Proof of Mordell-Weil Theorem

Christine Lyu Zhengyang Liu Shifan Zhao

The Ohio State University

DEPARTMENT OF MATHEMATICS

Abstract

The Mordell-Weil Theorem, originally conjectured by Poincaré and proved by Mordell in 1922, states that the group of rational points $E(\mathbb{Q})$ on an elliptic curve is finitely generated. This result laid the foundation for modern research in Diophantine equations and the arithmetic of elliptic curves. It has since become a cornerstone of number theory, with deep connections to modern topics such as the Birch and Swinnerton-Dyer Conjecture, the proof of Fermat's Last Theorem, and applications in cryptography. In this poster, we follow Tate and Silverman's approach, using **height functions** and **algebraic methods** to outline a proof of the Mordell-Weil Theorem.

The Mordell-Weil Theorem

(For curves with a rational point of order two) Let E be an elliptic curve given by an equation

$$E : y^2 = x^3 + ax^2 + bx,$$

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

Definition of Elliptic Curves and Group Law

An elliptic curve E is given by the set of solutions to an equation in the form

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

together with a point $\mathcal{O}$ at ∞, assuming the (complex) roots of $f(x)$ are distinct.

Rational points on an elliptic curve form an abelian group under addition. We describe the addition of two points here: Let P and Q be two rational points on E. To add P and Q, draw the line through P and Q and take the third intersection point $P * Q$. Then join it to $\mathcal{O}$ by another line, and take the third intersection point to be $P + Q$. In other words, set $P + Q = \mathcal{O} * (P * Q)$.
Then we briefly discuss how to find the inverse of a point P. Given a point P, we draw the line through $\mathcal{O}$ and P. Then the third intersection point will be $-P$.

Height Function: Let $x = m/n$ be a rational number written in lowest terms. We define:

$$H(x) = H\left(\frac{m}{n}\right) = \max\{|m|, |n|\}, \qquad h(x) = \log H(x).$$

Let $P = (x(P), y(P))$ be a rational point on E. Define the height of P to be

$$H(P) = H(x(P)), \qquad h(P) = \log H(P).$$

Important Propositions Leading to the Mordell-Weil Theorem

The Mordell-Weil Theorem follows from four propositions. We state these propositions and sketch the proofs. We then explain how they imply the Mordell-Weil Theorem.

Proposition 1: For every real number M, the set $\{P \in E(\mathbb{Q}) : h(P) \le M\}$ is finite.

Proposition 2: Let P_0 be a fixed rational point on E. There is a constant k_0 that depends on P_0, a, b, and c, so that

$$h(P + P_0) \le 2h(P) + k_0 \text{ for all } P \in E(\mathbb{Q}).$$

Proposition 3: There is a constant k, depending on a, b, and c, so that

$$h(2P) \ge 4h(P) - k \text{ for all } P \in E(\mathbb{Q}).$$

Proposition 4: The index $(E(\mathbb{Q}) : 2E(\mathbb{Q}))$ is finite.

Proof Sketch of the Four Propositions

Proposition 1: For a fixed height bound M, there are only finitely many coprime pairs (a, b) with $\max(|a|, |b|) \le M$. Therefore, only finitely many such rational numbers exist.

Proposition 2: Using the explicit formula for point addition on an elliptic curve, one can express $x(P + P_0)$ as a rational function of $x(P)$ and $x(P_0)$. Estimating the growth of the numerator and denominator gives a bound on the height of the sum.

Proposition 3: For a point $P = (x, y)$ on $E(\mathbb{Q})$, let $2P = (\xi, \eta)$, then the duplication formula gives us:

$$\xi = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c} = \frac{f'(x)^2 - (8x + 4a)f(x)}{4f(x)}.$$

Since $y^2 = f(x)$ is non-singular by assumption, $f(x)$ and $f'(x)$ have no common complex roots. As a result, the numerator and denominator also have no common complex roots.
The rest proof of **Proposition 3** relies on the following fact about polynomials.
Fact: For polynomials p and q with integer coefficients and no common complex roots, let $d = \max\{\deg(p), \deg(q)\}$. There are constants k_1 and k_2, so that for all rational m/n that are not roots of q,

$$dh\left(\frac{m}{n}\right) - k_1 \le h\left(\frac{p(m/n)}{q(m/n)}\right).$$

Since this fact is not specifically related to elliptic curves, we will briefly sketch the idea of the proof and how it leads to **Proposition 3**.

Proof: We start by proving the above fact. There exist some integer $R \ge 1$, independent of m and n, such that:

$$\frac{H\left(\frac{p(m/n)}{q(m/n)}\right)}{H(m/n)^d} \ge \frac{1}{2R}\frac{|p(\frac{m}{n})| + |q(\frac{m}{n})|}{\max\{|\frac{m}{n}|^d, 1\}}.$$

One can show that the right-hand side is greater than or equal to a constant $C_1 > 0$. Thus, this gives us:

$$H\left(\frac{p(m/n)}{q(m/n)}\right) \ge C_1 H\left(\frac{m}{n}\right)^d,$$

where the constant C_1 depends on p and q, but not on m or n. Then taking logarithms gives us the desired inequality:

$$h\left(\frac{p(m/n)}{q(m/n)}\right) \ge dh\left(\frac{m}{n}\right) - k_1 \qquad \text{with} \qquad k_1 = \log(1/C_1).$$

For the proof of Proposition 3, we set $p(x) = x^4 - 2bx^2 - 8cx + b^2 - 4ac$ and $q(x) = 4x^3 + 4ax^2 + 4bx + 4c$. The desired inequality then follows from the **Fact**.

