 4$?

Solution. It might come as a surprise because this equation seems so similar to the one presented in the previous example, but there are rational points that satisfy $3x^2+6y^2 = 4$, such as $(\frac{2}{3}, \frac{2}{3})$. □

Any beginning Abstract Algebra course discusses solving polynomial equations with integer coefficients by reducing the coefficients modulo p. If the polynomial equation has no solutions in $\mathbb{Z}/p\mathbb{Z}$, then it has no solutions in $\mathbb{Z}$. This is an example of looking at a polynomial "locally" to make claims about it "globally." We have a powerful existence theorem that allows us to know whether any quadratic form has solutions.

Definition 1.2.3. Let K be a field. A *quadratic form* over K is a degree-two polynomial in n variables of the form

$$f(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j$$

with each $a_{ij} \in K$.

The question as to the existence of rational points on a given quadratic form is answered nicely by the Hasse-Minkowski Local-to-Global Principle.

Theorem 1.2.5 (Hasse-Minkowski)**.** *A homogeneous quadratic form is solvable by integers, not all zero, if and only if it is solvable in* $\mathbb{R}$ *and* $\mathbb{Q}_p$ *for each prime* p.

Here, the field of p-adic numbers, denoted $\mathbb{Q}_p$, helps us determine the existence of zeros to any given quadratic form. The reader may consult Jeffrey Hatley's paper, Hasse-Minkowski and the Local-to-Global Principle for a great introduction to p-adic

numbers, a proof of Theorem 1.2.5 and an example of how the theorem is used [Hat09]. For the intention of this paper, it is enough to note that for every quadratic form over $\mathbb{Q}$, Theorem 1.2.5 tells us that the existence of a root in $\mathbb{Q}$ is equivalent to the existence of a root in each $\mathbb{Q}_p$ and in $\mathbb{R}$. If there is no root in some $\mathbb{Q}_p$ or in $\mathbb{R}$, then there is no root in $\mathbb{Q}$.

While the Hasse-Minkowski Local-to-Global Principle tells us all we need to know about the existence of rational solutions for a given conic, the theorem does not hold for cubics. Ernest Selmer showed that the equation

$$3x^3 + 4y^3 + 5z^3 = 0$$

has a solution in each $\mathbb{Q}_p$ and in $\mathbb{R}$ but not in $\mathbb{Q}$.

1.3 Rational Points on Cubic Polynomials

We have looked in detail at how to find the rational points on quadratic curves, but what methods are available to help us find rational roots for rational cubic curves? If we know two rational points on a rational cubic, then we can find a third. If we draw a line through the known rational points, say P and Q, then the third intersection of the line with the cubic, which we will call $P * Q$, will also be rational. This is true because the line will be a rational line since it has two rational points on it. We can find the intersection of the line with the cubic by substitution, which will yield a cubic with rational coefficients. If two of the roots of the cubic are rational, then the third is rational, otherwise not all of the coefficients of the cubic would be rational. Much of the work done in this chapter is an expansion of the work of contained in John Tate and Joseph Silverman's book, *Rational Points on Elliptic Curves* [ST92, pp. 9-99].

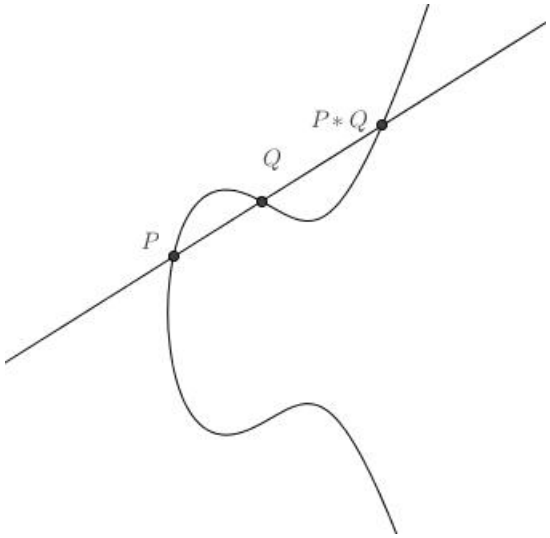


Figure 1.4: The Composition of Two Distinct Points on a Cubic

We can even obtain other rational points knowing only one rational point. If P is the rational point we know on the rational cubic, we can draw the tangent line at P, so that P is a double root of the cubic equation. Then the third root must also be rational.

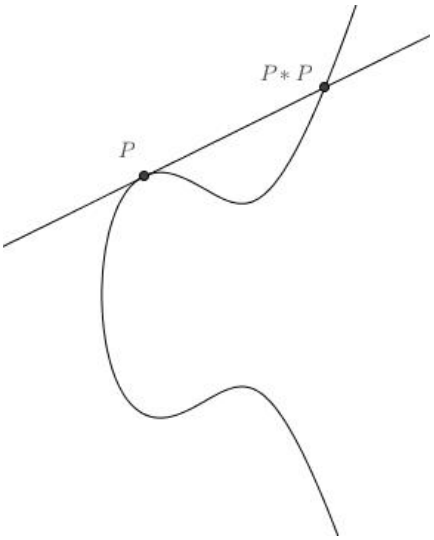


Figure 1.5: The Composition of Two Non-Distinct Points on a Cubic

Given any two rational points P and Q on a rational cubic curve, we have defined a composition law yielding a third point $P * Q$. Does the operation $*$ acting on the set of rational points on a given rational cubic curve form a group? It turns out that it

does not since there is no identity element. Sure, there exists a point Q on a given cubic curve such that $P * Q = P$. Simply draw the tangent to the curve at P and consider the line as intersecting the curve twice at P.

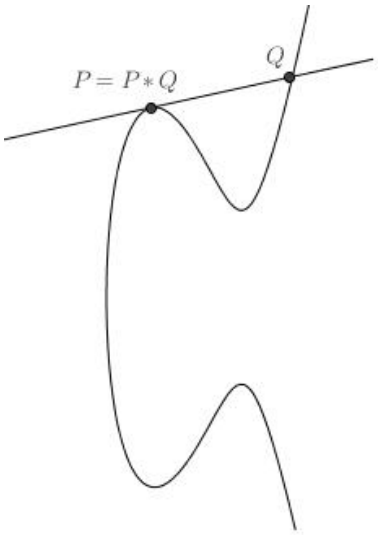


Figure 1.6: Identity For a Single Point Under $*$

However, in order for Q to be the identity element of the group, for all P' on the given cubic, it must be that $P' * Q = P'$, which is clearly not true. Despite its shortcomings as a group operation, the composition law $*$ is going to play a large role in the group operation we are going to define. Assume that we know one rational point on a given non-singular rational cubic curve. Call this point $\mathcal{O}$. Let $\oplus$ be defined as follows:

> For two rational points P and Q on a non-singular rational cubic curve, draw a line through $P * Q$ and $\mathcal{O}$. The third intersection point of this line with the curve will be $P \oplus Q$.

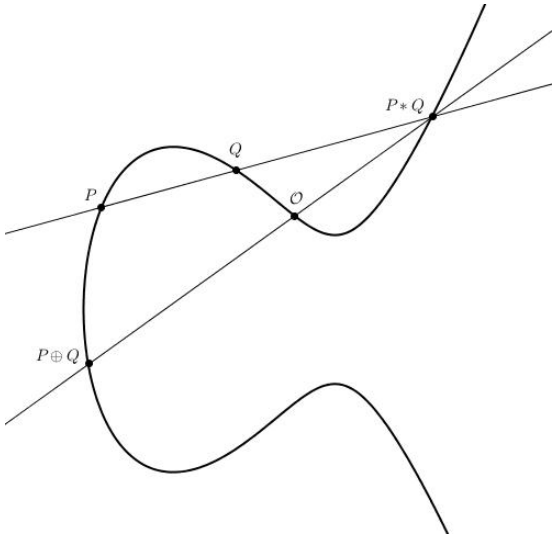


Figure 1.7: The Group Operation $\oplus$

Note that $P \oplus Q$ is equivalent to $\mathcal{O} * (P * Q)$.

We will be studying specific cubic curves in this paper. We will start by looking at cubics of the form $y^2 = x^3 + ax^2 + bx + c$. This form is called *Weierstrass normal form.* Using projective geometry, one can show that any cubic curve is birationally equivalent to a Weierstrass equation. The transformations used to put any cubic curve in Weierstrass form are a homomorphisms. That ensures that the structure of the group law described above will be preserved. So our study of the group of rational points on a non-singular rational cubic curve will be reduced to studying rational points on non-singular rational cubics in Weierstrass form.

For a cubic equation of the form $y^2 = f(x) = x^3 + ax^2 + bx + c$, if $f(x)$ has distinct roots, then the curve is called an *elliptic curve.* Let's rigorously define an elliptic curve since it is the basis for the group we will be studying in this paper.

Definition 1.3.1 (Elliptic Curve)**.** An *elliptic curve* is a nonsingular projective plane curve E over a field K of degree 3 together with a point $\mathcal{O} \in E(K)$ that serves as the identity.

We are going to study elliptic curves in Weierstrass normal form using a little projective geometry. Letting $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$, the homogeneous form of the Weierstrass curve is

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3.$$

To find the intersection of this curve with the line at infinity, we need to substitute $Z = 0$ into the equation above. This substitution gives the equation $X^3 = 0$. Thus $X = 0$ is a triple root and the cubic has only one point at infinity, the point at which all vertical lines meet.

We will let the point at infinity be the identity element $\mathcal{O}$ of our group, hence $\mathcal{O}$ is considered rational. So the points on our elliptic curve come from $\mathbb{A}^2 \cup \{\mathcal{O}\}$. Now every line will meet the given elliptic curve three times, which you may recall is necessary for the group operation. The line at infinity will meet the curve three times at $\mathcal{O}$. A vertical line will intersect the curve at two points in the ordinary affine xy-plane and once at $\mathcal{O}$. Any other line will intersect the curve three times in the xy-plane, if we allow our intersections to be complex points.

Given an elliptic curve E, we will denote the group of rational points on E together with $\mathcal{O}$ under the operation $\oplus$ as $E(\mathbb{Q})$. Let's discuss how $\oplus$ will work for this group.

Given two points P and Q on E in Weierstrass form, to find $P \oplus Q$, we start by drawing the line through P and Q. The third point of intersection is $P * Q$. Next, we draw the vertical line through $P*Q$ so that it intersects $\mathcal{O}$. The third point of intersection will be $P \oplus Q$. Since all elliptic curves are symmetric about the x-axis, you can also think about finding $P \oplus Q$ by reflecting $P * Q$ over the x-axis.

Now let's show that the operation $\oplus$ together with set of rational points on a given elliptic curve forms a group.

Theorem 1.3.1. *$E(\mathbb{Q})$, where E is a non-singular curve in the projective plane, forms an abelian group under $\oplus$ with the identity $\mathcal{O}$ being the point at infinity.*

Proof. Since $P * Q = Q * P$, it is clear that $P \oplus Q = Q \oplus P$. Thus $\oplus$ is a commutative operation. We showed earlier that if we have two rational points on a line, it is a rational line. We also showed that if a rational line intersects a rational cubic curve at two rational points, then the third intersection is rational as well. So if we start with points P and Q both rational, then $P * Q$ will be rational. Since $\mathcal{O}$ is rational as well, the line through $\mathcal{O}$ and $P * Q$ is a rational line. Hence $P \oplus Q$ is a rational point. Thus the the set of rational points on a rational cubic is closed under $\oplus$.

The point at infinity $\mathcal{O}$ is the identity element. To verify this, recall $P \oplus \mathcal{O}$ is equivalent to $\mathcal{O} * (P * \mathcal{O})$, and $P * \mathcal{O}$ is the third intersection point of the line through P and $\mathcal{O}$ with the curve. Thus the third point of intersection of the line through $P * \mathcal{O}$ and $\mathcal{O}$ is P. So $P \oplus \mathcal{O} = P$ and by commutativity, $\mathcal{O} \oplus P = P$ as well. Hence $\mathcal{O}$ is the identity element.

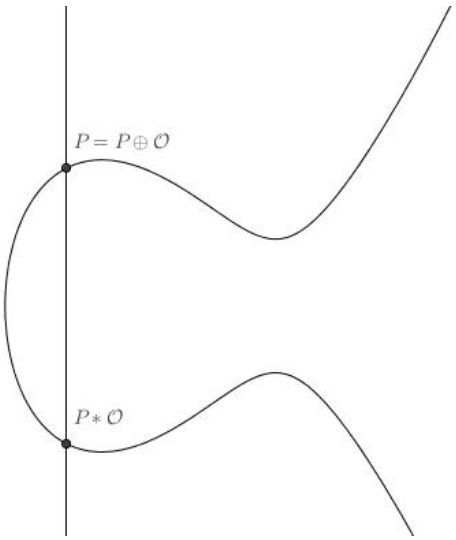


Figure 1.8: Verification of $\mathcal{O}$ as the Identity Element

The additive inverse of any point P will be $-P$ such that if $P = (x, y)$, then $-P = (x, -y)$. To verify this, we need to check that $P \oplus (-P) = \mathcal{O}$. If we connect P and $-P$, the vertical line's third point of intersection with E will be $\mathcal{O}$. Next we will connect $\mathcal{O}$ to $\mathcal{O}$, giving us the tangent line at $\mathcal{O}$ which we know intersects E three times at $\mathcal{O}$. Thus $P \oplus (-P) = (-P) \oplus P = \mathcal{O}$.

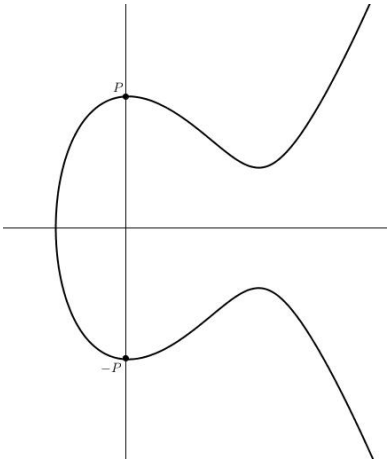


Figure 1.9: The Inverse of P

Showing that $\oplus$ is associative will take some work. First, let's verify it pictorally since it is not at all obvious that associativity holds. Let P, Q and R be rational points on a given rational cubic curve. We want to find $(P \oplus Q) \oplus R$ and $P \oplus (Q \oplus R)$.

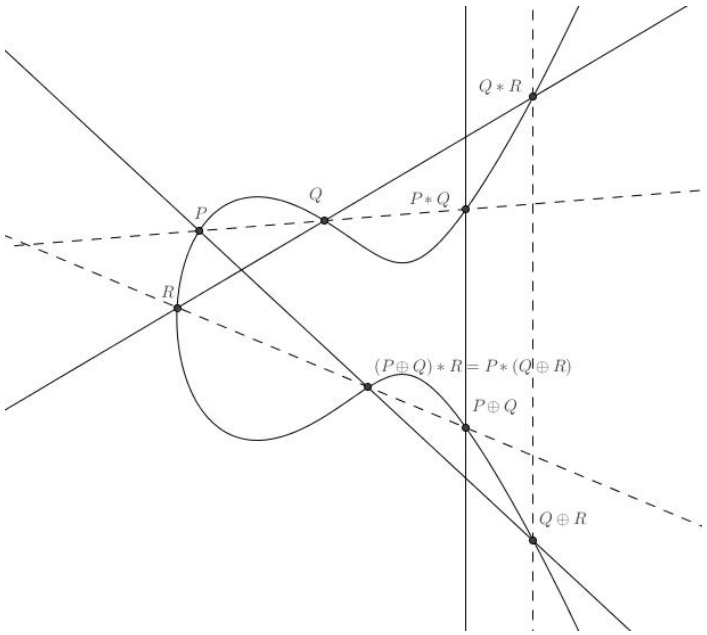


Figure 1.10: Investigating Associativity

It appears as though $(P \oplus Q) * R$ is the same point as $P * (Q \oplus R)$. If that is true, we are done. For if we adjoin that point to $\mathcal{O}$, the third intersection with the curve will be $(P \oplus Q) \oplus R$ and $P \oplus (Q \oplus R)$. So we will prove associativity by proving that $(P \oplus Q) * R = P * (Q \oplus R)$. In order to do this, we will need the following theorem.

Theorem 1.3.2 (Cayley-Bacharach [ST92, p. 240]). *Let C, C_1 and C_2 be three cubic curves. Suppose C goes through eight of the nine intersection points of C_1 and C_2. Then C goes through the ninth intersection point.*

We have nine points in the figure above–$\mathcal{O}$, P, Q, R, $P * Q$, $P \oplus Q$, $Q * R$, $Q \oplus R$, and the point at the intersection of ℓ_1 and ℓ_2, which we will prove lies on the curve C. A cubic equation can be formed by multiplying three linear equations. So let's create the cubic curve C_1 by multiplying the equations for the dashed lines and C_2 by multiplying the equations for the solid lines. Then the cubics C_1 and C_2 pass through the nine points listed above. We know that C passes through eight of those points, so by Theorem 1.6, it must pass through the ninth. Thus $(P \oplus Q) * R = P * (Q \oplus R)$, implying that $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$. So we have shown associativity. Therefore, the group of rational points on a non-singular rational cubic curve forms a commutative group under $\oplus$. □

Let's examine in detail the restriction that our cubic curves be non-singular. There are two types of singularities that can occur for an cubic curve in normal form depending on the if the point of singularity is a double or triple root of $f(x)$. The pictures for both cases are given in Figure 1.11 and Figure 1.12. For each figure, we have translated the point of singularity along the x-axis so that is at the origin. The Weierstrass form for each type of singularity after the translation is $y^2 = x^2(x+1)$ and $y^2 = x^3$, respectively.

