

# Torsion and Rank: Navigating the World of Elliptic Curves

A Senior Comprehensive Project

by

Ethan Borsh  
Allegheny College  
Meadville, PA

December 11, 2024

Submitted to the Department of Mathematics in partial fulfillment of the  
requirements for the degree of Bachelor of Science.

Project Advisor: Dr. Caryn Werner

Second Reader: Dr. Brent Carswell

I hereby recognize and pledge to fulfill my responsibilities, as defined in the  
Honor Code, and to maintain the integrity of both myself and the College  
community as a whole.

Pledge:

---

name

## Acknowledgments

I would like to express my deepest gratitude to all those who have supported me throughout the completion of this comprehensive project. This work would not have been possible without their guidance, encouragement, and kindness.

First and foremost, I would like to thank my advisor, Professor Werner, whose expertise, patience, and unwavering support were essential in shaping the trajectory of this project. At times, my ambition outpaced my clarity, but your thoughtful suggestions and encouragement motivated me to reflect on the greater picture, refine my work, and challenge my own thinking. I am eternally grateful for the time and energy you dedicated to helping me succeed. Also, I would like to thank my second reader, Professor Carswell, for his valuable insights and thoughtful critique. I would like to also thank Dr. Craig Dodge, whose belief in my potential and mentorship in my first few years here set me on my current career path. *Thanks for all the fish!*

To my peers, particularly my fraternity brothers of Fiji and my Candela RPG group, you have all been constant sources of support and companionship. Knowing that you were there for me kept me going through many late nights that inevitably turned into early mornings. I am a better person because of the growth and shared experiences we've had together.

I am also forever grateful to my parents, Jennifer and Peter Borsh, for their unwavering love and support. You have both been there for me during the smallest bumps of the road and the insurmountable car wrecks. Your belief in me has helped shape me into the person I am today, and I am truly

proud to call myself your son. I would also like to thank my siblings, Aidan and Regan. We have all grown so much over the past few years, and it has been an honor to share that journey with you. I would also like to thank my girlfriend, Mia Wayman, whose unwavering support has given me purpose and strength through the best and worst of times. Over the course of our six-plus years together, we have grown and changed in so many ways, and I am profoundly grateful for everything you have done to help me along this journey. Along with my family, you have been a cornerstone of my life, and I could not have done this without you.

Finally, I am deeply grateful to Allegheny College, whose faculty, resources, and commitment to student success provided the foundation for this project. The academic freedom and encouragement I experienced here have been invaluable, and I feel fortunate to have had the opportunity to complete a project of this scope at such an institution.

This journey has been as much about personal growth as it has been about academic achievement, and I am humbled by the incredible network of support I have had along the way. Thank you to everyone who played a part in this journey. Your contributions, no matter how big or small, have made this achievement a reality.

## **Abstract**

This thesis introduces elliptic curves to readers new to the topic, covering foundational concepts, key historical developments, and carefully including proofs of often-omitted results. Emphasis is placed on the group structure, elliptic curves over the rational and complex numbers, and the computation of ranks and torsion points, alongside connections to current research.

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>Foundations and Projective Geometry</b>	<b>4</b>
2.1	What is the Projective Plane? . . . . .	4
2.2	Introduction to Cubics . . . . .	10
<b>3</b>	<b>Group Structure of Elliptic Curves</b>	<b>13</b>
3.1	The Group Law . . . . .	14
3.2	Mordell's Theorem and $E(\mathbb{Q})$ . . . . .	23
3.3	Rational Torsion . . . . .	26
<b>4</b>	<b>Exploring Rank</b>	<b>28</b>
4.1	Computing Rank via Number Theory . . . . .	30
4.2	Higher Rank Subfamilies . . . . .	39
<b>5</b>	<b>Complex Elliptic Curves</b>	<b>42</b>
5.1	Elliptic Curves are Complex Tori . . . . .	43
5.2	Isomorphism Classes: the $j$ -invariant . . . . .	48
<b>6</b>	<b>Contemporary Results</b>	<b>51</b>
6.1	Elliptic Curve Cryptography . . . . .	52
6.2	Rank and the BSD Conjecture . . . . .	55
6.3	Modular Forms and Fermat's Last Theorem . . . . .	57
<b>A</b>	<b>Appendix</b>	<b>63</b>
A.1	Weierstraß Normal Form . . . . .	63

A.2 Reduction mod $p$ Theorem . . . . .	64
A.3 Eisenstein Series Converges . . . . .	65

# 1 Introduction

Elliptic curves stand at the crossroads of algebra, geometry, and number theory, offering profound insights into mathematical structures while playing a pivotal role in contemporary applications. From their ancient origins in Diophantine equations to their modern utility in cryptography and the proof of Fermat's Last Theorem, elliptic curves have continually evolved, revealing rich mathematical properties and inspiring groundbreaking results [34]. This paper aims to guide readers through the fascinating journey of elliptic curves, starting with their historical foundations and culminating in their cutting-edge applications.

The history of elliptic curves begins in the realm of classical mathematics. As early as ancient Greece, mathematicians like Diophantus studied equations involving integers and rational solutions. While his work in *Arithmetica* predated the formal development of elliptic curves, the equations he explored laid the groundwork for this field [8]. These equations were explored on and off for decades. However, it was not until the 17th and 18th centuries that elliptic curves received their name. Mathematicians like Bernoulli and Euler explored what are known as elliptic integrals, which are used to find the arc length of an ellipse (among many other things) [4][33, pg. 157].

The contemporary significance of elliptic curves was cemented in the late 20th century. Andrew Wiles's monumental proof of Fermat's Last Theorem relied heavily on the modularity theorem, which asserts a deep relationship between elliptic curves and modular forms [38].

Around the same time, the advent of elliptic curve cryptography revolu-

tionized secure communications, leveraging the computational intractability of certain problems related to elliptic curves for practical applications in digital security [26]. Today, elliptic curves remain at the forefront of mathematical research, with open problems like the Birch and Swinnerton-Dyer conjecture driving much of the field's activity [7, pg. 17–29].

This paper will explore the development and applications of elliptic curves in depth. In the sections that follow, we will provide a structured narrative, guiding readers through their mathematical and historical significance.

In Section 2, we begin with the geometric foundations of elliptic curves, tracing their development as solutions to cubic equations and the introduction of projective geometry. This framework provided the tools to understand intersections, singularities, and the algebraic structure of curves, setting the stage for later advancements.

In Section 3, we discuss the group structure of elliptic curves with a focus on the chord-tangent construction and the implications of Mordell's theorem. This section lays the groundwork for understanding the arithmetic and computational challenges of elliptic curves.

In Section 4, we delve into arithmetic and underlying history of rational points and their central role in number theory. We highlight specific families of curves, so that we can examine the elusive concept of rank and its implications for understanding rational solutions.

In Section 5, we transition to a complex-analytic perspective, exploring elliptic curves as tori associated with lattices in the complex plane. Through Weierstraß's pioneering work, we uncover a unified algebraic, geometric, and

analytic framework that informs both theory and applications.

Finally, in Section 6, we explore the modern applications of elliptic curves, including their pivotal role in cryptography, the outline of the proof of Fermat's Last Theorem, and introducing research into the Birch and Swinnerton-Dyer conjecture.

By weaving together the historical evolution and mathematical richness of elliptic curves with their contemporary relevance, this paper invites readers to appreciate their elegance and power. Each section builds on the previous, connecting foundational concepts with advanced ideas and practical applications, ensuring a comprehensive understanding of this cornerstone of modern mathematics.

## 2 Foundations and Projective Geometry

The study of elliptic curves begins with their description as solutions to certain cubic equations. To understand these curves properly, mathematicians had to develop tools that allowed them to work in a more general geometric setting. In the early 19th century, the introduction of projective geometry revolutionized algebraic geometry by allowing the inclusion of “points at infinity.” This innovation provided a natural framework in which the intersections of curves could be fully understood, including those that appeared “beyond” the affine plane.

By the mid-19th century, this projective perspective allowed for key insights into algebraic curves, such as Bézout’s theorem, which relates the degrees of two curves to the number of their intersection points in the projective plane. For elliptic curves, this result clarified how their intersections behave and how singularities can be classified and avoided. As we explore these foundational ideas, we’ll see how projective geometry became indispensable to the study of elliptic curves, providing tools to handle their algebraic structure with precision and elegance [29].

This section sets the stage for the deeper properties of elliptic curves, establishing a framework that will support the exploration of their group structure, arithmetic, and analytic aspects in the sections to come.

### 2.1 What is the Projective Plane?

The main goal of algebraic geometry is to utilize algebraic equations to study geometric objects and their properties. John Tate captures this interplay

between algebra and geometry well with the quote, “Think geometrically, prove algebraically” [17, pg. 103].

However, certain geometric statements are limited by the constraints of traditional spaces, such as  $\mathbb{R}^2$ . For instance, it would be nice to be able to say that any two distinct lines meet at exactly one point. However, in a space like  $\mathbb{R}^2$ , it is impossible to make this statement—what if the lines are parallel?

Interestingly, art played a large role in inspiring our mathematical solution to this problem. Renaissance artists, striving to depict realistic distance and depth in their work, developed techniques in perspective drawing. To create the illusion of depth, they made parallel lines appear to converge toward a single “vanishing point” that rests on the horizon line (see Figure 1).

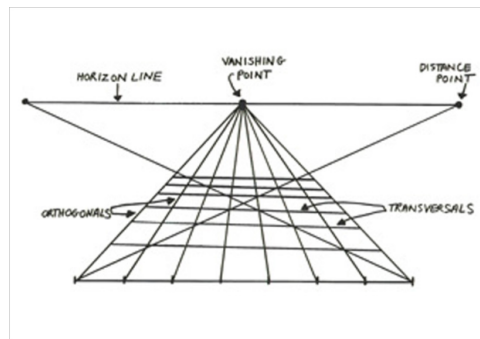


Figure 1: A Drawing with Perspective [36]

To address the limitations of traditional geometry in the plane, we introduce the *projective plane*. The projective plane  $\mathbb{P}^2$  extends  $\mathbb{R}^2$  by adding “points at infinity.”

In the projective plane, two distinct lines always meet at one point—



collectively form the *line at infinity*, where all distinct parallel lines intersect. Interestingly, this line is one-dimensional because any point with  $z = 0$  can be written as  $(x : y : 0)$ , which captures a direction in  $\mathbb{A}^2$  rather than a specific position.

Among the points on the line at infinity, certain points correspond to specific directions in  $\mathbb{A}^2$ . For instance, the point  $(0 : 1 : 0)$  corresponds to the direction parallel to the  $x$ -axis, while  $(1 : 0 : 0)$  corresponds to the  $y$ -axis. In this work, we will primarily refer to  $(0 : 1 : 0)$  as a representative *point at infinity*, but this choice is largely a matter of convention. The choice of representative does not affect the broader geometric framework, as all points on the line at infinity serve the same purpose of encoding directions in  $\mathbb{A}^2$ .

In algebraic geometry, we are interested in polynomials and their zero sets. The zero set of a polynomial  $P$ , denoted  $V(P)$ , is the set of all points where  $P(x, y, z) = 0$ .

However, to work within the projective plane we require that polynomials be *homogeneous*. A polynomial is homogeneous if all its terms have the same degree. For example,  $x^2 + 2xy + xz + z^2$  is homogeneous because every term is of degree two, while  $xyz + y^3 + 4xy$  is not, as it contains terms of different degrees.

We require polynomials to be homogeneous because the zero sets of non-homogeneous polynomials are not well defined in  $\mathbb{P}^2$ . For instance, if  $P(x, y, z) = xyz + y^3 + xy$  then  $(-1, -1, 0) \in V(P)$ , but the scalar multiple of this point  $(1, 1, 0)$  is not in  $V(P)$ . However, when  $P$  is homogeneous with degree  $n$ , we avoid this problem. Observe that  $P(\lambda x : \lambda y : \lambda z) = \lambda^n P(x : y : z)$  for any scalar  $\lambda$ .

If we have a polynomial in the affine plane which we want to work with in the projective plane, we can *homogenize* it. If  $p(x, y)$  is a degree  $n$  polynomial in  $\mathbb{A}^2$ , then the homogenization of  $p(x, y)$  in  $\mathbb{P}^2$  is

$$P(x, y, z) = z^n p\left(\frac{x}{z}, \frac{y}{z}\right).$$

For example, we can homogenize the degree three polynomial  $-x^3 + y^2 - x + 3$  as  $-x^3 + y^2z - xz^2 + 3z^3$ .

A foundational result of algebraic geometry that we will be using shortly is Bézout's Theorem. This theorem allows us to predict intersections and analyze curves in higher dimensional spaces.

**Theorem 2.1** (Bézout's Theorem). *Let  $C$  and  $D$  be curves in  $\mathbb{P}^2$  with  $\deg(C) = m$  and  $\deg(D) = n$ . As long as  $C$  and  $D$  share no common components, they intersect in  $mn$  points (counted up to multiplicity).*

A proof of this Theorem can be found in [16, pg. 57–59]. Below, we illustrate this result with a concrete example.

**Example 2.2.** Consider two curves  $C : x^2 + y^2 = 2$  and  $D : y = x^3 + 3xy^2 + 7x^2y$ . These curves have  $\deg(C) = 2$  and  $\deg(D) = 3$ , so we expect them to intersect in 6 places. In Figure 3, we see that they do. △

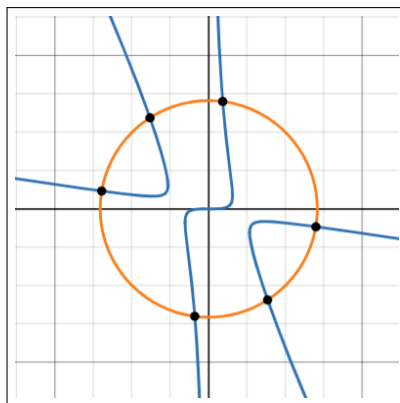


Figure 3: Intersections of  $y = x^3 + 3xy^2 + 7x^2y$  and  $x^2 + y^2 = 2$

In this example, all intersections occur with multiplicity one and are visible in  $\mathbb{R}^2$ , but this need not always be the case. Bézout's Theorem fundamentally hinges on the concept of *intersection multiplicity*. For instance, some of our intersections could occur in  $\mathbb{C}^2$  or a line might intersect a curve at one point with multiplicity of two or more (in which case we say the line is tangent to the curve at that point).

To formalize the second example in a little more detail, consider a degree  $d$  curve  $f(x, y) = 0$  in the affine plane, and a line  $\ell : y = mx + b$ . Substituting the line equation into  $f(x, y)$  yields the polynomial  $f(x, mx + b)$ , whose degree remains  $d$ . By the Fundamental Theorem of Algebra, this polynomial must have exactly  $d$  roots (counted with multiplicity) in the complex plane. We can express this polynomial in factored form as

$$f(x, mx + b) = \lambda \prod_{i=1}^d (x - r_i)$$

where each  $r_i$  is a root and  $\lambda$  is a leading coefficient. A root repeated  $k$  times corresponds to an intersection with multiplicity  $k$ . For instance, if  $r_1$  appears

twice in the factorization, the line  $\ell$  intersects the curve at  $(r_1, mr_1 + b)$  with multiplicity 2, indicating tangency.

