Elliptic Curves and the Birch and Swinnerton-Dyer Conjecture

Samuel Lowe
Faculty Consultant: Professor Evan Dummit

January 8, 2024

Abstract

Elliptic curves are a rich and exciting field of study. In the following pages, we will provide an introduction to the theory of elliptic curves and survey several foundational results. We will see that the points on an elliptic curve form a finitely generated abelian group, and that we can fully characterize the structure of this group's torsion subgroup. We will also discuss isogenies, which are structure-preserving maps between elliptic curves, and some of the structure that these maps possess. We conclude with a discussion of the Birch and Swinnerton-Dyer conjecture, which relates the group structure of the elliptic curve with the and analytic behavior of its L-function, and provide some computations supporting the conjecture.

Contents

This project was initially presented on April 20, 2023. This version is updated with additional citations.

1 Introduction

Elliptic curves were first discovered when computing the perimeters of ellipses (hence the name *elliptic* curve), but have become indispensible tools to resolve questions in analysis, algebra, cryptography, and especially number theory. Andrew Wiles's proof of Fermat's Last Theorem – a problem that had remained open for over 350 years – drew heavily upon and greatly expanded the theory of elliptic curves. We now provide the definition of an elliptic curve:

Definition (Elliptic Curve)**.** Let K be a field. We call an equation that can be written in the form

$$y^2 + a_1xy + a_3y = a_2x^3 + a_4x + a_6, \qquad a_1, \cdots a_6 \in K \tag{1}$$

an *elliptic curve* over K, and call this equation standard form.

Remark. Some texts [1] [2] introduce elliptic curves in the context of cubic curves, which are polynomials that are cubic in x and y, and can be reduced via a series of substitutions to the above form.

Equations in a form slightly reduced from (1) sometimes arise in unexpected places. For example, while evaluating the arc-length integral to find the perimeter of an ellipse, we must evaluate

$$\int \frac{1}{\sqrt{x^3 + Ax + B}}\, dx$$

for some $A, B \in \mathbb{C}$. By defining $y := \sqrt{x^3 + Ax + B}$ and squaring both sides, we recover an elliptic curve:

$$y^2 = x^3 + Ax + B, \qquad A, B \in K \tag{2}$$

We say that an elliptic curve of this form is in *reduced Weierstrass form*, and if the field K over which our elliptic curve is defined has characteristic not 2 or 3, then we can simplify the curve's equation to this form from standard form by completing the square in y and the cube in x. Some of the theorems that we will provide are stated for elliptic curves in slightly different forms, but when possible we will use Weierstrass form for convenience.

Sometimes the cubic polynomial $x^3 + Ax + B$ will have a repeated root over the field K in which we are working; we say that an elliptic curve with at least one repeated root is singular, and that an elliptic curve that has distinct roots is non-singular. Many of the results that we will discuss do not hold for elliptic curves that have repeated roots, so it makes sense to develop a quick test for determining whether an elliptic curve is singular or not. It turns out that an elliptic curve in Weierstrass form is singular exactly when the

discriminant of the elliptic curve, defined to be $\Delta := -16(4A^3 + 27B^2)$, equals zero over K. Note that this is just the discriminant of the cubic polynomial, and that the exact form that the discriminant takes will depend on whether the elliptic curve is in standard or some other form.

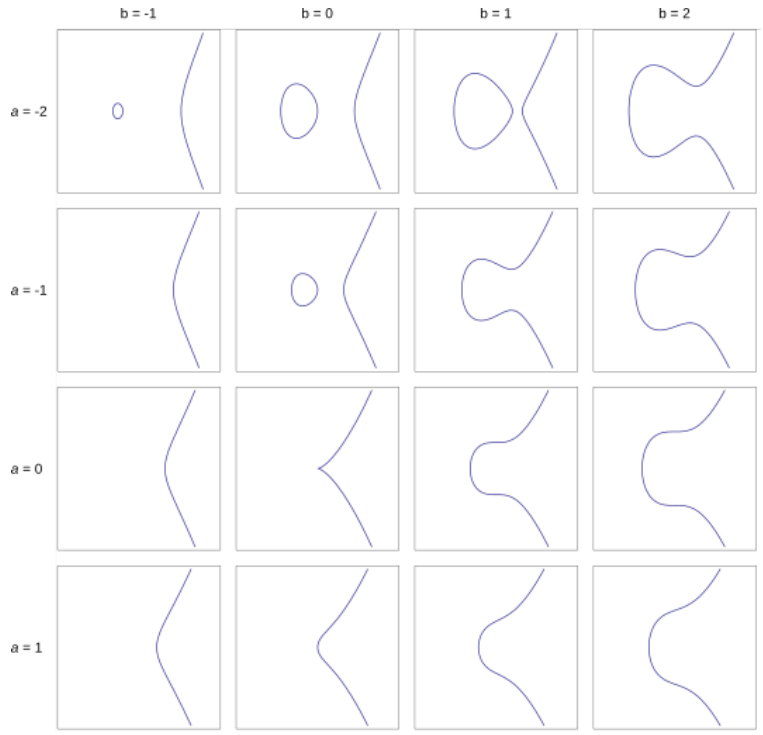


Figure 1: Various elliptic curves defined by varying the values of A and B.
Image Credit: Tos - Own work, Public Domain, https://commons.wikimedia.org/w/index.php?curid=3553836

1.1 Congruent Numbers and Elliptic Curves

In the style of [2], let's examine a motivating problem at the intersection of geometry and number theory that we can reduce to a problem of studying elliptic curves. Consider a positive integer n. We say that n is a *congruent number* if there exists a right triangle of area n with side lengths $a, b, c \in \mathbb{Q}$. We know that these quantities must satisfy the Pythagorean theorem and the area formula for a triangle:

$$a^2 + b^2 = c^2 \tag{3}$$

$$\frac{1}{2}ab = n \tag{4}$$

For example, $n = 5$ is a congruent number because the right triangle with side lengths $a = 20/3$, $b = 3/2$, and $c = 41/6$ has area 5. How can we find all the congruent numbers?

Suppose a, b, c satisfy the above equations. Letting $x = \frac{n(a+b)}{c}$ and $y = \frac{2n^2(a+c)}{b^2}$, we see that $y \neq 0$ (otherwise $b = 0$ and $\frac{1}{2}ab = 0$) and

$$y^2 = x^3 - n^2x, \quad y \neq 0 \tag{5}$$

Conversely, we see that if x, y satisfy (5) and $y \neq 0$, we can work backwards from our definitions of x and y to define $a = \frac{x^2-n^2}{y}$, $b = \frac{2nx}{y}$, and $c = \frac{x^2-n^2}{y}$, equations (3) and (4) are satisfied – so we have a bijection between rational solutions to (3)-(4) and rational solutions to (5) with $y \neq 0$. We also see that if n is a positive rational, then a, b, and c are positive rationals exactly when x and y are also positive rationals, leading us to the following conclusion about congruent numbers:

Theorem 1.1 (Congruent Numbers)**.** A positive rational n is a congruent number if and only if there is a pair of positive rationals x, y satisfying $y^2 = x^3 - n^2x$ with $y \neq 0$.