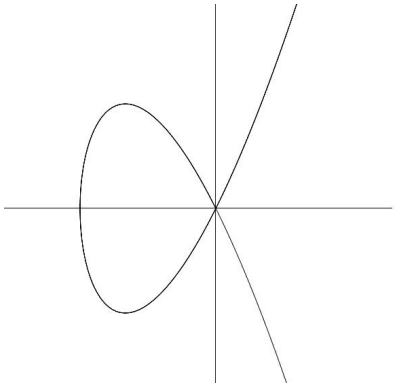


Figure 1.11: A Singularity For Which $f(x)$ Has a Double Root, Forming a Node

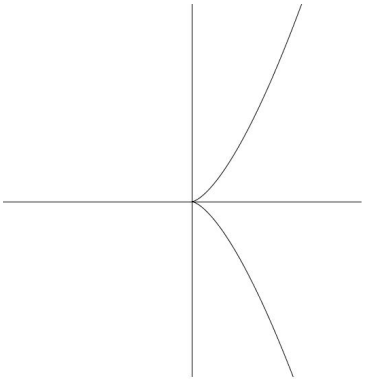


Figure 1.12: A Singularity For Which $f(x)$ Has a Triple Root, Forming a Cusp

One of the reasons that we have ruled out non-singular curves from our group is that we already know how to find rational points on them. If we project from the point of singularity onto a rational line, the line through the point of singularity will intersect the curve twice at the point of singularity and at one other point. So we get a one-to-one correspondence between any rational point on the cubic and a rational point on the rational line. Thus when we have singular points on our curve, we can mimick the strategy used in Example 1.2.1.

Let's start with the case for which the point of singularity is a double root of $f(x)$. For simplicity, let our rational line be $x = 1$. Since the lines of projection pass through the origin, they will have the form $y = mx$. Let S be the point of singularity and P be the point we are projecting onto $x = 1$.

We know that P lies on both the elliptic curve and the projection line, so to find P, we will substitute $y = mx$ into $y^2 = x^2(x + 1)$. For $x^2 \neq 0$, we have the following

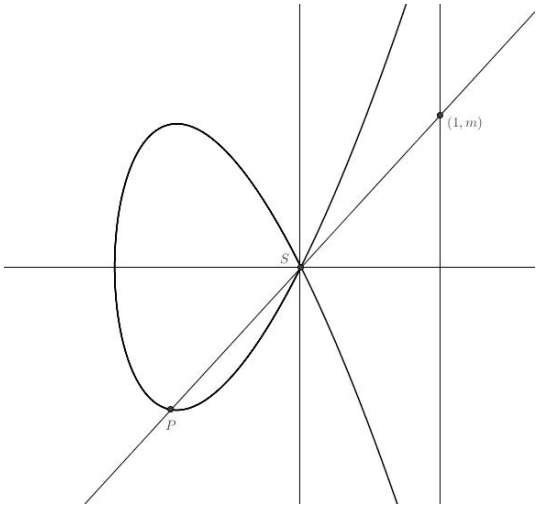


Figure 1.13: Projecting P Onto $x = 1$

simplifications:

$$\begin{aligned} y^2 &= x^2(x+1) \\ m^2x^2 &= x^2(x+1) \\ m^2 &= x+1 \\ x &= m^2-1. \end{aligned}$$

To find the y-coordinate of P, we can substitute $x = m^2 - 1$ into $y^2 = x^2(x+1)$:

$$\begin{aligned} y^2 &= x^2(x+1) \\ y^2 &= (m^2-1)^2 \cdot m^2 \\ y &= m^3 - m. \end{aligned}$$

Thus for any rational point (1, m) on our rational line, we have a corresponding rational point (m^2-1, m^3-m) on our elliptic curve. The choice of the rational line $x = 1$ was unnecessary since the coordinates of P depends only on the slope of the projection line, however, it was included here to mimick earlier strategies.

Similarly, for $y^2 = x^3$, the case of singularity for which $f(x)$ has a triple root, we have the formulas $x = n^2$ and $y = n^3$.

Thus, finding the rational points on a singular singular curve is trivial. Also, at the point of singularity, there is not a distinct tangent line, which makes our geometric discription of our operation $\oplus$ problematic. For these reasons, will only discuss elliptic (non-singular) curves.

1.4 Formulas for the Group Law

We have shown geometrically how to add points in our group. Now we will develop explicit formulas for adding two points. Let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ and $P * Q = (x_3, y_3)$. We learned above that $P \oplus Q$ must have coordinates $(x_3, -y_3)$. Also, let the line through P_1 and P_2 be $y = mx + v$ where $m = \frac{y_2 - y_1}{x_2 - x_1}$. To find $P * Q$, let's substitute $y = mx + v$ into $y^2 = x^3 + ax^2 + bx + c$:

$$\begin{aligned} y^2 &= x^3 + ax^2 + bx + c \\ (mx + v)^2 &= x^3 + ax^2 + bx + c \\ m^2x^2 + 2mvx + v^2 &= x^3 + ax^2 + bx + c \\ 0 &= x^3 + (a - m^2)x^2 + (b - 2mv)x + (c - v^2). \end{aligned}$$

We know that P_1, P_2, and $P_1 * P_2$ are roots of the equation above, implying that

$$\begin{aligned} & x^3 + (a - m^2)x^2 + (b - 2mv)x + (c - v^2) \\ = \; & (x - x_1)(x - x_2)(x - x_3) \\ = \; & x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3. \end{aligned}$$

Equating the coefficients of the x^2 term gives $m^2 - a = x_1 + x_2 + x_3$. Remember, our goal was to find $P_1 * P_2 = (x_3, y_3)$ given (x_1, y_1) and (x_2, y_2). We have that $x_3 = m^2 - a - x_1 - x_2$. Also, from $y = mx + v$, we have $y_3 = mx_3 + v$. Hence, if $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ and $y = mx + v$ is the line between them, then

$$P_1 \oplus P_2 = (x_3, -y_3) = \left(m^2 - a - x_1 - x_2, -(mx_3 + v)\right). \tag{1.3}$$

Our derivation of these formulas used the slope between the two given points.

We will have to alter our method slightly if the two given points are the same. If we want to find $P \oplus P$ or $2P$, where $P = (x, y)$, we will need the slope of the tangent line at P. From implicit differentiation on $y^2 = f(x) = x^3 + ax^2 + bx + c$ we have that

$$\begin{aligned} 2y\frac{dy}{dx} &= f'(x) \\ \frac{dy}{dx} &= \frac{f'(x)}{2y}. \end{aligned}$$

So the only changes necessary will be that $m = \frac{f'(x)}{2y}$. By substituting m into the formula for the x-coordinate of $P_1 \oplus P_2$ and letting x_1 and x_2 be the same value, x, we have a formula for the x-coordinate of $2P$.

$$\begin{aligned} m^2 - a - 2x &= \left(\frac{f'(x)}{2y}\right)^2 - a - 2x \\ &= \frac{(3x^2 + 2ax + b)^2}{4x^3 + 4ax^2 + 4bx + 4c} - a - 2x \\ &= \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}. \end{aligned}$$

We will denote the x-coordinate of $2P$ as $x(2P)$. Thus

$$x(2P) = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}. \tag{1.4}$$

We will refer to this formula as the *duplication formula*. Now let's find the y-coordinate for $2P$ or $y(2P)$. From (1.3), we know that the y-coordinate for $(x_1, y_1) \oplus (x_2, y_2)$ is $-(mx_3 + v)$ where x_3 was the resulting x-coordinate upon addition of the given points. Thus x_3 is given by (1.4). Also, $y = mx + v$ implies that $v = y - mx$. We also know that for $2P$, $m = \frac{f'(x)}{2y}$. Substituting m, v and x_3 into $-(mx_3 + v)$, we have

$$\begin{aligned} y(2P) &= -\tfrac{f'(x)}{2y}\left(\tfrac{x^4-2bx^2-8cx+b^2-4ac}{4x^3+4ax^2+4bx+4c}\right) - (y - mx) \\ &= -\tfrac{f'(x)\left(x^4-2bx^2-8cx+b^2-4ac\right)}{8y^3} - y + \tfrac{f'(x)x}{2y} \\ &= \tfrac{-f'(x)[(x^2-b)^2-8cx-4ac]-8y^4+4f'(x)xy^2}{8y^3} \\ &= \tfrac{x^6+2ax^5+5bx^4+20cx^3+(20ac-5b^2)x^2+(8a^2c-2ab^2-4bc)x+4abc-b^3-8c^2}{8y^3}. \end{aligned} \tag{1.5}$$

1.5 Properties of Points of Finite Order

We are going to examine some points of finite order since some properties of these points will be used in later proofs. Another advantage to looking at these points is that we will become more familiar with our group and some of its algebraic structure.

Definition 1.5.1. An element P of any group is said to have *order* m if

$$mP = \underbrace{P \oplus P \oplus \cdots \oplus P}_{m \text{ summands}} = \mathcal{O},$$

but $m'P \neq \mathcal{O}$ for all integers $1 \leq m' < m$. If such an m exists, then P has *finite order*; otherwise it has *infinite order*.

Let's prove the following proposition about points of order two and three.

Theorem 1.5.1 (Points of Order Two and Three)**.** *Let E be the non-singular cubic curve*

$$E\colon y^2 = f(x) = x^3 + ax^2 + bx + c.$$

[*Recall that E is non-singular provided $f(x)$ and $f'(x)$ have no common complex roots.*]

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

(b) *E has exactly four points of order dividing 2. These four points form a group which is a product of two cyclic groups of order two.*

(c) *A point $P = (x, y) \neq \mathcal{O}$ on E has order three if and only if x is a root of the polynomial*

$$\psi_3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + \left(4ac - b^2\right).$$

(d) *E has exactly nine points of order dividing 3. These nine points form a group which is a product of two cyclic groups of order three.*

Proof.

(a) Let $P = (x, y) \neq \mathcal{O}$ on E be a point of order two. Then $2P = \mathcal{O}$, or equivalently $P = -P$. If $(x, y) = (x, -y)$, then $y = 0$.

Suppose conversely that $P = (x, 0)$ is on E. From what we know about the shape of elliptic curves in Weierstrass form, there is a vertical tangent at P. This is supported by the fact that $\frac{dy}{dx} = \frac{3x^2+2ax+b}{2y}$ will result in division by zero for $P = (x, 0)$. To find $2P$, we draw the vertical tangent to the curve at P, giving us $P * P = \mathcal{O}$. Now we draw the line connecting $\mathcal{O}$ to $\mathcal{O}$, the line at infinity, which meets the cubic at the point $\mathcal{O}$ three times. Hence $2P = \mathcal{O}$.

(b) From above, we know that points of order two have the property $y = 0$. For $y^2 = f(x) = x^3 + ax^2 + bx + c$, the only way $y = 0$ is if $f(x) = 0$. Allowing for complex coordinates, since $f(x)$ is non-singular, it has three distinct roots, say P_1, P_2 and P_3. So there are three points of order two. The only other point on E with order dividing 2 is $\mathcal{O}$, the only point of order one. Thus E has exactly four points of order dividing 2, the set $\{\mathcal{O}, P_1, P_2, P_3\}$.

Now let's show that these four points form a group isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. The identity $\mathcal{O}$ is an element of the group. Every element is its own inverse. We can check for closure and that the group is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ by checking that for any points excluding the identity, the sum of any two points is the third point. It is clear that any element added to the identity will still be in the group. If we draw the line through P_1 and P_2, we have that $P_1 * P_2 = P_3$. If we draw the line through P_3 and $\mathcal{O}$ we get a vertical line whose third point of intersection is again P_3. Since the points are colinear, it is clear that if we chose to add any two of the points, we would get the third. Finally, associativity is inherited from the group. So the set above is a group isomorphic to the Klein group if we allow complex coordinates. If we allow only real coordinates, it is either isomorphic to the Klein group or a cyclic group of order two since we can have three or one real root as depicted in Figure 1.14 and Figure 1.15. If we allow only rational coordinates, our set is either isomorphic to the Klein group, a cyclic group of order two, or is the trivial group.

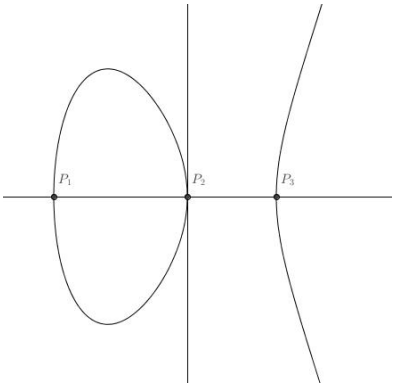


Figure 1.14: $f(x)$ with Three Real Roots

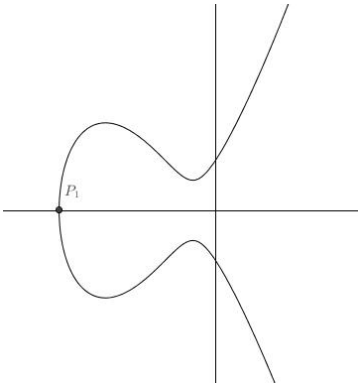


Figure 1.15: $f(x)$ with One Real Root

(c) Let $P = (x, y) \neq \mathcal{O}$ on E be a point of order three. Then $3P = \mathcal{O}$ or rather $2P = -P$. Setting the duplication formula equal to x, we have

$$\begin{aligned} \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c} &= x \\ x^4 - 2bx^2 - 8cx + b^2 - 4ac &= 4x^4 + 4ax^3 + 4bx^2 + 4cx \\ 3x^4 + 4ax^3 + 6bx^2 + 12cx + \left(4ac - b^2\right) &= 0. \end{aligned} \tag{1.6}$$

Thus x is a root of $\psi_3 = 3x^4 + 4ax^3 + 6bx^2 + 12cx + \left(4ac - b^2\right)$.

On the other hand, let $P = (x, y) \neq \mathcal{O}$ be a point on E such that $\psi_3(x) = 0$. Then following the sequence of equations above backwards, we have (1.6). That implies that $2P = P$ or $2P = -P$. If $2P = P$, then $P = \mathcal{O}$, which we have excluded. Thus $2P = -P$, implying that $3P = \mathcal{O}$. Therefore, P has order three.

(d) Recall from our derivation of the duplication formula that $x(2P) = \frac{f'(x)^2}{4f(x)} - a - 2x$.

If we set this equal to x, we have

$$\begin{aligned}
\frac{f'(x)^2}{4f(x)} - a - 2x &= x \\
\frac{f'(x)^2 - 4af(x) - 8xf(x)}{4f(x)} &= x \\
f'(x)^2 - 4af(x) - 8xf(x) &= 4xf(x) \\
12xf(x) + 4af(x) - f'(x)^2 &= 0 \\
2f(x)(6x + 2a) - f'(x)^2 &= 0.
\end{aligned}$$

From $f(x) = x^3 + ax^2 + bx + c$, it follows that $f''(x) = 6x + 2a$. So an alternate form for ψ_3 is

$$\psi_3 = 2f(x)f''(x) - f'(x)^2.$$

Since we are allowing complex coordinates and ψ_3 is of degree four, we have four solutions. To show that they are distinct, we need to show that $\psi_3(x)$ and $\psi_3'(x)$ have no common roots. We know that $\psi_3(x) = 2f(x)f''(x) - f'(x)^2$, from which we have that

$$\begin{aligned}
\psi_3'(x) &= 2f(x)f'''(x) + 2f'(x)f''(x) - 2f'(x)f''(x) \\
&= 2f(x)f'''(x) \\
&= 12f(x).
\end{aligned}$$

The only way for $2f(x)f''(x) - f'(x)^2$ and $12f(x)$ to have a common root is if $f(x)$ and $f'(x)$ have a common root, but we are given that $f(x)$ is non-singular. Thus the four roots of ψ_3 are distinct. We showed in (c) that for $P = (x, y) \neq \mathcal{O}$, if x is a root of ψ_3, then $3P = \mathcal{O}$. So we can conclude that if x_1, x_2, x_3 and x_4 are the four distinct roots of ψ_3, then the set

$$S = \{\mathcal{O}, (x_1, \pm\sqrt{f(x_1)}), (x_2, \pm\sqrt{f(x_2)}), (x_3, \pm\sqrt{f(x_3)}), (x_4, \pm\sqrt{f(x_4)})\}$$

is the complete set of points of order dividing three. To show that (x_i, y_i) are distinct, we just need to show that $y_i \neq 0$. If $y_i = 0$, from (a), the given point would have order two. Thus there are eight distinct points of order three. Including $\mathcal{O}$, there

are nine points of order dividing 3. Thus, if we can show that S is a group, then $S \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3$.

We know that $S \subseteq E(\mathbb{C})$. Let's use the One-Step Subgroup Test. Let a and b be any two distinct points of S of order 3. It follows that $a^3 = b^3 = \mathcal{O}$. Since S is abelian, we have that

$$\begin{aligned} \left(ab^{-1}\right)^3 &= a^3 \left(b^{-1}\right)^3 \\ &= a^3 \left(b^3\right)^{-1} \\ &= \mathcal{O}. \end{aligned}$$

It follows that $ab^{-1} \in S$ since S contains the complete set of elements of order 3. Therefore, S is a group.

□

Note that a point on an elliptic curve is an inflection point if and only if $3P = \mathcal{O}$. Consider Figure 1.16 below, which shows the group operation for $2P$. If P and $-2P$ were to collide (or $-P$ and $2P$), we would obtain and inflection point as depicted in Figure 1.17, for which it is clear that $3P = \mathcal{O}$.

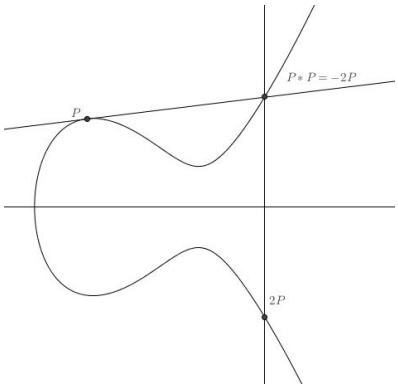


Figure 1.16: Finding $2P$

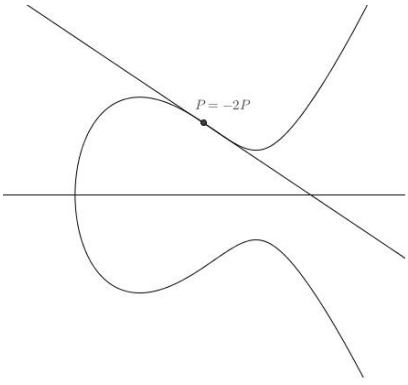


Figure 1.17: The Collision of P and $-2P$

We will conclude this chapter with an important theorem that we will use later to find the rank of $E(\mathbb{Q})$.