Finally, we develop the notion of smoothness in algebraic curves. Let  $F$  be a homogeneous function. We say a point in  $V(F)$  is *singular* if  $F_x(p) = F_y(p) = F_z(p) = 0$  (where  $F_x$  is the partial derivative with respect to  $x$ ). In the graph of  $V(f)$ , singular points appear as points where the curve intersects itself. Singular points have two types: nodes and cusps (see Figure 4). A curve is *nonsingular* or *smooth* when none of the points in  $V(f)$  are singular.

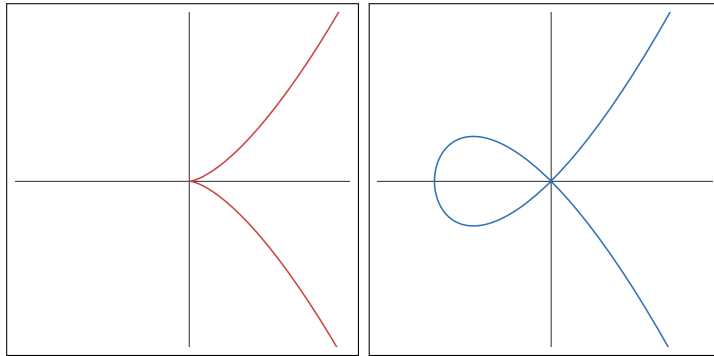


Figure 4: Cusp (left) and Node (right)

## 2.2 Introduction to Cubics

Cubics are the zero sets of degree three homogeneous polynomials. They hold a special place in algebraic geometry. Unlike conics (zero sets of degree two homogeneous polynomials), which are isomorphic to  $\mathbb{P}^1$  or a degenerate conic and can be parameterized by rational equations, many cubics cannot be parameterized in this way [29, pg. 36]. We will also see in Section 5.2 that smooth cubics have a much larger set of isomorphism classes (given by  $\mathbb{C}$ ).

Cubics, in short, are studied since they contain rich underlying geometric and algebraic structures but are computationally simple enough to study directly.

Our chief interest, elliptic curves, are a special class of cubic. *Elliptic curves* are smooth cubics that are topologically equivalent to tori (see Section 5.1 for details). As we will see in the next section, elliptic curves can be equipped with a group law which has applications in cryptography and several other fields.

Before defining the group law, we must establish some conventions. A cubic in the affine plane is said to be in its *general* form when it is expressed in the form:

$$ax^3 + by^3 + cx^2y + dxy^2 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

with coefficients  $a, \dots, j \in \mathbb{C}$ . We say that a cubic is in *Weierstraß form* when it can be written as

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

If the cubic is smooth, we can simplify this further to  $y^2 = x^3 + Ax + B$ , which is called the *Weierstraß normal form* (or just the normal form). If we want to work in the projective plane, we can homogenize these equations as described in the previous subsection.

Any cubic in general form can be expressed in Weierstraß form via a projective change of coordinates (the same as an affine transformation from linear algebra but with a  $3 \times 3$  matrix to account for the third coordinate). This computation is rather tedious, so we provide a quick series of equations

to summarize this in Appendix A.1. Whenever possible, we elect to use the normal form because it is computationally the simplest.

An important fact to note is that the *discriminant* of an cubic curve in normal form is given by  $\Delta_{(A,B)} := -16(4A^2 + 27B^3)$ . When the context is strong enough, we elect not to write the subscript.

The discriminant also gives us another way to check whether a cubic curve is smooth [33, pg. 45–47].

**Theorem 2.3.** *A cubic in Weierstraß form is smooth if and only if  $\Delta \neq 0$ .*

*Proof.* Let  $E$  be given by the equation

$$f(x, y) = y^2 + axy + by - x^3 - cx^2 - dx - e = 0.$$

First, we need to show that the point at infinity  $(0 : 1 : 0)$  is never singular. Homogenizing our equation for  $E$ , we obtain

$$F(x : y : z) = y^2z + axyz + byz^2 - x^3 - cx^2z - dxz^2 - ez^3 = 0.$$

To see why  $(0 : 1 : 0)$  is never singular, observe that

$$F_z = y^2 + axy + 2byz - cx^2 - 2dxz - 3ez^2$$

always evaluates to 1 at  $(0 : 1 : 0)$ . This means the curve is never singular at  $(0 : 1 : 0)$  since a point is singular if and only if all of its partials evaluate to 0.

Switching back to affine coordinates, if  $E$  is singular at  $(x_0, y_0)$  we can perform a change of variables  $(x, y) \mapsto (x - x_0, y - y_0)$  which moves  $(x_0, y_0)$  to  $(0, 0)$ . This change of variables also sets  $c = d = e = 0$  because  $f(0, 0) = f_x(0, 0) = f_y(0, 0) = 0$ . This gives us  $\Delta = 0$ .

For the converse, we can consider an elliptic curve of the form

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6.$$

(this is an intermediary step in Appendix A.1). Taking both partials of this curve and noting when they are both equal to zero, we see that a point  $(x_0, y_0)$  is singular whenever

$$2y_0 = 12x_0^2 + 2b_2x_0 + 2b_4 = 0.$$

These are the points where  $x_0$  is a double root of  $4x^3 + b_2x^2 + 2b_4x + b_6$ .

This happens precisely when its discriminant, given by  $16\Delta$ , is zero.  $\square$

### 3 Group Structure of Elliptic Curves

The geometric elegance of elliptic curves conceals a surprising algebraic property: the points on an elliptic curve, along with a well-defined addition operation, form an abelian group. This discovery was developed in the 19th century through the work of mathematicians like Henri Poincaré, who investigated the properties of intersections and symmetries on algebraic curves. They found that the addition of points, defined geometrically via the chord-tangent construction, obeys the axioms of a group [28].

This group structure became one of the most powerful tools in the study of elliptic curves. Particularly, a result from Louis Mordell in 1922 established that the rational points could be broken into a finite torsion subgroup and a number of copies of  $\mathbb{Z}$ , called the *rank* [34, pg. 95]. This section will explore these ideas and prepare us to investigate the arithmetic and computational challenges associated with rank in the proceeding sections.

### 3.1 The Group Law

Let  $E$  be the elliptic curve in the affine plane, given by

$$E = \{(x, y) \in \mathbb{A}^2 \mid x^3 + Ax + B - y^2 = 0\} \cup \{\mathcal{O}\}$$

where  $\mathcal{O} = (0 : 1 : 0)$  is the point at infinity in  $\mathbb{P}^2$ .

We will define *chord-tangent addition* on  $E$  and show how any smooth cubic in normal form equipped with this operation satisfies the axioms of a group. Precisely, we will prove the existence of:

1. **Identity:**  $\mathcal{O}$  serves as the identity of  $E$  (*Theorem 3.2*)
2. **Inverses:** For each  $P \in E$ , there exists a unique  $-P \in E$  such that  $P + (-P) = \mathcal{O}$ . (*Theorem 3.3*)
3. **Associativity:** For all  $P, Q, R \in E$ ,  $(P + Q) + R = P + (Q + R)$ . (*Theorem 3.7*)

We first will display a geometric construction for chord-tangent addition. To do so, we will need the following corollary to Bézout's Theorem.

**Corollary 3.1.** *When counted up to multiplicity, any line  $\ell$  in the projective plane intersects a cubic three times.*

With this corollary in hand, we can define the chord-tangent addition. Let  $\mathcal{O}$  be the point at infinity and note that any line in  $\mathbb{P}^2$  through  $\mathcal{O}$  is necessarily of the form  $\alpha x + \beta z = 0$ . These lines appear as vertical lines in  $\mathbb{A}^2$  because they correspond to directions in the  $xz$ -plane, which is perpendicular to  $\mathbb{A}^2$ . For any two distinct points  $P, Q \in E$ , we define  $P + Q$  as follows:

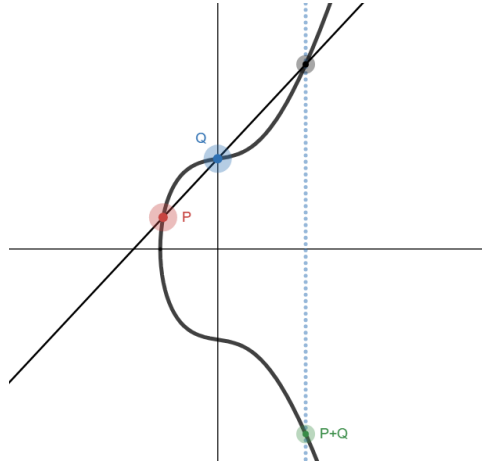


Figure 5: Chord-Tangent Addition

1. Draw the line  $\ell(P, Q)$ . By Corollary 3.1, we know this will intersect  $E$  at some third point which we denote by  $PQ$ .
2. Draw the vertical line  $\ell(PQ, \mathcal{O})$ . This intersects  $E$  at a point which we call  $P + Q$ .

If  $P = Q$ , we use the tangent line at  $P$  instead of the secant line  $\ell(P, Q)$ . The tangent line intersects the curve at  $P$  with multiplicity 2, ensuring that the chord-tangent addition remains consistent even when  $P$  and  $Q$  coincide.

The normal form of  $E$ ,  $y^2 = x^3 + Ax + B$ , is symmetric about the  $x$ -axis due to the  $y^2$  term. Consequently, any vertical line will intersect the curve twice in the affine plane —once above and once below the  $x$ -axis. In the case of points lying directly on the  $x$ -axis, the vertical line will intersect the curve at a single point, but with multiplicity two. Notice that then Step 2 is equivalent to reflecting  $PQ$  across the  $x$ -axis.

Also, notice that  $P + Q = Q + P$  because  $\ell(P, Q) = \ell(Q, P)$  and that

$P + Q \in E$  for all  $P, Q \in E$ . In other words,  $+$  is a commutative binary operation.

We can also define chord-tangent addition algebraically. Indeed, if  $P = (x_1, y_1)$  and  $Q = (x_2, y_2)$  are points on  $y^2 = x^3 + Ax + B$ , we have that  $P + Q$  has coordinates  $(x, y)$  given by

$$x = \begin{cases} \left( \frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2 & \text{if } P \neq Q \\ \left( \frac{3x_1^2 + A}{2y_1} \right)^2 - 2x_1 & \text{if } P = Q, y_1 \neq 0 \end{cases}$$

$$y = \begin{cases} -(y_1 + \left( \frac{y_2 - y_1}{x_2 - x_1} \right)(x - x_1)) & \text{if } P \neq Q \\ -(y_1 + \left( \frac{3x_1^2 + A}{2y_1} \right)(x - x_1)) & \text{if } P = Q, y_1 \neq 0. \end{cases}$$

These formulas allow for the exact calculation of the group law without relying on geometric constructions. They are derived by setting the point-slope form of the line between  $P$  and  $Q$  equal to  $y^2 = x^3 + Ax + B$  to find the third point of intersection,  $-(P + Q)$ , then replacing  $y$  with  $-y$  to arrive at  $P + Q$ . In the case  $P = Q$  and  $y_1 \neq 0$ , we use the tangent line at  $P$  which has slope  $(3x_1^2 + A)/(2y_1)$ . When  $P = Q$  and  $y_1 = 0$ , we can use the tangent line (which is vertical in this case) to see that  $2P = \mathcal{O}$ . We are now ready to tackle our first group axiom.

**Theorem 3.2.**  $\mathcal{O}$  is the identity of  $E$ .

*Proof.* Let  $P \in E$  be arbitrary. We show that  $P + \mathcal{O} = P$ . To compute  $P + \mathcal{O}$ , we draw the vertical line  $\ell(\mathcal{O}, P)$ . This intersects  $E$  at  $P$ 's reflection across the  $x$ -axis,  $\mathcal{O}P$  (later, we will show that this is the inverse of  $P$ ,  $-P$ ). Then, we draw the vertical line  $\ell(\mathcal{O}, \mathcal{O}P) = \ell(\mathcal{O}, P)$  which intersects  $E$  at  $P + \mathcal{O} = P$  as desired (see Figure 6).  $\square$

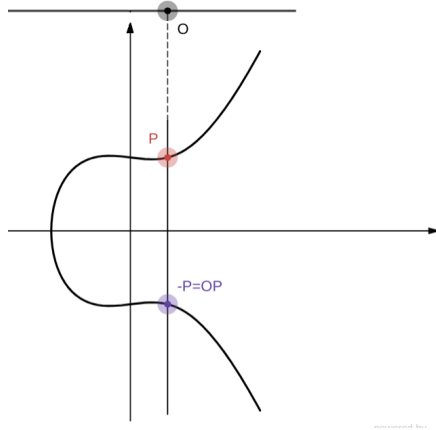


Figure 6: Vertical Line to  $\mathcal{O}$

**Theorem 3.3.** *If  $P = (x_1, y_1)$  then its inverse is given by  $-P = (x_1, -y_1)$ .*

*Proof.* We show that  $P + (-P) = \mathcal{O}$ . First, notice that  $P$  and  $-P$  lie on a vertical line, so  $\mathcal{O}$  is colinear with them. Performing the chord-tangent law we see that  $P - P = \mathcal{O}$  by construction (see Figure 6).  $\square$

Finally, we tackle associativity. To do so, we will consider  $S_3$ , the set of all degree three homogeneous polynomials. We are considering  $S_3$  because we will later construct cubics corresponding to  $(P+Q)+R$  and  $P+(Q+R)$  and use facts about  $S_3$  to show that these cubics must be equivalent.

For any point  $P_1 = (x_1 : y_1 : z_1)$ , we can consider the set of degree three polynomials containing  $P_1$  in their vanishing set (the set where that polynomial evaluates to zero). We call this

$$S_3(\{P_1\}) := \{F \in S_3 \mid F(P_1) = 0\}.$$

Similarly, we can extend this definition to any number of points

$$S_3(\{P_1, \dots, P_n\}) := \{F \in S_3 \mid F(P_1) = 0, F(P_2) = 0, \dots, F(P_n) = 0\}.$$

If we think of  $S_3$  as a vector space in the coefficients, each new point we add will create an additional linear restriction on which cubics are in our set (as long as these points are sufficiently independent of one another).

