Elliptic Curves and the Birch and Swinnerton-Dyer Conjecture

Begüm Gülgen

Advisor: Assoc. Prof. Dr. Haydar Göral

Motivation

Determining all rational solutions to a cubic equation in two variables remains an open problem in mathematics. While rational solutions to polynomial equations of lower degrees can be systematically determined, cubic equations in two variables are the first case for which no general method exists. Furthermore, there is currently no general algorithm for determining whether a given cubic equation has a finite or an infinite number of rational solutions. The Birch and Swinnerton-Dyer Conjecture (BSD), one of the seven Millennium Prize Problems, offers a potential algorithm for addressing this issue. If proven, the BSD conjecture would provide a way to determine whether the number of rational solutions is finite or infinite.

Elliptic Curves

An **elliptic curve** is a smooth algebraic curve, defined by the general equation:

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

where $a_1, a_2, a_3, a_4, a_6 \in K$ (the field of definition).

If the field has characteristic not equal to 2 or 3, the equation with change of variables can be transformed into the **Weierstrass normal form**:

$$y^2 = x^3 + Ax + B,$$

where $A, B \in K$.

Discriminant and Smoothness

The smoothness of an elliptic curve is determined by its **discriminant**, defined as:

$$\Delta' = 4A^3 + 27B^2,$$
$$\Delta = -16\Delta'.$$

- If $\Delta' = 4A^3 + 27B^2 = 0$, the curve has singularities (e.g., a cusp or self-intersection).
- If $\Delta' \neq 0$, the curve is smooth, meaning it has no singular points.

This condition is equivalent to the cubic polynomial $f(x) = x^3 + Ax + B$ having no double roots.

Thus, E is an elliptic curve in the field K if and only if $\Delta' \neq 0$.

Elliptic Curves as Groups

Let E be an elliptic curve given by a Weierstrass equation in the projective form:

$$y^2z = x^3 + axz^2 + bz^3.$$

Thus, $E \subset \mathbb{P}^2$ consists of points $P = (x, y)$ satisfying the Weierstrass equation, together with the point $\mathcal{O} = [0 : 1 : 0]$ at infinity.
Let $L \subset \mathbb{P}^2$ be a line. Since the Weierstrass equation has degree 3, the line L intersects E at exactly three points, say P, Q, and R, counted with multiplicities.

Composition Law: The points P, Q, and R are related via the group law, defining the addition operation on the elliptic curve.

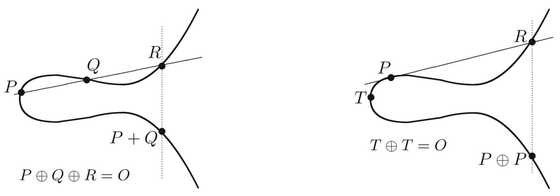

Figure 1: Composition law.

The composition law has the following properties:

(a) If a line L intersects E at the (not necessarily distinct) points P, Q, R, then:
$$(P \oplus Q) \oplus R = \mathcal{O}.$$
(b) $P \oplus \mathcal{O} = P$ for all $P \in E$.
(c) $P \oplus Q = Q \oplus P$ for all $P, Q \in E$.
(d) Let $P \in E$. There exists a point $\ominus P$, satisfying:
$$P \oplus (\ominus P) = \mathcal{O}.$$
(e) Let $P, Q, R \in E$. Then:
$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R).$$
In other words, the composition law makes E into an abelian group with the identity element $\mathcal{O}$.

Group Law Algorithm

Let E be an elliptic curve given by a Weierstrass equation:

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

(a) Let $P_0 = (x_0, y_0)$. Then:
$$-P_0 = (x_0, -y_0 - a_1x_0 - a_3).$$
(b) Next, let $P_1 + P_2 = P_3$ with $P_i = (x_i, y_i) \in E$ for $i = 1, 2, 3$.
- If $x_1 = x_2$ and $y_1 + y_2 + a_1x_2 + a_3 = 0$, then:
$$P_1 + P_2 = \mathcal{O}.$$
- Otherwise, define λ and ν by the following formulas:

	λ	ν
$x_1 \neq x_2$	$\frac{y_2 - y_1}{x_2 - x_1}$	$\frac{y_1x_2 - y_2x_1}{x_2 - x_1}$
$x_1 = x_2$	$\frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}$	$\frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$

Then $y = \lambda x + \nu$ is the line through P_1 and P_2, or tangent to E if $P_1 = P_2$.

Mordell's Theorem

For a rational elliptic curve E, the group of rational points on E is denoted by $E(\mathbb{Q})$.

Mordell's Theorem (1922): The group $E(\mathbb{Q})$ of rational points on E is finitely generated.

Since $E(\mathbb{Q})$ is a finitely generated abelian group, we have:

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}}$$

for some $r \geq 0$, and $E(\mathbb{Q})_{\text{tors}}$ is a finite abelian group, referred as the torsion part of $E(\mathbb{Q})$.