Theorem 1.5.2 (Nagell-Lutz [ST92, pp. 49-57])**.** *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 $f(x)$*,*

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

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

Chapter 2

Curves of the Form $y^2 = x^3 + ax^2 + bx + c$

2.1 Mordell's Theorem

In 1922, German mathematician Louis Mordell proved the following theorem as an answer to a question posed by Poincare in 1908.

Theorem 2.1.1 (Mordell's Theorem)**.** *Let E be a non-singular cubic curve given by an equation*

$$E\colon y^2 = x^3 + ax^2 + bx + c$$

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

A more general case was proven in 1928 by André Weil in his dissertation.

Theorem 2.1.2 (Mordell-Weil)**.** *Let E be an elliptic curve defined over a number field K. The group $E(K)$ is a finitely generated Abelian group.*

Mordell conjectured that any non-singular projective curve of genus greater than 1 defined over a number field K contains only finitely many K-rational points, but never

proved it. Gerd Faltings won a Fields Medal in 1986 for proving Mordell's conjecture.

By Mordell's theorem, $E(\mathbb{Q})$ is a finitely generated abelian group. From the Fundamental Theorem of Abelian Groups, $E(\mathbb{Q})$ is isomorphic to a direct sum of infinite cyclic groups and finite cyclic groups of order a power of a prime. Thus

$$E(\mathbb{Q}) \cong \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r \text{ summands}} \oplus \mathbb{Z}_{p_1^{v_1}} \oplus \mathbb{Z}_{p_2^{v_2}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{v_s}} \tag{2.1}$$

where each p_i is prime, and r is the *rank* of $E(\mathbb{Q})$.

We know from Mordell's theorem that we can generate all rational points on an elliptic curve from just a finite set using the group law. So how do we find the set of generators? At this point, that question cannot always be answered. That is what makes the study of the group of rational points on elliptic curves so interesting, much is unanswered. This chapter will culminate with a theorem that provides a formula for the rank of $E(\mathbb{Q})$. If the rank is zero, then $E(\mathbb{Q})$ is finite. We will show a few examples for which we can actually find $E(\mathbb{Q})$.

In this chapter, we are going to consider the specific Weierstrass curve $y^2 = f(x) = x^3 + ax^2 + bx$. Recall that using the group law, we only need one rational point on our elliptic curve to generate other rational points. So we want to make the assumption that the polynomial $f(x)$ has at least one rational root; this is equivalent to saying that the curve has at least one point of order two. Let the rational point of order two be P. Then $P = (x_0, 0)$. We can translate the curve so that P lies at the origin. Any rational points found on the translated curve will still be rational after translating back since x_0 is rational. Knowing that $(0, 0)$ is a solution to E implies that $c = 0$. Thus,

$$E\colon y^2 = f(x) = x^3 + ax^2 + bx.$$

2.2 Some Useful Homomorphisms

Before proving the theorem on the rank of $E(\mathbb{Q})$, we will need a few propositions. These propositions and the techniques used in their proofs will help us prove the theorem

on the rank of $E(\mathbb{Q})$.

Proposition 2.2.1. *Let E and E' be the elliptic curves given by the equations*

$$E\colon y^2 = x^3 + ax^2 + bx \quad \textit{and} \quad E'\colon y^2 = x^3 + \overline{a}x^2 + \overline{b}x,$$

where

$$\overline{a} = -2a \quad \textit{and} \quad \overline{b} = a^2 - 4b.$$

Let $T = (0,0) \in E$.

(a) *There is a homomorphism $\phi\colon E \to E'$ defined by*

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

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

(b) *Applying the same process to E' gives a map $\overline{\phi}\colon E' \to E''$. The curve E'' is isomorphic to E via the map $(x,y) \to \left(\frac{x}{4}, \frac{y}{8}\right)$. There is thus a homomorphism $\psi\colon E' \to E$ defined by*

$$\psi(\overline{P}) = \begin{cases} \left(\frac{\overline{y}^2}{4\overline{x}^2}, \frac{\overline{y}(\overline{x}^2-\overline{b})}{8\overline{x}^2}\right), & \textit{if } \overline{P} = (\overline{x},\overline{y}) \neq \overline{\mathcal{O}}, \overline{T}, \\ \mathcal{O}, & \textit{if } \overline{P} = \overline{\mathcal{O}} \textit{ or } \overline{P} = \overline{T}. \end{cases}$$

We will not prove this proposition, but it is worth noting that in order to show that ϕ is a homomorphism, it is enough to show that for P_1, P_2, and P_3 on E, if $P_1 \oplus P_2 \oplus P_3 = \mathcal{O}$, then $\phi(P_1) \oplus \phi(P_2) \oplus \phi(P_3) = \overline{\mathcal{O}}$. For if this were true, then

$$\phi(P_1 \oplus P_2) = \phi(\ominus P_3) = \ominus\phi(P_3) = \phi(P_1) \oplus \phi(P_2).$$

This technique for showing that a map is a homomorhism will be used again.

Proposition 2.2.2. *Let ϕ and ψ be the homomorphisms described above. If $P = (x, y) \in E(\mathbb{Q})$ where $E\colon y^2 = x^3 + ax^2 + bx$, then $(\psi \circ \phi)(P) = 2P$.*

Proof. First, note that $c = 0$ for E. Thus, formulas (1.4) and (1.5) reduce to

$$2P = \left(\frac{x^4 - 2bx^2 + b^2}{4x^3 + 4ax^2 + 4bx}, \frac{x^6 + 2ax^5 + 5bx^4 - 5b^2x^2 - 2ab^2x - b^3}{8y^3} \right),$$

for $P = (x, y) \neq \mathcal{O} \in E$. Now,

$$\begin{aligned}
(\psi \circ \phi)(x, y) &= \psi(\phi(x, y)) \\
&= \psi\left(\frac{y^2}{x^2}, \frac{y(x^2 - b)}{x^2} \right) \\
&= \left(\frac{\left(\frac{y(x^2-b)}{x^2}\right)^2}{4\left(\frac{y^2}{x^2}\right)^2}, \frac{\frac{y(x^2-b)}{x^2}\left(\left(\frac{y^2}{x^2}\right)^2 - (a^2 - 4b)\right)}{8\left(\frac{y^2}{x^2}\right)^2} \right) \\
&= \left(\frac{x^2 - 2bx^2 + b^2}{4y^2}, \frac{x^6 + 2ax^5 + 5bx^4 - 5b^2x^2 - 2ab^2x - b^3}{8y^3} \right)
\end{aligned}$$

Therefore, $(\psi \circ \phi)(P) = 2P$. □

If we allow complex numbers, $\phi\colon E \to E'$ is onto. Since the focus of this paper is rational points, we want to know what properties ϕ has when acting on $E(\mathbb{Q})$.

Proposition 2.2.3 (Properties of $\phi\colon E(\mathbb{Q}) \to E'(\mathbb{Q})$)**.**

(i) $\overline{\mathcal{O}} \in \phi\big(E(\mathbb{Q})\big)$.

(ii) $\overline{T} = (0, 0) \in \phi\big(E(\mathbb{Q})\big)$ *if and only if* $\overline{b} = a^2 - 4b$ *is a perfect square.*

(iii) *Let* $\overline{P} = (\overline{x}, \overline{y}) \in E'(\mathbb{Q})$ *with* $\overline{x} \neq 0$. *Then* $\overline{P} \in \phi\big(E(\mathbb{Q})\big)$ *if and only if* $\overline{x}$ *is the square of a rational number.*

Proof.

(i) Recall that $\mathcal{O}$ is considered rational and is therefore an element of $E(\mathbb{Q})$. From the definition of ϕ, we can conclude that $\phi(\mathcal{O}) = \overline{\mathcal{O}}$. Thus $\overline{\mathcal{O}} \in \phi\big(E(\mathbb{Q})\big)$.

(ii) Assume $\overline{T} = (0, 0) \in \phi\big(E(\mathbb{Q})\big)$. Then there exists $(x, y) \in E(\mathbb{Q})$ such that $\phi(x, y) = (0, 0)$. It follows by the definition of ϕ that $\frac{y^2}{x^2} = 0$. Thus $y = 0$. Substituting

$y = 0$ into $y^2 = x^3 + ax^2 + bx$, we have $0 = x(x^2 + ax + b)$. Note that $x = 0$ is an impossibility for if $x = 0$ and $y = 0$, then $\phi(x, y) = \overline{\mathcal{O}}$, not $\overline{T}$. So $x^2 + ax + b = 0$. This only has rational solutions if its discriminant is a perfect square. Thus $a^2 - 4b$ is a perfect square.

Conversely, if $a^2 - 4b$ is a perfect square, then $0 = x^3 + ax^2 + bx = x(x^2 + ax + b)$ has rational zeros other than zero. Hence, there exist $(x, y) \in E(\mathbb{Q})$ such that $\phi(x, y) = (0, 0) = \overline{T}$.

(iii) Let $\overline{P} = (\overline{x}, \overline{y}) \in E'(\mathbb{Q})$ with $\overline{x} \neq 0$. Assume $\overline{P} \in \phi\big(E(\mathbb{Q})\big)$. Then there exists $(x, y) \in E(\mathbb{Q})$ such that $\phi(x, y) = (\overline{x}, \overline{y})$. Thus by the definition of ϕ, it follows that $\overline{x} = \frac{y^2}{x^2} = \left(\frac{y}{x}\right)^2$. Therefore $\overline{x}$ is the square of a rational number.

Suppose conversely that $\overline{x} = t^2$ for $t \in \mathbb{Q}^*$. We need to show that there exists a point $(x, y) \in E(\mathbb{Q})$ such that $\phi(x, y) = \overline{P}$. Consider the points (x_1, y_1) and (x_2, y_2) where $x_1 = \frac{1}{2}\left(t^2 - a + \frac{\overline{y}}{t}\right)$, $x_2 = \frac{1}{2}\left(t^2 - a - \frac{\overline{y}}{t}\right)$, $y_1 = x_1 t$ and $y_2 = -x_2 t$. Since $t \neq 0$, we have that x_1 and x_2 are well defined.

Let's start by showing that (x_1, y_1) and (x_2, y_2) are contained in $E(\mathbb{Q})$. First, we have that

$$\begin{aligned}
x_1 x_2 &= \frac{1}{2}\left(t^2 - a + \frac{\overline{y}}{t}\right) \cdot \frac{1}{2}\left(t^2 - a - \frac{\overline{y}}{t}\right) \\
&= \frac{1}{4}\left((t^2 - a)^2 - \frac{\overline{y}^2}{t^2}\right) \\
&= \frac{1}{4}\left((\overline{x} - a)^2 - \frac{\overline{y}^2}{\overline{x}}\right) \\
&= \frac{1}{4}\left(\frac{\overline{x}^3 - 2a\overline{x}^2 + a^2\overline{x} - \overline{y}^2}{\overline{x}}\right) \\
&= \frac{1}{4}\left(\frac{\overline{x}^3 - 2a\overline{x}^2 + a^2\overline{x} - (\overline{x}^3 - 2a\overline{x}^2 + a^2\overline{x} - 4b\overline{x})}{\overline{x}}\right) \\
&= b.
\end{aligned}$$

Also, it is easy to see that $x_1 + x_2 = t^2 - a$. Thus, $x_i + \frac{b}{x_i} = \left(\frac{y_i}{x_i}\right)^2 - a$ for $i = \{1, 2\}$, which upon multiplication by x_i^2 yields $x_i^3 + ax_i^2 + bx_i = y_i^2$. Hence (x_1, y_1) and

(x_2, y_2) are contained in $E(\mathbb{Q})$.

Let's show that $\phi\,(x_1, y_1) = \phi\,(x_2, y_2) = (\overline{x}, \overline{y})$. We will start with $\phi\,(x_1, y_1)$. From $y_1 = x_1 t$, we have that $t = \frac{y_1}{x_1}$. Thus

$$\begin{aligned} \frac{y_1^2}{x_1^2} &= \left(\frac{y_1}{x_1}\right)^2 \\ &= t^2 \\ &= \overline{x}. \end{aligned}$$

Now, notice that $x_1 - x_2 = \frac{\overline{y}}{t}$. It follows that

$$\begin{aligned} \frac{y_1(x_1^2 - b)}{x_1^2} &= \frac{x_1 t(x_1^2 - x_1 x_2)}{x_1^2} \\ &= t(x_1 - x_2) \\ &= t\left(\frac{\overline{y}}{t}\right) \\ &= \overline{y}. \end{aligned}$$

Therefore, $\phi(x_1, y_1) = (\overline{x}, \overline{y})$. A similar argument will show that $\phi(x_2, y_2) = (\overline{x}, \overline{y})$ as well.

□

We will now set out to prove that for the map $\psi\colon E' \to E$, the index $\Big[E(\mathbb{Q}) : \psi\big(E'(\mathbb{Q})\big)\Big] \leq 2^{t+1}$, where t is the number of distinct prime factors of b. In the process, we will introduce a useful map α and describe some of its properties. This map will be used later in our proof of a formula for the rank of $E(\mathbb{Q})$.

Let $\mathbb{Q}^*$ be the multiplicative group of nonzero rational numbers, and let $\mathbb{Q}^{*2}$ be the subgroup of the squares of the elements of $\mathbb{Q}^*$. Also, let $\alpha\colon E(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ be the map defined by

$$\alpha(P) = \begin{cases} x \pmod{\mathbb{Q}^{*2}}, & \text{if } P = (x,y) \neq \mathcal{O}, T, \\ 1 \pmod{\mathbb{Q}^{*2}}, & \text{if } P = \mathcal{O}, \\ b \pmod{\mathbb{Q}^{*2}}, & \text{if } P = T. \end{cases}$$

Proposition 2.2.4.

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

(b) *The kernel of* α *is the image* $\psi\big(E'(\mathbb{Q})\big)$*. Hence* α *induces a one-to-one homomorphism*

$$\frac{E(\mathbb{Q})}{\psi\big(E'(\mathbb{Q})\big)} \hookrightarrow \frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}}.$$

(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 of* $\mathbb{Q}^*/\mathbb{Q}^{*2}$ *consisting of the elements*

$$\{\pm p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_t^{\varepsilon_t} : \text{ each } \varepsilon_i \text{ equals 0 or 1}\}.$$

(d) *The index* $\Big[E(\mathbb{Q}) : \psi\big(E'(\mathbb{Q})\big)\Big]$ *is at most* 2^{t+1}*.*

Proof.

(a) Let's use a similar strategy to the one outlined for the proof of Proposition 3.1.3. That is, we will show that α sends inverses to inverses and that if $P_1 \oplus P_2 \oplus P_3 = \mathcal{O}$, then $\alpha(P_1)\alpha(P_2)\alpha(P_3) \equiv 1 \pmod{\mathbb{Q}^{*2}}$. For then $\alpha(P_1 \oplus P_2) = \alpha(-P_3) \equiv \alpha(P_3)^{-1} = \alpha(P_1)\alpha(P_2) \pmod{\mathbb{Q}^{*2}}$.

Let $P = (x,y) \in E(\mathbb{Q})$. Then

$$\alpha(-P) = \alpha(x,-y) = x \equiv \frac{1}{x} = \alpha(x,y)^{-1} = \alpha(P)^{-1} \pmod{\mathbb{Q}^{*2}}.$$

We used the fact that if $n^2 \equiv 1 \pmod{\mathbb{Q}^{*2}}$, then $n \equiv \frac{1}{n} \pmod{\mathbb{Q}^{*2}}$.

Now, let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ and $P_3 = (x_3, y_3)$ be elements of $E(\mathbb{Q})$. We know that if $P_1 \oplus P_2 \oplus P_3 = \mathcal{O}$, then P_1, P_2 and P_3 are colinear. Let $y = mx + v$ be the line passing through them. Since these points are the intersections of $y = mx + v$ with $E\colon y^2 = x^3 + ax^2 + bx$, we have

$$\begin{aligned} y^2 &= x^3 + ax^2 + bx \\ (mx+v)^2 &= x^3 + ax^2 + bx \\ m^2x^2 + 2mvx + v^2 &= x^3 + ax^2 + bx \\ 0 &= x^3 + (a-m^2)x^2 + (b-2mv)x - v^2. \end{aligned} \tag{2.2}$$

We also know that since P_1, P_2 and P_3 are roots of (2.2), it follows that

$$\begin{aligned} & x^3 + (a-m^2)x^2 + (b-2mv)x - v^2 \\ = \;& (x-x_1)(x-x_2)(x-x_3) \\ = \;& x^3 - (x_1+x_2+x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3. \end{aligned}$$

If we equate the final terms, then $x_1x_2x_3 = v^2 \in \mathbb{Q}^{*2}$. Thus

$$\alpha(P_1)\alpha(P_2)\alpha(P_3) = x_1x_2x_3 = v^2 \equiv 1 \pmod{\mathbb{Q}^{*2}}.$$

So we have completed the proof of (a) if the three points given are not $\mathcal{O}$ or T. We will leave it to the reader to verify the other cases.

(b) The kernel of α is all of the elements of $E(\mathbb{Q})$ that map to 1 modulo $\mathbb{Q}^{*2}$. From the definition of α, we can see that these are the elements $\mathcal{O}$, T if b is a perfect square, and the elements of $E(\mathbb{Q})$ whose x-coordinates are perfect squares. If we apply Proposition 2.2.3 to ψ instead of ϕ, it is clear that the image $\psi\big(E'(\mathbb{Q})\big)$ is exactly the points mentioned above. Thus the kernel of α is the image $\psi\big(E'(\mathbb{Q})\big)$.