**Example 3.4.** For example, consider the degree three polynomials  $F \in S_3$  that vanish at the points  $(1 : 1 : 1)$  and  $(0 : 1 : 3)$ . The general homogeneous cubic polynomial in three variables is given by

$$\begin{aligned} F(x, y, z) = & c_1x^3 + c_2x^2y + c_3x^2z + c_4xy^2 + c_5xyz \\ & + c_6xz^2 + c_7y^3 + c_8y^2z + c_9yz^2 + c_{10}z^3, \end{aligned}$$

where  $c_1, \dots, c_{10} \in \mathbb{C}$  are the coefficients. We require

$$F(1, 1, 1) = 0 \quad \text{and} \quad F(0, 1, 3) = 0.$$

Substituting the points  $(1, 1, 1)$  and  $(0, 1, 3)$  into  $F(x, y, z)$  gives the two linear equations:

$$c_1 + c_2 + c_3 + c_4 + c_5 + c_6 + c_7 + c_8 + c_9 + c_{10} = 0,$$

$$c_7 + 3c_8 + 9c_9 + 27c_{10} = 0.$$

If we add more points, say  $(2, -1, 0)$ , we would substitute  $x = 2$ ,  $y = -1$ , and  $z = 0$  into  $F$  to generate a third linear equation. Each additional independent point reduces the dimension of the solution space by one. However, if the points are not independent (e.g., they lie on the same curve), the constraints may overlap, and the dimension of the space is reduced less.  $\triangle$

What we obtain from this way of thinking is the following theorem.

**Theorem 3.5.** *Let  $P_1, \dots, P_8 \in \mathbb{P}^2$  be distinct points and suppose that no 4 of  $P_1, \dots, P_8$  are colinear and no 7 of them lie on a nondegenerate conic. Then  $\dim S_3(P_1, \dots, P_8) = 2$ .*

The proof of this theorem is rather lengthy but can be found in [29, pg. 37]. From this, we arrive at the following corollary.

**Corollary 3.6.** *Let  $C_1$  and  $C_2$  be two distinct degree three homogeneous polynomials whose intersection consists of 9 points. Then, any cubic that passes through 8 of these points must also pass through the ninth point.*

This follows since  $C_1$  and  $C_2$  would form a basis for  $S_3(P_1, \dots, P_8)$  so any other cubic in  $S_3(P_1, \dots, P_8)$  can be written as  $C = \lambda_1 C_1 + \lambda_2 C_2$  for  $\lambda_i \in \mathbb{C}$ . No matter what these  $\lambda$  are, we see that  $C$  must contain  $P_9$ .

Now we have the necessary tools to prove that chord-tangent addition is associative.

**Theorem 3.7.** *Chord-tangent addition is associative, i.e. for all  $P, Q$  and  $R$ ,  $(P + Q) + R = P + (Q + R)$ .*

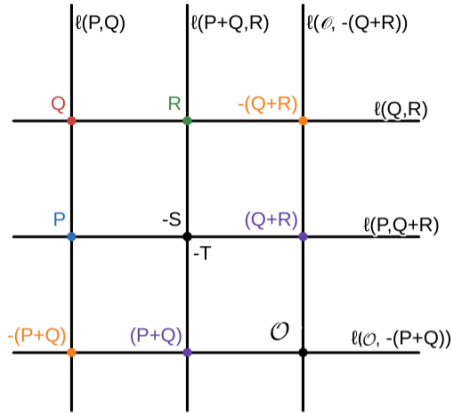
*Proof.* We prove this theorem for the case that  $P$ ,  $Q$ , and  $R$  are distinct, the other cases are covered below in Remark 3.8.

Let  $C$  be a cubic with distinct points  $P$ ,  $Q$ , and  $R$ . Also, let  $S = (P + Q) + R$  and  $T = P + (Q + R)$ . To simplify our work, we show the equivalent statement that  $-S = -T$ . The construction of  $-S$  and  $-T$  each use three lines. To construct  $-S$ , we proceed as follows:

1. First, draw the line  $\ell(P, Q)$ , which intersects the curve at a third point. Label this point  $-(P + Q)$ .

2. Next, draw the line  $\ell(\mathcal{O}, -(P + Q))$  (where  $\mathcal{O}$  is the identity element on the curve). This line intersects the curve again at the point  $P + Q$ .
3. Finally, draw the line  $\ell(P + Q, R)$ . This line intersects the curve at another point, which we label  $-S$ .

To construct  $-T$ , follow a similar approach but begin with the line  $\ell(Q, R)$ . This sequence will lead to the point  $-T$  (see Figure 3.1).



$$\begin{aligned}
 \text{-S} &: \ell(P, Q) \quad \ell(\mathcal{O}, -(P + Q)) \quad \text{and} \quad \ell(P + Q, R) \\
 \text{-T} &: \ell(Q, R) \quad \ell(\mathcal{O}, -(Q + R)) \quad \text{and} \quad \ell(P, Q + R)
 \end{aligned}$$

From the figure, we can see that  $-S$  and  $-T$  appear equal, but to confirm it, we can consider the defining equations of each line to construct two cubics

$$C_1 = \{(x, y) \in \mathbb{A}^2 \mid \ell(P, Q) \cdot \ell(-(Q + R), \mathcal{O}) \cdot \ell(P, Q + R) = 0\}$$

and

$$C_2 = \{(x, y) \in \mathbb{A}^2 \mid \ell(P, Q + R) \cdot \ell(-(P + Q), \mathcal{O}) \cdot \ell(P, Q + R) = 0\}.$$

This gives us

$$C_1 \cap C = \{\mathcal{O}, P, Q, R, (P + Q), (Q + R), -(Q + R), -(P + Q), \text{ and } -S\}$$

and

$$C_2 \cap C = \{\mathcal{O}, P, Q, R, (P + Q), (Q + R), -(Q + R), -(P + Q), \text{ and } -T\}.$$

By Corollary 3.6, any cubic passing through eight points of intersection must also pass through the ninth. Since  $C_1$  and  $C_2$  both intersect  $C$  in 8 identical points, we must have that  $-S = -T$ . This proves the desired result, and we conclude that chord-tangent addition is associative.  $\square$

**Remark 3.8.** In the proof of associativity, we assumed that all 8 points were distinct. However, we often encounter cases where they are not, e.g.  $P = Q$ . Luckily for us, these cases still hold because of the greater multiplicity of intersection.

To see why, say we were in the case that  $P = Q = (x : y : z)$ . Requiring  $P = Q$  means we will need to use the tangent line  $\ell(P, P)$  given by the equation  $m_1x + m_2y + m_3z = 0$  for our construction. It will be useful later to write this as

$$x + \frac{m_2}{m_1}y + \frac{m_3}{m_1}z = 0.$$

It is a known fact that  $3F(P) = 0$  can be expressed equivalently as  $xF_x(P) + yF_y(P) + zF_z(P) = 0$  [37]. Scaling this we see that

$$x + \frac{F_y(P)}{F_x(P)}y + \frac{F_z(P)}{F_x(P)}z = 0.$$

When we require tangency at  $P$ , we need that

$$x + \frac{F_y(P)}{F_x(P)}y + \frac{F_z(P)}{F_x(P)}z = x + \frac{m_2}{m_1}y + \frac{m_3}{m_1}z = 0.$$

From this, we can create the following two restrictions.

$$F_y(P) - \frac{m_2}{m_1}F_x(P) = 0 \quad \text{and} \quad F_z(P) - \frac{m_3}{m_1}F_x(P) = 0.$$

As it turns out, the restriction that  $F(P) = 0$  can be expressed as a linear combination of the two restrictions derived above. Thus, even when two points coincide, introducing tangency at a single point imposes two restrictions on the cubic. As a result, the dimension of the space remains unchanged, and the associativity result still holds.  $\triangle$

To see the group law in action, we compute an example of adding points.

**Example 3.9.** Consider the elliptic curve  $y^2 = x^3 - x + 1$  (named LMFDB 92.a1 in the elliptic curve and modular forms database [9]). This elliptic curve has the integer points,  $(0, 1)$  and  $(3, 5)$ . We can use the previously provided formulas to find  $(0, 1) + (3, 5)$ . Observe that if we let  $(x_1, y_1) = (0, 1)$  and  $(x_2, y_2) = (3, 5)$ , then we obtain

$$\begin{aligned} x &= \left(\frac{5-1}{3-0}\right)^2 - 3 - 0 = -\frac{11}{9} \\ y &= -\left(1 + \left(\frac{5-1}{3-0}\right)\left(-\frac{11}{9} - 0\right)\right) = \frac{17}{27} \\ (0, 1) + (3, 5) &= \left(-\frac{11}{9}, \frac{17}{27}\right) \end{aligned}$$

which aligns with our geometric construction below.  $\triangle$

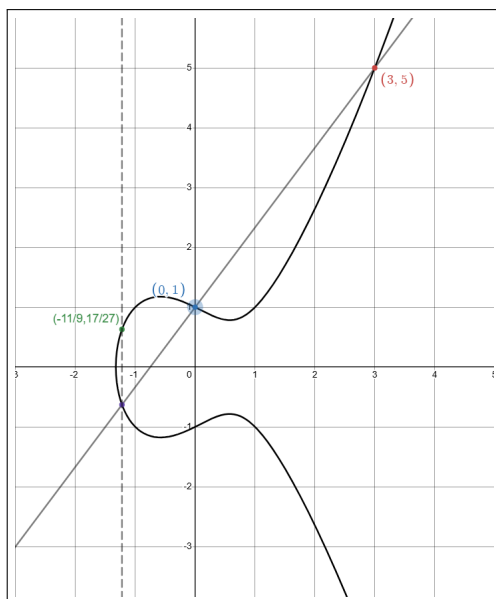


Figure 7:  $(0, 1) + (3, 5)$  Geometrically

### 3.2 Mordell's Theorem and $E(\mathbb{Q})$

Now that we have laid the groundwork by understanding the group structure of chord-tangent addition on  $E$ , we can explore—in a general way—several key results in this area of study.

We say  $y^2 = x^3 + Ax + B$  is an *elliptic curve over  $\mathbb{Q}$*  when  $A$  and  $B$  are integers. As previously mentioned, there is a vast history of finding the rational solutions to elliptic curves over  $\mathbb{Q}$  [8][6].

We denote the set of all rational points on an elliptic curve  $E$  as

$$E(\mathbb{Q}) := \{(x, y) \in E : x, y \in \mathbb{Q}\} \cup \{\mathcal{O}\}.$$

This set is a subgroup of  $E$ , which we obtain as a corollary to the following theorem.

**Theorem 3.10.** *Let  $K$  be a field and suppose  $E$  is an elliptic curve in normal form. Then,  $E(K)$  is a subgroup of  $E$ .*

This theorem implies that for any field  $K$  (in our specific case  $\mathbb{Q}$ ), the set of points on the curve with coordinates in  $K$  is a subgroup of the curve.

*Proof.* Let  $E$  and  $K$  be defined as above. To show that  $E(K) \leq E$ , we use the two-step subgroup test, which requires us to verify that  $E(K)$  is closed under chord-tangent addition operation and contains inverses.

First, we show that  $P + Q \in E(K)$  whenever  $P, Q \in E(K)$ . Recall that the group law can be expressed algebraically via

$$x = \begin{cases} \left( \frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2 & \text{if } P \neq Q \\ \left( \frac{3x_1^2 + A}{2y_1} \right)^2 - 2x_1 & \text{if } P = Q, y_1 \neq 0 \end{cases}$$

$$y = \begin{cases} -(y_1 + \left( \frac{y_2 - y_1}{x_2 - x_1} \right) (x - x_1)) & \text{if } P \neq Q \\ -(y_1 + \left( \frac{3x_1^2 + A}{2y_1} \right) (x - x_1)) & \text{if } P = Q, y_1 \neq 0. \end{cases}$$

By definition, any field is closed under addition, multiplication, and division (for non-zero elements). This means that  $E(K)$  is closed under chord-tangent addition since these are the only operations we use to add points algebraically. Notably, in the case where  $P = Q$  and  $y = 0$  or the case that  $P \neq Q$  and  $x_P = x_Q$ , then  $P + Q = \mathcal{O} \in E(K)$ .

Also, if  $P = (x, y) \in E(K)$  there must exist a  $-P = (x, -y)$  since any field has inverses for every non-zero element (if  $y = 0$ , then  $P = -P$ ). Overall, we have that  $E(K) \leq E$ , as desired.  $\square$

However, the underlying algebraic structure of a field was essential for

this result. This result does not necessarily hold for any set, as we see in the following example.

**Example 3.11.**  $E(\mathbb{Z})$  is not always a subgroup of  $E$ . Consider Example 3.9, where we showed that  $(0, 1) + (3, 5) = \left(-\frac{11}{9}, \frac{17}{27}\right)$ . From this, we see that  $E(\mathbb{Z})$  fails the closure property of a subgroup.  $\triangle$

This does raise the natural question: what does  $E(\mathbb{Q})$  look like? Before we can tackle this question, it is important to define a few key terms. Recall that the *order* of an element in a group is the smallest integer  $n$  such that reapplying the group operation  $n$  times to that element gives the identity.

**Example 3.12.** All points of order two on an elliptic curve in normal form  $y^2 = x^3 + Ax + B$  take the form  $(x_1, 0)$ . When we try to compute  $(x_1, 0) + (x_1, 0)$ , we need to use the vertical tangent line, which intersects the curve again at  $\mathcal{O}$ . Therefore,  $(x_1, 0) + (x_1, 0) = \mathcal{O}$ .  $\triangle$

We call a point on an elliptic curve a *torsion* point if it has finite order. We next show the set of torsion points forms a subgroup of  $E$

**Theorem 3.13.** *The set of torsion points of  $E$ ,  $E_{\text{TORS}}$ , is a subgroup of  $E$ .*

*Proof.* To see why  $E_{\text{TORS}} \leq E$ , first note that  $\mathcal{O}$  is always in  $E_{\text{TORS}}$ , so  $E_{\text{TORS}}$  is non-empty. Now, let  $P, Q \in E_{\text{TORS}}$  with orders  $m$  and  $n$  respectively. Then, note that  $P + Q \in E_{\text{TORS}}$  since

$$nm(P + Q) = nmP + nmQ = \mathcal{O}$$

(due to  $+$  being abelian) means that the order of  $P + Q$  is less than or equal to  $mn$  (notably, finite).

Also,  $-P \in E_{\text{TORS}}$  since  $P + (m - 1)P = \mathcal{O}$  and  $-P = (m - 1)P$  has order less than or equal to  $m$ .  $\square$

Back to our question, we have the following theorem thanks to Louis Mordell [34, pg. 95].

**Theorem 3.14.** *If  $E$  is an elliptic curve over  $\mathbb{Q}$ , then  $E(\mathbb{Q})$  is finitely generated.*

A direct consequence of the proof of this theorem is that we can write

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{TORS}} \times \mathbb{Z}^r$$

where  $E(\mathbb{Q})_{\text{TORS}}$  is the subgroup of rational torsion points and  $r$  is a non-negative integer called the *rank* of  $E$  and is written as  $\text{rank}(E)$  [34, pg. 95–96]. Therefore, to understand  $E(\mathbb{Q})$ , we need to understand  $E(\mathbb{Q})_{\text{TORS}}$  and the  $\text{rank}(E)$ .

### 3.3 Rational Torsion

The torsion subgroup  $E(\mathbb{Q})_{\text{TORS}}$  is a well-studied object and is relatively “well-understood.” We devote the remainder of this section to discussing results related to this subgroup and computing several examples using these results.

We have an efficient algorithm for computing the points of  $E(\mathbb{Q})_{\text{TORS}}$  given  $E$ , which was separately discovered by Nagell and Lutz [24] [27].