How many rational points (x, y) satisfy this equation? To determine that, we need to study the structure of points on elliptic curves.

1.2 Points on Elliptic Curves and the Group Law

One of the foundational theorems on elliptic curves states that if we have two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ on a non-singular elliptic curve $E := y^2 = x^3 + Ax + B$ over K, then we can construct a third point on E. If $x_1 \neq x_2$, then there is some secant line $L := y = mx + b$ that connects these two points. We know that

$$(mx + b)^2 = x^3 + Ax + B \tag{6}$$

is a cubic polynomial with roots x_1, x_2, and x_3 that correspond to three points $(x_1, 0), (x_2, 0)$, and $(x_3, 0)$ on the curve. The x-coordinates of two of these points x_1 and x_2 must be roots of the polynomial (6), so the x-coordinate x_3 of the new point P_3 must be the third root.

If $x_1 = x_2$ then the line is simply $L := x = a$, and it appears that this line does not intersect the curve at a third point. We will address this case shortly.

We recognize that elliptic curves are symmetric about the x-axis, so if $P = (x, y)$ lies on the curve, the point $-P = (x, -y)$, which we call the *reflection* of P, must also lie on the curve. Combining this fact with the previous procedure, we can now define a law that will allow us to construct many more points on the elliptic curve.

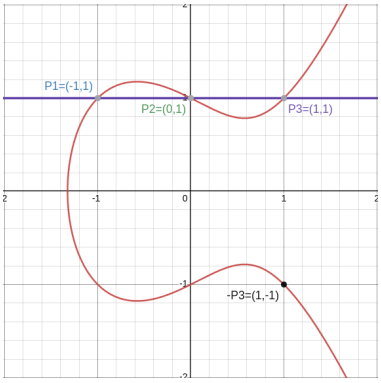
1.3 The Group Law

Definition (Group Law, Part 1)**.** If P_1 and P_2 are two distinct points on the elliptic curve E, let $P_3 = (x_3, y_3)$ be the third intersection point of E with the line L joining P_1 and P_2 (this is the $y = mx+b$ line from earlier). We define the sum P_1+P_2 to be the point *reflection* $-P_3$ of the third point on the line.

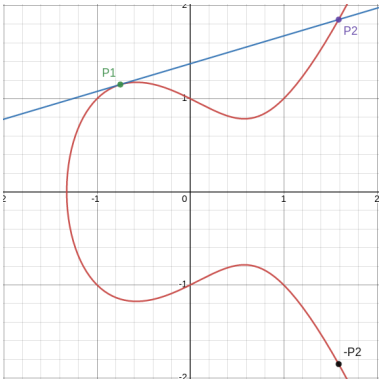
Remark. Note that define the resulting point to be the reflection $-P_3$ so we can "escape" the line L, generate new points beyond P_1, P_2, and P_3.

As the name of this law suggests, our goal is to put some structure on the set of points on the elliptic curve to give this set a group structure. However, we have several special cases we must consider to verify that this law is well-defined and that it possesses the necessary properties of a group operation.

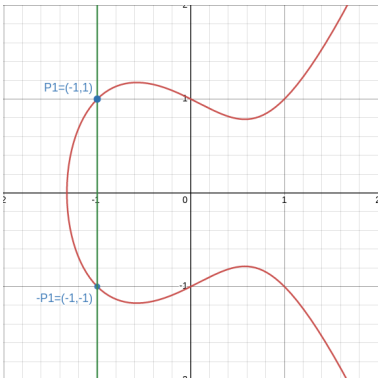
Figure 2: The Group Law on the elliptic curve $E := y^2 = x^3 - x + 1$ over $\mathbb{R}$.



(a) We define $P_1 + P_2$ not to be P_3, but the reflection of P_3 over the x-axis, $-P_3$.



(b) The line defined by P_1+P_1 is not a secant line – it's the line tangent to E at P_1.



(c) One case where we get a vertical line is when adding $P + (-P)$.

If $P_1 = P_2$ (that is, if we try to add a point to itself) the group law as we have described it does not apply. Thinking geometrically in the case where $K = \mathbb{R}$, we see that if we fix P_1 and allow P_2 to approach P_1, the secant line L connecting P_1 and P_2 will approach the line tangent to the curve at P_1, and P_3 will vary continuously as the slope of L varies continuously. This naturally leads us to take the limit as $P_2 \to P_1$, So we define $P_1 + P_1$ to be the other point where the line tangent to E at P_1 intersects E.

However, this tangent line is vertical in the case where $y = 0$. We actually obtain a vertical line whenever $x_1 = x_2$ – that is, in the case where we add $P + (-P)$ – because of the symmetry of the curve, and it appears that our line-drawing method fails to yield a third point. However, if we imagine that any vertical line intersects the elliptic curve at infinity – or more precisely, at *the point at infinity* which we denote ∞ – then this problem is resolved by defining $P + (-P) = \infty$.

We've appealed to notions of continuity on $\mathbb{R}$ to define how we can add a point to itself, but we want to work in a more general setting (e.g. in $\mathbb{F}_p$ or $\mathbb{F}_{p^n}$) so we need to formulate the group law more algebraically.

Theorem 1.2 (Group Law, Part 2)**.** Let E be a non-singular elliptic curve over a field K with Weierstrass equation $y^2 = x^3 + Ax + B$, and define the sum of two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ on E to be $P_3 = (x_3, y_3)$ where $x_3 := m^2 - x_1 - x_2$, $y_3 := -m(x_3 - x_1) - y_1$ and

$$m := \begin{cases} (y_2 - y_1)/(x_2 - x_1) & \text{if } P_1 \neq P_2 \text{ and } x_2 \neq x_1 \\ (3(x_1)^2 + A)/(2y_1) & \text{if } P_1 = P_2 \text{ and } y_1 \neq 0 \\ \infty & \text{otherwise} \end{cases}$$

and define $P + \infty = \infty + P = P$ for all points P.

Then the set of K-rational points together with the point ∞ form an abelian group under this operation; that is,

- $P + \infty = \infty + P = P$, so ∞ acts as an identity element.

- The group law is associative: for points P_1, P_2, and P_3, we have $P_1 + (P_2 + P_3) = P_1 + (P_2 + P_3)$.
- The group law always yields a point on the curve, so it is closed.
- $P + -P = \infty = -P + P$, so every point on the curve has an inverse.
- $P_1 + P_2 = P_2 + P_1$, so the group law is commutative.

We denote this group $E(K)$, and call it the *Mordell-Weil group*.

Proof. We prove this law by cases in the style of [2].