Since $E(\mathbb{Q})$ and $\mathbb{Q}^*/\mathbb{Q}^{*2}$ are both groups and we showed in (a) that α is a homomor-

phism, by the first isomorphism theorem

$$im\,\alpha \cong E(\mathbb{Q})/ker\,\alpha = E(\mathbb{Q})/\psi(E'(\mathbb{Q})).$$

Thus α induces a one-to-one homomorphism

$$\frac{E(\mathbb{Q})}{\psi\big(E'(\mathbb{Q})\big)} \hookrightarrow \frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}}.$$

(c) If we want to know what the image of α looks like, we just need to analyze the x-coordinates of points in $E(\mathbb{Q})$. It turns out that if $P = (x, y)$ is on E, then $x = \frac{m}{e^2}$ and $y = \frac{n}{e^3}$ for integers m, n and e, where $e > 0$ and $\gcd(m, e) = \gcd(n, e) = 1$. (For a derivation of these formulas, see Silverman-Tate pg. 68-69.) Substituting x and y into the equation for E gives

$$\begin{aligned}
\left(\frac{n}{e^3}\right)^2 &= \left(\frac{m}{e^2}\right)^3 + a\left(\frac{m}{e^2}\right)^2 + b\left(\frac{m}{e^2}\right) \\
n^2 &= m^3 + am^2e^2 + bme^4 \\
n^2 &= m\left(m^2 + ame^2 + be^4\right).
\end{aligned}$$

If m and $m^2 + ame^2 + be^4$ are relatively prime, then each of them would be a positive or negative square. Hence $x = \frac{m}{e^2}$ would be a positive or negative square. Thus $\alpha(P) \equiv 1 \pmod{\mathbb{Q}^{*2}}$, and $1 \in \{\pm p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_t^{\varepsilon_t}\}$ where the p_i are as described above. If m and $m^2 + ame^2 + be^4$ are not relatively prime, then let

$$d = \gcd(m, m^2 + ame^2 + be^4).$$

Then d divides m and be^4. We know that m and e are relatively prime, thus d divides b. Now, the primes that divide m but do not divide b must be of even power. The primes dividing m and b can be of either even or odd power. Thus

$$m = \pm(\text{integer})^2 \cdot p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_t^{\varepsilon_t},$$

where each ε_i is either 0 or 1 and $p_1, \ldots, p_t$ are the distinct primes dividing b. There-

fore,

$$\alpha(P) = x = \frac{m}{e^2} \equiv \pm p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_t^{\varepsilon_t} \pmod{\mathbb{Q}^{*2}}.$$

If $x = 0$, then the method above fails. However, if $x = 0$, then $y = 0$ since $E\colon y^2 = x^3 + ax^2 + bx$. Now $\alpha(T) = b \pmod{\mathbb{Q}^{*2}}$ and $b = \pm p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_t^{\varepsilon_t}$. Thus the image of α is is contained in the subgroup of $\mathbb{Q}^*/\mathbb{Q}^{*2}$ consisting of the elements

$$B = \{\pm p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_t^{\varepsilon_t} : \text{ each } \varepsilon_i \text{ equals 0 or 1}\}.$$

(d) Let's find the order of the subgroup from (c). Since each power ε_i can be either 0 or 1, there are two choices for each $p_i^{\varepsilon_i}$. Thus $|\{p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_t^{\varepsilon_t}\}| = 2^t$. Since all of the elements of the subgroup can be either positive or negative, there are $2(2^t) = 2^{t+1}$ elements.

We know from (b) that $im\ \alpha \cong E(\mathbb{Q})/\psi(E'(\mathbb{Q}))$ and from (c) that $im\ \alpha \subseteq B$. Therefore, the index $\Big[E(\mathbb{Q}) : \psi\big(E'(\mathbb{Q})\big)\Big] \leq 2^{t+1}$.

□

2.3 Modules and Exact Sequences

At this point, we will take some time to discuss modules over a ring. We will use some module theory in future proofs.

Definition 2.3.1. Let R be a commutative ring. An *R-module* is an additive abelian group A together with a function $R \times A \to A$ (the image of (r, a) being denoted ra) such that for all $r, s \in R$ and $a, b \in A$:

(i) $r(a + b) = ra + rb$

(ii) $(r + s)a = ra + sa$

(iii) $r(sa) = (rs)a$.

If R has an identity element 1_R and

(iv) $1_R a = a$ for all $a \in A$,

then A is said to be a *unitary R-module*. If R is a field, then a unitary R-module is called a *vector space*.

It is clear from the definition above that every additive abelian group G is a unitary $\mathbb{Z}$-module, specifically our group $(E(\mathbb{Q}), \oplus)$.

Definition 2.3.2. Let A and B be modules over a ring R. A function $f\colon A \to B$ is an *R-module homomorphism* provided that for all $a, c \in A$ and $r \in R$:

$$f(a+c) = f(a) + f(c) \quad \textit{and} \quad f(ra) = rf(a).$$

Definition 2.3.3. A pair of module homomorphisms, $A \xrightarrow{f} B \xrightarrow{g} C$, is said to be *exact* at B provided $im\ f = ker\ g$. A finite sequence of module homomorphisms, $A_0 \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2 \xrightarrow{f_3} \cdots \xrightarrow{f_{n-1}} A_{n-1} \xrightarrow{f_n} A_n$, is *exact* provided $im\ f_i = ker\ f_{i+1}$ for $i = 1, 2, \ldots, n-1$. An infinite sequence of module homomorphisms , $\cdots \xrightarrow{f_{i-1}} A_{i-1} \xrightarrow{f} A_i \xrightarrow{f_{i+1}} A_{i+1} \xrightarrow{f_{i+2}} \cdots$ is *exact* provided $im\ f_1 = ker\ f_{i+1}$ for all $i \in \mathbb{Z}$.

Definition 2.3.4. If $f\colon A \to B$ is a module homomorphism, then $A/ker\ f$ [resp. $B/im\ f$] is called the *coimage* [resp. *cokernel*] of f and is denoted *coim* f [resp. *coker* f].

Note that from the definitions above, the following claims are true. The sequence $0 \to A \xrightarrow{f} B$ is an exact sequence if and only if f is a module monomorphism. Similarly, $B \xrightarrow{g} C \to 0$ is exact if and only if g is a module epimorphism. If $A \xrightarrow{f} B \xrightarrow{g} C$ is exact, then $gf = 0$ since $im\ f = ker\ g$. Also, if $A \xrightarrow{f} B \xrightarrow{g} C \to 0$ is exact, then $coker\ f = B/im\ f = B/ker\ g = coim\ g \cong C$.

Definition 2.3.5. A *commutative diagram* is a diagram of objects (also known as *vertices*) and morphisms (also known as *arrows* or *edges*) such that all directed paths in the diagram with the same start and endpoints lead to the same result by composition.

For example, the diagram below would be commutative if $h \circ f = k \circ g$.

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle h} \\ C & \xrightarrow[k]{} & D \end{array}$$

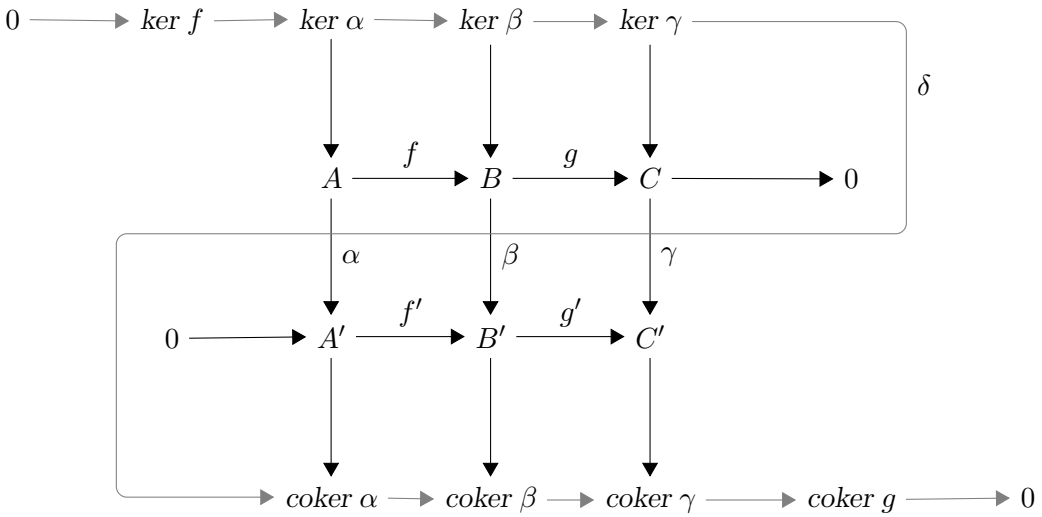
Lemma 2.3.1 (Snake Lemma [Lan02, p. 100])**.** *Consider the commutative diagram of Abelian groups and group homomorphisms below:*

$$\begin{array}{ccccccccc} & & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & & \end{array}$$

where rows are exact sequences. Then there is an exact sequence relating the kernels and cokernels of α, β and γ:

$$\ker \alpha \to \ker \beta \to \ker \gamma \xrightarrow{\delta} \operatorname{coker} \alpha \to \operatorname{coker} \beta \to \operatorname{coker} \gamma.$$

In order to follow the maps from the statement above, one would have to wind through the commutative diagram like a snake, as depicted below, giving the lemma its name.



We can actually extend the Snake Lemma as below.

Lemma 2.3.2 (Extended Snake Lemma)**.** *Under the same assumptions as the Snake Lemma, the sequence*

$$0 \to \ker f \to \ker \alpha \to \ker \beta \to \ker \gamma \xrightarrow{\delta} \operatorname{coker} \alpha \to \operatorname{coker} \beta \to \operatorname{coker} \gamma \to \operatorname{coker} g \to 0 \quad (*)$$

is exact.

Proof. By the Snake Lemma, we know that $\ker \alpha \to \ker \beta \to \ker \gamma \xrightarrow{\delta} \operatorname{coker} \alpha \to \operatorname{coker} \beta \to \operatorname{coker} \gamma$ is exact. It remains to show that $0 \to \ker f \to \ker \alpha$ and $\operatorname{coker} \gamma \to \operatorname{coker} g \to 0$ are exact. Recall that if the map from $\ker f$ to $\ker \alpha$ is a module monomorphism, then $0 \to \ker f \to \ker \alpha$ is exact. Let's show that $\ker f \subseteq \ker \alpha$, then the inclusion map will be injective. Let $a \in \ker f$. By commutativity,

$$f'\alpha(a) = \beta f(a) = \beta(f(a)) = \beta(0) = 0.$$

It follows that $\alpha(a) = 0$ since f' is a module monomorphism from the exactness of the second row, implying that $a \in \ker \alpha$.

To prove that $\operatorname{coker} \gamma \to \operatorname{coker} g \to 0$ is exact, we just need to show that the map taking $\operatorname{coker} \gamma$ to $\operatorname{coker} g$ is an epimorphism. Since $A \xrightarrow{f} B \xrightarrow{g} C \to 0$ is exact, g is an epimorphism. It follows that $\operatorname{coker} g = C/\operatorname{im} g = 0$. Thus, the map taking $\operatorname{coker} \gamma$ to $\operatorname{coker} g$ is onto. Therefore, $(*)$ is exact. □

Lemma 2.3.3. *If* $0 \to A_1 \to A_2 \to A_3 \to \ldots \to A_n \to 0$ *is an exact sequence such that* $|A_i| < \infty$*, then*

$$\begin{aligned} |A_1||A_3|\ldots|A_n| &= |A_2||A_4|\ldots|A_{n-1}| \quad \text{if } n \text{ is odd} \\ &\text{and} \\ |A_2||A_4|\ldots|A_n| &= |A_1||A_3|\ldots|A_{n-1}| \quad \text{if } n \text{ is even.} \end{aligned}$$

Proof. Let $f_n : A_n \to A_{n+1}$. We are given that $A_{i-1} \to A_i \to A_{i+1} \to A_{i+2}$ is exact. Then

$$coker\ f_{i-1} = A_i/im\ f_{i-1} = A_i/ker\ f_i \cong im\ f_i = ker\ f_{i+1}. \tag{2.3}$$

Since $0 \to A_1 \xrightarrow{f_1} A_2$ is an exact sequence, f_1 is injective, implying that $coker\ f_1 = A_2/im\ f_1 \cong A_2/A_1$. By Lagrange's Theorem, $|coker\ f_1| = |A_2|/|A_1|$, or equivalently

$$|A_2| \quad = \quad |A_1||coker\ f_1|. \tag{2.4}$$

Consider the sequence $0 \to coker\ f_{i-1} \to A_{i+1} \to coker\ f_1 \to 0$. By (2.3) above, $coker\ f_{i-1} = ker\ f_{i+1}$. So clearly the map from $coker\ f_{i-1}$ to A_{i+1} is injective. Also, since $coker\ f_i = A_{i+1}/im\ f_i$, the map $A_{i+1} \to coker\ f_i$ is surjective. Therefore, the sequence $0 \to coker\ f_{i-1} \to A_{i+1} \to coker\ f_i \to 0$ is exact. Then

$$coker\ f_i = A_{i+1}/im\ f_i = A_{i+1}/ker\ f_{i+1} \cong A_{i+1}/coker\ f_{i-1}.$$

Therefore, $|coker\ f_i| = |A_{i+1}|/|coker\ f_{i-1}|$, or equivalently

$$|coker\ f_{i-1}| \quad = \quad |A_{i+1}|/|coker\ f_i|. \tag{2.5}$$

Now consider the sequence $0 \to coker\ f_{n-3} \to A_{n-1} \to A_n \to 0$. By (2.3), $coker\ f_{n-3} \cong ker\ f_{n-1}$. So if the injective map i takes $ker\ f_{n-1}$ to A_{n-1} and $f_{n-1} : A_{n-1} \to A_n$, then $im\ i = ker\ f_{n-1}$. Thus the sequence is exact. So $A_n \cong A_{n-1}/ker\ f_{n-1} = A_{n-1}/coker\ f_{n-3}$. Which yields the equality

$$|coker\ f_{n-3}| \quad = \quad |A_{n-1}|/|A_n|. \tag{2.6}$$

So for even n, by (2.4) we have $|A_2| = |A_1||coker\ \alpha_1|$.

Inductively using (2.5), we have

$$\begin{aligned} |A_2| &= |A_1||coker\ f_1| \\ |A_2||coker\ f_2| &= |A_1||A_3| \\ |A_2||A_4| &= |A_1||A_3||coker\ f_3| \\ &\vdots \\ |A_2||A_4|\dots|A_{n-2}| &= |A_1||A_3|\dots|A_{n-3}||coker\ f_{n-3}|. \end{aligned}$$

Using (2.6), we have

$$\begin{aligned} |A_2||A_4|\dots|A_{n-2}| &= |A_1||A_3|\dots|A_{n-3}||A_{n-1}|/|A_n|. \\ |A_2||A_4|\dots|A_{n-2}||A_n| &= |A_1||A_3|\dots|A_{n-3}||A_{n-1}|. \end{aligned}$$

A similar result is produced if n is odd. □

Theorem 2.3.4. *If A, B and C are abelian groups and $f\colon A \to B$ and $g\colon B \to C$ are group homomorphisms with $\ker f$, $\ker g$, $coker\ f$ and $coker\ g$ finite, then $\ker(g \circ f)$ and $coker(g \circ f)$ are finite and*

$$\frac{|coker(f \circ g)|}{|ker(f \circ g)|} = \frac{|coker\ f||coker\ g|}{|ker\ f||ker\ g|}.$$

Proof. Consider the following diagram of Abelian groups and group homomorphisms.

$$\begin{array}{ccccccccc} & & & & A & \xrightarrow{f} & B & \longrightarrow & coker\ f & \longrightarrow & 0 \\ & & & & \Big\downarrow{\scriptstyle g\circ f} & & \Big\downarrow{\scriptstyle g} & & \Big\downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & C & \xrightarrow{id} & C & \longrightarrow & 0 & & & & \end{array}$$

It is clear that the diagram commutes, the rows are exact and $ker\ h = coker\ f$. By the Extended Snake Lemma,

$$0 \to ker\ f \to ker(g \circ f) \to ker\ g \to coker\ f \to coker(g \circ f) \to coker\ g \to 0 \qquad (2.7)$$

is an exact sequence. Let α and β be group homorphisms such that $\alpha\colon ker\ f \to ker(g \circ f)$ and $\beta\colon ker(g \circ f) \to ker\ g$. By the first isomorphism theorem,

$$ker(g \circ f)/ker\ \beta \cong im\ \beta. \tag{2.8}$$

From the exactness of (2.7), $ker\ \beta = im\ \alpha$. Since $\alpha\colon ker\ f \to ker(g \circ f)$ and we are given that $ker\ f$ is finite, $im\ \alpha$ is finite. Also, since $\beta\colon ker(g \circ f) \to ker\ g$, $im\ \beta \subseteq ker\ g$. We are given that $ker\ g$ is finite, thus $im\ \beta$ is finite as well. Therefore, from (2.8), we can see that $ker(g \circ f)$ is finite. By a similar argument, it can be shown that $coker(g \circ f)$ is finite.

Since we are given that $ker\ f$, $ker\ g$, $coker\ f$ and $coker\ g$ are finite and we showed that $ker(g \circ f)$ and $coker(g \circ f)$ are finite as well, by Lemma 2.3.3,

$$|ker\ f||ker\ g||coker(g \circ f)| = |ker(g \circ f)||coker\ f||coker\ g|.$$

Thus,

$$\frac{|coker(g \circ f)|}{|ker(g \circ f)|} = \frac{|coker\ f||coker\ g|}{|ker\ f||ker\ g|}.$$

□

2.4 The Rank of $E(\mathbb{Q})$

Before we begin our proof on the rank of $E(\mathbb{Q})$, let us examine the structure of some key sets in our proof. Recall that

$$E(\mathbb{Q}) \cong \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r \text{ summands}} \oplus \mathbb{Z}_{p_1^{v_1}} \oplus \mathbb{Z}_{p_2^{v_2}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{v_s}} \tag{2.9}$$

where each p_i is prime, and r is the *rank* of $E(\mathbb{Q})$.