Proposition 4: We will explain the proof of Proposition 4 in more details, as it is the most difficult part. Recall the elliptic curve E is given by the following equation

$$E : y^2 = f(x) = x^3 + ax^2 + bx, \quad a, b \in \mathbb{Z}.$$

We consider $\overline{E}$ given by

$$\overline{E} : y^2 = x^3 + \overline{a}x^2 + \overline{b}x,$$

where $\overline{a} = -2a$, $\overline{b} = a^2 - 4b$, and $\overline{\overline{E}}$ given by

$$\overline{\overline{E}} : y^2 = x^3 + \overline{\overline{a}}x^2 + \overline{\overline{b}}x,$$

where $\overline{\overline{a}} = -2\overline{a}$, $\overline{\overline{b}} = \overline{a}^2 - 4\overline{b}$.

We then define $\varphi : E \to \overline{E}$ by

$$\varphi(x, y) = (\overline{x}, \overline{y}) = \left(\frac{y^2}{x^2}, y\left(\frac{x^2 - b}{x^2}\right)\right), \text{ with } x \ne 0.$$

And both $\mathcal{O}$ and $T = (0, 0)$ get mapped to $\overline{\mathcal{O}}$ under φ. Then the kernel of φ is $\{\mathcal{O}, T\}$.
Applying the same process to $\overline{E}$ gives a map $\overline{\varphi} : \overline{E} \to \overline{\overline{E}}$. The curve $\overline{\overline{E}}$ is isomorphic to E via the map $(x, y) \mapsto (\frac{1}{4}x, \frac{1}{8}y)$. There is thus a homomorphism $\psi : \overline{E} \to E$ given by

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

It can be directly verified that the composition $\psi \circ \varphi : E \to E$ is the multiplication by two map

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

Then we introduce a map $\alpha : E(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ defined by

$$\begin{aligned} \alpha(\mathcal{O}) &= 1 \pmod{\mathbb{Q}^{*2}} \\ \alpha(T) &= b \pmod{\mathbb{Q}^{*2}} \\ \alpha(x, y) &= x \pmod{\mathbb{Q}^{*2}} \text{ if } x \ne 0. \end{aligned}$$

It turns out that α is a homomorphism, with its kernel being $\psi(\overline{E}(\mathbb{Q}))$. Hence α induces an injective homomorphism $E(\mathbb{Q})/\psi(\overline{E}(\mathbb{Q})) \hookrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$.
Let $p_1, \ldots, p_t$ be the distinct primes dividing b. Then the image of α is contained in the subgroup of $\mathbb{Q}^*/\mathbb{Q}^{*2}$ consisting of the elements

$$\{\pm p_1^{\epsilon_1} p_2^{\epsilon_2} \cdots p_t^{\epsilon_t} : \text{ each } \epsilon_i \text{ equals 0 or 1}\}.$$

The index $(E(\mathbb{Q}) : \psi(\overline{E}(\mathbb{Q})))$ is at most 2^{t+1}. Therefore, we get $(\overline{E}(\mathbb{Q}) : \varphi(E(\mathbb{Q}))$ and $(E(\mathbb{Q}) : \psi(\overline{E}(\mathbb{Q})))$ are finite. Then we use the following lemma about abelian groups to conclude the proof.
Lemma: Let A and B be abelian groups, and suppose that $\varphi : A \to B$ and $\psi : B \to A$ are homomorphisms satisfying

$$\psi \circ \varphi(a) = 2a \text{ for all } a \in A \text{ and } \varphi \circ \psi(b) = 2b \text{ for all } b \in B.$$

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

$$(A : 2A) \le (A : \psi(B))(B : \varphi(A)).$$

Applying the above lemma to $A = E(\mathbb{Q})$ and $B = \overline{E}(\mathbb{Q})$ yields Proposition 4.

Proof of the Mordell-Weil Theorem

Let $\Gamma \subset E(\mathbb{Q})$ be a set of coset representatives of $E(\mathbb{Q})/2E(\mathbb{Q})$. Since we know there are only finitely many cosets, Γ is finite.
Now consider any $P \in E(\mathbb{Q})$. There exists a coset representative $Q \in \Gamma$ such that $P \in Q + 2E(\mathbb{Q})$, i.e., $P = Q + 2R$ for some $R \in E(\mathbb{Q})$. Applying **Proposition 3** repeatedly to $R, 2R, 4R, \ldots$, we obtain a sequence of points with decreasing height. Then by **Proposition 1**, only finitely many points can occur in such a descent sequence. Eventually, we reach points with height bounded by a constant depending on Γ, and therefore, the descent terminates.
Thus, we can express every $P \in E(\mathbb{Q})$ as a sum of finitely many points in Γ. As a result, $E(\mathbb{Q})$ is finitely generated.