**Theorem 3.15.** *Let  $E$  be an elliptic curve over  $\mathbb{Q}$ . If  $(x, y) \in E(\mathbb{Q})_{\text{TORS}} - \{\mathcal{O}\}$ , then  $x, y \in \mathbb{Z}$  and either  $y = 0$  or  $y^2 \mid (\Delta/16)$ .*

This theorem gives us a way to directly compute  $E(\mathbb{Q})_{\text{TORS}}$  by hand (or perhaps by a computer if the coefficients are large).

**Example 3.16.** Consider the elliptic curve  $y^2 = x^3 - 2$  (LMFDB 1728.o3) which has discriminant  $\Delta = -1728$ . To find the rational torsion points, we need to check if there are any integer points with  $y = 0$  or  $y^2|108$ , i.e. we need to check if there are integer points with  $y = 0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 6$ . In this case, it is enough to check if  $y^2 + 2$  is a cube since we know  $x$  must be an integer to be in  $E(\mathbb{Q})_{\text{TORS}}$ . We summarize this calculation in the following table.

$y$	$y^2 + 2$	Cube?	$y$	$y^2 + 2$	Cube?
0	2	no	$\pm 3$	11	no
$\pm 1$	3	no	$\pm 4$	18	no
$\pm 2$	6	no	$\pm 6$	28	no

Table 1: Calculating Rational Torsion

We see that there are no cubes, and so we conclude that  $E(\mathbb{Q})_{\text{TORS}}$  is trivial. △

A much more profound result of Mazur provides a complete classification of  $E(\mathbb{Q})_{\text{TORS}}$  [25, pg. 129–162].

**Theorem 3.17.** *Let  $E$  be an elliptic curve over  $\mathbb{Q}$ . The possible torsion subgroups of  $E(\mathbb{Q})$  are:*

1.  $\mathbb{Z}/n\mathbb{Z}$ , where  $1 \leq n \leq 10$  or  $n = 12$ ;
2.  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ , where  $n = 1, 2, 3, 4$ .

This theorem can simplify our work significantly.

**Example 3.18.** The following example is borrowed from [31, pg. 457].

Consider the family of elliptic curves

$$y^2 + (1 - t - t^2)xy + (t^2 + t^3)y = x^3 + (t^2 + t^3)x^2$$

where  $t \in \mathbb{Q}$  and  $t \neq 0, -1$ . Observe that  $(0, 0)$  is a point on this curve. A lengthy calculation shows that  $(0, 0)$  has order 7 (regardless of  $t$ ).

By Lagrange's theorem, we know the order of an element of a finite group must divide the group's order (the group's order is the number of elements in that group). The only torsion group with order divisible by 7 is  $\mathbb{Z}/7\mathbb{Z}$ . We can conclude that for this family of curves,  $E(\mathbb{Q})_{\text{TORS}} \cong \mathbb{Z}/7\mathbb{Z}$ .  $\triangle$

Though  $E(\mathbb{Q})_{\text{TORS}}$  is well understood, it is still being researched. It has been shown that all of these groups occur an infinite number of times over all elliptic curves [31, pg. 456], but a relatively new area of research concerns itself with finding the distribution of these groups. For example, it has been shown that a large proportion of elliptic curves over  $\mathbb{Q}$  (roughly 5/6) have trivial torsion [21][35].

## 4 Exploring Rank

Mordell's theorem, which we introduced in the previous section, was revolutionary because it established that the group of rational points on an elliptic curve can be expressed as

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

where  $r$  is a non-negative integer called the rank of  $E$ . Understanding  $E(\mathbb{Q})$  is then broken down into a problem of understanding  $E(\mathbb{Q})_{\text{TORS}}$  and

$\text{rank}(E)$ . As we saw in the previous section,  $E(\mathbb{Q})_{\text{TORS}}$  is relatively well-understood.

However, understanding  $E(\mathbb{Q})$  for all curves remains a central challenge in number theory because  $\text{rank}(E)$  has proven to be rather elusive. While the rank of many of the curves we have looked at can be computed using a variety of techniques, a universal solution for all curves is still out of reach.

A large contributor to this is that unlike torsion points, which are well-known due to Theorems 3.15 and 3.17, there are no similar rules or bounds on  $\text{rank}(E)$ . The largest ranks discovered so far are known to reach 29 or higher, but it's still uncertain whether there is an absolute upper bound for all elliptic curves [13][31].

Nevertheless, some families of curves lend themselves to analysis using elementary techniques from number theory. In this section, we study the family of elliptic curves  $E_m$  given by

$$E_m : y^2 = x^3 - x + m^2,$$

where  $m$  is a positive integer. This family was studied extensively in [6], where it was shown that the rank of  $E_m$  is at least 2 for all  $m \geq 2$ . This result demonstrates that  $E_m$  always has an infinite number of rational points for  $m \geq 2$ , which is both surprising and historically significant given the roots of the problem in Diophantine equations.

We also further explore subfamilies of  $E_m$  which have consistently higher rank.

## 4.1 Computing Rank via Number Theory

We now seek to expand on the results provided in [6], where The authors consider the family of elliptic curves

$$E_m : y^2 = x^3 - x + m^2$$

where  $m \in \mathbb{Z}_{\geq 0}$ . This family of elliptic curves is particularly receptive to techniques from number theory —making them an interesting first case for computing rank. First, we consider the cases  $m = 0$  and  $m = 1$ .

**Theorem 4.1.** *We have that  $\text{rank}(E_0) = 0$  and  $\text{rank}(E_1) = 1$ .*

*Proof.* First, observe that the discriminant of  $E_0$  is  $\Delta_{(-1,0)} = 64$ , while the discriminant of  $E_1$  is  $\Delta_{(-1,1)} = -368$ . By the Nagell–Lutz Theorem (Theorem 3.15), any non-trivial point with rational torsion must have integer coordinates, with either  $y = 0$  or  $y^2 \mid \Delta/16$ .

For  $E_0$ , we compute the potential torsion points as

$$(-1, 0), \quad (0, 0), \quad \text{and} \quad (1, 0).$$

In Lemma 4.4, we will show that these are indeed the only rational points on  $E_0$ , so we conclude that  $\text{rank}(E_0) = 0$ .

Now, for  $E_1$ , the Nagell–Lutz Theorem again informs us that  $E_1$  has no torsion points. This is because there is no point with  $y = 0$ , and the equation  $y^2 \equiv 0 \pmod{23}$  has no solution. Here, the modulus 23 arises from the term  $\Delta_{(-1,1)}/16 = -23$ .

However,  $(1, 1) \in E_1$  is a rational point with infinite order. A quick computation in Sage shows that every other rational point on  $E_1$  can be expressed as a multiple of  $(1, 1)$ , so we conclude that  $\text{rank}(E_1) = 1$ .  $\square$

The bulk of our work lies in proving the following result for this family of curves [6].

**Theorem 4.2.** *For  $m \geq 2$ ,  $\text{rank}(E_m) \geq 2$ .*

To show this, we will prove that  $E_m$  has trivial rational torsion and that  $E_m$  has three rational points:  $P = (0, m)$ ,  $Q = (-1, m)$ , and  $P + Q = (1, -m)$  which can not be written as doubles of other rational points. From there, we will leverage the following theorem [11, pg. 78–80].

**Theorem 4.3.** *Let  $E(\mathbb{Q})$  be the group of rational points on an elliptic curve  $E$  and let  $2E(\mathbb{Q})$  be doubles of rational points. Suppose that  $E$  has trivial rational torsion. Then the quotient group  $E(\mathbb{Q})/2E(\mathbb{Q})$  is an elementary abelian 2-group of order  $2^r$ , where  $r$  is the rank of  $E(\mathbb{Q})$ .*

**Remark.** An abelian 2-group is an abelian group where each non-identity element has order 2.

To utilize this theorem to prove Theorem 4.2, we will need to prove:

1.  $E_m(\mathbb{Q})_{\text{TORS}}$  is trivial for  $m \geq 1$ . (*Theorem 4.6*)
2.  $P$ ,  $Q$ , and  $P+Q$  belong to distinct equivalence classes under  $E(\mathbb{Q})/2E(\mathbb{Q})$ . (*Lemma 4.9*)
3.  $P$  and  $Q$  are independent. (*Lemma 4.10*)

If we can show these to be true, then we will have that  $|E(\mathbb{Q})/2E(\mathbb{Q})| \geq 4$ , and therefore,  $\text{rank}(E_m) \geq 2$  by Theorem 4.3. The first step of our journey is to prove the following lemma [6].

**Lemma 4.4.** *The following statements hold:*

- (1.) *If  $(x, y)$  is a rational point on  $E : y^2 = x^3 + Ax + B$  then  $x = u/r^2$  and  $y = v/r^3$  for some  $u, v, r \in \mathbb{Z}$  with  $\gcd(u, r) = \gcd(v, r) = 1$*
- (2.) *The set of rational points on  $E_0 : y^2 = x^3 - x$  is  $\{\mathcal{O}, (0, 0), (1, 0), (-1, 0)\}$ .*

Before continuing, we note that for a prime  $p$  and non-negative integers  $a$  and  $e$ ,  $p^e \parallel a$  means that  $p^e$  divides  $a$  but  $p^{e+1}$  does not.

*Proof.* We will prove (1.) directly, then use the results to inform our proof of (2.).

(1.) Consider a rational point  $(x, y)$  on the elliptic curve  $y^2 = x^3 + Ax + B$ . We can express  $x$  and  $y$  as fractions,  $x = u/s$  and  $y = v/t$ , where  $\gcd(u, s) = \gcd(v, t) = 1$ . Substituting these into the equation for  $E$ , we obtain:

$$s^3v^2 = t^2(u^3 + Aus^2 + Bs^3).$$

Now, let  $p$  be an arbitrary prime, and assume  $p^e \parallel s$ . We then naturally have that  $p^{3e} \mid s^3$ . This implies  $p^{3e} \mid s^3v^2$ , so we must have that  $p^{3e} \mid t^2(u^3 + Aus^2 + Bs^3)$ . Since  $\gcd(u, s) = 1$ , it follows that  $p \nmid u$ , and thus  $p^{3e} \mid t^2$ .

But if  $p^{3e+1} \mid t^2$ , it would force  $p \mid v$ , contradicting  $\gcd(v, t) = 1$ . Hence, we conclude that  $p^{3e} \parallel t^2$ . If  $p^f \parallel t$ , then we must have that  $f = 3n$  and  $e = 2n$  for some  $n$ . Since our prime was arbitrary, we have that this holds for all primes. We can conclude that  $s = r^2$  and  $t = r^3$  for some integer  $r$ .

(2.) Now, let  $(x, y)$  be a rational point of  $E_0$ . Substituting our results from (1.) into  $E_0$ , we arrive at the following equation,

$$v^2 = u(u^2 - r^4).$$

When  $u = 0, 1,$  or  $1$  and  $v = 0$  we obtain the three points  $(0, 0), (1, 0),$  and  $(-1, 0)$ . Let  $g = \gcd(u, v)$  and write  $u = u_1g$  and  $v = v_1g$ . Substituting these into our equation we see that

$$gv_1^2 = u_1(g^2u_1^2 - r^4).$$

Since  $v_1$  and  $u_1$  share no common factors, we have that  $u_1 \mid g$ . We can write this as  $g = u_1u_2$  and substitute for  $g$  to obtain the equation

$$u_2v_1^2 = u_1^4u_2^2 - r^4.$$

Observe from (1.) that  $\gcd(u, r) = 1$  and so  $u_2 = 1$ . We have arrived at the equation  $v_1^2 = u_1^4 - r^4$  which has no non-zero integer solutions. This is proven by Fermat's method of descent, see [29, pg. 37].  $\square$

We now wish to show that  $E_m$  has trivial rational torsion for  $m \geq 1$  (a necessary condition to utilize Theorem 4.3).

For the next result we will need to utilize reductions of elliptic curves. A reduction of an elliptic curve at a prime  $p$  is a homomorphism

$$\text{red}_p : E(\mathbb{Q}) \rightarrow E(\mathbb{F}_p),$$

where  $\mathbb{F}_p$  denotes the finite field of order  $p$ . If the defining polynomial has distinct roots over  $\mathbb{F}_p$ , we call it a *good reduction* at  $p$ . Distinct roots appear if and only if  $p \nmid \Delta_{(A,B)}$  [33, pg. 196].

**Example 4.5.** Consider the elliptic curve over  $\mathbb{Q}$ ,  $y^2 = x^3 - x + 9$  (LMFDB 8732.b1) which we wish to reduce modulo 5. This curve has discriminant

$$\Delta = -16(4(-1)^3 + 27(9)^2) = -34416.$$

Since  $5 \nmid -34416$ , we have a good reduction given by  $y^2 \equiv x^3 - x + 4$ . Over

$\mathbb{F}_5$  the solutions to this are

$$E(\mathbb{F}_5) = \{\mathcal{O}, (0, 2), (1, 2), (2, 0), (4, 2), (0, 3), (1, 3), (4, 3)\}. \quad \triangle$$

If there is a good reduction at  $p$ , the Reduction mod  $p$  Theorem guarantees an injection from  $E(\mathbb{Q})_{\text{TORS}}$  into  $E(\mathbb{F}_p)$  [33, p. 192] (see Appendix A.2 for a proof and further resources on this result).

Using reductions, we can now prove the following theorem [6].

**Theorem 4.6.**  $E_m(\mathbb{Q})_{\text{TORS}} = \{\mathcal{O}\}$  for  $m \geq 1$ .

*Proof.* The discriminant of  $E_m$  is given by  $\Delta(E_m) = -16(27m^4 - 4)$ . Observe that  $3 \nmid 16(27m^4 - 4)$  and  $5 \nmid 16(27m^4 - 4)$ , so  $E_m$  has good reductions at 3 and 5.

If  $3 \mid m$ , then  $E_m$  reduces to  $y^2 = x^3 - x$  over  $\mathbb{F}_3$ . From Lemma 4.4 (2.), we know that the only points on  $E_m(\mathbb{F}_3)$  are  $\mathcal{O}, (0, 0), (1, 0)$ , and  $(-1, 0)$ . Moreover,  $E_m(\mathbb{F}_3)$  is isomorphic to  $V_4$ , the Klein Four Group (since each element has order 2 and any two non-identity elements add up to the third).

Since  $E(\mathbb{Q})_{\text{TORS}}$  injects into  $E(\mathbb{F}_p)$ , we know that all of the points of  $E(\mathbb{Q})_{\text{TORS}}$  have order two. The only points of order 2 on  $E_m$  are  $\mathcal{O}$  and the points of the form  $(r, 0)$ . However, by Lemma 4.4 (1.) we know that such a root cannot exist. Therefore, we can conclude that  $E_m(\mathbb{Q})_{\text{TORS}} = \{\mathcal{O}\}$ .