Now, $2E(\mathbb{Q})$ is important since we know by Proposition 2.2.2 that $\psi \circ \phi\colon E(\mathbb{Q}) \to E(\mathbb{Q})$ results in multiplication by two. Hence

$$im(\psi \circ \phi) = 2E(\mathbb{Q}) \cong 2\mathbb{Z} \oplus 2\mathbb{Z} \oplus \cdots \oplus 2\mathbb{Z} \oplus 2\mathbb{Z}_{p_1^{v_1}} \oplus 2\mathbb{Z}_{p_2^{v_2}} \oplus \cdots \oplus 2\mathbb{Z}_{p_s^{v_s}}.$$

So the quotient group

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}_{p_1^{v_1}}}{2\mathbb{Z}_{p_1^{v_1}}} \oplus \frac{\mathbb{Z}_{p_2^{v_2}}}{2\mathbb{Z}_{p_2^{v_2}}} \oplus \cdots \oplus \frac{\mathbb{Z}_{p_s^{v_s}}}{2\mathbb{Z}_{p_s^{v_s}}}. \tag{2.10}$$

We will also be interested in what the elements in the kernel of $\psi \circ \phi$ look like. So let $E(\mathbb{Q})_2$ be the 2-torsion subgroup of $E(\mathbb{Q})$ (*i.e.* $E(\mathbb{Q})_2$ is the subgroup of all $Q \in E(\mathbb{Q})$ such that $2Q = \mathcal{O}$). By (2.9), there exist generators, say $P_1, P_2, \ldots, P_r, Q_1, Q_2, \ldots, Q_s \in E(\mathbb{Q})$ such that every point $P \in E(\mathbb{Q})$ can be written as

$$P = n_1P_1 \oplus \cdots \oplus n_rP_r \oplus m_1Q_1 \oplus \cdots \oplus m_sQ_s$$

where each integer n_i is uniquely determined by P and the integers m_j are determined modulo $p_j^{v_j}$.

In order to find $|E(\mathbb{Q})_2|$, let us examine when $2(n_1P_1 + \cdots + n_rP_r + m_1Q_1 + \cdots + m_sQ_s) = \mathcal{O}$. This will only happen if $n_i = 0$ for each i and $2m_j \equiv 0 \pmod{p^{v_j}}$ for each j. If p is odd, $2m \equiv 0 \pmod{p^v}$ if an only if $m \equiv 0 \pmod{p^v}$. If $p = 2$, then $2m \equiv 0 \pmod{p^v}$ if $m \equiv 0 \pmod{p^{v-1}}$ or $m \equiv 0 \pmod{p^v}$. So for each term n_iP_i, we have one choice, $n_i = 0$. For each term m_jQ_j, we have one choice if p is odd and two choices if $p = 2$. Thus

$$|E(\mathbb{Q})_2| = 2^N \tag{2.11}$$

where N is the number of $p_j = 2$.

Now we are ready to prove a theorem regarding the rank of $E(\mathbb{Q})$.

Theorem 2.4.1. *Let $\phi\colon E(\mathbb{Q}) \to E'(\mathbb{Q})$, $\psi\colon E'(\mathbb{Q}) \to E(\mathbb{Q})$, $\alpha\colon E(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$, and $\alpha'\colon E'(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ be group homorphisms as previously defined. Then*

$$\frac{|im\ \alpha| \cdot |im\ \alpha'|}{4} = 2^r$$

where r is the rank of $E(\mathbb{Q})$.

Proof. From (2.10), we know that

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong \left(\bigoplus_{i=1}^{r} \frac{\mathbb{Z}}{2\mathbb{Z}}\right) \oplus \left(\bigoplus_{j=1}^{s} \frac{\mathbb{Z}_{p_j^{v_j}}}{2\mathbb{Z}_{p_j^{v_j}}}\right).$$

Since $\mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}_2$, it has order 2. For each $\dfrac{\mathbb{Z}_{p_i^{v_i}}}{2\mathbb{Z}_{p_i^{v_i}}}$, we have

$$\frac{\mathbb{Z}_{p_i^{v_i}}}{2\mathbb{Z}_{p_i^{v_i}}} \cong \begin{cases} \mathbb{Z}_2 & p_i = 2 \\ 0 & p_i \neq 2 \end{cases}.$$

Thus

$$\left|E(\mathbb{Q})/2E(\mathbb{Q})\right| = 2^r \cdot 2^N.$$

Since $\psi \circ \phi$ is multiplication by two, from the definition of *cokernel* and equation (2.11), we know that

$$|coker(\psi \circ \phi)| = \left|E(\mathbb{Q})/2E(\mathbb{Q})\right| = 2^r \cdot 2^N = 2^r \cdot |E(\mathbb{Q})_2|.$$

This gives us

$$\frac{|coker(\psi \circ \phi)|}{|E(\mathbb{Q})_2|} = 2^r.$$

Since $E(\mathbb{Q})_2$ is defined to be all $Q \in E(\mathbb{Q})$ such that $2Q = \mathcal{O}$, and we know that $\psi \circ \phi$ results in multiplication by two, it follows that $E(\mathbb{Q})_2 = ker(\psi \circ \phi)$, and therefore

$$\frac{|coker(\psi \circ \phi)|}{|ker(\psi \circ \phi)|} = 2^r.$$

Which, by Theorem 2.3.4, gives us

$$\frac{|coker\ \psi|\,|coker\ \phi|}{|ker\ \psi|\,|ker\ \phi|} = 2^r. \tag{2.12}$$

From the defintion of ϕ, the $ker\ \phi = \{\mathcal{O}, T\}$, implying that $|ker\,\phi| = 2$. Similarly, $|ker\,\psi| = 2$. Also, from Proposition 2.2.4 part b, $ker\ \alpha = im\ \psi$. So by the definition of cokernel and the first isomorphism theorem,

$$coker\ \psi = \frac{E(\mathbb{Q})}{im\ \psi} = \frac{E(\mathbb{Q})}{ker\ \alpha} \cong im\ \alpha.$$

Likewise, $im\ \alpha' \cong coker\ \phi$. Therefore, from equation (2.12), we have

$$\frac{|im\ \alpha| \cdot |im\ \alpha'|}{4} = 2^r. \tag{2.13}$$

□

In order to compute the rank of $E(\mathbb{Q})$ for a given curve, we can see by (2.13) that we will need to find the cardinality of $im\ \alpha$ and $im\ \alpha'$. Recall from the proof of Proposition 2.2.4 part c that if (x, y) is a rational point on a Weierstrass elliptic curve, then

$$x = \frac{m}{e^2} \quad \text{and} \quad y = \frac{n}{e^3}$$

where e, m, $n \in \mathbb{Z}$, $e > 0$ and any two of e, m and n are relatively prime. The examples we are going to consider below contain curves of the form $E\colon y^2 = x^3 + bx$. If we substitute x and y into $y^2 = x^3 + bx$ and clear the denominators, we have

$$n^2 = m(m^2 + be^4). \tag{2.14}$$

Let $b_1 = \pm\gcd(m, b)$ where the sign of b_1 is the same as that of m. Then there exist integers m_1 and b_2 such that $m = b_1 m_1$ and $b = b_1 b_2$ with $\gcd(m_1, b_2) = 1$. Since m and b_1 have the same sign, $m_1 > 0$. If we substitute these values into (2.14), we have

$$n^2 = b_1^2 m_1 (b_1 m_1^2 + b_2 e^4) \tag{2.15}$$

We can conclude that $b_1^2 \mid n^2$, implying that $b_1 \mid n$. So there exists an integer n_1 such that $n = b_1 n_1$. Thus (2.15) becomes

$$n_1^2 = m_1 (b_1 m_1^2 + b_2 e^4). \tag{2.16}$$

Since $\gcd(m_1, b_2) = \gcd(m_1, e) = 1$, we have that m_1 and $b_1 m_1^2 + b_2 e^4$ are relatively prime. It follows that m_1 and $b_1 m_1^2 + b_2 e^4$ are perfect squares. Let

$$m_1 = M^2 \quad \text{and} \quad b_1 m_1^2 + b_2 e^4 = N^2,$$

where $n_1 = MN$. Substituting m_1 into N^2 yields

$$N^2 = b_1M^4 + b_2e^4.$$

So any point $(x, y) \in E(\mathbb{Q})$ with $y \neq 0$ can be written as

$$x = \frac{b_1M^2}{e^2} \quad \text{and} \quad y = \frac{b_1MN}{e^3}. \tag{2.17}$$

Recall that for any (x, y) other than $\mathcal{O}$ and T, we have that $\alpha(x, y) = x \pmod{\mathbb{Q}^{*2}}$. It follows that $im\ \alpha$ is contained in the set of divisors of b. So we only have a finite number of possibilities to check. In the examples that follow, we will find the rank of $E(\mathbb{Q})$ by writing all possible equations $N^2 = b_1M^4 + b_2e^4$, where b_1 and b_2 are integers such that $b = b_1b_2$. For each equation with a solution (M, N, e) that satisfies the conditions above, we will obtain an element in $im\ \alpha$. Note that if $m = 0$, the above method does not apply. However, if $m = 0$, then $(x, y) = T$ and $\alpha(T) = b$. An obvious drawback to this method is finding solutions (M, N, e) to $N^2 = b_1M^4 + b_2e^4$; there is no way of knowing if a solution even exists.

There are many unanswered questions regarding the rank of elliptic curves. For example, there is no known algorithm to find the rational points on elliptic curves over $\mathbb{Q}$. There is also no known algorithm for computing the rank of $E(\mathbb{Q})$. Here we will do a couple of examples of situations for which we are lucky enough to answer one or both of the preceding questions by using the method outlined above.

Example 2.4.1. Find the rank of the group of rational points on the curve $E\colon y^2 = x^3 - x$, and if possible, find $E(\mathbb{Q})$ and $E'(\mathbb{Q})$.

Solution. The only factors of $b = -1$ are ± 1. Since $\alpha(\mathcal{O}) = 1$ and $\alpha(T) = b = -1$,

$$im\ \alpha = \{\pm 1 \pmod{\mathbb{Q}^{*2}}\}.$$

Thus $|im\ \alpha| = 2$.

If $E\colon y^2 = x^3 - x$, then $E'\colon y^2 = x^3 + 4x$. The factors of $\bar{b} = 4$ are $\pm 1, \pm 2$ and ± 4. Since $\pm 4 \equiv \pm 1 \left(\mathrm{mod}\ \mathbb{Q}^{*2}\right)$, we only have to consider the following equations:

(i) $N^2 = M^4 + 4e^4$

(ii) $N^2 = -M^4 - 4e^4$

(iii) $N^2 = 2M^4 + 2e^4$

(iv) $N^2 = -2M^4 - 2e^4$.

Clearly, for (ii) and (iv), the right sides of the equations are negative, while the left sides are positive, so they have no solutions. Equation (i) has solution $(M, N, e) = (1, 1, 0)$, which by (2.17), corresponds to the point at infinity, but of course $1 \in \alpha'(E(\mathbb{Q}))$. With very little work, one can see that $(1, 2, 1)$ is a solution to (iii), for which $b_1 = 2$. So $im\ \alpha' = \{1, 2 \left(\mathrm{mod}\ \mathbb{Q}^{*2}\right)\}$, giving us $|im\ \alpha'| = 2$. Thus, by (2.13), we have that the rank of $E(\mathbb{Q})$ is zero, from which we can conclude that $E(\mathbb{Q})$ is finite. Let's proceed to find $E(\mathbb{Q})$ and $E'(\mathbb{Q})$.

Since $E(\mathbb{Q})$ is finite, its elements are of finite order, so Theorem 1.5.2 applies. It follows that x and y are integers, and either $y = 0$ or y divides D, which in our case is 4. To find the points for which $y = 0$, we need to solve $0 = x^3 - x$, which has solutions 0 and ± 1. Thus $(0, 0)$ and $(\pm 1, 0)$ are in $E(\mathbb{Q})$. To find the points for which y divides D, we would need to check all equations E with y equal to ± 1, ± 2 or ± 4. After some work, one will find no other integer solutions. Thus,

$$E(\mathbb{Q}) = \{\mathcal{O}, (0, 0), (1, 0), (-1, 0)\}.$$

Similarly, to find $E'(\mathbb{Q})$, if $y = 0$, then we can solve $0 = x^3 + 4x$, whose only integer solution is 0. Hence, $(0, 0) \in E'(\mathbb{Q})$. Next we need to check all equations E' for which y is a divisor of $D = -256$, so $y = \pm 1, \pm 2, \pm 4, \pm 8, \pm 16, \pm 32, \pm 64, \pm 128, \pm 256$. After some work, one will find $x^3 + 4x = 16$ has an integer solution of 2. Thus $(2, 4)$ and $(2, -4)$ are also $E'(\mathbb{Q})$. So

$$E'(\mathbb{Q}) = \{\mathcal{O}, (0, 0), (2, 4), (2, -4)\}.$$

□

Example 2.4.2. Find the rank of $y^2 = x^3 - 17x$.

Solution. The only factors of -17 are ± 1 and ± 17. So we only need to look at (M, N, e) satisfying

(i) $N^2 = M^4 - 17e^4$

(ii) $N^2 = -M^4 + 17e^4$

(iii) $N^2 = 17M^4 - e^4$

(iv) $N^2 = -17M^4 + e^4$.

Since equations (i) and (ii) are the same as (iv) and (iii), respectively, it is enough to consider (i) and (ii). Equation (i) has the trivial solution $(1, 1, 0)$, implying that (iv) has the solution $(0, 1, 1)$. Thus 1 and -17 are are contained in the image of α. Equation (ii) has the solution $(1, 4, 1)$, from which we can conclude that (iii) has the solution $(1, 4, 1)$ as well. So -1 and 17 are also contained in the image of α. Thus,

$$im\ \alpha = \{\pm 1, \pm 17 \left(\text{mod } \mathbb{Q}^{*2}\right)\}$$

which has order 4.

Now let's consider $E' : y^2 = x^3 + 68x$. The only factors of 68 are ± 1, ± 2, ± 4, ± 17, ± 34 and ± 68. Since $\pm 4 \equiv \pm 1 \left(\text{mod } \mathbb{Q}^{*2}\right)$ and $\pm 68 \equiv \pm 17 \left(\text{mod } \mathbb{Q}^{*2}\right)$, we can narrow our list of factors to ± 1, ± 2, ± 17 and ± 34. So we have the following equations to consider:

(i) $N^2 = M^4 + 68e^4$

(ii) $N^2 = -M^4 - 68e^4$

(iii) $N^2 = 2m^4 + 34e^4$

(iv) $N^2 = -2M^4 - 34e^4$

(v) $N^2 = 17m^4 + 4e^4$

(vi) $N^2 = -17M^4 - 4e^4$

(vii) $N^2 = 34m^4 + 2e^4$

(viii) $N^2 = -34M^4 - 2e^4$.

Clearly, (ii), (iv), (vi) and (viii) have no solutions. Also, (iii) and (vii) are the same. So we only have to consider (i), (iii) and (v). Equation (i) has the trivial solution $(1, 1, 0)$. Equations (iii) and (vii) have the solution $(1, 6, 1)$. Finally, equation (v) has the solution $(1, 9, 2)$. Thus,

$$im\ \alpha' = \{1, 2, 17, 34 \pmod{\mathbb{Q}^{*2}}\}$$

which has order 4. So by (2.13), the rank of $E(\mathbb{Q})$ is 2. □

For curves of the form $E\colon y^2 = x^3 + bx$, the rank of $E(\mathbb{Q})$ for various values of b is given below for reference [Hus, p. 37].

Rank	b
0	1, 2, 4, 6, 7, 10, 11, 12, 22
	-1, -3, -4, -8, -9, -11, -13, -18, -19
1	3, 5, 8, 9, 13, 15, 18, 19, 20
	-2, -5, -6, -7, -10, -12, -14, -15, -20
2	14, 33, 34, 39, 46
	-17, -56, -65, -77
3	82

Table 2.1: Values of the rank r for $E\colon y^2 = x^3 + bx$

One of the many unanswered questions regarding the rank of elliptic curves is the Birch and Swinnerton-Dyer conjecture, a Millennium Prize Problem. Bryan Birch and Peter Swinnerton-Dyer, with the help of computer computation, posed the following conjecture in the 1960's:

> Let E be an elliptic curve of a number field K. Let $L(E, s)$ be defined as
>
> $$L(E, s) = \prod_p L_p(E, s)^{-1}$$

where, for a given prime p,

$$L_p(E,s) = \begin{cases} (1 - a_p p^{-s} + p^{1-2s}), & \text{if } p \nmid N \\ (1 - a_p p^{-s}), & \text{if } p \,||\, N \\ 1, & \text{if } p^2 \mid N \end{cases}$$

where, in the case of good reduction, a_p is $p + 1-$(number of points of E mod p), and in the case of multiplicative reduction, a_p is ± 1 depending on whether E has split or non-split multiplicative reduction at p.

The rank of the abelian group $E(K)$ of points of E is the order of the zero of $L(E,s)$ at $s = 1$, and the first non-zero coefficient in the Taylor expansion of $L(E,s)$ at $s = 1$ is given by more refined arithmetic data attached to E over K.

Currently, the conjecture has only been proven true in special cases, and nothing has been proven for curves with rank greater than 1.

Chapter 3

Curves of the Form $y^2 = x^3 + c$

In this chapter, we will discuss how the results in Chapter 2 will differ if we change our curve from $E: y^2 = x^3 + ax^2 + bx + c$ to $E: y^2 = x^3 + c$, where $c \in \mathbb{Q}^*$. Much of what we will do will parallel Chapter 2, however, there are differences. The homomorphisms ϕ and ψ will change. As a consequence, the composition $(\psi \circ \phi)(P)$ will change from $2P$ to $3P$, giving us a new formula for the rank of E. Also, you may recall that the map α and our method for computing the rank of specific curves relied heavily on b. So how will the map α change, and how will we compute the rank for our new curve for which $b = 0$?