- If $P_1 \neq P_2$ and $x_1 \neq x_2$, then the line joining the two is given in point-slope form by

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

  Plugging this $y^2 = x^3 + Ax + B$, we have $L := (mx - mx_1 + y_1)^2 = x^3 + Ax + B$, which is a cubic in x of the form $x^3 - m^2x^2 + a_1x + a_2$ for some constants a_1, a_2. We expect this formula to factor as $(x - x_1)(x - x_2)(x - x_3)$ because $x_1, x_2 \in K$, so multiplying out and matching coefficients yields $x_1 + x_2 + x_3 = m^2$, so confirming the formula for x_3. y must then be $y_3 = m(x_3 - x_1) + y_1$ because we multiply by -1 to reflect over the x-axis.

- If $P_1 = P_2$ and $y_1 \neq 0$, then the line is given in the same point slope form but with m as the slope of the tangent line. We can implicitly differentiate to get $2yy' = 3x^2 + A$ so $m = \frac{3x_1^2 + A}{2y_1}$.
- If $P_1 \neq P_2$ but $x_1 = x_2$, or if $P_1 = P_2$ and $y = 0$, then in both cases the secant or tangent line will be vertical, which we define to intersect the curve at ∞.

We now verify each of the group axioms:

1. Identity is immediate by definition.
2. Associativity can be seen by tedious algebraic manipulation; according to [3], it was common in the 1960s to say that checking this proof would take only "a few days."
3. The polynomial $(mx + b)^2 = x^3 + Ax + B$ has two roots in K so the third root must also be in K, so the formula is closed.
4. $P + -P = \infty$ because we have $P_1 \neq P_2$ but $x_2 \neq x_1$.
5. Commutativity either follows by checking cases with algebra, or by following the geometric intuition that a line is uniquely defined by the two points it goes through, so the line through P_1 and P_2 is the same as the line through P_2 and P_1 – the order does not matter. The same intuition applies for tangent lines.

□

Notice that for an elliptic curve E over K, all points in $E(K)$ must also be in K^2. In particular when K is finite, $E(K)$ is also finite, so we can list all points on $E(K)$ and write the group explicitly. Our general procedure will be to test out all possible x-coordinates, calculate the value of y^2 as a function of x, then determining which values of y (if any) satisfy the elliptic curve equation.

Example 1.1. Let $E := y^2 = x^3 + 2x$ be an elliptic curve over the field $K = \mathbb{F}_3$. Plugging in $x = 0, 1, 2$, we get the table

x	0	1	2
$x^3 + 2x$	0	0	0
y	0	0	0

so in addition to ∞, we have $(0, 0), (1, 0)$, and $(2, 0)$. We want to compute the addition table for this group; we might notice that each point has order two because they all have $y = 0$. This indicates that $E(\mathbb{F}_3) \cong K_4 \cong C_2 \oplus C_2$ is the Klein-4 group, but we still have to compute nontrivial sums to complete the table:

- $(1, 0) + (2, 0) = (0, 0)$ because $m = (0 - 0)/(2 - 1) = 0$, so $x_3 = 0 - 1 - 2 = 0$ and $y_3 = -0(x_3 - 1) - 0 = 0$
- $(2, 0) + (0, 0) = (1, 0)$ because $m = (0 - 0)/(0 - 2) = 0$, so $x_3 = 0 - 2 - 0 = 1$ and $y_3 = -0(x_3 - 2) - 0 = 0$
- $(1, 0) + (0, 0) = (2, 0)$ because $m = (0 - 0)/(0 - 1) = 0$, so $x_3 = 0 - 1 - 0 = 2$ and $y_3 = -0(x_3 - 1) - 0$

So the addition table is:

$+$	∞	$(0,0)$	$(1,0)$	$(2,0)$
∞	∞	$(0,0)$	$(1,0)$	$(2,0)$
$(0,0)$	$(0,0)$	∞	$(2,0)$	$(1,0)$
$(1,0)$	$(1,0)$	$(2,0)$	∞	$(0,0)$
$(2,0)$	$(2,0)$	$(1,0)$	$(0,0)$	∞

Example 1.2. Let $E := y^2 = x^3 + 3x + 3$ be an elliptic curve over the field $K = \mathbb{F}_5$. Plugging in $x = 0, 1, 2, 3, 4$, we get the table

x	0	1	2	3	4
$x^3 + 3x + 3$	3	2	2	4	4
y	n/a	n/a	n/a	± 2	± 2

so in addition to ∞, we have $(3, 2), (3, 3), (4, 2)$ and $(4, 3)$. Immediately we see that this group has order 5 which is prime, so $E(\mathbb{F}_5) \cong C_5$.

2 Mordell's Theorem

For a given elliptic curve E over $\mathbb{Q}$, we would like to understand when there are infinitely many points on E and when there are only finitely many. If $E(\mathbb{Q})$ has one or more generators of infinite order, then we can construct infinitely many points using those generators. On the other hand, if $E(\mathbb{Q})$ has no points of infinite order, then can we necessarily conclude that there are only finitely many points in $E(\mathbb{Q})$?

We can start by looking at the generators of several curves.

Example 2.1. For $E := y^2 = x^3 - 64x + 1$ over $\mathbb{Q}$, the group of rational points $E(\mathbb{Q})$ is generated by $\{(-8, 1), (-6, 13), (-5, 14), (-2, 11)\}$; each of these points has infinite order.

Example 2.2. For $E := y^2 = x^3 + x^2 + x + 1$ over $\mathbb{Q}$, the group of rational points $E(\mathbb{Q})$ is generated by $\{(-1, 0), (0, 1)\}$. The point $(-1, 0)$ has order 2, and the point $(0, 1)$ has infinite order.

Example 2.3. For $E := y^2 = x^3 - x^2 - 4x + 4$ over $\mathbb{Q}$, the group of rational points $E(\mathbb{Q})$ is generated by $\{(1, 0), (4, 6)\}$. The point $(1, 0)$ has order 2, and the point $(4, 6)$ has order 4.

Example 2.4. For $E := y^2 = x^3 - 219x + 1654$ over $\mathbb{Q}$, the group of rational points $E(\mathbb{Q})$ is generated by the point $(11, 24)$ which has order 9.

We can resolve these questions by proving that $E(\mathbb{Q})$ is finitely generated. Recall that we say a group G is *finitely generated* if every element in G can be written in terms of a finite set of elements $\{g_1, g_2, \ldots, g_n\} \subseteq G$ of G, called the *generators*. That is, every element $h \in G$ can be written as $h = a_1 g_2 + a_2 g_2 + \cdots + a_n g_n$ for integers $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. We call the set $\{g_1, g_2, \ldots, g_n\}$ a *generating set* for G. The proof that $E(\mathbb{Q})$ is finitely generated is Mordell's theorem:

Theorem 2.1 (Mordell)**.** The group of rational points $E(\mathbb{Q})$ on a non-singular elliptic curve E over $\mathbb{Q}$ is finitely generated.

To prove this theorem, we need to establish several terms and lemmas.