In the case that  $3 \nmid m$ , we know that  $m^2 \equiv 1 \pmod{3}$ . Therefore  $E_m$  reduces to  $y^2 = x^3 - x + 1$  over  $\mathbb{F}_3$ . Observe that

$$E_m(\mathbb{F}_3) = \{\mathcal{O}, (0, 1), (1, 1), (2, 1), (0, 2), (1, 2), (2, 2)\}.$$

Since  $E(\mathbb{Q})_{\text{TORS}}$  injects into  $E(\mathbb{F}_p)$ , we know that  $\#E(\mathbb{Q})_{\text{TORS}}$  must divide 7. So,  $\#E(\mathbb{Q})_{\text{TORS}}$  is either 1 or 7.

We can consider the reduction over  $\mathbb{F}_5$  in a similar fashion. Here,  $E_m$  is reduced to  $y^2 = x^3 - x$ ,  $y^2 = x^3 - x + 1$ , or  $y^2 = x^3 - x - 1$  depending on what  $m^2 \pmod{5}$  is. We compute these in the following table.

$E_m(\mathbb{F}_5)$	Points
$y^2 = x^3 - x$	$\mathcal{O}, (0, 0), (1, 0), (2, 1), (3, 2), (4, 0), (2, 4), (3, 3)$
$y^2 = x^3 - x + 1$	$\mathcal{O}, (0, 1), (1, 1), (3, 0), (4, 1), (0, 4), (1, 4), (4, 4)$
$y^2 = x^3 - x - 1$	$\mathcal{O}, (0, 2), (1, 2), (2, 0), (4, 2), (0, 3), (1, 3), (4, 3)$

Table 2: Reductions Mod 5

In every case  $|E_m(F_5)| = 8$ , so  $\#E(\mathbb{Q})_{\text{TORS}}$  must divide 8, i.e.  $\#E(\mathbb{Q})_{\text{TORS}} = 1, 2, 4$ , or 8. The only overlap between the reductions over 3 and 5 is when  $\#E(\mathbb{Q})_{\text{TORS}} = 1$  and we can therefore conclude that  $E_m(\mathbb{Q})_{\text{TORS}} = \{\mathcal{O}\}$ .  $\square$

It will be critical to provide some conditions on when a given rational point is not a double of any other rational point [6].

**Theorem 4.7.** *Let  $w, v, s, t \in \mathbb{Z}$  such that  $I = (u/s^2, v/s^3)$  and  $J = (w/t^2, z/t^3)$  are points on  $E$  with  $\gcd(uv, s) = \gcd(wz, t) = 1$ . Each of the following conditions is sufficient for  $I \neq 2J$ :*

1.  $u$  is even
2.  $u$  and  $s$  are odd and  $m$  is even
3.  $u \equiv 1 \pmod{4}$  and  $s$  and  $m$  are odd
4.  $u = -1$ ,  $s = 1$ , and  $m > 1$

*Proof.* Suppose by way of contradiction that  $I = 2J$ . Then, we can use the algebraic equations for the chord-tangent law to see that

$$\frac{u}{s^2} = \frac{(w/t^2)^4 + 2(w/t^2)^2 + 1 - 8m^2(w/t^2)}{4((w/t^2)^3 - (w/t^2) + m^2)}$$

which can be rearranged as

$$4u(wt^2(w^2 - t^4) + m^2t^8) = s^2((w^2 + t^4)^2 - 8m^2wt^6).$$

For each of the conditions, we will utilize this equation to arrive at a contradiction and therefore conclude that  $I \neq 2J$ .

**Condition 1:** If  $u$  is even, then we obtain

$$0 \equiv 4u(wt^2(w^2 - t^4) + m^2t^8) \pmod{8}$$

so we have

$$s^2(w^2 + t^4)^2 \equiv 0 \pmod{8}.$$

We know that  $\gcd(uv, s) = 1$  so  $s$  must be odd. Since any odd square must be congruent to 1 modulo 8, we then must have that

$$w^2 + t^4 \equiv 0 \pmod{8}.$$

If  $t$  is even, then we must necessarily have that  $w^2 \equiv 0 \pmod{8}$ , which only has solutions when  $w$  is even. This contradicts that  $\gcd(wz, t) = 1$ . If  $t$  is odd, then  $w^2 + 1 \equiv 0 \pmod{8}$  has no integer solutions.

**Condition 2:** The case where  $u$  and  $s$  are odd and  $m$  is even follows from a similar argument.

**Condition 3:** The case where  $u \equiv 1 \pmod{4}$  and  $s$  and  $m$  are odd is much more computationally difficult (it must be computed modulo 16) but also follows similarly.

**Condition 4:** Finally, suppose that  $u = -1$ ,  $s = 1$ , and  $m > 1$ . Substituting these values in, we see that

$$-4(wt^2(w^2 - t^4) + m^2t^8) = (w^2 + t^4)^2 - 8m^2wt^6$$

which can be rearranged to obtain

$$(w + t^2)^4 = 4t^4(w^2 + 2wt^2 + m^2t^2(2w - t^2)).$$

From this, we see that  $t \mid w$  which implies that  $t = 1$  since  $\gcd(w, t) = 1$ .

Substituting this into our equation yields that

$$(w^2 + 2w - 1)^2 = 4m^2(2w - 1)$$

However, this means that  $(2w - 1) \mid w^2$ .

We wish to show that  $\gcd((2w - 1), w^2) = 1$ . Let  $p$  be a prime in the prime factorization of  $w^2$ . Then  $p \mid w$ . Writing  $w = pk$ , we see that

$$2w - 1 = 2(pk) - 1 \equiv -1 \pmod{p}$$

and therefore  $p \nmid 2w - 1$ . Since this holds for all primes, we see that  $\gcd(2w - 1, w^2) = 1$ .

From this fact, we see that  $w$  necessarily equals 1 and therefore  $m = 1$ . This is a contradiction since we supposed that  $m > 1$ .

Overall, we have arrived at the desired result for each case.  $\square$

**Remark 4.8.** Where this comes into play is that we naturally see that  $P = (0, m)$ ,  $Q = (-1, m)$ , and  $P + Q = (1, -m)$  are not doubles of rational points since they satisfy conditions 1, 4, and both 2 and 3, respectively.

All that remains to prove Theorem 4.2 via Theorem 4.3 is to show that  $P$ ,  $Q$ , and  $P + Q$  are not in the same equivalence classes and that  $P$  and  $Q$  are independent [6].

**Lemma 4.9.** *Let  $m > 1$ , with  $P = (0, m)$  and  $Q = (-1, m)$ . Then  $H = \{[O], [P], [Q], [P + Q]\}$  is a four-element subgroup of  $E_m(\mathbb{Q})/2E_m(\mathbb{Q})$ .*

Before we proceed with the proof, it is important to clarify our notation in the quotient group  $E_m(\mathbb{Q})/2E_m(\mathbb{Q})$ . Specifically, for any point  $T \in E_m(\mathbb{Q})$ , we denote the equivalence class of  $T$  under the quotient map as  $[T]$ . The double of any point, say  $2T$ , is automatically in the same equivalence class as  $[\mathcal{O}]$  by construction.

*Proof.* Since  $P$ ,  $Q$ , and  $P + Q$  are not doubles of rational points (Remark 4.8), we know that none of them are in the same equivalence class as  $\mathcal{O}$ . If  $[P] = [Q]$ , then  $[P + Q] = [2P] = [\mathcal{O}]$  which is a contradiction. Also, we have that  $[P] \neq [P + Q]$  and  $[Q] \neq [P + Q]$ .

To show this, suppose  $[P] = [P + Q]$ . Then  $[(P + Q) + P] = [2P + Q] = [Q]$  but we also see that  $[(P + Q) + P] = [P + P] = [\mathcal{O}]$ . Setting these two expressions equal we realize that  $[Q] = [\mathcal{O}]$ , a contradiction. The argument for  $[Q] \neq [P + Q]$  is similar.

Therefore,  $H = \{[\mathcal{O}], [P], [Q], [P + Q]\}$  is a four-element subgroup of  $E_m(\mathbb{Q})/2E_m(\mathbb{Q})$ . □

**Lemma 4.10.**  *$P$  and  $Q$  are independent points on  $E_m(\mathbb{Q})$  for  $m \geq 2$ .*

*Proof.* Assume, for contradiction, that there exist integers  $n, m \in \mathbb{Z}$  such that  $nP + mQ = \mathcal{O}$ . Without loss of generality, suppose  $n$  and  $m$  are the smallest such integers. We proceed by cases.

**Case 1:**  $n$  is even and  $m$  is odd.

Write  $n = 2k$  and  $m = 2l + 1$  for some  $k, l \in \mathbb{Z}$ . Then:

$$[\mathcal{O}] = [nP + mQ] = [2kP + (2l + 1)Q] = [2(kP + lQ) + Q] = [Q].$$

This implies  $[Q] = [\mathcal{O}]$ , which contradicts what we showed in Lemma 4.9, i.e.  $[Q] \neq [\mathcal{O}]$ .

**Case 2:**  $n$  is odd and  $m$  is even.

Similarly, write  $n = 2k + 1$  and  $m = 2l$  for some  $k, l \in \mathbb{Z}$ . Then:

$$[\mathcal{O}] = [nP + mQ] = [(2k + 1)P + 2lQ] = [2(kP + lQ) + P] = [P].$$

This implies  $[P] = [\mathcal{O}]$ , which also contradicts Lemma 4.9.

**Case 3:** Both  $n$  and  $m$  are odd.

Write  $n = 2k + 1$  and  $m = 2l + 1$  for some  $k, l \in \mathbb{Z}$ . Then:

$$[\mathcal{O}] = [nP + mQ] = [(2k + 1)P + (2l + 1)Q] = [2(kP + lQ) + (P + Q)] = [P + Q].$$

This implies  $[P + Q] = [\mathcal{O}]$ , again contradicting Lemma 4.9.

**Case 4:** Both  $n$  and  $m$  are even.

If both  $n$  and  $m$  are even, then we write  $n = 2k$  and  $m = 2l$  for some  $k, l \in \mathbb{Z}$ . Then, we see that  $2(kP + lQ) = \mathcal{O}$  implies that  $2(kP + lQ)$  has order 2 in  $E(\mathbb{Q})$ . This is a contradiction since we know  $E_m$  has trivial rational torsion (via Theorem 4.6).  $\square$

With this proof, we have completed our journey and shown that Theorem 4.2 holds!

## 4.2 Higher Rank Subfamilies

In the last section, we proved that  $\text{rank}(E_m) \geq 2$  whenever  $m \geq 2$ , but there seem to be subfamilies of  $E_m$  which consistently have a higher rank. In this section, we seek to uncover some of them.

Before continuing, we provide the following generalization of Lemma 4.10

[6].

**Lemma 4.11.** *Let  $R$  be a rational point on  $E(\mathbb{Q})$  and let  $P_1, \dots, P_k$  be independent points in  $E(\mathbb{Q})$ . If  $[R] \notin \langle [P_1], \dots, [P_k] \rangle$  in  $E(\mathbb{Q})/E(2\mathbb{Q})$  and if  $E$  has trivial rational 2-torsion then  $R$  is independent from  $P_1, \dots, P_k$ .*

*Proof.* Suppose for contradiction that there are integers  $a_0, \dots, a_k$  such that

$$a_0R + a_1P_1 + \dots + a_kP_k = \mathcal{O}$$

and at least one of these integers is non-zero. Moreover, assume that  $a_0$  is the smallest positive integer so that this holds.

If  $a_0$  is odd then  $[a_0R] = [R]$  and we see that  $[R + a_1P_1 + \dots + a_kP_k] = [\mathcal{O}]$ .

This contradicts  $a_0$  being the smallest positive integer.

If  $a_0$  is even, then  $[a_0R] = [2R] = [\mathcal{O}]$ , we have that  $[a_1P_1 + \dots + a_kP_k] = [\mathcal{O}]$ . Since  $P_1, \dots, P_k$  are independent, we must have that each  $a_i$  is even. If we write  $a_i = 2b_i$  for each  $i$ , we see that  $2(b_1P_1 + \dots + b_kP_k) = \mathcal{O}$ . Since  $E(\mathbb{Q})$  has trivial rational torsion, we must have  $b_1P_1 + \dots + b_kP_k = \mathcal{O}$ . This contradicts  $a_0$  being the smallest positive integer.

In either case, we arrive at a contradiction and the result follows.  $\square$

We can also extend Theorem 4.7 to provide an additional condition for when  $A \neq 2B$  [6].

**Lemma 4.12.** *Let  $A = (u/s^2, v/s^3)$  and  $B = (w/t^2, z/t^3)$  with  $\gcd(uv, s) = \gcd(wz, t) = 1$ . If  $m \equiv 0 \pmod{3}$  and  $s \not\equiv 0 \pmod{3}$ , then  $A \neq 2B$ .*

*Proof.* Recall the following equation from the proof of Theorem 4.7.

$$4u(wt^2(w^2 - t^4) + m^2t^8) = s^2((w^2 + t^4)^2 - 8m^2wt^6).$$

Taking this equation modulo three reveals that

$$4uwt^2(w^2 - t^4) \equiv (w^2 + t^4)^2 \pmod{3}$$

since  $\gcd(wz, t) = 1$  we know that  $(w^2 + t^4)^2 \not\equiv 0$ . However, for all  $w, t \in \mathbb{Z}$  it can be shown that  $(w^2 - t^4) \equiv 0$ , so we have arrived at a contradiction.  $\square$

These two results enable us to generate infinite subfamilies of  $E_m$  with rank greater than two. The key to this is to find two additional independent points in distinct equivalence classes under  $E(\mathbb{Q})/2E(\mathbb{Q})$ . However, the computational complexity of this method escalates quickly, as the work doubles with each additional point.

**Example 4.13.** The following example is borrowed from [6]. We can consider  $E_{M(t)}$  for  $M(t) = 54t^2 - 165t - 90$  and  $R = (6t + 17, 54t^2 + 267t + 114)$  for any  $t \in \mathbb{Z}$ . Along with  $P + R$ , this forms an infinite subfamily of curves with rank of at least three (by Theorem 4.3).

This result was generalized in the doctorate thesis of Eikenberg where they considered “lifts” of rational points (which is to say that they find suitable points  $R$  then generalize it to a polynomial in  $\mathbb{Q}(t)$ ) [15, pg. 28].

**Theorem 4.14.** *For any  $m_0 \in \mathbb{Q}$  with  $m_0 \neq 0$  and any point  $(p, q) \in E_{m_0}(\mathbb{Q})$ , there exists a quadratic polynomial  $M(t)$  with  $M(0) = m_0$  and a point  $R(t)$  with  $R(0) = (p, q)$  such that  $P = (0, M(t))$ ,  $Q = (1, M(t))$  and  $R(t)$  are independent points in  $E_{M(t)}(\mathbb{Q}(t))$ .*

The proof of this result is well beyond the scope of this paper, but can be found in [15, pg. 28].