3.1 Homomorphisms for the New Curve

Theorem 3.1.1. *Let E be an elliptic curve of the form $E: y^2 = x^3 + c$, $c \in \mathbb{Q}^*$.*

(i) *The points $(0, \pm\sqrt{c})$ are inflection points and have order 3 on E.*

(ii) *For* $P = (x, y) \neq \mathcal{O} \in E(\mathbb{Q})$,

$$P \oplus (0, \sqrt{c}) \quad = \quad \begin{cases} \left(\frac{-2x\sqrt{c}}{y+\sqrt{c}}, \frac{\sqrt{c}(y-3\sqrt{c})}{y+\sqrt{c}} \right) & \text{if } y \neq -\sqrt{c}, \\ \mathcal{O} & \text{if } y = -\sqrt{c} \end{cases}$$

and

$$P \oplus (0, -\sqrt{c}) \quad = \quad \begin{cases} \left(\frac{2x\sqrt{c}}{y-\sqrt{c}}, \frac{-\sqrt{c}(y+3\sqrt{c})}{y-\sqrt{c}} \right) & \text{if } y \neq \sqrt{c}, \\ \mathcal{O} & \text{if } y = \sqrt{c}. \end{cases}$$

(iii) *Let* $(x_1, y_1) = (x, y) \oplus (0, \sqrt{c})$ *and* $(x_2, y_2) = (x, y) \oplus (0, -\sqrt{c})$. *Then*

$$(x + x_1 + x_2, y + y_1 + y_2) = \left(\frac{x^3 + 4c}{x^2}, \frac{y^3 - 9cy}{x^3} \right) \text{ if } (x, y) \neq (0, \pm\sqrt{c}),$$

and this is a rational point of the elliptic curve $E' : y^2 = x^3 - 27c$.

Proof.

(i) Recall that a point on E is an inflection point if and only if $3P = \mathcal{O}$. Thus, it suffices to show that $(0, \pm\sqrt{c})$ have order 3 on E. For $P = (0, \pm\sqrt{c}) \in E$, since a and b both equal zero, by formulas (1.4) and (1.5),

$$\begin{aligned} 2P &= \left(0, \frac{-8c^2}{8(\pm\sqrt{c})^3} \right) \\ &= \left(0, \mp\sqrt{c} \right). \end{aligned}$$

Thus, $2P = -P$, implying that $3P = \mathcal{O}$.

(ii) Recall that given two points (x_1, y_1) and (x_2, y_2), the formula $x_3 = m^2 - x_2 - x_1$ gives the x-coordinate of the point (x_3, y_3) where $(x_3, y_3) = (x_1, y_1) \oplus (x_2, y_2)$ and m is the slope of the line that passes through the given points. Considering the case

of $(x,y) \oplus (0,\sqrt{c})$ where $(x,y) \neq (0,\pm\sqrt{c})$ we have the following:

$$\begin{aligned} x_3 &= \left(\frac{y-\sqrt{c}}{x}\right)^2 - x \\ &= \frac{y^2 - 2y\sqrt{c} + c - x^3}{x^2} \\ &= \frac{(x^3+c) - 2y\sqrt{c} + c - x^3}{x^2} \\ &= \frac{2c - 2y\sqrt{c}}{x^2} \\ &= \frac{-2\sqrt{c}(y-\sqrt{c})}{x^2} \\ &= \frac{-2x\sqrt{c}(y-\sqrt{c})}{x^3} \\ &= \frac{-2x\sqrt{c}(y-\sqrt{c})}{y^2-c} \\ &= \frac{-2x\sqrt{c}}{y+\sqrt{c}}. \end{aligned}$$

Substituting this result into $y^2 = x^3 + c$ to get the y-coordinate, we have that $(x,y) \oplus (0,\sqrt{c}) = \left(\frac{-2x\sqrt{c}}{y+\sqrt{c}}, \frac{\sqrt{c}(y-3\sqrt{c})}{y+\sqrt{c}}\right)$. Using the same process, it can be shown that $(x,y) \oplus (0,-\sqrt{c}) = \left(\frac{2x\sqrt{c}}{y-\sqrt{c}}, \frac{-\sqrt{c}(y+3\sqrt{c})}{y-\sqrt{c}}\right)$ for $(x,y) \neq (0,\pm\sqrt{c})$. If $(x,y) = (0,\sqrt{c})$, we showed in part (i) using the duplication formula that $2(0,\sqrt{c}) = (0,-\sqrt{c})$. Substituting $(0,\sqrt{c})$ into $\left(\frac{-2x\sqrt{c}}{y+\sqrt{c}}, \frac{\sqrt{c}(y-3\sqrt{c})}{y+\sqrt{c}}\right)$ gives is the desired result of $(0,-\sqrt{c})$. The same is true for $(x,y) = (0,-\sqrt{c})$. Finally, it is clear that $(0,\pm\sqrt{c}) \oplus (0,\mp\sqrt{c}) = \mathcal{O}$ since the two points are additive inverses and elliptic curves are symmetric about the x-axis.

(iii) Since $(x_1,y_1) = (x,y) \oplus (0,\sqrt{c})$ and $(x_2,y_2) = (x,y) \oplus (0,-\sqrt{c})$, we know from (ii) that

$$(x_1,y_1) = \left(\frac{-2x\sqrt{c}}{y+\sqrt{c}}, \frac{\sqrt{c}(y-3\sqrt{c})}{y+\sqrt{c}}\right) \quad \text{and} \quad (x_2,y_2) = \left(\frac{2x\sqrt{c}}{y-\sqrt{c}}, \frac{-\sqrt{c}(y+3\sqrt{c})}{y-\sqrt{c}}\right).$$

Hence, we have the following result:

$$\begin{aligned}
& (x + x_1 + x_2, y + y_1 + y_2) \\
= \; & \left(x + \left(\tfrac{-2x\sqrt{c}}{y+\sqrt{c}}\right) + \left(\tfrac{2x\sqrt{c}}{y-\sqrt{c}}\right), y + \left(\tfrac{\sqrt{c}(y-3\sqrt{c})}{y+\sqrt{c}}\right) + \left(\tfrac{-\sqrt{c}(y+3\sqrt{c})}{y-\sqrt{c}}\right)\right) \\
= \; & \left(\tfrac{x(y^2-c)-2x\sqrt{c}(y-\sqrt{c})+2x\sqrt{c}(y+\sqrt{c})}{y^2-c}, \tfrac{y(y^2-c)+\sqrt{c}(y^2-4y\sqrt{c}+3c)-\sqrt{c}(y^2+4y\sqrt{c}+3c)}{y^2-c}\right) \\
= \; & \left(\tfrac{xy^2+3cx}{y^2-c}, \tfrac{y^3-9cy}{y^2-c}\right) \\
= \; & \left(\tfrac{x(y^2+3c)}{x^3}, \tfrac{y^3-9cy}{x^3}\right) \\
= \; & \left(\tfrac{y^2+3c}{x^2}, \tfrac{y^3-9cy}{x^3}\right) \\
= \; & \left(\tfrac{(x^3+c)+3c}{x^2}, \tfrac{y^3-9cy}{x^3}\right) \\
= \; & \left(\tfrac{x^3+4c}{x^2}, \tfrac{y^3-9cy}{x^3}\right).
\end{aligned}$$

To simplify the result above, we used the fact that if $(x, y) \in E$, then $y^2 = x^3 + c$.

It remains to show that $(x + x_1 + x_2, y + y_1 + y_2)$ is a rational point of the elliptic curve $E' : y^2 = x^3 - 27c$. We know that $c \in \mathbb{Q}$ and $(x, y) \in E(\mathbb{Q})$. It follows that $\left(\tfrac{x^3+4c}{x^2}, \tfrac{y^3-9cy}{x^3}\right)$ is a rational point since the rational numbers are a field and are therefore closed under the operations presented above.

Now let's show that $\left(\tfrac{x^3+4c}{x^2}, \tfrac{y^3-9cy}{x^3}\right)$ is on the curve $y^2 = x^3 - 27c$.

$$\text{LHS:} \qquad \left(\frac{y^3 - 9cy}{x^3}\right)^2 = \frac{y^6 - 18cy^4 + 81c^2y^2}{x^6}$$

$$\begin{aligned}
\text{RHS:} \quad \left(\frac{x^3 + 4c}{x^2}\right)^3 - 27c &= \left(\frac{(y^2 - c) + 4c}{x^2}\right)^3 - 27c \\
&= \frac{y^6 + 9cy^4 + 27c^2y^2 + 27c^3 - 27cx^6}{x^6} \\
&= \frac{y^6 + 9cy^4 + 27c^2y^2 + 27c^3 - 27c(y^2 - c)^2}{x^6} \\
&= \frac{y^6 - 18cy^4 + 81c^2y^2}{x^6}
\end{aligned}$$

Therefore,

$$(x + x_1 + x_2, y + y_1 + y_2) = \left(\frac{x^3 + 4c}{x^2}, \frac{y^3 - 9cy}{x^3} \right) \text{ if } (x, y) \neq (0, \pm\sqrt{c}),$$

and is a rational point of the elliptic curve $E' \colon y^2 = x^3 - 27c$.

□

In Chapter 2, we discovered the homomorphisms $\phi \colon E \to E'$ and $\psi \colon E' \to E$. There exist similar homomorphisms for curves of the form $y^2 = x^3 + c$. We want to show that the formula in part (iii) above is the desired map ϕ, but before we can prove that is true, we will need an important theorem.

Theorem 3.1.2 (Vélu's Theorem [V71])**.** *Let E and E' be elliptic curves of the form $y^2 = x^3 + bx + c$. Let $\phi \colon E \to E'$ be defined as*

$$\phi(P) = \Big(x + \sum_{Q \in K - \{\mathcal{O}\}} \big(x(P \oplus Q) - x(Q) \big),\ y + \sum_{Q \in K - \{\mathcal{O}\}} \big(y(P \oplus Q) - y(Q) \big) \Big)$$

where K is the kernel of ϕ and $P = (x, y) \notin F$. If K is of odd order, then ϕ is a homomorphism.

Now, let us prove that the formula from part (iii) above is indeed a homorphism.

Proposition 3.1.3. *Let E and E' be the elliptic curves given by the equations*

$$E \colon y^2 = x^3 + c \quad \textit{and} \quad E' \colon y^2 = x^3 + \overline{c},$$

where

$$\overline{c} = -27c.$$

Let $T_1 = (0, \sqrt{c})$ and $T_2 = (0, -\sqrt{c}) \in E$.

(a) *There is a homomorphism $\phi \colon E \to E'$ defined by*

$$\phi(P) = \begin{cases} \left(\frac{x^3+4c}{x^2}, \frac{y^3-9cy}{x^3} \right), & \text{if } P = (x, y) \neq \mathcal{O}, T_1, T_2 \\ \overline{\mathcal{O}}, & \text{if } P = \mathcal{O}, T_1, T_2. \end{cases}$$

The kernel of ϕ is $\{\mathcal{O}, T_1, T_2\}$.

(b) *Applying the same process to E' gives a map $\overline{\phi}\colon E' \to E''$. The curve E'' is isomorphic to E via the map $(x,y) \to \left(\frac{x}{9}, \frac{y}{27}\right)$. There is thus a homomorphism $\psi\colon E' \to E$ defined by*

$$\psi(\overline{P}) = \begin{cases} \left(\frac{\overline{x}^3+4\overline{c}}{9\overline{x}^2}, \frac{\overline{y}^3-9\overline{cy}}{27\overline{x}^3}\right), & \text{if } \overline{P} = (\overline{x},\overline{y}) \neq \overline{\mathcal{O}}, \overline{T}_1, \overline{T}_2 \\ \mathcal{O}, & \text{if } \overline{P} = \overline{\mathcal{O}}, \overline{T}_1, \overline{T}_2. \end{cases}$$

Proof. From formula (1.3), we have that

$$P \oplus T_1 = \left(\frac{2c - 2\sqrt{c}y}{x^2}, \frac{c\sqrt{c} - 4cy + 3\sqrt{c}y^2}{x^3}\right)$$

and

$$P \oplus T_2 = \left(\frac{2c + 2\sqrt{c}y}{x^2}, \frac{-c\sqrt{c} - 4cy - 3\sqrt{c}y^2}{x^3}\right).$$

Since *ker* ϕ has odd order and E is of the form $y^2 = x^3 + 0x + c$, we can use Vélu's theorem to compute the homomorphism ϕ. Thus,

$$\begin{aligned}
\phi(P) &= \left(x + \sum_{i=1}^{2}\big(x(P \oplus T_i) - x(T_i)\big), y + \sum_{i=1}^{2}\big(y(P \oplus T_i) - y(T_i)\big)\right) \\
&= \left(x + x(P \oplus T_1) + x(P \oplus T_2), y + y(P \oplus T_1) - \sqrt{c} + y(P \oplus T_2) + \sqrt{c}\right) \\
&= \left(x + x(P \oplus T_1) + x(P \oplus T_2), y + y(P \oplus T_1) + y(P \oplus T_2)\right) \\
&= \left(x + \frac{2c - 2\sqrt{c}y}{x^2} + \frac{2c + 2\sqrt{c}y}{x^2}, y + \frac{c\sqrt{c} - 4cy + 3\sqrt{c}y^2}{x^3} + \frac{-c\sqrt{c} - 4cy - 3\sqrt{c}y^2}{x^3}\right) \\
&= \left(\frac{x^3 + 4c}{x^2}, \frac{x^3y - 8cy}{x^3}\right) \\
&= \left(\frac{x^3 + 4c}{x^2}, \frac{(y^2 - c)y - 8cy}{x^3}\right) \\
&= \left(\frac{x^3 + 4c}{x^2}, \frac{y^3 - 9cy}{x^3}\right).
\end{aligned}$$

It can be easily shown that ψ is indeed a homomorphism as well. □

Proposition 3.1.4. *Let ϕ and ψ be the homomorphisms described above. If $P = (x,y) \in E(\mathbb{Q})$ where $E\colon y^2 = x^3 + c$ for $c \in \mathbb{Q}^*$ then $(\psi \circ \phi)(P) = 3P$.*

Proof. Let's start by considering $P \neq \mathcal{O}, T_1$ or T_2. Note that a and b are both zero for

E. Thus, formulas (1.4) and (1.5) reduce to

$$2P = \left(\frac{x^4 - 8cx}{4y^2}, \frac{x^6 + 20cx^3 - 8c^2}{8y^3} \right).$$

By (1.3) we have that

$$\begin{aligned}
x(2P \oplus P) &= \left(\frac{\frac{x^6+20cx^3-8c^2}{8y^3} - y}{\frac{x^4-8cx}{4y^2} - x} \right)^2 - \frac{x^4 - 8cx}{4y^2} - x \\
&= \left(\frac{\frac{x^6+20cx^3-8c^2-8y^4}{8y^3}}{\frac{x^4-8cx-4xy^2}{4y^2}} \right)^2 - \frac{x^4 - 8cx}{4y^2} - x \\
&= \left(\frac{x^6 + 20cx^3 - 8c^2 - 8(x^3+c)^2}{2y(x^4 - 8cx - 4x(x^3+c))} \right)^2 - \frac{x^4 - 8cx}{4y^2} - x \\
&= \left(\frac{-7x^6 + 4cx^3 - 16c^2}{2y(-3x^4 - 12cx)} \right)^2 - \frac{x^4 - 8cx}{4y^2} - x \\
&= \frac{(-7x^6 + 4cx^3 - 16c^2)^2 - (x^4 - 8cx)(-3x^4 - 12cx)^2 - x(4y^2)(-3x^4 - 12cx)^2}{4y^2(-3x^4 - 12cx)^2} \\
&= \frac{4(10x^{12} - 14x^9 + 168c^2x^6 + 256c^3x^3 + 64c^4 - y^2(9x^9 + 72cx^6 + 144c^2x^3))}{36x^2y^2(x^3 + 4c)^2} \\
&= \frac{4((x^3+c)(10x^9 - 24cx^6 + 192c^2x^3 + 64c^3) - y^2(9x^9 + 72cx^6 + 144c^2x^3))}{36x^2y^2(x^3 + 4c)^2} \\
&= \frac{4(y^2(10x^9 - 24cx^6 + 192c^2x^3 + 64c^3) - y^2(9x^9 + 72cx^6 + 144c^2x^3))}{36x^2y^2(x^3 + 4c)^2} \\
&= \frac{x^9 - 96cx^6 + 48c^2x^3 + 64c^3}{9x^2(x^3 + 4c)^2}.
\end{aligned}$$

From (1.3) and the computations above,

$$\begin{aligned}
y(2P \oplus P) &= -\left(\tfrac{-7x^6+4cx^3-16c^2}{2y(-3x^4-12cx)} \right) \left(\tfrac{x^9-96cx^6+48c^2x^3+64c^3}{9x^2(x^3+4c)^2} \right) - \left[y - \left(\tfrac{-7x^6+4cx^3-16c^2}{2y(-3x^4-12cx)} \right) x \right] \\
&= \left(\tfrac{(7x^6-4cx^3+16c^2)(x^9-96cx^6+48c^2x^3+64c^3)}{18x^2y(-3x^4-12cx)(x^3+4c)^2} \right) - \left(\tfrac{2y^2(-3x^4-12cx)+7x^7-4cx^4+16c^2x}{2y(-3x^4-12cx)} \right) \\
&= \tfrac{7x^{15}-676cx^{12}+736c^2x^9-128c^3x^6+512c^4x^3+1024c^5-9x^2(x^3+4c)^2(x^7-34cx^4-8c^2x)}{18x^2y(-3x^4-12cx)(x^3+4c)^2} \\
&= -\tfrac{2(x^9+228cx^6+48c^2x^3+64c^3)(x^3+c)(x^3-8c)}{18x^2y(-3x^4-12cx)(x^3+4c)^2} \\
&= \tfrac{y(x^3-8c)(x^9+228cx^6+48c^2x^3+64c^3)}{27x^3(x^3+4c)^3}.
\end{aligned}$$

Thus,

$$3P = \left(\frac{x^9 - 96cx^6 + 48c^2x^3 + 64c^3}{9x^2(x^3+4c)^2}, \frac{y(x^3-8c)(x^9+228cx^6+48c^2x^3+64c^3)}{27x^3(x^3+4c)^3} \right).$$

Now,

$$\begin{aligned}
(\psi \circ \phi)(x,y) &= \psi(\phi(x,y)) \\
&= \psi\left(\tfrac{x^3+4c}{x^2}, \tfrac{y^3-9cy}{x^3}\right) \\
&= \left(\frac{\left(\frac{x^3+4c}{x^2}\right)^3 + 4(-27c)}{9\left(\frac{x^3+4c}{x^2}\right)^2}, \frac{\left(\frac{y^3-9cy}{x^3}\right)^3 - 9(-27c)\left(\frac{y^3-9cy}{x^3}\right)}{27\left(\frac{x^3+4c}{x^2}\right)^3} \right) \\
&= \left(\tfrac{x^9-96cx^6+48c^2x^3+64c^3}{9x^2(x^3+4c)^2}, \tfrac{y(x^3-8c)(x^9+228cx^6+48c^2x^3+64c^3)}{27x^3(x^3+4c)^3} \right).
\end{aligned}$$

It is clear that if $P = \mathcal{O}, T_1$ or T_2, then $3P = \mathcal{O}$ and $(\psi \circ \phi)(P) = \mathcal{O}$. Therefore, $(\psi \circ \phi)(P) = 3P$. □

Recall that $\mathbb{Q}(\sqrt{c})^*$ is the multiplicative group whose elements are of the form $m + n\sqrt{c}$, where m and n are elements of $\mathbb{Q}$, and $\mathbb{Q}(\sqrt{c})^{*3}$ is the subgroup of the cubes of the elements of $\mathbb{Q}(\sqrt{c})^*$.

