Proving the Mordell-Weil Theorem on Elliptic Curves

Yunus Annanepesov

July 10, 2025

The Mordell-Weil Theorem

Statement

Let $E/\mathbb{Q}$ be a non-singular elliptic curve. Then:

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T$$

where T is a finite torsion subgroup and r is the rank of E.

What is an Elliptic Curve?

- Curve defined by $y^2 = x^3 + Ax + B$, with $A, B \in \mathbb{Q}$
- Smooth if $\Delta = -16(4A^3 + 27B^2) \neq 0$
- Rational points form a group with a geometric addition law

The Group Law (Geometric View)

- Add P and Q: draw line through them
- Intersects curve at third point R; reflect R to get $P + Q$
- Identity is the point at infinity O

Torsion Points and Nagell-Lutz

- Torsion: points P with $nP = O$
- Nagell–Lutz Theorem:
  - If E has integer coefficients, torsion points have integer coordinates
  - If $P = (x, y)$ has finite order and $y \neq 0$, then $y^2 \mid \Delta$

Height Functions

- For $x = \frac{m}{n}$ in lowest terms, define $H(x) = \max(|m|, |n|)$
- For $P = (x, y)$ on $E(\mathbb{Q})$, set $H(P) = H(x)$
- Logarithmic height: $h(P) = \log H(P)$
- Finiteness: only finitely many points with height $\leq M$

Behavior of Heights

- $h(P + Q) \leq 2h(P) + \kappa$ (fixed Q)
- $h(2P) \geq 4h(P) - \kappa$
- This gives control over how heights grow under group operations

Weak Mordell-Weil Theorem

- $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite
- Use homomorphism $\alpha : E(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$
- Image of α is finite $\Rightarrow$ only finitely many cosets mod $2E(\mathbb{Q})$

Descent and the Proof

- Given P, write $P = Q_1 + 2P_1$, then $P_1 = Q_2 + 2P_2$, etc.
- Heights drop: $h(P_{n+1}) \leq \frac{1}{2}h(P_n) + C$
- Sequence must stop: heights cannot go below zero

Bounding $E(\mathbb{Q})$

- Each P becomes a sum of:
  - Elements from finitely many cosets
  - Points of small height (only finitely many of those)
- So $E(\mathbb{Q})$ is finitely generated

Conclusion: The Mordell-Weil Theorem

- $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T$
- T is finite (torsion), $\mathbb{Z}^r$ part comes from descent
- Elliptic curves combine algebra, geometry, and number theory

Why It Matters

- Used in Fermat's Last Theorem (via modularity)
- Basis for elliptic curve cryptography (ECC)
- Illustrates the power of descent and finiteness techniques

References

- Silverman and Tate, *Rational Points on Elliptic Curves*
- Cassels, *Lectures on Elliptic Curves*
- Washington, *Elliptic Curves in Cryptography*