**Example 4.15.** We can utilize this result to find more subfamilies of  $E_m$  with rank of at least 3. For example, consider  $M(0) = 2$ . Then, we utilize Theorem 3.4.1 in [15, pg. 25–26] to find the polynomial and point

$$M(t) = \frac{1}{t^2} + \frac{23}{12}t + 2$$

$$R(t) = \left( t + 4, \frac{1}{t^2} + \frac{23}{12}t + 8 \right)$$

This along with  $P = (0, M(t))$  and  $Q = (1, M(t))$  is an infinite subfamily of  $E_m$  with rank at least 3.

A member of this family ( $t = 12$ ) is the curve  $E_{73}$ . It has the three independent points  $P = (0, 73)$ ,  $Q = (1, 73)$ , and  $R = (16, 97)$ . A quick computation in Sage shows that the rank of this curve is indeed 3.  $\triangle$

Apart from subfamilies of rank 3, the curious reader can also find results for much larger ranks in [15] (though they are omitted here due to complexity).

## 5 Complex Elliptic Curves

As we shift our perspective to elliptic curves over the complex numbers, we uncover their dual nature as both algebraic and analytic objects. This transition, pioneered by Karl Weierstraß, provides new tools from complex analysis and geometry that deepen our understanding of their structure and inform the arithmetic questions we have explored so far [33, pg. 157–171].

Weierstraß's key insight was to associate an elliptic curve with a lattice  $\Lambda \subset \mathbb{C}$ , showing that the curve can be expressed as a quotient  $\mathbb{C}/\Lambda$ , resulting in a torus. He introduced the  $\wp$ -function, a doubly-periodic meromorphic

function, to parametrize points on these curves and recast their equations in the familiar form

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

where  $g_2$  and  $g_3$  are lattice-dependent invariants [33, pg. 170–171].

This analytic framework unifies the algebraic, geometric, and arithmetic properties of elliptic curves. It also introduces the  $j$ -invariant, which classifies elliptic curves up to isomorphism. By grounding elliptic curves in the complex numbers, we gain a geometric lens that complements our earlier exploration of their arithmetic properties, setting the stage for modern applications of elliptic curve theory.

## 5.1 Elliptic Curves are Complex Tori

Let  $\omega_1$  and  $\omega_2$  be two complex numbers such that  $\frac{\omega_1}{\omega_2} \notin \mathbb{R}$ . We define the integer lattice  $A$  as follows:

$$A = \{m\omega_1 + n\omega_2 : m, n \in \mathbb{Z}\}.$$

The set  $A$  consists of all integer linear combinations of  $\omega_1$  and  $\omega_2$ , forming a discrete subgroup of  $\mathbb{C}$ . The parallelogram defined by the vectors  $\omega_1$  and  $\omega_2$  emanating from the origin is referred to as the *fundamental period parallelogram*.

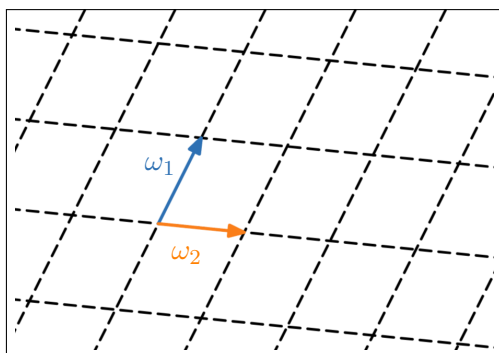
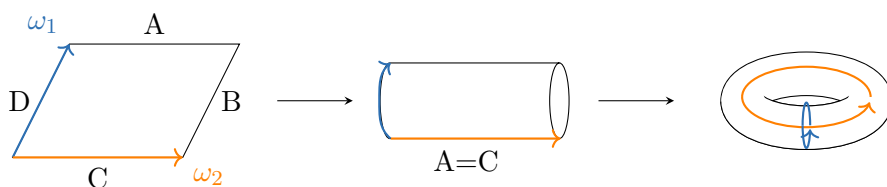


Figure 8:  $\Lambda$  with  $\omega_1$  and  $\omega_2$

To understand the structure of the quotient space  $\mathbb{C}/\Lambda$ , we can visualize it as a torus, denoted  $S^1 \times S^1$ . We begin with the fundamental period parallelogram and imagine the following process:



1. **Rolling the Parallelogram:** First, we roll the parallelogram such that the side labeled A is glued to the side labeled C. This creates a cylindrical shape.
2. **Connecting the Ends:** Next, we connect the two circular ends of the cylinder to form a torus.

With this construction, moving in the direction of  $\omega_1$  corresponds to tracing the inner ring of the torus, while moving in the direction of  $\omega_2$  traces the outer ring. Thus, we establish that  $\mathbb{C}/\Lambda \cong S^1 \times S^1$ .

Next, we introduce the Weierstraß  $\wp$ -function, a fundamental tool in the study of elliptic functions (read as the Weierstraß elliptic function). This is defined as follows:

$$\wp(z) = \frac{1}{z^2} + \sum_{(m,n) \in \mathbb{Z}^2 \setminus \{(0,0)\}} \left( \frac{1}{(z - m\omega_1 - n\omega_2)^2} - \frac{1}{(m\omega_1 + n\omega_2)^2} \right).$$

The  $\wp$ -function maps points from the quotient space  $\mathbb{C}/\Lambda$  to the complex plane  $\mathbb{C}$  [33, pg. 165]. It has a few key properties which make it especially useful. Particularly,  $\wp$  is an *elliptic function*. An elliptic function is defined over  $\mathbb{C}$  and has two essential characteristics: it is both meromorphic and doubly-periodic.

To clarify, a function  $f$  is said to be *meromorphic* if it is analytic on its entire domain except for a discrete set of isolated singularities (in this case, the lattice points  $\Lambda$ ). Furthermore,  $f$  is *doubly-periodic* if there exist two complex periods  $u, v \in \mathbb{C}$  such that  $f(z + u) = f(z)$  and  $f(z + v) = f(z)$  [33, pg. 166]. For the function  $\wp$ , the periods are the  $\omega_1$  and  $\omega_2$  from  $\Lambda$ .

We first introduce the following lemma to establish that  $\wp$  is indeed an elliptic function.

**Lemma 5.1.** *The Eisenstein series  $\sum_{\omega \in \Lambda \setminus \{0\}} \omega^{-2k}$  converges absolutely for  $k > 1$ .*

*Proof.* This proof is rather lengthy, so it can be found in Appendix A.3.  $\square$

We can use this lemma to show that  $\wp$  is meromorphic over  $\mathbb{C}$  [33, pg. 165–166].

**Theorem 5.2.** *The series defining  $\wp$  converges absolutely and uniformly on each compact subset of  $\mathbb{C} - \Lambda$ .*

*Proof.* We aim to show that the series

$$\sum_{(m,n) \in \mathbb{Z}^2 \setminus \{(0,0)\}} \left( \frac{1}{(z - m\omega_1 - n\omega_2)^2} - \frac{1}{(m\omega_1 + n\omega_2)^2} \right)$$

converges absolutely and uniformly on each compact subset of  $\mathbb{C} - \Lambda$ . By Theorem 4 in [22, pg. 277], this establishes that  $\wp$  is analytic on  $\mathbb{C} - \Lambda$ . At the points of  $\Lambda$ ,  $\wp$  has poles of order 2 [33, pg. 165–166], which implies that  $\wp$  is meromorphic on all of  $\mathbb{C}$ .

To this end, let  $\omega = m\omega_1 + n\omega_2 \neq 0$  and suppose that  $|\omega| > 2|z|$ . Then,

$$\left| \frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right| = \left| \frac{\omega^2 - (z - \omega)^2}{\omega^2(z - \omega)^2} \right| = \left| \frac{z(2\omega - z)}{\omega^2(z - \omega)^2} \right|.$$

Using our assumption that  $|\omega| > 2|z|$  and the triangle inequality, the numerator satisfies

$$|z(2\omega - z)| \leq |z| \cdot (2|\omega| + |z|) \leq \frac{5|\omega||z|}{2}$$

and the denominator satisfies

$$|\omega^2(z - \omega)^2| = |\omega^2| \cdot |z - \omega|^2 \geq |\omega^2| \cdot (|\omega| - |z|)^2 \geq \frac{|\omega^4|}{4}.$$

Substituting these bounds in, we see that

$$\left| \frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right| = \left| \frac{z(2\omega - z)}{\omega^2(z - \omega)^2} \right| \leq \frac{5|\omega||z|}{\frac{|\omega^4|}{4}} = \frac{10|z|}{|\omega^3|}.$$

Using Lemma 5.1, we see that this series converges uniformly and absolutely.

We conclude that  $\wp$  is meromorphic on all of  $\mathbb{C}$ .  $\square$

All that remains to show that  $\wp$  is an elliptic function is to show that it is doubly-periodic.

**Theorem 5.3.**  *$\wp$  is doubly-periodic*

*Proof.* First, observe that  $\wp(z) = \wp(-z)$  so  $\wp$  is an even function. Then, we consider

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

which must be an odd function (the derivative of any even differentiable function is odd). Evaluating at  $z + \omega_0$  just rearranges the terms in the sum, so  $\wp'(z)$  is doubly-periodic.

Since  $\wp'(z)$  is doubly-periodic, we have that  $\wp'(z + \omega_i) = \wp'(z)$  for  $i = 1, 2$ . Integrating and rearranging, we see that  $\wp(z + \omega_i) - \wp(z) = c$  for some constant  $c$ . Evaluating at  $z = -\omega_i/2$ , we see that  $\wp(\omega_i/2) - \wp(\omega_i/2) = c$ . Since  $\wp$  is even, we must have that  $c = 0$ . Therefore,  $\wp$  is doubly-periodic by definition.  $\square$

By leveraging  $\wp$  and its properties, we can construct an elliptic curve over  $\mathbb{C}$  given by:

$$\wp'(z) = 4[\wp(z)]^3 - g_2\wp(z) - g_3,$$

where  $g_2$  and  $g_3$  are invariants associated with the lattice  $\Lambda$ .

This construction gives us a direct isomorphism  $\psi : \mathbb{C}/\Lambda \rightarrow E$  [33, pg. 173]. Since  $\mathbb{C}/\Lambda$  can be realized as a torus, this gives us that every elliptic curve over  $\mathbb{C}$  is topologically equivalent to a complex torus.

## 5.2 Isomorphism Classes: the $j$ -invariant

The  $j$ -invariant of an elliptic curve  $E$  in normal form  $y^2 = x^3 + Ax + B$  is given by

$$j(E) = -1728 \frac{4A^3}{4A^3 + 27B^2},$$

The  $j$ -invariant is an invaluable object for classifying elliptic curves. Specifically, we have the following theorem [33, pg. 44].

**Theorem 5.4.** *Two elliptic curves  $E$  and  $E'$  are isomorphic over  $\mathbb{C}$  if and only if  $j(E) = j(E')$*

*Proof.* We prove this under the assumption that  $E$  and  $E'$  can be written in normal form. Let

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

$$E' : y^2 = x^3 + A'x + B'.$$

We first show that if  $E$  and  $E'$  are isomorphic, then  $j(E) = j(E')$ . Any isomorphism from  $E$  to  $E'$  must have the form  $(x, y) \mapsto (u^2x, u^3y)$  for some  $u \in \mathbb{C}$  with  $u \neq 0$  [33, pg. 44]. Using this change of coordinates,  $y^2 = x^3 + Ax + B$  becomes

$$(u^3y)^2 = (u^2x)^3 + A(u^2x) + B.$$

Expanding this equation, we obtain

$$u^6y^2 = u^6x^3 + Au^2x + B$$

Which we can write equivalently as

$$y^2 = x^3 + u^{-4}Ax + u^{-6}B.$$

Thus,  $A' = u^{-4}A$  and  $B' = u^{-6}B$ .

Now we compute the  $j$ -invariants of  $E$  and  $E'$ . For  $E$ , the  $j$ -invariant is

$$j(E) = -1728 \frac{4A^3}{4A^3 + 27B^2}.$$

For  $E'$ , we have

$$j(E') = -1728 \frac{4(A')^3}{4(A')^3 + 27(B')^2} = -1728 \frac{4(u^{-4}A)^3}{4(u^{-4}A)^3 + 27(u^{-6}B)^2}.$$

Simplifying, we find

$$j(E') = -1728 \frac{4A^3}{4A^3 + 27B^2} = j(E),$$

which is our desired result.

Next, we show that if  $j(E) = j(E')$  then  $E$  and  $E'$  are isomorphic. By the definition of the  $j$ -invariant, we have

$$-1728 \frac{4A^3}{4A^3 + 27B^2} = -1728 \frac{4A'^3}{4A'^3 + 27B'^2}.$$

Simplifying, this implies that

$$A^3B'^2 = A'^3B^2.$$

So we must look for an isomorphism of the form  $(x, y) \mapsto (u^2x', u^3y')$ . We now consider cases based on the values of  $A$  and  $B$ .

If  $A = 0$ , then  $B \neq 0$  or else the discriminant of  $E$ ,  $\Delta$  is zero (or in other words,  $E$  is singular). Observe that  $j(E) = 0$ . Since  $j(E) = j(E')$ , we must have  $B' \neq 0$ . In this case, the curves  $E$  and  $E'$  are isomorphic under the change of coordinates  $(x, y) \mapsto ((B/B')^{1/3}u, (B/B')^{1/2}v)$ .

If  $B = 0$ , then  $j(E) = 1728$ . Consequently, we see that  $A' \neq 0$ . In this case, the curves  $E$  and  $E'$  are isomorphic under the change of coordinates  $(x, y) \mapsto ((A/A')^{1/2}u, (A/A')^{3/4}v)$ .

In the case  $AB \neq 0$ , either transformation will send  $E$  to  $E'$ .  $\square$

We can combine this with the following theorem to get a rather surprising result.

**Theorem 5.5.** *If  $\gamma$  is any complex number, then there exists an elliptic curve whose  $j$ -invariant is  $\gamma$ .*

*Proof.* If  $\gamma$  is 0 or 1728, then  $y^2 + y = x^3$  and  $y^2 = x^3 + x$  have  $j$ -invariants 0 and 1728 respectively.

In all other cases for  $\gamma \in \mathbb{C}$ , consider the elliptic curve

$$y^2 + xy = x^3 - \frac{36}{\gamma - 1728}x - \frac{1}{\gamma - 1728}.$$

A straightforward but tedious computation shows this curve has a  $j$ -invariant of  $\gamma$ .  $\square$

Therefore, we see that for any complex number, there is a unique isomorphism class of elliptic curves. Notably, we spent this section working with  $E(\mathbb{C})$ . It would be nice if we had an analog of Corollary 5.4 for elliptic curves over  $\mathbb{Q}$ . However, we do not since  $\mathbb{Q}$  is not algebraically closed (we do have an analog for this over the algebraic closure of  $\mathbb{Q}$  though). We can see this in the following example.

**Example 5.6.** Let  $E_1$  and  $C_3$  be the elliptic curves

$$E_1 : y^2 = x^3 + x$$

$$C_3 : y^2 = x^3 + 3x$$

Over  $\mathbb{C}$  these two curves are isomorphic because they both have a  $j$ -invariant of 1728. However, we will show that they don't have the same rational

subgroups, i.e.  $E_1(\mathbb{Q}) \not\cong C_3(\mathbb{Q})$ .