Proposition 3.1.5 (Properties of $\psi\colon E'(\mathbb{Q}) \to E(\mathbb{Q})$)**.**

(i) $\mathcal{O} \in \psi\big(E'(\mathbb{Q})\big)$.

(ii) $T_2 \in \psi\big(E'(\mathbb{Q})\big)$ *if and only if* $c = 2^{6j-2}m^{6k}$ *where* $j, k \in \mathbb{Z}$ *and* $m \in \mathbb{Q}$.

(iii) *Let* $P = (x,y) \neq \mathcal{O} \in E(\mathbb{Q})$ *with* $y \neq -\sqrt{c}$. *Then* $P \in \psi\big(E'(\mathbb{Q})\big)$ *if and only if* $y + \sqrt{c} \equiv 1 \pmod{\mathbb{Q}(\sqrt{c})^{*3}}$.

Proof.

(i) Recall that $\overline{\mathcal{O}}$ is considered rational and is therefore an element of $E'(\mathbb{Q})$. Thus by the definition of ψ, it follows that $\mathcal{O} \in \psi\big(E'(\mathbb{Q})\big)$.

(ii) ($\Rightarrow$) Let $T_2 \in \psi\big(E'(\mathbb{Q})\big)$. Then there exists $(x,y) \in E'(\mathbb{Q})$ such that $\psi(x,y) = (0, -\sqrt{c})$. From the definition of ψ, we can conclude that $x^3 - 108c = 0$, giving us that $x^3 = 108c$. Since $(x,y) \in E'(\mathbb{Q})$, it follows that $y^2 = x^3 - 27c$, or equivalently

$y = \pm\sqrt{x^3 - 27c}$. Substituting $x^3 = 108c$ into $y = \pm\sqrt{x^3 - 27c}$, we have that $y = \pm\sqrt{81c} = \pm 9\sqrt{c}$. Since $y \in \mathbb{Q}$, it must be that c is a perfect square. Also, since $x = \sqrt[3]{108c} = 3\sqrt[3]{4c}$ and $x \in \mathbb{Q}$, we can conclude that $4c$ must be a perfect cube. Therefore, $c = 2^{6j-2}m^{6k}$ where $j, k \in \mathbb{Z}$ and $m \in \mathbb{Q}$.

($\Leftarrow$) Let $c = 2^{6j-2}m^{6k}$ where $j, k \in \mathbb{Z}$ and $m \in \mathbb{Q}$. Then

$$(x, y) = \left(3 \cdot 2^{2j} m^{2k}, -3^2 2^{3j-1} m^{3k}\right) \in E'(\mathbb{Q})$$

and $\psi(x, y) = T_2$. Therefore, $T_2 \in \psi\big(E'(\mathbb{Q})\big)$.

(iii) ($\Rightarrow$) Let $P = (x, y) \neq \mathcal{O} \in E(\mathbb{Q})$ with $y \neq -\sqrt{c}$, and let $P \in \psi\big(E'(\mathbb{Q})\big)$. Then by the definition of ψ, there exists $(x_1, y_1) \in E'(\mathbb{Q})$ such that

$$(x, y) = \left(\frac{x_1^3 - 108c}{9x_1^2}, \frac{y_1^3 + 243cy_1}{27x_1^3}\right).$$

Thus,

$$\begin{aligned}
y + \sqrt{c} &= \frac{y_1^3 + 243cy_1}{27x_1^3} + \sqrt{c} \\
&= \frac{y_1^3 + 3^5 cy_1 + 3^3 x_1^3 c^{1/2}}{27x_1^3} \\
&= \frac{y_1^3 + 3^5 cy_1 + 3^3 (y_1^2 + 27c) c^{1/2}}{27x_1^3} \\
&= \frac{y_1^3 + 3^3 c^{1/2} y_1^2 + 3^5 cy_1 + 3^6 c^{3/2}}{27x_1^3} \\
&= \left(\frac{y_1 + 9\sqrt{c}}{3x_1}\right)^3 \\
&\equiv 1 \ \big(\mathrm{mod}\ \mathbb{Q}(\sqrt{c})^{*3}\big).
\end{aligned}$$

($\Leftarrow$) Let $P = (x, y) \neq \mathcal{O} \in E(\mathbb{Q})$ with $y \neq -\sqrt{c}$, and let $y + \sqrt{c} \equiv 1 \ \big(\mathrm{mod}\ \mathbb{Q}(\sqrt{c})^{*3}\big)$. Then $y + \sqrt{c} = t^3$ for some $t \in \mathbb{Q}(\sqrt{c})^*$. Let $\bar{t} = \frac{x}{t}$, which is well defined as $t \neq 0$. It follows that $\bar{t}^3 = \frac{x^3}{t^3} = y - \sqrt{c}$ and $t\bar{t} = x$. Since t and $\bar{t} \in \mathbb{Q}(\sqrt{c})^*$, we know that $t = r + s\sqrt{c}$ and $\bar{t} = r - s\sqrt{c}$ where $r, s \in \mathbb{Q}$. So

$$t + \bar{t} = 2r \qquad \text{and} \qquad t - \bar{t} = 2s\sqrt{c}. \tag{3.1}$$

Also, note that

$$t^3 - \bar{t}^3 = 2\sqrt{c} \qquad \text{and} \qquad t^3 + \bar{t}^3 = 2y. \tag{3.2}$$

Consider

$$(x_1, y_1) = \left(\frac{6\sqrt{c}}{t - \bar{t}}, \frac{9\sqrt{c}(t + \bar{t})}{t - \bar{t}} \right),$$

which is well defined as $t \neq \bar{t}$. We claim that $(x_1, y_1) \in E'(\mathbb{Q})$ and $\psi(x_1, y_1) = (x, y)$. Let's start by showing that $(x_1, y_1) \in E'(\mathbb{Q})$. Using (3.1), we have the following simplifications:

$$\begin{aligned} (x_1, y_1) &= \left(\frac{6\sqrt{c}}{t - \bar{t}}, \frac{9\sqrt{c}(t + \bar{t})}{t - \bar{t}} \right) \\ &= \left(\frac{6\sqrt{c}}{2s\sqrt{c}}, \frac{9\sqrt{c}(2r)}{2s\sqrt{c}} \right) \\ &= \left(\frac{3}{s}, \frac{9r}{s} \right). \end{aligned}$$

Since $r, s \in \mathbb{Q}$, it follows that x_1 and y_1 are rational.

Now let's show that (x_1, y_1) satisfies $y^2 = x^3 - 27c$. Consider the following:

$$\begin{aligned} 3(t + \bar{t})^2 &= 4(t^2 + t\bar{t} + \bar{t}^2) - (t - \bar{t})^2 \\ 3(t - \bar{t})(t + \bar{t})^2 &= 4(t - \bar{t})(t^2 + t\bar{t} + \bar{t}^2) - (t - \bar{t})^3 \\ 3(t - \bar{t})(t + \bar{t})^2 &= 4(t^3 - \bar{t}^3) - (t - \bar{t})^3. \end{aligned}$$

By (3.2),

$$\begin{aligned}
3(t-\bar{t})(t+\bar{t})^2 &= 8\sqrt{c}-(t-\bar{t})^3 \\
81c(t-\bar{t})(t+\bar{t})^2 &= 216c\sqrt{c}-27c(t-\bar{t})^3 \\
\frac{81c(t+\bar{t})^2}{(t-\bar{t})^2} &= \frac{216c\sqrt{c}}{(t-\bar{t})^3}-27c \\
\left(\frac{9\sqrt{c}(t+\bar{t})}{t-\bar{t}}\right)^2 &= \left(\frac{6\sqrt{c}}{t-\bar{t}}\right)^3-27c \\
y_1^2 &= x_1^3-27c.
\end{aligned}$$

Therefore, $(x_1, y_1) \in E'(\mathbb{Q})$.

Now let's show that $\psi(x_1, y_1) = (x, y)$. From the definition of ψ, we have

$$\begin{aligned}
\psi(x_1,y_1) &= \psi\left(\frac{6\sqrt{c}}{t-\bar{t}}, \frac{9\sqrt{c}(t+\bar{t})}{t-\bar{t}}\right) \\
&= \left(\frac{\left(\frac{6\sqrt{c}}{t-\bar{t}}\right)^3-108c}{9\left(\frac{6\sqrt{c}}{t-\bar{t}}\right)^2}, \frac{\left(\frac{9\sqrt{c}(t+\bar{t})}{t-\bar{t}}\right)^3+243c\left(\frac{9\sqrt{c}(t+\bar{t})}{t-\bar{t}}\right)}{27\left(\frac{6\sqrt{c}}{t-\bar{t}}\right)^3}\right) \\
&= \left(\frac{2^3 3^3 c\sqrt{c}-2^2 3^3 c(t-\bar{t})^3}{2^2 3^4 c(t-\bar{t})}, \frac{3^6 c\sqrt{c}(t+\bar{t})^3+3^7 c\sqrt{c}(t+\bar{t})(t-\bar{t})^2}{2^3 3^6 c\sqrt{c}}\right) \\
&= \left(\frac{2\sqrt{c}-(t-\bar{t})^3}{3(t-\bar{t})}, \frac{(t+\bar{t})^3+3(t+\bar{t})(t-\bar{t})^2}{8}\right) \\
&= \left(\frac{3t^2\bar{t}+3t\bar{t}^2}{3(t-\bar{t})}, \frac{(t+\bar{t})(t^2-t\bar{t}+\bar{t}^2)}{2}\right) \\
&= \left(\frac{3t\bar{t}(t-\bar{t})}{3(t-\bar{t})}, \frac{t^3+\bar{t}^3}{2}\right) \\
&= (x,y).
\end{aligned}$$

Therefore, we have $P \in \psi\big(E'(\mathbb{Q})\big)$.

□

Let $\alpha\colon E(\mathbb{Q}) \to \mathbb{Q}(\sqrt{c})^*/\mathbb{Q}(\sqrt{c})^{*3}$ be the map defined by

$$\alpha(P) = \begin{cases} y + \sqrt{c} \pmod{\mathbb{Q}(\sqrt{c})^{*3}}, & \text{if } P = (x,y) \neq \mathcal{O}, (0, -\sqrt{c}), \\ 1 \pmod{\mathbb{Q}(\sqrt{c})^{*3}}, & \text{if } P = \mathcal{O}, \\ 4c \pmod{\mathbb{Q}(\sqrt{c})^{*3}}, & \text{if } P = (0, -\sqrt{c}). \end{cases}$$

Proposition 3.1.6.

(i) *The map $\alpha\colon E(\mathbb{Q}) \to \mathbb{Q}(\sqrt{c})^*/\mathbb{Q}(\sqrt{c})^{*3}$ described above is a homomorphism.*

(ii) *The kernel of α is the image $\psi\big(E'(\mathbb{Q})\big)$.*

Proof.

(i) We will use the same strategy as that of Proposition 2.2.4. That is, we will show that α takes inverses to inverses and that if $P_1 \oplus P_2 \oplus P_3 = \mathcal{O}$, then $\alpha(P_1)\alpha(P_2)\alpha(P_3) \equiv 1 \big(\mathrm{mod}\ \mathbb{Q}(\sqrt{c})^{*3}\big)$.

Let $P = (x,y) \neq \mathcal{O}$ or $(0, \pm\sqrt{c})$. Then

$$\begin{aligned} \alpha(-P) &= \alpha(x, -y) \\ &= -y + \sqrt{c} \\ &\equiv \frac{1}{(-y+\sqrt{c})^2} \ \big(\mathrm{mod}\ \mathbb{Q}(\sqrt{c})^{*3}\big) \\ &= \left(\frac{y+\sqrt{c}}{y^2 - c}\right)^2 \\ &= \frac{(y+\sqrt{c})^2}{x^3} \\ &\equiv (y+\sqrt{c})^2 \ \big(\mathrm{mod}\ \mathbb{Q}(\sqrt{c})^{*3}\big) \\ &= \alpha(P)^{-1}. \end{aligned}$$

If $P = \mathcal{O}$, it is clear that $\alpha(-P) = \alpha(P)^{-1}$. If $P = (0, \sqrt{c})$, then $\alpha(P) = 2\sqrt{c}$. So $\alpha(P)^{-1} = 4c$. Now $\alpha(-P) = \alpha(0, -\sqrt{c}) \equiv 4c \ \big(\mathrm{mod}\ \mathbb{Q}(\sqrt{c})^{*3}\big)$, as desired. Hence, α sends inverses to inverses.

Let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ and $P_3 = (x_3, y_3)$ be distinct from $\mathcal{O}$ and $(0, -\sqrt{c})$. Assume that $P_1 \oplus P_2 \oplus P_3 = \mathcal{O}$ and let $y = mx + v$ be the line that passes through all three points, or equivalently $x = \frac{y-v}{m}$. Let's find the intersection of this line with the curve E:

$$\begin{aligned} x^3 &= y^2 - c \\ \left(\frac{y-v}{m}\right)^3 &= y^2 - c \\ \frac{y^3 - 3y^2v + 3yv^2 - v^3}{m^3} &= y^2 - c \\ y^3 - (3v + m^3)y^2 + 3v^2y + cm^3 - v^3 &= 0. \end{aligned} \tag{3.3}$$

Since P_1, P_2 and P_3 are the intersections of the line $y = mx + v$ with E, then y_1, y_2 and y_3 are roots of (3.3). It follows that

$$\begin{aligned} & y^3 - (3v + m^3)y^2 + 3v^2y + cm^3 - v^3 \\ = \; & (y - y_1)(y - y_2)(y - y_3) \\ = \; & y^3 - (y_1 + y_2 + y_3)y^2 + (y_1y_2 + y_1y_3 + y_2y_3)y - y_1y_2y_3. \end{aligned}$$

Equating the coefficients, we have that

$$\begin{aligned} 3v + m^3 &= y_1 + y_2 + y_3 \\ 3v^2 &= y_1y_2 + y_1y_3 + y_2y_3 \\ v^3 - cm^3 &= y_1y_2y_3. \end{aligned}$$

Now let's show that $\alpha(P_1)\alpha(P_2)\alpha(P_3) \equiv 1 \left(\mathrm{mod}\ \mathbb{Q}(\sqrt{c})^{*3}\right)$. Using the definition of

α and the equations above,

$$\begin{aligned}
\alpha(P_1)\alpha(P_2)\alpha(P_3) &= (y_1+\sqrt{c})(y_2+\sqrt{c})(y_3+\sqrt{c}) \\
&= y_1y_2y_3 + (y_1y_2+y_1y_3+y_2y_3)\sqrt{c} + (y_1+y_2+y_3)(\sqrt{c})^2 + (\sqrt{c})^3 \\
&= v^3 - cm^3 + 3v^2\sqrt{c} + (3v+m^3)(\sqrt{c})^2 + (\sqrt{c})^3 \\
&= v^3 + 3v^2\sqrt{c} + 3v(\sqrt{c})^2 + (\sqrt{c})^3 \\
&= (v+\sqrt{c})^3 \\
&\equiv 1 \pmod{\mathbb{Q}(\sqrt{c})^{*3}}.
\end{aligned}$$

As with the proof of Proposition 2.2.4, the other cases can be easily checked.

(ii) It is clear from the definition of α and Proposition 3.1.5 that $\mathcal{O} \in \ker\ \alpha$ and $\mathcal{O} \in \mathit{im}\ \psi$.