2.1 A Brief Discussion of Height

Definition (Height of a Rational)**.** Let p/q be rational and in lowest terms. We define the *height* of p/q to be

$$H(p/q) = \max(|p|, |q|).$$

Definition (Height of a Point)**.** For a point $P = (x, y)$ on an elliptic curve, we define the height to be $H(P) = H(x)$; if $P = \infty$, we define $H(\infty) = 1$ by convention.

We define height because we want a rough notion of "size" or "complexity" of a point. We can also define the log-height by

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

when we want our height function to behave additively while still respecting order.

We'll rely on nontrivial properties of the height function in our proof, as well as the fact that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite, but these lemmas are difficult to prove and some rely on tools that we have not yet developed.

2.2 The Descent Theorem

In the style of [1], we'll prove the Descent Theorem for an abelian group G satisfying several conditions, then show that $E(\mathbb{Q})$ satisfies these conditions. Before we proceed, we need to define one more term: for an abelian group G, define

$$2G := \{g + g \ : \ g \in G\}.$$

This is a subgroup of G (closure and identity follow immediately, and the inverse of $g + g$ is clearly $(-g) + (-g)$). In the proof of the Descent Theorem, we'll work with an abelian group G and require that the number of cosets of $2G$ in G is finite. We'll select a set S of coset representatives, and use this finite set to construct a finite generating set.

Theorem 2.2 (Descent Theorem)**.** Let G be a commutative group such that $\#G/2G = n$ is finite, and let h be a "height" function

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

such that

1. For every $M \in \mathbb{R}$, $\{P \in G \ : \ h(P) \leq M\}$ (the set of all elements with height less than M) is finite.

2. For every $P_0 \in G$, there is a constant κ_0 such that $h(P + P_0) \leq 2h(P) + \kappa_0$ for all $P \in G$.

3. There is a constant κ such that

$$h(2P) \geq 4h(P) - \kappa$$

for all $P \in G$.

Then G is finitely generated.

Proof. Let S be a fixed set of coset representatives for the n cosets of $G/2G$ and label elements from S using the letter Q: thus $Q_1, Q_2, \ldots, Q_n$ will represent the points chosen from this specific set of coset representatives.

Let P be an arbitrary element of G. Because P is an element of some coset, suppose its representative is $Q_1 \in S$; then $P \in Q_1 + 2G$, so $P - Q_2 = 2P_1$ for some $P_1 \in G$. Now repeat this process by considering the coset representative of P_1 to obtain a point P_2 with $P_1 - Q_2 = 2P_2$ for some $P_2 \in G$. Continuing this process, we obtain a list:

$$\begin{aligned} P \ - Q_1 &= 2P_1 \\ P_1 - Q_2 &= 2P_2 \\ P_2 - Q_3 &= 2P_3 \\ &\vdots \\ P_{m-1} - Q_m &= 2P_m \end{aligned}$$

where $Q_1, Q_2, \ldots, Q_m$ are chosen from the coset representatives and $P_1, P_2, \ldots, P_m \in G$.

Substituting each of these equalities into each other, we can write

$$P = Q_1 + 2Q_2 + 4Q_3 + \cdots + 2^{m-1}Q_m + 2^m P_m \tag{7}$$

so this arbitrary element $P \in G$ is in the subgroup of G generated by the coset representatives Q_i and P_m. We want to show that for large enough m, then there are only finitely many possible P_m. (This set of choices of P_m and the coset representatives Q_i will generate G.)

We will show this by considering the sequence of points $P, P_1, P_2, \ldots, P_m$ and use some of the properties of the height function to prove that the height of P_j is less than the height of the previous element in the sequence, P_{j-1}.

By property 2 (with $P_0 = -Q_i$), we have $h(P - Q_i) \leq 2h(P) + \kappa_i$ for all $P \in G$. Applying this inequality for each $1 \leq i \leq n$ and letting κ' be the greatest of the κ_i's, we see that the value of κ' doesn't depend on which Q_i or which P we're working with and

$$h(P - Q_i) \leq 2h(P) + \kappa'$$

for all $P \in G$ and $1 \leq i \leq n$.

Let κ be the constant from property 3, which again does not depend on our choice of P or Q_i. Applying the properties above to P_j, we see that

$$4h(P_j) \leq h(2P_j) + \kappa \leq 2h(P_{j-1}) + \kappa' + \kappa$$

and therefore in the case where $h(P_{j-1}) \geq \kappa' + \kappa$, then

$$h(P_j) \leq \frac{3}{4} h(P_{j-1}).$$

So considering again the sequence of points $P, P_1, P_2, \ldots$, this means that so long as $h(P_{j-1}) \geq \kappa' + \kappa$, then the next point in the sequence will have a smaller height: $h(P_j) \leq \frac{3}{4} h(P_{j-1})$. Because the height decreases with every iteration, we eventually have a point P_m in the sequence in equation (7)

$$P = Q_1 + 2Q_2 + 4Q_3 + \cdots + 2^{m-1}Q_m + 2^m P_m \tag{7 revisited}$$

with $h(P_m) \leq \kappa' + \kappa$. This P_m must belong to the finite set $\{P \in G \ : \ h(P) \leq \kappa' + \kappa\}$ by property 1. Because $\kappa' + \kappa$ doesn't depend on our choice of P or any of the Q_i's, we see that by equation (7) that every $P \in G$ is a linear combination of

$$S \cup \{P \in G \ : \ h(P) \leq \kappa' + \kappa\} \tag{8}$$

where S is the set of coset representatives defined above. Because S is finite and the set of points of height at most $\kappa + \kappa'$ is finite, we have constructed a finite generating set for G. □

Corollary 2.3. If E is an elliptic curve over $\mathbb{Q}$, then the group of points $E(\mathbb{Q})$ is finitely generated.

Proof. We must show that $E(\mathbb{Q})$ satisfies hypotheses for the Descent Theorem; (1), is straightforward, but (2), (3), and (4) are harder to prove so we will provide only an outline of their proofs.

1. The set of all rational numbers with height less than some constant

$$\{x \in \mathbb{Q} \ : \ h(x) \leq M\} \text{ for } M \in \mathbb{R}$$

is finite because both $|x|$ and $|y|$ are integers and must be less than M.

2. We begin by observing that if P is a rational point, then we must have $P = (x, y) = (m/e^2, n/e^3)$ for some $e > 0$ relatively prime to m and n. This can be shown by substituting $x = m/M$ and $y = n/N$ into the equation for the elliptic curve and clearing denominators to see that $N^2 \mid M^3$; further computation reveals $M^3 \mid N^2$, so $M^3 = N^2$. Defining $e = N/M$ yields the desired result. The rest of the proof follows by constructing κ_0 via direct computation with the triangle inequality.

3. This proof follows from a "doubling formula" that gives the coordinates of $2P$ in terms of the point P. Specifically, it gives the x-coordinate of $2P$, which is

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

Because E is non-singular, $f(x) = x^3 + ax^2 + bx + c$ has no repeated roots and therefore shares no roots with $f'(x)$. The result follows from reasoning about the heights of the quotient of the two relatively prime polynomials.