By the Nagell-Lutz Theorem (Theorem 3.15) we know that any point with rational torsion must have integer coordinates with  $y = 0$  or  $y^2 | (\Delta/16)$ .

From this, we arrive at the following candidates for points in  $E_1(\mathbb{Q})_{\text{TORS}}$  and  $C_3(\mathbb{Q})_{\text{TORS}}$ .

$$E_1 : (0, 0) (1, \pm 2) (3, \pm 6) (12, \pm 42)$$

$$C_3 : (0, 0) (1, \pm 2) (3, \pm 6) (12, \pm 42)$$

In both curves, we know that  $(0, 0)$  has order 2. A proof by infinite descent can be used to show that  $\text{rank}(E_1) = 0$  (because there are no rational points other than  $(0, 0)$ ). Therefore,  $E_1(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ .

However, a computation in Sage shows us that  $(1, 2)$  has infinite order in  $C_3$ . So,  $\text{rank}(C_3) \geq 1$ . Notably, the rest of our potential points for  $C_3$  also have infinite order but are dependent on  $(1, 2)$ . Specifically,  $(3, 6) = (0, 0) - (1, 2)$  and  $(12, 42) = (0, 0) + 2(1, 2)$ .

Though we have not yet developed the tools to prove it explicitly, a Sage computation shows that  $\text{rank}(C_3)=1$ , so  $C_3(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$ .

Even though these curves are isomorphic over  $\mathbb{C}$  they are not isomorphic over  $\mathbb{Q}$ . △

## 6 Contemporary Results

Having developed the foundational tools to study elliptic curves, we now see their profound impact on contemporary mathematics. The group structure and arithmetic properties of elliptic curves, which we explored earlier,

play a crucial role in elliptic curve cryptography, ensuring secure digital communication. We will also encounter their connection to the Birch and Swinnerton-Dyer conjecture, one of the most famous open problems in mathematics.

Finally, we will also scratch the surface of how elliptic curves are deeply tied to modular forms through the modularity theorem, a pivotal result that enabled Andrew Wiles to prove Fermat's Last Theorem. This rich interplay between algebra, geometry, and analysis demonstrates the unifying role of elliptic curves across diverse areas of mathematics. It explains why elliptic curves are continuously studied to this day.

## 6.1 Elliptic Curve Cryptography

Securing sensitive information has been a challenge long predating the digital age. Throughout history, creative solutions emerged through physical concealment, intricate ciphers, and other ingenious tricks [32]. Notably, some of the earliest computers were specifically designed to break complex codes, the Enigma code is a prime example [32]. As technology advanced, so did the methods for encoding information, evolving to meet new security demands. The field of *cryptography* today is perhaps more essential—and complex—than ever before.

One of the most significant breakthroughs in cryptography was the development of the Diffie-Hellman key exchange. Introduced by Whitfield Diffie and Martin Hellman, this method transformed secure communication by creating a system for secure key exchange, laying the foundation for many modern cryptographic protocols [12].

Before their revolutionary work, the most common approach to secure messaging involved a *symmetric* key exchange, where two parties would agree on a shared key or passphrase beforehand. When one party sends an encoded message, the other could use this shared key to decode it, and vice versa. However, this approach presented major vulnerabilities: intercepting or deducing the shared key was often relatively easy, and securely distributing such keys posed a serious challenge [12].

Diffie and Hellman’s method, however, sidesteps these issues. Instead of relying on a shared pass-key, each party generated a private key, which, when combined with a public key, allowed them to securely exchange information. This approach often leverages a mathematical principle known as the *discrete logarithm problem* (DLP), which states:

**DLP:** Given a group  $G$  with elements  $a \in G$  and  $b \in \langle a \rangle$ , find the smallest integer  $n$  such that  $a^n = b$ .

In cryptographic contexts, it is straightforward to compute  $a^n$  when  $n$  is known, but finding  $n$  from the result is much harder—especially as  $G$  becomes more complex.

To illustrate this method, let’s imagine two agents, Alice and Bob, attempting to securely share a secret, such as the code to a Swiss vault. They proceed as follows:

1. Alice publicly shares a large prime number  $p$  and a base integer  $x < p$ .
2. Alice selects a secret integer  $a$ , and Bob chooses a secret integer  $b$ .
3. Alice computes  $A \equiv x^a \pmod{p}$ , and Bob computes  $B \equiv x^b \pmod{p}$ .

4. Alice and Bob exchange their computed values,  $A$  and  $B$ , with each other.
5. Alice then computes  $B^a$  and Bob computes  $A^b$ . Both arrive privately at the shared secret  $x^{ab}$ : the code to the Swiss vault.

This method allows Alice and Bob to establish a shared secret without ever directly exchanging the key, enhancing security against potential eavesdroppers.

The advent of elliptic curve cryptography (ECC) introduced the innovative idea of utilizing elliptic curves  $E$ , under the chord-tangent addition law, as the group for the Diffie-Hellman key exchange [26]. The form of the discrete logarithm problem for  $E$  is called the elliptic curve discrete logarithm problem, or ECDLP for short.

**Example 6.1.** Suppose Alice and Bob want to generate a shared passcode to access a file on their laptops. They publicly declare that they will use the elliptic curve  $E : y^2 = x^3 - x + 9$ , the prime 167449, and the point  $P = (1, 3)$ . Notably,  $E$  has a good reduction at 167449 because  $167449 \nmid \Delta_{(-1,9)}$ . Alice privately decides to use the integer  $a = 37$  and Bob privately chooses to utilize the integer  $b = 112$ . Then, Alice uses the reduction of  $E$  over  $\mathbb{F}_{167449}$  to compute

$$A = 37 \cdot (1, 3) = (152614, 148780)$$

and Bob similarly computes

$$B = 112 \cdot (1, 3) = (36051, 32968).$$

They share both of these results publicly, and multiply the other's result by

their secret integer to arrive at the ordered pair

$$37 \cdot 112 \cdot P = (80843, 123461)$$

Since both arrive at this same result, their laptops use this shared point as a passcode to enable data access.  $\triangle$

Using elliptic curves is a dramatic improvement over traditional Diffie-Hellman key exchange. As we saw in the example, we can share a lengthy code, even with small private keys and a simple elliptic curve. This ease of access to computational complexity makes it nearly 20 times better than traditional Diffie Hellman (or the relatively comparable RSA) encryption (measured in required bytes of data to obtain the same security) [18][3, pg. 19–23].

## 6.2 Rank and the BSD Conjecture

Without an effective way to compute  $\text{rank}(E)$  consistently, mathematicians began to try creative, out-of-the-box solutions to chip away at this dilemma. Mathematicians Bryan Birch and Peter Swinnerton-Dyer were amongst some of the most influential mathematicians in this era of the problem. Their idea was to study  $E(\mathbb{Q})$  indirectly through reductions of elliptic curves (modulo  $p$ ).

This approach would simplify the analysis, as  $E(\mathbb{F}_p)$  is finite and therefore easier to work with, while still reflecting properties of  $E(\mathbb{Q})$ . Their intuition was that if  $E(\mathbb{Q})$  contained many rational points, then the size of  $E(\mathbb{F}_p)$  should tend to be large “on average” across primes  $p$  [31].

To quantify this relationship, Birch and Swinnerton-Dyer looked at the

product:

$$\pi_E(X) := \prod_{p \leq X, p \nmid \Delta} \frac{\epsilon_p}{p},$$

where  $\epsilon_p = \#E(\mathbb{F}_p)$  represents the number of points on  $E$  over  $\mathbb{F}_p$ . From this search, they conjectured the estimate that

$$\pi_E(X) \approx C(\log(X))^{\text{rank}(E)}$$

for some constant  $C$  that depends on  $E$ . This provided interesting insights into  $\text{rank}(E)$  but the behavior of  $\pi_E(X)$  proved too erratic for practical analysis, leading the mathematicians to seek a new pathway: the Hasse-Weil  $L$ -function. [31].

The Hasse-Weil  $L$ -function, is defined as

$$L(E, s) = \prod_{p \nmid \Delta} \left( 1 - \frac{1 + p - \epsilon_p}{p^s} + \frac{p}{p^{2s}} \right)^{-1} \times \prod_{p \mid \Delta} \ell_p(E, s)^{-1}.$$

Notably, this function only converges for  $\text{Re}(s) > 3/2$ . This function extends the reach of  $\pi_E(X)$  into the complex plane (smoothing out its erratic nature significantly).

Birch and Swinnerton-Dyer defined the *analytic rank*, which we refer to as  $\text{rank}_{an}(E)$ , to be the order of vanishing at  $s = 1$ . For the unfamiliar reader, the order of vanishing at the pole or zero  $z_0$  is the smallest positive integer  $n$  such that when you multiply the function by  $(z - z_0)^n$ , the resulting function has a removable singularity at that point (goes from becoming undefined to defined at that point).

Notice that, though this function does not necessarily converge at  $s = 1$ ,

evaluating at  $s = 1$  yields

$$L(E, 1) = \prod_{p \nmid \Delta} \left( \frac{\epsilon_p}{p} \right)^{-1} \times \prod_{p \mid \Delta} \ell_p(E, 1)^{-1}.$$

Since the right term is finite, we see that (if everything is sufficiently “nice”) the behavior around  $s = 1$  reflects the average size of  $\epsilon_p$  (This is because as  $\epsilon_p$  gets larger,  $L(E, s)$  will converge to 0 faster as  $s$  tends to 1—the negative exponent is key for this realization). This led Birch and Swinnerton-Dyer to the following conjecture.

**Conjecture 6.2** (Weak BSD). *For every elliptic curve  $E$ ,*

$$\text{rank}(E) = \text{rank}_{\text{an}}(E).$$

Reflecting on this, one appreciates the elegance of the BSD conjecture: it proposes a bridge between the seemingly discrete world of rational points on elliptic curves and the continuous, complex landscape of  $L$ -functions. Yet, despite the coherence of the conjecture, proving it remains one of the great challenges in number theory [7].

### 6.3 Modular Forms and Fermat’s Last Theorem

A few centuries after Diophantus began work with elliptic curves, we encounter Pierre de Fermat. His interest in Diophantine equations led him to scribble the following theorem into the margins of his copy of Diophantus’s *Arithmetica*,

“It is impossible for a cube to be a sum of two cubes, a fourth power to be a sum of two fourth powers, or in general for any number that is a power greater than the second to be the sum

of two like powers. I have discovered a truly remarkable proof, but this margin is too small to contain it” [19].

In modern notation, this says that for any natural number  $n > 2$ , there are no non-zero integer solutions to  $x^n + y^n = z^n$  (which we call Fermat’s equation). The proof of this result, which came to be known as Fermat’s Last Theorem (FLT), baffled mathematicians for centuries. To answer this question, mathematicians had to discover bridges between the world of complex analysis and number theory. In the following section, we briefly outline this development.

There were many attempts to prove FLT throughout the past few centuries. One notable one was by mathematician Sophie Germain, who considered FLT over what she called *Sophie Germain Primes*. These are primes which can be expressed as  $2p + 1$  where  $p$  is another prime. From this, she achieved the following result [14, pg. 61–65].

**Theorem 6.3.** *Let  $p$  be an odd prime such that  $2p + 1$  is a Sophie Germain Prime. If  $x^p + y^p = z^p$ , then at least one of  $x$ ,  $y$ , or  $z$  is divisible by  $p$ .*

This theorem gives a strategy for proving FLT in several cases: show that  $x^p + y^p + z^p \neq 0$  with the additional assumption that one of  $x$ ,  $y$ , or  $z$  is divisible by  $p$ , then show that it also holds when none of them are divisible by  $p$  [14, pg. 61–65].

Several other results proved FLT for specific cases, but the solution for all  $n > 2$  still evaded mathematicians. Several developments in the study of elliptic curves were critical to the now-celebrated proof.

First, mathematician Gerhard Frey noticed that if  $(A, B, C)$  was a solution to Fermat's equation, then one could make the elliptic curve

$$y^2 = x(x - A^n)(x - B^n).$$

We call curves of this form *Frey Curves*. After playing around with these curves, Frey realized that they were likely not *modular* [10, pg. 8–10] (this was later proved by Kenneth Ribet [30]). This spurred mathematician Andrew Wiles to seek out a new angle of attack: prove that all (or at least sufficiently many) elliptic curves are modular. If this were the case, then a Frey curve could not exist, and therefore neither could a solution to Fermat's equation.

To understand Wiles's approach, we need to delve into the concept of modular forms. Before we do so, we define a *group action*. A group action formalizes the notion of a group “acting” on a set. Formally, we say that a group  $G$  *acts* on a set  $S$  if there is a function  $\alpha : G \times S \rightarrow S$  satisfying two properties:

1. **Identity:** The identity element  $e \in G$  leaves every element of  $S$  unchanged, i.e.,  $\alpha(e, s) = s$  for all  $s \in S$ .
2. **Compatibility:** For all  $g, h \in G$  and  $s \in S$ , the action satisfies  $\alpha(g, \alpha(h, s)) = \alpha(gh, s)$ .

for all  $g, h \in G$  and  $s \in S$  [23, pg. 25].

**Example 6.4.** To see this in action, let  $C_4$  be the cyclic group of order 4. This group acts on the set of vertices of a square  $S = \{v_1, v_2, v_3, v_4\}$ . Specifically, each element  $r \in C_4$  gives us a rotation of the vertices.

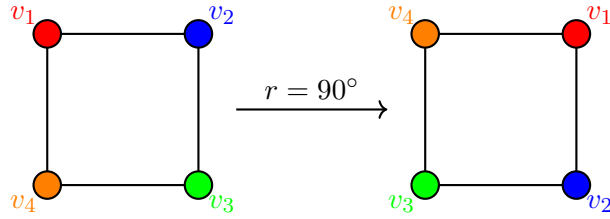


Figure 9:  $C_4$  acts on a Square

Returning to our discussion of modular forms, the group  $SL_2(\mathbb{Z})$  (the group of  $2 \times 2$  integer matrices with determinant 1 under multiplication) acts on the upper half-plane  $\mathcal{H}$ , defined as the set of all complex numbers  $z$  with  $\text{Im}(z) > 0$  [2, pg. 25–28]. The action is given by:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az + b}{cz + d}.$$

With this, we have what it takes to define a modular form. A modular form of weight  $k$  and level  $N$  is a holomorphic function  $f : \mathcal{H} \rightarrow \mathbb{C}$  that satisfies:

1. **Modularity condition:** For all  $\gamma \in \Gamma_0(N)$ ,  $f$  obeys the transformation law:

$$f(\gamma z) = (cz + d)^k f(z).$$

2. **Growth condition:**  $f(z)$  grows at most polynomially as  $\text{Im}(z) \rightarrow \infty$ , ensuring it extends holomorphically to the cusps of the modular curve.

Due to these conditions, Modular forms are highly symmetric and are geometrically considered to be fractals.



