Points on Elliptic Curves (6)

Mordell's Theorem (1922)
The rational points on an elliptic curve are **finitely generated**.

Example

- $Y^2 = X^3 - 2$ has **infinitely many** rational points. All of them are generated by a single rational point (3,5).

Louis Joel Mordell (1888-1972)

https://en.wikipedia.org/wiki/Louis_J._Mordell

Points on Elliptic Curves (7)

$E : Y^2 = X^3 + AX + B$

- $Q_1, \cdots, Q_M$ are **independent** if

  $$[N_1]Q_1 \oplus \cdots \oplus [N_M]Q_M$$

  (for integers $N_1, \cdots, N_M$) are **distinct**.
- **R** = maximum # of indep rational points

  $= \operatorname{rank} E(\mathbb{Q})$
- $R < \infty$ by **Mordell's Thm**.
- $R = 0 \Leftrightarrow$ only finitely many rational points

Points on Elliptic Curves (8)

Example

- $Y^2 = X^3 - X$ has only 4 rational points.

  $\Rightarrow$ **rank R = 0**

- $Y^2 = X^3 + 1$ has only 6 rational points.

  $\Rightarrow$ **rank R = 0**

- $Y^2 = X^3 - 2$ All the rational points are generated by a **single rational point (3,5)**.

  $\Rightarrow$ **rank R = 1**

Points on Elliptic Curves (9)

Problem (unsolved)

Elliptic curve

$$E : Y^2 = X^3 + AX + B$$

- How can we calculate $R = \mathrm{rank}\,\mathrm{E}(\mathbb{Q})$?
- How can we find rational points $Q_1, \cdots, Q_M$ which generate the whole rational points on E?

Interlude: Elliptic Curves of Large Rank

- It is difficult to find elliptic curves of large rank.
- **World Record**: rank $\geq$ **28** (Elkies, 2006)

$$Y^2 + XY + Y = X^3 - X^2 - 20067762415575526585033208209338542750930230312178956502\,X + 34481611795030556467032985690390720374855944359319180361266008296291939448732243429$$

Noam Elkies (1966-)

https://en.wikipedia.org/wiki/Noam_Elkies