4. The proof that $\#E(\mathbb{Q})/2E(\mathbb{Q})$ is finite provided in [1] requires E to have at least one rational root because the more general proof requires algebraic number theory or facts about the ideal class group which the authors prefer to avoid. The proof proceeds by showing that if an elliptic curve E has a rational root, it can be shifted in the plane to yield $E_1 := y^2 = x^3 + ax^2 + b$ so its root is at $x = 0$. We then introduce a second elliptic curve $E_2 := y^2 = x^3 - 2ax^2 + (a^2 - 4b)$ and two maps $\phi : E_1 \to E_2$ and $\psi : E_2 \to E_1$ where $\psi \circ \phi(P) = 2P$. After proving that ϕ and ψ are homomorphisms of elliptic curves, proving that $\#E_1(\mathbb{Q})/\psi(E_2(\mathbb{Q})) \leq 2^{r+1}$ where r is the number of distinct prime factors of b is sufficient to show that $\#E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.

□

The Mordell-Weil theorem extends this proof to finite-degree field extensions of $\mathbb{Q}$. The machinery required to prove Mordell-Weil goes far beyond the scope of this text (see [3]), but the idea of establishing a height function, proving that $E(K)/2E(K)$ is finite, and applying the Descent Theorem is broadly the same.

2.3 Decomposition of $E(\mathbb{Q})$

By the fundamental theorem of finitely generated abelian groups, we can decompose $E(\mathbb{Q})$ into a direct product of infinite cyclic groups with cyclic groups of prime power order:

$$E(\mathbb{Q}) \cong \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r \text{ times}} \oplus C_{p_1^{v_1}} \oplus C_{p_2^{v_2}} \oplus \cdots \oplus C_{p_n^{v_n}} \tag{9}$$

We define the integer r to be the *rank* of $E(\mathbb{Q})$. The points of finite order in $E(\mathbb{Q})$ are called *torsion points*. The set of torsion points forms a subgroup called the *torsion subgroup*, which in the above decomposition consists of

$$C_{p_1^{v_1}} \oplus C_{p_2^{v_2}} \oplus \cdots \oplus C_{p_n^{v_n}}$$

denoted $\operatorname{Tor} E(\mathbb{Q})$. With this terminology, one might see equation (9) written

$$E(\mathbb{Q}) = \mathbb{Z}^r \oplus \operatorname{Tor} E(\mathbb{Q}) \tag{10}$$

So we can completely characterize the structure of $E(\mathbb{Q})$ just from the rank r of $E(\mathbb{Q})$ and the structure of the torsion subgroup $\operatorname{Tor} E(\mathbb{Q})$. The rank of $E(\mathbb{Q})$ is tricky to pin down (we will discuss this more when we introduce the Birch and Swinnerton-Dyer conjecture), but we can comprehensively dissect the structure of $\operatorname{Tor} E(\mathbb{Q})$. We can examine the group structure of several previous examples:

Example 2.5. For $E := y^2 = x^3 - 64x + 1$ over $\mathbb{Q}$, the group of rational points is generated by $\{(-8, 1), (-6, 13), (-5, 14), (-2, 11)\}$; each of these points has infinite order, so $E(\mathbb{Q}) \cong \mathbb{Z}^4$, so E has rank $r = 4$ and a trivial torsion subgroup.

Example 2.6. For $E := y^2 = x^3 + x^2 + x + 1$ over $\mathbb{Q}$, the group of rational points is generated by the point $(-1, 0)$ which has order 2 and the point $(0, 1)$ which has infinite order, so $E(\mathbb{Q}) \cong \mathbb{Z} \oplus C_2$, so E has rank $r = 1$ and torsion subgroup C_2.

Example 2.7. For $E := y^2 = x^3 - x^2 - 4x + 4$ over $\mathbb{Q}$, the group of rational points is generated by the point $(1, 0)$ which has order 2 and the point $(4, 6)$ which has order 4, so $E(\mathbb{Q}) \cong C_2 \oplus C_4$, so E has rank $r = 0$ and torsion subgroup $C_2 \oplus C_4$.

Example 2.8. For $E := y^2 = x^3 - 219x + 1654$ over $\mathbb{Q}$, the group of rational points is generated by the point $(11, 24)$ which has order 9, so $E(\mathbb{Q}) \cong C_9$, so E has rank $r = 0$ and torsion subgroup C_9.

3 Torsion Points

In any group, it is natural to study the orders of elements in the group and to characterize which elements of the group have a particular order. On an elliptic curve, the only points of finite order are by definition the torsion points, so we seek to understand the possible structure of the torsion subgroup of $E(\mathbb{Q})$. To begin, we establish some notation for the set of points with order dividing m, which actually forms a subgroup:

Definition (m-Torsion Subgroup)**.** The m-torsion subgroup of $E(K)$, denoted $E_K[m]$, is the subgroup of $E(K)$ consisting of all elements P such that

$$mP = \underbrace{P + P + \cdots + P}_{m \text{ times}} = \infty$$

for some integer m.

Remark. This definition of a torsion subgroup is valid for any abelian group.

Example 3.1. For the non-singular elliptic curve $E := y^2 = x^3 - 25x$ over $\mathbb{Q}$, the torsion subgroup is generated by $(5, 0)$ and $(-4, 6)$. Both points have order 2, so $\operatorname{Tor} E(\mathbb{Q}) = C_2 \oplus C_2$.

Remark. $E := y^2 = x^3 - 25x$ over $\mathbb{Q}$ is the elliptic curve associated to the congruent number $n = 5$.

Example 3.2. For the non-singular elliptic curve $E := y^2 = x^3 + x^2 - x$ over $\mathbb{Q}$, the torsion subgroup is generated by $(-1, -1)$. This point has order 6, so $\operatorname{Tor} E(\mathbb{Q}) = C_6$.

In general, $E_K[1] = \{\infty\}$ for any elliptic curve. For a non-singular elliptic curve E over $\mathbb{Q}$, interpreting the group law geometrically tells us that all the points P on E that have vertical tangents have order two – these are exactly the points with $y = 0$; setting $0 = x^3 + Ax + B$, we see that there can be at most three (and exactly three, if $E = y^2 = x^3 + Ax + B$ is non-singular), so $E_{\mathbb{Q}}[2]$ is exactly the set of points with $y = 0$. $E_{\mathbb{Q}}[3]$ consists of all inflection points on the E because the tangent line given by $P + P$ intersects P a third time, so the first and second derivative share a zero.

Recalling our discussion on congruent numbers from the introduction, we can surmise that a positive rational n is congruent when the group of rational points $E(\mathbb{Q})$ on the elliptic curve $y^2 = x^3 - n^2x^2$ does not consist only of the group of points with $y = 0$ (that is, $E(\mathbb{Q})$ does not consist only of the 2-torsion points).

3.1 The Nagell-Lutz Theorem and Mazur's Theorem

To motivate the Nagell-Lutz theorem, we revisit the previous two examples of torsion subgroups and notice that they consist only of integral points.