Figure 10: Graph of a Modular Form [20]

Modular forms of a given weight form a linear space over  $\mathbb{C}$ , but many of these spaces have dimension zero, i.e. there are no non-trivial modular forms of that weight (the function that always gives an output of 0 is a trivial modular form that exists for all weights). For example, there are no modular forms with weight  $k = 2$  or odd weight [1, pg. 116].

Any modular form can be written as a Laurent Series of the form

$$f(z) = \sum_{n=1}^{\infty} c_n e^{2\pi iz}$$

where  $c_n$  are coefficients dependent on  $n$  [2, pg. 26].

With this definition in hand, we have what it takes for an elliptic curve to be modular. Recall that the Hasse-Weil  $L$ -function associated to each elliptic curve is defined as

$$L(E, s) = \prod_{p|\Delta} \left( 1 - \frac{1+p-\epsilon_p}{p^s} + \frac{p}{p^{2s}} \right)^{-1} \times \prod_{p|\Delta} \ell_p(E, s)^{-1}$$

and that this function is only convergent for  $\text{Re}(s) > 3/2$ . This function can be expressed as a *Dirichlet Series*

$$L(E, s) = \sum_{n=1}^{\infty} \frac{\epsilon_n}{n^s}.$$

An elliptic curve  $E$  is *modular* whenever there exists a modular form  $f$  such that the Dirichlet Series of  $L(E, s)$  and the Laurent Series of  $f$  have

the same coefficients. It has been shown that all elliptic curves over  $\mathbb{Q}$  are indeed modular [5].

In [38], Andrew Wiles proved that all semi-stable elliptic curves are modular (this is the “sufficiently many” we alluded to earlier. Frey curves are necessarily semi-stable). If Frey curves existed, then they would not be modular, as seen in [30]. We have arrived at a contradiction, and therefore there cannot be a solution to Fermat’s Equation. Though we have omitted many of the details leading up to this result, its significance cannot be understated.

## A Appendix

### A.1 Weierstraß Normal Form

To put a cubic in Weierstraß Normal Form:

1. Find any inflection point  $P$  and the tangent line at that point.
2. Find a projective change of coordinates to send  $P \rightarrow (0 : 1 : 0)$  and the tangent line to  $z = 0$
3. Substitute variables so that  $cx^3 \rightarrow 1x^3$  and  $cy^2z \rightarrow -y^2z$ . Set  $z = 1$ .

Your cubic will now be of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Then, we complete the square and perform an affine change of coordinates.

4. Overall, let

$$b_2 = a_1^2 + 4a_2,$$

$$b_4 = a_1a_3 + 2a_4,$$

$$b_6 = a_3^2 + 4a_6,$$

$$c_4 = b_2^2 - 24b_4,$$

$$c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

5. Your cubic in Weierstraß Normal Form will have the form

$$y^2 = x^3 - 27c_4x - 54c_6.$$

Notably, for an elliptic curve over a (potentially finite) field  $K$ , completing the square is only possible if  $\text{char}(K) \neq 2, 3$ .

**Remark.**  $\text{char}(K)$  is the characteristic of the field. It is how often you must add the additive identity to itself to arrive at 0. For example,  $\text{char}(\mathbb{Z}/3\mathbb{Z}) = 3$  since  $1 + 1 + 1 = 3 = 0$  modulo three.

Whenever  $\text{char}(K) = 2, 3$ , we use the expanded Weierstraß form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

## A.2 Reduction mod $p$ Theorem

We show that  $E(\mathbb{Q})_{\text{TORS}}$  injects into  $E(\mathbb{F}_p)$  for some fixed prime  $p$ .

To do so we will need the following definitions:

- $E_0(\mathbb{Q})$  is the set of points such that  $E(\mathbb{F}_p)$  is non-singular.
- $E_1(\mathbb{Q}) = \ker(\text{red}_p)$  where  $\text{red}_p$  is our map from  $E(\mathbb{Q})$  to  $E(\mathbb{F}_p)$
- $E(\mathbb{Q})[m]$  are the rational torsion points of order  $m$
- $E_{ns}(\mathbb{F}_p)$  are the nonsingular points after applying  $\text{red}_p$

*Proof.* Let  $E(\mathbb{Q})$  be an elliptic curve over  $\mathbb{Q}$  and  $m \geq 1$  be an arbitrary integer.

We have the following short exact sequence [33, p.188]

$$0 \longrightarrow E_1(\mathbb{Q}) \longrightarrow E_0(\mathbb{Q}) \longrightarrow E_{ns}(\mathbb{F}_p) \longrightarrow 0$$

A short exact sequence is a diagram of functions that is *exact*. This means that for each function  $f_i$  in the sequence (labeled from left to right),

the kernel of the next function equals the image of the current one:  $\ker(f_{i+1}) = \text{im}(f_i)$ . If we have a good reduction at  $p$ , then this diagram becomes

$$\begin{array}{ccccccc} 0 & \longrightarrow & E_1(\mathbb{Q}) & \longrightarrow & E(\mathbb{Q}) & \longrightarrow & E(\mathbb{F}_p) \longrightarrow 0 \\ & & \cup & & \cup & & \cup \\ & & 0 & \longrightarrow & E(\mathbb{Q})[m] & \longrightarrow & E(\mathbb{F}_p)[m] \longrightarrow 0 \end{array}$$

Since  $E_1(\mathbb{Q})[m]$  has no nontrivial points of order  $m$ —a tricky fact to prove, but nonetheless true [33, p.192]—we can use the fact that  $\ker(\text{red}_p) = E_1(\mathbb{Q})$  to see that  $E(\mathbb{Q})[m]$  must inject into  $E(\mathbb{F}_p)$  (due to exactness; specifically, we have that  $E(\mathbb{Q})[m] \cong E(\mathbb{F}_p)[m] \subset E(\mathbb{F}_p)$ ).

This holds for all  $m \geq 1$ , so we can conclude that  $E(\mathbb{Q})_{\text{TORS}}$  injects into  $E(\mathbb{F}_p)$ .  $\square$

For another (more detailed) explanation see [34, pg. 300–305]. For an additional application of this theorem see [34, pg. 136–137].

### A.3 Eisenstein Series Converges

The *Eisenstein series* with weight  $2k$  of a given lattice  $\Lambda$  is given by

$$G_{2k}(\Lambda) = \sum_{\omega \in \Lambda \setminus \{0\}} \omega^{-2k}.$$

We prove the following lemma.

**Lemma A.1.** *The Eisenstein series  $G_{2k}(\Lambda)$  converges absolutely for  $k > 1$ .*

*Proof.* Let  $A_n$  be the annulus defined by  $n - 1 \leq |z| \leq n$  for some  $n \in \mathbb{N}$ . Let  $d$  be the smallest positive integer greater than the maximum distance between points in the fundamental period parallelogram of the lattice. Then

the larger annulus defined by  $n - 1 - d \leq |z| \leq n + d$  contains all of  $A_n$  (see Figure 11).

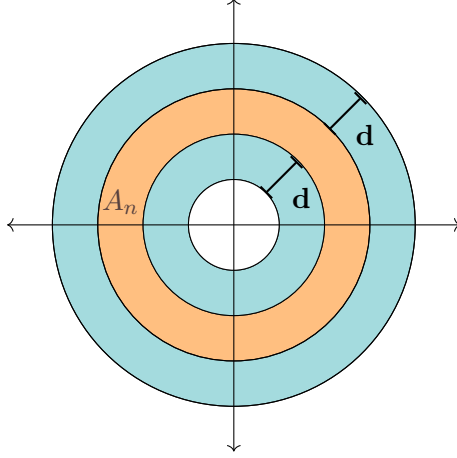


Figure 11:  $A_n$  is Contained

Since the area of an annulus is proportional to its radius, the area of the larger annulus can be bounded by  $c \cdot n$  for some constant  $c > 0$  that depends only on the lattice  $\Lambda$  [33, pg. 165, 178]. Moreover, the number of lattice points in  $A_n$  is bounded by the number of fundamental parallelograms intersecting  $A_n$ . Each fundamental parallelogram has area  $P$  and can contribute at most one lattice point, so the number of lattice points in  $A_n$  is bounded above by  $A/P$ , where  $A$  is the area of  $A_n$ .

Going back to our series, we can use these bounds to obtain that for sufficiently large  $N$ ,

$$\sum_{\omega \in \Lambda \mid |\omega| \geq 1} \frac{1}{|\omega|^{2k}} \leq \sum_1^\infty \frac{c \cdot n}{n^{2k}} = \sum_1^\infty \frac{c}{n^{2k-1}}.$$

The far right sum converges for  $k > 1$ , so we conclude that  $\sum_{\omega \in \Lambda \setminus \{0\}} \omega^{-2k}$  converges absolutely for  $k > 1$ , as desired.  $\square$

## References

- [1] Tom M. Apostol. *Modular Functions and Dirichlet Series in Number Theory*, volume 41 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1976.
- [2] Allison F. Arnold-Roksandich. *There and Back Again: Elliptic Curves, Modular Forms, and L-Functions*. Senior thesis, Harvey Mudd College, 2014.
- [3] Elaine Barker and Allen Roginsky. Transitioning the use of cryptographic algorithms and key lengths, March 2019.
- [4] Jose Barrios. A brief history of elliptic integral addition theorems. *Rose-Hulman Undergraduate Mathematics Journal*, 10(2), 2009.
- [5] Christophe Breuil, Brian Conrad, Fred Diamond, and R. Taylor. On the modularity of elliptic curves over  $\mathbb{Q}$ : Wild 3-adic exercises. *J. Amer. Math. Soc.*, 14:843–939, 2001.
- [6] Ezra Brown and Bruce T. Myers. Elliptic curves from mordell to diophantus and back. *The American Mathematical Monthly*, 109(7):639–649, 2002.
- [7] Ashay A. Burungale, Christopher Skinner, and Ye Tian. The birch and swinnerton-dyer conjecture: A brief survey. In A. Kechris, N. Makarov, D. Ramakrishnan, and X. Zhu, editors, *Nine Mathematical Challenges - An Elucidation*, Proceedings of Symposia in Pure Mathematics, pages 11–29, United States, 2021. American Mathematical Society. Publisher

Copyright: © 2021 American Mathematical Society.; Linde Hall Inaugural Math Symposium, 2019 ; Conference date: 22-02-2019 Through 24-02-2019.

- [8] Jean Christianidis, Jeffrey A. Oaks, and Diophantus. *The Arithmetica of Diophantus: A Complete Translation and Commentary*. Scientific Writings from the Ancient and Medieval World. Routledge, Taylor & Francis Group, Abingdon, Oxon, 2023.
- [9] The LMFDB Collaboration. The l-functions and modular forms database. <https://www.lmfdb.org>, 2024. [Online; accessed 1 November 2024].
- [10] David A. Cox. Introduction to fermat’s last theorem. *Amer. Math. Monthly*, 101:3–14, 1994.
- [11] John E. Cremona. *Algorithms for Modular Elliptic Curves*. Cambridge University Press, Cambridge, 2nd edition, 1997.
- [12] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Trans. Inf. Theory*, 22(6):644–654, November 1976.
- [13] Andrej Dujella. Trivial torsion group, rank  $\geq 29$ . <https://web.math.pmf.unizg.hr/~duje/tors/z1.html>, 2024.
- [14] H. M. Edwards. *Fermat’s Last Theorem: A Genetic Introduction to Algebraic Number Theory*. Graduate Texts in Mathematics. Springer, New York, 1977.

- [15] Edward Vincent Eikenberg. Rational points on some families of elliptic curves. <https://api.semanticscholar.org/CorpusID:118353032>, 2004.
- [16] William Fulton and Richard Weiss. *Algebraic Curves: An Introduction to Algebraic Geometry*. Addison-Wesley, Redwood City, CA, 1989.
- [17] Jean Gallier. *Basics of Projective Geometry*, pages 87–161. Springer, New York, NY, 2001.
- [18] GMO Internet Group GlobalSign. Elliptic curve cryptography. <https://www.globalsign.com/en/blog/elliptic-curve-cryptography>, November 2020.
- [19] Thomas Heath. *Diophantus of Alexandria*. Cambridge University Press, Cambridge, 2nd edition, 1910.
- [20] Fredrik Johansson. Modular forms in arb. <https://fredrikj.net/blog/2014/10/modular-forms-in-arb/>, 2014.
- [21] Nathan Jones. Almost all elliptic curves are serre curves. *Transactions of the American Mathematical Society*, 362(3):1547–1570, March 2010.
- [22] Steven G. Krantz. On limits of sequences of holomorphic functions. *Rocky Mountain Journal of Mathematics*, 43(1):273–283, 2013.
- [23] Serge Lang. *Algebra*. Springer, New York, 2002.
- [24] Elisabeth Lutz. Sur l'équation  $y^2 = x^3 - ax - b$  dans les corps p-adiques. *J. Reine Angew. Math.*, 177:238–247, 1937.

- [25] Barry Mazur and David Goldfeld. Rational isogenies of prime degree. *Inventiones Mathematicae*, 44(2):129–162, June 1978.
- [26] Victor S. Miller. Use of elliptic curves in cryptography. In *Advances in Cryptology — CRYPTO '85 Proceedings*, volume 85 of *Lecture Notes in Computer Science*, pages 417–426. Springer, 1986.
- [27] Trygve Nagell. Sur les propriétés arithmétiques des cubiques planes du premier genre. *Acta Math.*, 52(1):93–126, July 1929.
- [28] Henri Poincaré. Sur les propriétés arithmétiques des courbes algébriques. *Journal de Mathématiques Pures et Appliquées*, 5:161–234, 1901.
- [29] Miles Reid. *Undergraduate Algebraic Geometry*. Cambridge University Press, Cambridge, 2001.
- [30] Kenneth A. Ribet. From the taniyama-shimura conjecture to fermat's last theorem. *Ann. Fac. Sci. Toulouse Math. (6)*, 11:116–139, 1990.
- [31] Karl Rubin and Alice Silverberg. Ranks of elliptic curves. *Bulletin of the American Mathematical Society*, 39(4):455–474, July 2002.
- [32] Josh Schneider. The history of cryptography. <https://www.ibm.com/think/topics/cryptography-history>, August 2024.
- [33] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, Cham, 2009.
- [34] Joseph H. Silverman and John Torrence Tate. *Rational Points on Elliptic Curves*. Springer, Cham, 2015.

- [35] Andrew Snowden. On the distribution of torsion subgroups of elliptic curves. University of Michigan, 2013. <https://www-personal.umich.edu/~asnowden/papers/torsion-112013.pdf>.
- [36] Gordon Tian. A gentle introduction to perspective. <https://www.gordontian.com/perspective/perspective1/>, April 2020.
- [37] Eric W. Weisstein. Euler's homogeneous function theorem. <https://mathworld.wolfram.com/EulersHomogeneousFunctionTheorem.html>, 2024. From *MathWorld—A Wolfram Web Resource*.
- [38] Andrew Wiles. Modular elliptic curves and fermat's last theorem. *Ann. Math.*, 141(3):443–551, 1995.