Algebraic Rank: Let E be an elliptic curve defined over the rational numbers $\mathbb{Q}$. The *algebraic rank* of E, denoted by r, is the rank of the finitely generated abelian group $E(\mathbb{Q})$, which is given by above.

- If $r = 0$, the group $E(\mathbb{Q})$ is finite, and E has only finitely many rational points.
- If $r \geq 1$, E has infinitely many rational points.

The rank of E measures the number of points needed to generate all rational points on the curve. By **Mordell's Theorem**, this number is always finite.

Mazur's Theorem (1977):

1. $E(\mathbb{Q})_{\text{tors}}$ is a cyclic group of order n, where $1 \leq n \leq 10$ or $n = 12$, or
2. $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to one of the following groups:
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}, \quad \text{for } 1 \leq m \leq 4.$$

Elliptic Curves over $\mathbb{F}_p$

Now, we consider the elliptic curves defined over finite fields and their points.

Let us take the elliptic curve as

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

For any prime p, we look at the solutions over the finite field $\mathbb{F}_p$. Reduce E modulo p, that is, reduce the coefficients of the equation modulo p and write

$$y^2 \equiv x^3 + \overline{A}x + \overline{B} \pmod{p}.$$

Let us examine the solutions of this equation modulo p (in fact, this operation might not make sense if the coefficients of the equation are not integers. For now, let us assume A and B are integers). We denote the set of solutions by $E(\mathbb{F}_p)$.

However, reducing modulo p does not always result in an elliptic curve, as the discriminant of the equation modulo p might be zero. If $p > 2$ divides the discriminant of E, the reduction of E modulo p produces a singular curve; otherwise, it defines an elliptic curve over $\mathbb{F}_p$.

Definition: Let Δ denote the discriminant of E.

- If $p \nmid \Delta$, then p is said to have *good reduction*.
- If $p \mid \Delta$, then p is said to have *bad reduction*.

For any elliptic curve E, there are only finitely many primes p with bad reduction, specifically the prime divisors of Δ.

Hasse's Theorem

Hasse's Theorem (1933): Let E be a rational elliptic curve, and let $p > 2$ be a prime with good reduction for E. Then the following inequality holds:

$$|p + 1 - \#E(\mathbb{F}_p)| \leq 2\sqrt{p}.$$

Example: Consider the elliptic curve E given by:

$$y^2 = x^3 + 1.$$

For a prime $p > 3$, we compute the solutions of this equation modulo p to determine $\#E(\mathbb{F}_p)$, the number of points on E over $\mathbb{F}_p$. Using Hasse's Theorem, we know that:

$$p + 1 - 2\sqrt{p} \leq \#E(\mathbb{F}_p) \leq p + 1 + 2\sqrt{p}.$$

Prime p	$E(\mathbb{F}_p)$ Count	Hasse Lower Bound	Hasse Upper Bound	In Bounds
5	6	1.53	10.47	Yes
7	12	2.71	13.29	Yes
11	12	5.37	18.63	Yes
13	12	6.79	21.21	Yes
17	18	9.75	26.25	Yes
19	12	11.28	28.72	Yes
23	24	14.41	33.59	Yes
29	30	19.23	40.77	Yes
31	36	20.86	43.14	Yes
37	48	25.83	50.17	Yes

Table 1: Elliptic Curve Point Counts and Hasse Bounds

The BSD Conjecture

In 1960, Birch and Swinnerton-Dyer computed ranks of elliptic curves and the number of solutions modulo p on these curves. They observed that the behavior of $\#E(\mathbb{F}_p)/p$ correlates with the rank r of the curve. This insight led them to propose the famous conjecture:

$$\prod_{p \leq X} \frac{\#E(\mathbb{F}_p)}{p} \sim c \cdot (\log X)^r,$$

where c is a constant depending on the curve E, and r is its rank.

Birch and Swinnerton-Dyer also gave an explicit expression for c in terms of E; this is called the strong form of the conjecture.

L-function and Analytic Rank

The L-function of an elliptic curve E is defined as:

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

where, $a_p = p + 1 - \#E(\mathbb{F}_p)$.

$L(E, s)$ can also be expressed as a Dirichlet series:

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

where a_n are coefficients determined by the a_p values of the prime factors of n.

Dirichlet Series Convergence: Let $L(E, s)$ denote the Dirichlet series defined as:

$$L(E, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \quad \text{for } \mathrm{Re}(s) > \frac{3}{2}.$$

The series converges absolutely for $\mathrm{Re}(s) > \frac{3}{2}$ by Hasse's Theorem and defines an analytic function in the half-plane

$$H = \{s \in \mathbb{C} \mid \mathrm{Re}(s) > \tfrac{3}{2}\}.$$

Taylor Series Expansion: The function $L(E, s)$ is analytic in the half-plane H. While a Taylor series expansion in H is possible, the point $s = 1$ does not belong to H, so a direct expansion around $s = 1$ cannot be performed.