Example 3.3. For the non-singular elliptic curve $E := y^2 = x^3 - 25x$ over $\mathbb{Q}$, the torsion subgroup consists of $\{(0, 1), (25, 0), (-25, 0), \infty\}$.

Example 3.4. For the non-singular elliptic curve $E := y^2 = x^3 + x^2 - x$ over $\mathbb{Q}$, the torsion subgroup consists of $\{(-1, -1), (-1, 1), (0, 0), (1, -1), (1, 1), \infty\}$.

Do points of finite order on rational elliptic curves always have integer coordinates? Yes – and a slightly stronger result was proven independently by Nagell and Lutz in the 1930s:

Theorem 3.1 (Nagell-Lutz)**.** Suppose E is a non-singular elliptic curve over $\mathbb{Q}$ with Weierstrass equation $y^2 = x^3 + ax^2 + bx + c$ with $a, b, c \in \mathbb{Z}$, and define the *discriminant* of E to be $D := -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$. If $P = (x, y)$ is a rational point of finite order, then x and y are integers. Furthermore, either $y = 0$ or $y^2 \mid D$.

Remark. In particular, rational torsion points are integral points.

The proof for this theorem is too long and difficult to give a full exposition here, but the central idea is to prove that if x and y are rational and in lowest terms, their denominators are positive integers not divisible by any primes – hence they are exactly 1.

This is accomplished by considering the set

$$C(p^v) := \left\{ \left(\frac{x_1}{x_2}, \frac{y_1}{y_2} \right) \in E(\mathbb{Q}) \ : \ p^{2v} \mid x_2 \right\} \cup \{\infty\}$$

for p prime and $v \in \mathbb{Z}$. By using a change of variables put to the points on our elliptic curve into bijection with a cubic curve that possesses structure similar to the group law, we can show that the only point in $C(p)$ with finite order is ∞, and then showing that this implies that rational points of finite order on our elliptic curve are integer points.

The rest of Nagell-Lutz relies on two lemmas, which are also too difficult to prove here:

1. If P has integer coordinates, then $2P$ has integer coordinates.

2. If P and $2P$ have integer coordinates, then $y \mid D$.

However, combining these lemmas into the final proof is quite quick: let P be a point of finite order, so P has integer coordinates. If $2P = \infty$, then $y = 0$ and we're done. If $2P \neq \infty$, then $2P$ must be an integer point by lemma 2, so by lemma 3 $y \mid D$. Some algebra and decomposing the formula for the discriminant reveals that $y^2 \mid D$, and we're done.

3.2 Finding Torsion Points

To find each of the torsion points of an elliptic curve $y^2 = x^3 + ax^2 + bx + c$, we simply calculate the set of points satisfying Nagell-Lutz: $S := \{P = (x, y) \ : \ y = 0 \text{ or } y^2 \mid D\}$; this set is finite because only finitely many points on the curve can have $y = 0$ or $y^2 \mid D$. For each point P in S, we calculate $2P, 3P, 4P, \ldots$ and eventually we will either find a point not in S (in which case P has infinite order) or the list will repeat (in which case P has finite order).

Example 3.5. Let $E := y^2 = x^3 + x^2 + x + 1$ be a non-singular elliptic curve over $\mathbb{Q}$. Then $D = -256 = -(2^8)$, so we're looking for x-coordinates that can yield $x^3 + x^2 + x + 1 = 0$ or $x^3 + x^2 + x + 1 \mid 256$. A quick search yields only the points $P_1 = (-1, 0), P_2 = (1, -2)$, and $P_3 = (1, 2)$. P_1 has $y = 0$, so it is a 2-torsion point. However, $2P_2 = (-3/4 : -5/8)$ and $2P_3 = (-3/4 : 5/8)$, so ∞ and P_1 are the only torsion points and we see $\operatorname{Tor} E(\mathbb{Q}) \cong C_2$.

An extraordinary theorem of Mazur gives the precise characterization of the possible structures of the group of rational torsion points:

Theorem 3.2 (Mazur)**.** Suppose E is a non-singular elliptic curve over $\mathbb{Q}$. Then the torsion subgroup $\operatorname{Tor} E(\mathbb{Q})$ of E is isomorphic to one of:

- C_n for $1 \leq n \leq 10$ or $n = 12$, or
- $C_2 \oplus C_{2n}$ for $1 \leq n \leq 4$.

To say that the proof of this theorem is outrageously difficult is an understatement, so we omit it. However, Mazur's theorem is notable for fully characterizing all possible torsion subgroups of any rational elliptic curve, and it can speed up the calculation of subgroups by hand by process of elimination.

4 Isogenies and Endomorphisms

For any additive abelian group G and any $n \in \mathbb{Z}$, we can always define the *multiplication-by-n homomorphism* $[n] : g \mapsto ng$ for $g \in G$; the kernel of this homomorphism is precisely the elements in G of order dividing n. Defining this map on $E(K)$, we see that $[n]$ has kernel $E[n]$.

This multiplication-by-n map is one example of an *isogeny*.

Definition (Isogeny)**.** Let E_1, E_2 be elliptic curves over a field K. An isogeny is a group homomorphism $\phi : E_1(K) \to E_2(K)$ given by rational functions; that is,

$$\phi(x, y) = \left(\frac{p_1(x, y)}{p_2(x, y)}, \frac{p_3(x, y)}{p_4(x, y)} \right)$$

where each p_i is a polynomial in x and y.

Example 4.1. Consider $E_1 := y^2 = x^3 + ax^2 + bx$ and $E_2 := y^2 = x^3 - 2ax^2 + (a^2 - 4b)x$. The map

$$\phi : (x, y) \mapsto \left(\frac{y^2}{x^2}, \frac{y(x^2 - b)}{x^2} \right)$$

is an isogeny.

Proof. We have

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

So if (x, y) is on E_1, then $\phi(x, y)$ is on E_2. □

In fact, an isogeny is either constant or surjective, so "isogenous" is an equivalence relation on elliptic curves:

Definition (Isogenous)**.** We say two elliptic curves E_1 and E_2 over a field K are *isogenous* if there is an isogeny $\phi : E_1(K) \to E_2(K)$ such that $\phi(P) \neq \{\infty\}$ only if $P = \infty$; in other words, if $\ker \phi = \{\infty\}$. In this case, ϕ is one-to-one.

Showing that this is an equivalence relationship is too difficult to prove (specifically showing that there is an inverse also given by rational functions), so we must omit the proof.

As with other algebraic objects, we can learn a lot by studying structure-preserving maps from an object to itself.

Definition (Endomorphism)**.** An isogeny from an elliptic curve to itself is called an *endomorphism*.

We can also construct new endomorphisms from old ones.