Let $T_2 \in \psi\big(E'(\mathbb{Q})\big)$. Then by Proposition 3.1.5, $c = 2^{6j-2}m^{6k}$, giving us that $4c = 2^{6j}m^{6k} = \big(2^{2j}m^{2k}\big)^3 \equiv 1 \pmod{\mathbb{Q}(\sqrt{c})^{*3}}$. Hence, $T_2 \in \ker\ \alpha$. To show containment the other way, assume $T_2 \in \ker\ \alpha$. Then $T_2 \in E(\mathbb{Q})$ and $\alpha(0,-\sqrt{c}) \equiv 1 \pmod{\mathbb{Q}(\sqrt{c})^{*3}}$. Since $T_2 = (0,-\sqrt{c}) \in E(\mathbb{Q})$, it must be that c is a perfect square. Also, in order for $\alpha(0,-\sqrt{c})$ to map to 1 modulo $\mathbb{Q}(\sqrt{c})^{*3}$, we have that $4c$ must be a perfect cube in $\mathbb{Q}(\sqrt{c})^*$. If c is a perfect square, then $\mathbb{Q}(\sqrt{c}) = \mathbb{Q}$. Thus $4c$ must be a perfect square and perfect cube in $\mathbb{Q}$, implying that $4c = 2^{6j}m^{6k}$ for $j,k \in \mathbb{Z}$ and $m \in \mathbb{Q}$. By Proposition 3.1.5 part (ii), $T_2 \in \psi\big(E'(\mathbb{Q})\big)$.

Let $(x_1,y_1) \neq \mathcal{O} \in \psi\big(E'(\mathbb{Q})\big)$ for $y \neq -\sqrt{c}$. Then $y_1 + \sqrt{c} \equiv 1 \pmod{\mathbb{Q}(\sqrt{c})^{*3}}$ by Proposition 3.1.5 part (iii). So $(x_1,y_1) \in \ker\ \alpha$. Now assume $(x_1,y_1) \in \ker\ \alpha$. Then $\alpha(x_1,y_1) \equiv 1 \pmod{\mathbb{Q}(\sqrt{c})^{*3}}$. Thus, $(x_1,y_1) \in \psi\big(E'(\mathbb{Q})\big)$ again by Proposition 3.1.5 part (iii). Therefore, the kernel of α is the image $\psi\big(E'(\mathbb{Q})\big)$.

□

3.2 A New Formula for Rank

Recall that

$$E(\mathbb{Q}) \cong \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r \text{ summands}} \oplus \mathbb{Z}_{p_1^{v_1}} \oplus \mathbb{Z}_{p_2^{v_2}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{v_s}} \tag{3.4}$$

where each p_i is prime, and r is the *rank* of $E(\mathbb{Q})$.

We know by Proposition 3.1.4 that $\psi \circ \phi$: $E(\mathbb{Q}) \to E(\mathbb{Q})$ results in multiplication by three. Hence

$$im\,(\psi \circ \phi) = 3E(\mathbb{Q}) \cong \left(\bigoplus_{i=1}^{r} 3\mathbb{Z} \right) \oplus \left(\bigoplus_{j=1}^{s} 3\mathbb{Z}_{p_j^{v_j}} \right).$$

So the quotient group

$$E(\mathbb{Q})/3E(\mathbb{Q}) \cong \left(\bigoplus_{i=1}^{r} \frac{\mathbb{Z}}{3\mathbb{Z}} \right) \oplus \left(\bigoplus_{j=1}^{s} \frac{\mathbb{Z}_{p_j^{v_j}}}{3\mathbb{Z}_{p_j^{v_j}}} \right). \tag{3.5}$$

Let $E(\mathbb{Q})_3$ be the 3-torsion subgroup of $E(\mathbb{Q})$ (*i.e.* $E(\mathbb{Q})_3$ is the subgroup of all $Q \in E(\mathbb{Q})$ such that $3Q = \mathcal{O}$). By (3.4), there exist generators, say

$$P_1, P_2, \ldots, P_r, Q_1, Q_2, \ldots, Q_s \in E(\mathbb{Q})$$

such that every point $P \in E(\mathbb{Q})$ can be written as

$$P = n_1P_1 \oplus \cdots \oplus n_rP_r \oplus m_1Q_1 \oplus \cdots \oplus m_sQ_s$$

where each integer n_i is uniquely determined by P and the integers m_j are determined modulo $p_j^{v_j}$.

In order to find $|E(\mathbb{Q})_3|$, let us examine when $3(n_1P_1 + \cdots + n_rP_r + m_1Q_1 + \cdots + m_sQ_s) = \mathcal{O}$. This will only happen if $n_i = 0$ for each i and $3m_j \equiv 0 \pmod{p^{v_j}}$ for each j. If $p \neq 3$, then $3m \equiv 0 \pmod{p^v}$ if an only if $m \equiv 0 \pmod{p^v}$. If $p = 3$, then $3m \equiv 0 \pmod{p^v}$ if $m \equiv 0 \pmod{p^v}$ or $m \equiv 0 \pmod{p^{v-1}}$, which will occur if $m = p^{v-1}$

or if $m = 2p^{v-1}$. So for each term n_iP_i, we have one choice, $n_i = 0$. For each term m_jQ_j, we have one choice if $p \neq 3$ and three choices if $p = 3$. Thus

$$|E(\mathbb{Q})_3| = 3^N \tag{3.6}$$

where N is the number of $p_j = 3$.

Now we are ready to prove a theorem regarding the rank of $E(\mathbb{Q})$ for our new curve $E\colon y^2 = x^3 + c$.

Theorem 3.2.1. *Let $\phi\colon E(\mathbb{Q}) \to E'(\mathbb{Q})$, $\psi\colon E'(\mathbb{Q}) \to E(\mathbb{Q})$, $\alpha\colon E(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}(\sqrt{c})^{*3}$, and $\alpha'\colon E'(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}(\sqrt{c})^{*3}$ be group homorphisms as previously defined. Then*

$$\frac{|im\ \alpha| \cdot |im\ \alpha'|}{|ker\ \psi| \cdot |ker\ \phi|} = 3^r$$

where r is the rank of $E(\mathbb{Q})$.

Proof. From (3.5), we know that

$$E(\mathbb{Q})/3E(\mathbb{Q}) \cong \left(\bigoplus_{i=1}^{r} \frac{\mathbb{Z}}{3\mathbb{Z}} \right) \oplus \left(\bigoplus_{j=1}^{s} \frac{\mathbb{Z}_{p_j^{v_j}}}{3\mathbb{Z}_{p_j^{v_j}}} \right).$$

Since $\mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}_3$, it has order 3. For each $\dfrac{\mathbb{Z}_{p_i^{v_i}}}{3\mathbb{Z}_{p_i^{v_i}}}$, we have

$$\frac{\mathbb{Z}_{p_i^{v_i}}}{3\mathbb{Z}_{p_i^{v_i}}} \cong \begin{cases} \mathbb{Z}_3 & p_i = 3 \\ 0 & p_i \neq 3 \end{cases}.$$

Thus

$$\left|E(\mathbb{Q})/3E(\mathbb{Q})\right| = 3^r \cdot 3^N.$$

Since $\psi \circ \phi$ is multiplication by three, from the definition of *cokernel* and equation (3.5), we know that

$$|coker(\psi \circ \phi)| = \left|E(\mathbb{Q})/3E(\mathbb{Q})\right| = 3^r \cdot 3^N = 3^r \cdot |E(\mathbb{Q})_3|.$$

This gives us

$$\frac{|coker(\psi \circ \phi)|}{|E(\mathbb{Q})_3|} = 3^r.$$

Since $E(\mathbb{Q})_3$ is defined to be all $Q \in E(\mathbb{Q})$ such that $3Q = \mathcal{O}$, and we know that $\psi \circ \phi$ results in multiplication by three, it follows that $E(\mathbb{Q})_3 = ker(\psi \circ \phi)$, and therefore

$$\frac{|coker(\psi \circ \phi)|}{|ker(\psi \circ \phi)|} = 3^r.$$

Which, by Theorem 2.3.4, gives us

$$\frac{|coker\ \psi|\,|coker\ \phi|}{|ker\ \psi|\,|ker\ \phi|} = 3^r. \tag{3.7}$$

□

Also, from Proposition 3.1.6 part (ii), we have $ker\ \alpha = im\ \psi$. So by the same argument as used in our proof for the theorem of rank in Chapter 2, $|coker\ \psi| = |im\ \alpha|$ and $|coker\ \phi| = |im\ \alpha'|$. Therefore,

$$\frac{|im\ \alpha| \cdot |im\ \alpha'|}{|ker\ \psi| \cdot |ker\ \phi|} = 3^r$$

where r is the rank of $E(\mathbb{Q})$.

Corollary 3.2.2. *The formula for the rank of $E\colon y^2 = x^3 + c$ for $c \in \mathbb{Q}^*$ can be found by considering the following cases for c.*

(i) *If c or $-27c$ is a perfect square, then $|im\ \alpha| \cdot |im\ \alpha'| = 3^{r+1}$.*

(ii) *If neither c nor $-27c$ are perfect squares, then $|im\ \alpha| \cdot |im\ \alpha'| = 3^r$.*

Proof.

(i) If c is a perfect square, then $T_1 = (0, \sqrt{c})$ and $T_2 = (0, -\sqrt{c})$ are contained in $E(\mathbb{Q})$. So $ker\ \phi = \{\mathcal{O}, T_1, T_2\}$, which has order 3. However, for $E'\colon y^2 = x^3 - 27c$, the points $\overline{T}_1 = (0, \sqrt{-27c})$ and $\overline{T}_2 = (0, -\sqrt{-27c})$ are not contained in $E'(\mathbb{Q})$. So $ker\ \psi$ has only one element, $\mathcal{O}$. A similar argument holds $-27c$ is a perfect square. Thus the formula from (3.7) simplifies to $|im\ \alpha| \cdot |im\ \alpha'| = 3^{r+1}$.

(ii) If neither c nor $-27c$ is a perfect square, then T_1, T_2, $\overline{T}_1$ and $\overline{T}_2$ are either imaginary or irrational. Thus $|ker\ \phi| = 1$ and $|ker\ \psi| = 1$. Therefore, $|im\ \alpha| \cdot |im\ \alpha'| = 3^r$.

□

In Chapter 2, we looked at a few examples for which we computed the rank of a given curve. Recall that $im\ \alpha \subseteq \{\pm p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_t^{\varepsilon_t}\}$ where each p_i is a distinct prime divisor of $b \pmod{\mathbb{Q}^{*2}}$. For our new curve, the following theorem can help us to find the rank of certain curves.

Theorem 3.2.3 ([HHW93]). *Let $E\colon y^2 = x^3 + n^2$, $n \in k^*$ be an elliptic curve over k and $\omega = \frac{-1+\sqrt{-3}}{2}$. Then $\mathrm{im}\,\alpha$ lies in the $\mathbb{Z}/3\mathbb{Z}$-vector space generated by*

(i) *all primes dividing the third-power-free part of $2n$, if $k = \mathbb{Q}$, or*

(ii) *ω and all primes dividing the third-power-free part of $2n$, if $k = \mathbb{Q}(\omega)$.*

Example 3.2.1. Show that the rank of $E\colon y^2 = x^3 + 16$ and $E'\colon y^2 = x^3 - 432$ is 0 and find $E(\mathbb{Q})$ and $E'(\mathbb{Q})$.

Solution. Applying Theorem 3.2.3 to the curve E, we have that $n = 4$, so that $2n = 8 = 2^3$. Since there are no prime divisors of the cube free part of 8, $im\ \alpha = \{\overline{1}\}$.

For the curve E', we have that $n = \sqrt{-432} = \sqrt{-27 \cdot 16} = 2^2\left(\sqrt{-3}\right)^3$, from which it follows that $2n = 2^3\left(\sqrt{-3}\right)^3$. Thus, by part (ii) of Theorem 3.2.3, the $im\ \alpha' \subseteq \{\overline{1}, \overline{\omega}, \overline{\omega}^2\}$. Now, E' contains the rational point $(12, 36)$. From the definition of α',

$$\begin{aligned}
\alpha'(12,36) &= 36 + \sqrt{-27 \cdot 16} \\
&= 36 + 4\sqrt{-27} \\
&= 2^2\left(\sqrt{-3}\right)^4 - 2^2\left(\sqrt{-3}\right)^3 \\
&= \frac{2^3\left(\sqrt{-3}\right)^4 - 2^3\left(\sqrt{-3}\right)^3}{2} \\
&= 2^3\left(\sqrt{-3}\right)^3 \cdot \frac{\sqrt{-3}-1}{2} \\
&\equiv \frac{-1+\sqrt{-3}}{2} \left(\mathrm{mod}\ \mathbb{Q}(\sqrt{-432})^{*3}\right) \\
&= \omega.
\end{aligned}$$

Since α' is a homomorphism, and $(12,-36)$ is the additive inverse of $(12,36)$ in $E'(\mathbb{Q})$, it follows that $\alpha'(12,-36)$ must be the multiplicative inverse of $\alpha'(12,36)$ in $\mathbb{Q}(\sqrt{-432})/\mathbb{Q}(\sqrt{-432})^{*3}$. Hence, $\alpha'(12,-36) = \omega^{-1} \equiv \overline{\omega}^2$. Thus, $im\ \alpha' = \{\overline{1}, \overline{\omega}, \overline{\omega}^2\}$. Since $|im\ \alpha| = 1$ and $|im\ \alpha'| = 3$, by Corollary 3.2.2 part (i), the rank of E and E' is 0.

Now let's find $E(\mathbb{Q})$ and $E'(\mathbb{Q})$. Some obvious rational points on E are $(0, \pm 4)$. So at least $\mathcal{O}$, $(0,4)$ and $(0,-4)$ are contained in $E(\mathbb{Q})$. To continue, we will need the following well-known theorem.

Theorem 3.2.4 ([Hus, p. 35])**.** *Let c be a non-zero integer which is sixth power free. Let E be the elliptic curve*

$$E : y^3 = x^3 + c,$$

and let $\Phi \subseteq E(\mathbb{Q})$ be the subgroup consisting of all points of finite order.

(a) *The order of Φ divides 6.*

(b) *The isomorphisms of Φ are given by the following table:*

$$\Phi \cong \begin{cases} \frac{\mathbb{Z}}{6\mathbb{Z}}, & \text{if } c = 1, \\ \frac{\mathbb{Z}}{3\mathbb{Z}}, & \text{if } c \neq 1 \text{ is a square, or if } c = -432, \\ \frac{\mathbb{Z}}{2\mathbb{Z}}, & \text{if } c \neq 1 \text{ is a cube,} \\ \mathcal{O}, & \text{otherwise.} \end{cases}$$

Since $c = 16$ is sixth power free and $c \neq 1$ is a square, we know from the theorem above that the torsion subgroup of $E(\mathbb{Q})$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$. We know that there are no points of infinite order in $E(\mathbb{Q})$ since the rank of E is 0. Thus, $E(\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$. It follows that $E(\mathbb{Q}) = \{\mathcal{O}, (0, \pm 4)\}$. For $E'(\mathbb{Q})$, since $c = -432$, we can again use the theorem above to show that $E'(\mathbb{Q}) = \{\mathcal{O}, (12, \pm 36)\}$. □

For our new curve, the following table provides the rank of $E(\mathbb{Q})$ for various values of c [Hus, p. 37].

Rank	c
0	1,4, 6, 7, 13, 14, 16, 20, 21
	-1, -3, -5, -6, -8, -9, -10, -14, -432
1	2, 3, 5, 8, 9, 10, 11, 12, 18
	-2, -4, -7, -13, -15, -18, -19, -20, -21
2	15, 17, 24, 37, 43
	-11, -26, -39, -47
3	113, 141, 316, 346, 359
	-174, -307, -362

Table 3.1: Values of the rank r for $E\colon y^2 = x^3 + c$

Chapter 4

Conclusion

We would like to conclude with some ideas on how the reader can expand upon the concepts presented in this paper. It would be interesting to find what questions are still unanswered regarding elliptic curves, and which of these unanswered questions are considered significant?

We mentioned the Birch and Swinnerton-Dyer conjecture, but more time could be devoted to understanding the Hasse-Weil L-function, the statement of the conjecture, and its significance. The Clay Mathematics Institute chose the Millenium Prize Problems not only because they are difficult problems to solve, but also because they are considered to be important and relevant. So why is the solution of the Birch and Swinnerton-Dyer conjecture so crucial?

Another extension of this paper might be to see how Andrew Wiles used elliptic curves to prove Fermat's last theorem. His proof of the semistable modularity conjecture was key to the proof. *An Overview of the Proof of Fermat's Last Theorem* by Glenn Stevens outlines all of the work leading up to Wiles's work that shows the key role elliptic curves and Galois representations had in the final proof [Ste97]. It also shows that Wiles's work was really the culmination of the work many people.

Finally, all of the work we have done here has been very abstract, but it would be interesting to study the applications of elliptic curves. Elliptic curves are used in

cryptography to factor composite numbers that are the product of two extremely large primes. The factorization of these composite numbers plays are large role in the privacy of our information when it is exchanged through the internet. Elliptic curves have taken algorithms that computers were using, and have sped up the process. A good place start when studying this topic further is with Pollard's $p-1$ Algorithm and Lenstra's Elliptic Curve Algorithm.

Bibliography

[Hat09] Jeffrey Hatley. *Hasse-Minkowski and the Local-to-Global Principle.* Technical report, The College of New Jersey, 2009.

[HHW93] Darrell E. Haile, Ilsesop Han, and Adrian R. Wadsworth. *Curves C That Are Cyclic Twists of $y^2 = x^3 + c$ and the Relative Brauer Groups $Br(k(C)/k)$.* *Trans American Mathematical Society*, 364(9):4875–4908, 1993.

[Hus] D. Husemoller. *Elliptic Curves.* Springer, New York, 2nd, edition.

[Lan02] S. Lang. *Algebra.* Springer, New York, 2nd edition, 2002.

[ST92] Joseph H. Silverman and John Tate. *Rational Points on Elliptic Curves.* Springer, New York, 1992.

[Ste97] Glenn Stevens. *An Overview of the Proof of Fermat's Last Theorem.* Technical report, Boston University, 1997.

[V́71] Jacques Vélu. *Isogénies Entre Courbes Elliptiques.* C.R. Acad. Sc. Paris, Série A., 273, pp. 238-241, 1971. (French).