Wiles-Taylor Theorem (1995): Let E be an elliptic curve defined over $\mathbb{Q}$. According to the Wiles-Taylor theorem, $L(E, s)$ can be analytically continued to the entire complex plane $\mathbb{C}$.
This implies that $L(E, s)$ is analytic so is differentiable at $s = 1$.

Analytic Rank: The analytic continuation allows the Taylor series expansion of $L(E, s)$ around $s = 1$:

$$L(E, s) = c(s - 1)^m + k_1(s - 1)^{m+1} + \dots$$

where $c \neq 0$, and the analytic rank r_{an} of E is m. If $L(E, 1) \neq 0$, then the analytic rank is 0.

Modern Formulation

When we substitute $s = 1$ into the good reduction part of the L-function, we get

$$L(E, 1) \approx \prod_{p \leq x} \frac{p}{\#E(\mathbb{F}_p)},$$

where p runs over all primes less than the given x. Here, notice that this is the reciprocal of

$$\prod_{p \leq x} \frac{\#E(\mathbb{F}_p)}{p}.$$

Now, we can give the modern formulation of the Birch and Swinnerton-Dyer Conjecture.

BSD Conjecture (1963)

Let E be an elliptic curve over $\mathbb{Q}$. Then the algebraic and analytic ranks of E are the same.

The Birch and Swinnerton-Dyer conjecture immediately implies that an elliptic curve E has infinitely many rational points if and only if $L(E, 1) = 0$.

The conjecture, made in the 1960's, has been studied by many mathematicians over four decades. Wiles et al.'s work on modularity in late 1999, along with earlier contributions from Gross, Zagier, Kolyvagin, and others, proved a partial result toward the conjecture.

Theorem: Suppose E is an elliptic curve over $\mathbb{Q}$ and that $r_{an} \leq 1$. Then the algebraic and analytic ranks of E are the same.

The Power of BSD

Example ① $r = 0$:
Objective: Show that $L(E, 1) \neq 0$ for $E : y^2 = x^3 + 1$ with $r = 0$.
Method: Compute
$$L(E, 1) \approx \prod_{p \leq 1000} \frac{p}{\#E(\mathbb{F}_p)}.$$
Result: The value is approximately 0.5276016202421178.
Interpretation: This confirms that $r = 0$.

Since $r = 0$, $E(\mathbb{Q})$ contains only a finite group of points which is the $E(\mathbb{Q})_{tors}$, and we can show that $E(\mathbb{Q}) \cong \mathbb{Z}/6\mathbb{Z}$.
The points of $E(\mathbb{Q})$ are
$\{(0, 1), (0, -1), (2, 3), (2, -3), (-1, 0), \mathcal{O}\}$.

Example ② $r = 2$:
Objective: Verify $L(E, 1) = 0$, $L'(E, 1) = 0$, $L''(E, 1) \neq 0$ for $E : y^2 = x^3 - 34^2x$.
Method: Compute the L-series and the derivatives at $s = 1$ using finite differences ($h = 10^{-5}$).
Result:
$$L(E, 1) \approx -1.16658388158845 \times 10^{-18},$$
$$L'(E, 1) \approx -1.59460547815251 \times 10^{-9},$$
$$L''(E, 1) \approx 12.7703039565201.$$
Interpretation: This confirms that $r = 2$.

Now, for $E : y^2 = x^3 - 34^2x$ with rank $r = 2$, consider the product

$$\prod_{p \leq 1000} \frac{\#E(\mathbb{F}_p)}{p},$$

and dividing it by $\log^2 1000$, yields a constant.

Result: The value is approximately 0.6558212571499893.
Interpretation: The normalized product is constant, confirming the prediction of the BSD conjecture in its classical formulation with $r = 2$ for this example.

For the above example, we can show that $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
The points of $E(\mathbb{Q})_{\text{tors}}$ are
$\{(34, 0), (-34, 0), (0, 0), \mathcal{O}\}$.

References

- **[1]** Kul, H. (2017). *Bir Milyon Dolarlık Milenyum Problemi: BSD Sanısı.* Matematik Dünyası, 105.
- **[2]** Silverman, J. H. (2009). *The Arithmetic of Elliptic Curves.* Springer-Verlag.
- **[3]** Silverman, J. H., Tate, J. (1992). *Rational Points on Elliptic Curves.* Springer-Verlag.
- **[4]** Sinnott, W. (1995). *The Conjecture of Birch and Swinnerton-Dyer.* Notices of the AMS, 42(2), 123–132.
- **[5]** Stein, W. A. (2007). *The Birch and Swinnerton-Dyer Conjecture: A Computational Approach.* In Algorithmic Number Theory (pp. 1–22). Springer.
- **[6]** Stewart, I., Tall, D. (2001). *Algebraic Number Theory and Fermat's Last Theorem* (3rd ed.). A K Peters/CRC Press.
- **[7]** YouTube Video. (n.d.). *Birch and Swinnerton-Dyer Conjecture.* Retrieved from `https://www.youtube.com/watch?v=_-feKGb6-gc&t=2600s`.