Theorem 4.1 (Endomorphism Composition)**.** Let E be an elliptic curve and let ϕ_1, ϕ_2 be endomorphisms $E \to E$. Then

- $\phi_1 + \phi_2$ given by $(\phi_1 + \phi_2)(P) = \phi_1(P) + \phi_2(P)$ is an endomorphism,
- $\phi_1 \circ \phi_2 : E \to E$ given by $(\phi_1 \circ \phi_2)(P) = \phi_1(\phi_2(P))$ is an endomorphism, and
- $\phi_1(\phi_2 + \phi_3) = \phi_1 \circ \phi_2 + \phi_1 \circ \phi_3$ is an endomorphism.

The proof that these all yield valid endomorphisms is difficult, but provided in [3]. However, we can still prove that the set of all endomorphisms from an elliptic curve E to itself is a ring:

Theorem 4.2 (End E is a Ring)**.** The set of all endomorphisms from an elliptic curve E to itself is a (not necessarily commutative) ring with 1 and no zero divisors.

Proof. We simply verify the various ring axioms for End E:

- Closure and associativity are immediate from the closure and associativity of $E(K)$ under the group law.
- The additive identity endomorphism is given by $[0]$ because $(\phi + [0])(P) = \phi(P) + \infty = \phi(P)$.
- For any endomorphism ϕ, the additive inverse is given by $-\phi = [-1] \circ \phi$ because for all P we have $(\phi + [-1] \circ \phi)(P) = \phi(P) + [-1](\phi(P)) = P + (-P) = \infty$, so $\phi + [-1] \circ \phi = [0]$.
- Distributivity holds because $\phi_1(\phi_2 + \phi_3) = \phi_1 \circ \phi_2 + \phi_1 \circ \phi_3$ is an endomorphism.
- Multiplicative identity is (unsurprisingly) given by the multiplication-by-1 map $[1]$ because $(\phi \circ [1])(P) = \phi(1P) = \phi(P) = 1\phi(P) = ([1] \circ \phi)(P)$.
- End E has no zero divisors because the composition of surjective (i.e. nonzero) endomorphisms must be surjective and therefore cannot be $[0]$.

□

We conclude with the interesting remark that the structure of the endomorphism ring of an elliptic curve is invariant under isogeny.

Proof. Suppose $\phi \in \text{End}\, E_1$ and $\varphi : E_1 \to E_2$ is an isogeny with inverse $\varphi^{-1} : E_2 \to E_1$. Then $\varphi\phi\varphi^{-1}$ is an isogeny of E_2, so the conjugation map $\phi \mapsto \varphi\phi\varphi^{-1}$ is an isomorphism between End E_1 and End E_2. □

4.1 Complex Multiplication

Every elliptic curve has a multiplication-by-n map $P \mapsto nP$ for each integer n.Are there other kinds of endomorphisms that are not simply multiplication-by-n maps? For most elliptic curves over $\mathbb{Q}$, the answer turns out to be no, in which case the endomorphism ring is isomorphic to $\mathbb{Z}$. But for some special elliptic curves, the answer is yes: these endomorphisms are called *complex multiplication* endomorphisms, or simply *complex multiplications*.

Definition (Complex Multiplication)**.** Let E be an elliptic curve defined over $\mathbb{Q}$. We say that E has *complex multiplication* if there is an endomorphism $\phi : E(\mathbb{Q}) \to E(\mathbb{Q})$ that is not a multiplication by n map.

We provide one example from [1]:

Example 4.2. The curve $E := y^2 = x^3 + x$ has complex multiplication given by $\phi(x, y) = (-x, iy)$ because if $(x, y) \in E$, then $(iy^2) = -(x^3 + x)$ reduces to $-y^2 = (-x)^3 + (-x)$, which is on the curve by symmetry.

Why are these isogenies called "complex multiplications"? We might notice an interesting parallel between the map ϕ given in example 4.2 and the complex unit i if we iterate ϕ several times:

$$\begin{aligned}\phi\ (x, y) &= (-x, iy)\\ \phi^2(x, y) &= (x, -y)\\ \phi^3(x, y) &= (-x, -iy)\\ \phi^4(x, y) &= (x, y)\end{aligned}$$

So ϕ behaves like the complex unit i in that its square is the multiplication-by-(-1) map. In fact, the endomorphism ring of the elliptic curve in 4.2 is isomorphic to the ring $\mathbb{Z}[i]$ of Gaussian integers, with the complex number $a+bi \in \mathbb{Z}[i]$ corresponding to the endomorphism $[a] + [b]\phi \in \operatorname{End} E$.

5 Zeta and L-Functions

We now switch focus to study elliptic curves from an analytic point of view. As initial motivation consider the *Riemann zeta function*:

Definition (Riemann Zeta Function)**.** We define the Riemann zeta function to be

$$\zeta(s) := \sum_{n=0}^{\infty} n^{-s}.$$

Remark. While this series converges only on the region $\{s \in \mathbb{C} : \operatorname{Re}(s) > 1\}$, we typically are concerned with the behavior of the analytic continuation of $\zeta(s)$ (that is, the unique extension of $\zeta(s)$ to all of $\mathbb{C}$ such that $\zeta(s)$ is holomorphic everywhere), so we consider $\zeta(s)$ to be defined on the entire complex plane.

Euler proved by the fundamental theorem of arithmetic that we can write

$$\zeta(s) = \prod_{p \text{ prime}}^{\infty} (1 - p^{-s})^{-1}.$$

The zeta function is an invaluable tool in the study of number theory; we are interested in studying zeta functions over finite fields and determining what information these functions can tell us about elliptic curves [4] [1]. Many of the results we reference here are too complex to state or prove in full, so we will be content to only indicate how they allow us to rewrite several of our formulas.

Let E be an elliptic curve over the field $\mathbb{F}_{p^m}$, and let $N_{p^m} := \#E(\mathbb{F}_{p^m})$ denote the number of points on E over $\mathbb{F}_{p^m}$. We define the *congruence zeta function of* E to be

$$Z(E, u) := \exp\left(\sum_{m=1}^{\infty} N_{p^m} \frac{u^m}{m}\right)$$

Example 5.1. Let $E := y^2 = x^3 + x + 1$ be a non-singular elliptic curve over $\mathbb{F}_3$. We can then calculate $\#E(\mathbb{F}_3) = 4, \#E(\mathbb{F}_9) = 16, \#E(\mathbb{F}_{27}) = 28, \#E(\mathbb{F}_{81}) = 64, \#E(\mathbb{F}_{243}) = 244, \#E(\mathbb{F}_{729}) = 784, \ldots$, so the first 5 terms of the series are

$$4u + 8u^2 + \frac{28}{3}u^3 + 16u^4 + \frac{244}{5}u^5 + \cdots$$

By the Riemann-Roch theorem, $Z(E, u)$ is given in closed form by

$$Z(E, s) = \frac{1 - a_p u + pu^2}{(1 - u)(1 - pu)}$$

where $a_p := p + 1 - N_p$. Hasse's theorem for elliptic curves over finite fields implies that $a_p^2 \leq 4p$, meaning

$$1 - a_p u + pu^2 = (1 - \pi u)(1 - \bar{\pi} u)$$

where $\pi\overline{\pi} = p$. Changing variables from u to s, where s is given by $u = p^{-s}$, we finally arrive at a simplified definition of the local zeta function of E at p.

Definition (Local Zeta Function of E at p)**.** For a fixed non-singular elliptic curve E over $\mathbb{F}_p$, the local zeta function of E at p, denoted $\zeta(E, s)$, is a function $\mathbb{C} \to \mathbb{C}$ given by

$$\zeta(E, s) = \frac{1 - a_p p^{-s} + p^{1-2s}}{(1 - p^{-s})(1 - p^{1-s})}.$$

We can now combine the values of each of these local zeta functions at each p to obtain the global zeta function of E.

Definition (L-function of an Elliptic Curve)**.** Let E be a non-singular elliptic curve over a field K with discriminant Δ. The *global zeta function of* E is

$$\zeta(E, s) := \prod_{p} \zeta(E, s) = \zeta(s)\zeta(s - 1)L(E, s)^{-1}$$

where

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

We call $L(E,s)$ the *Hasse-Weil L-function* (or just the *L-function*) of E.

Hasse conjectured that $\zeta(E,s)$ could be analytically continued to all of $\mathbb{C}$. Weil proved this was possible in special cases, and Deuring proved it for elliptic curves possessing complex multiplication.

6 The Birch and Swinnerton-Dyer Conjecture

Working with the L-function led Birch and Swinnerton-Dyer to conjecture in the 1960s that the behavior of the L-function at $s = 1$ is related to the group of rational points on the associated elliptic curve E over $\mathbb{Q}$. To make this connection more precise, we must establish one last term.

Definition 6.1 (Order of Vanishing)**.** Let $f : \mathbb{C} \to \mathbb{C}$ be a holomorphic function and let $z_0 \in \mathbb{C}$. We say that *the order of vanishing of f at z_0 is m* (or that *f has a zero of order m at z_0*) if

$$f(z_0) = f^{(1)}(z_0) = f^{(2)}(z_0) = \cdots = f^{(m-1)}(z_0) = 0$$

but $f^{(m)}(z_0) \neq 0$, in which case we write

$$\operatorname*{ord}_{z_0=0} f(z) = m.$$

Example 6.1. $f(z) = (z-5)^2(z-6)$ has a zero of order 2 at 5 and a zero of order 1 at 6.

Example 6.2. $f(z) = \sin(z)$ has a zero of order 1 at $n\pi$ for $n \in \mathbb{Z}$.

We now have the background sufficient to present the Birch and Swinnerton-Dyer conjecture:

Conjecture (Birch and Swinnerton-Dyer Conjecture)**.** If E is a non-singular elliptic curve over $\mathbb{Q}$, then

$$\operatorname*{ord}_{s=1} L(E,s) = \operatorname{rank} E(\mathbb{Q}).$$

Remark. We may sometimes refer to $\operatorname{ord}_{s=1} L(E,s)$ as the analytic rank of E and $\operatorname{rank} E(\mathbb{Q})$ as the algebraic rank of E, so the Birch and Swinnerton-Dyer conjecture may be restated as "Non-singular elliptic curves over $\mathbb{Q}$ have equal analytic and algebraic rank."

We find that this relationship holds for all elliptic curves E over $\mathbb{Q}$ for which we can calculate $\operatorname*{ord}_{s=1} L(E,s)$ and $\operatorname{rank} E(\mathbb{Q})$ – this was the initial observation made by Birch and Swinnerton-Dyer. However, there are several related results that agree with the conjecture.

Let E be an elliptic curve over $\mathbb{Q}$.

1. Arthaud (1978) extended a result of Wiles and Coates (1977) to show that if E has complex multiplication and $L(E,1) \neq 0$, then $E(\mathbb{Q})$ is finite.

2. The proof of the modularity theorem by Breuil et al. (2001) extended the results of Kolyvagin (1989) to show that if $L(E, s) \neq 0$ then E has rank 0, and if $\text{ord}_{s=1} L(E, s) = 1$, then the curve has rank 1.

3. Bhargava and Shankar (2015) proved that a positive proportion of curves satisfy the conjecture.

Remark. The first theorem by Arthaud, Wiles, and Coates corresponds to the case where E has complex multiplications and algebraic or analytic rank 0. The second theorem by Breuil et al. shows one direction of the conjecture if the analytic rank is 0 or 1.

In light of this evidence and the usefulness of the conjecture, in 2000 the Clay Mathematics Institute listed the Birch and Swinnerton-Dyer conjecture as one of the seven Millennium Prize Problems, for which they offer a $1,000,000US prize to anyone who can prove or disprove the conjecture.

7 Computational Evidence for the Birch and Swinnerton-Dyer Conjecture

An enormous amount of interesting work has been done on elliptic curves, both related and unrelated to the Birch and Swinnerton-Dyer conjecture. There is significantly more information related to equivalence relations between elliptic curves and invariants of elliptic curves necessary for understanding the strong Birch and Swinnerton-Dyer conjecture.

A large number of curves have had their ranks computed, and the data is available from the L-Function and Modular Forms database (at https://www.lmfdb.org/). Using SageMath, we attempted to compute the algebraic and analytic rank of all elliptic curves $E := y^2 = x^3 + Ax + B$ over $\mathbb{Q}$ with integer coefficients $|A|, |B| \leq 100$. Of these 40,000 curves, we successfully computed the analytic and algebraic ranks of 38,366 curves; all of these curves had equal ranks (Figure 3a). Notably, only 4 curves were found to have analytic and algebraic rank 4 (Figure 3b).

Rank	Number of curves
0	11559
1	19204
2	6985
3	614
4	4

(a) Distribution of curves with $|A|, |B| \leq 100$ and matching algebraic and analytic rank

$$y^2 = x^3 - 97x + 25$$
$$y^2 = x^3 - 70x - 83$$
$$y^2 = x^3 - 64x + 1$$
$$y^2 = x^3 + 97x + 81$$

(b) Curves that have analytic and algebraic rank 4

Figure 3: Ranks of 38,366 curves $y^2 = x^3 + Ax + B$ with integer $|A|, |B| \leq 100$ over $\mathbb{Q}$ with matching algebraic and analytic rank.

References

[1] J. Joseph H. Silverman, Rational Points on Elliptic Curves. Springer, 2 ed., 2015.

[2] Evan Dummit, "Elliptic Curves." https://web.northeastern.edu/dummit/teaching_sp21_4527/numthy_7_elliptic_curves_v1.00.pdf, 2021.

[3] Joseph H. Silverman, The Arithmetic of Elliptic Curves. Springer, 2 ed., 2009.

[4] Evan Dummit, "Analytic Number Theory." https://web.northeastern.edu/dummit/teaching_fa22_4527/numthy_10_analytic_number_theory_v1.00.pdf, 2022.

[5] Michael Rosen and Kenneth Ireland, A Classical Introduction to Modern Number Theory. Springer, 2 ed., 1990.