Ranks of elliptic curves

Edwina Aylward

UCL PGR Seminar

HallowEve

Motivation and Background

Motivation: Diophantine problems

A **Diophantine equation** is a polynomial equation with integer coefficients.

Example

Consider the Pythagorean equation $x^2 + y^2 = z^2$. All rational solutions can be written as

$$(x, y, z) = (m^2 - n^2,\ 2mn,\ m^2 + n^2) \quad m, n \in \mathbb{Q}.$$

When can we determine all rational solutions of a Diophantine equation?

- **One variable, any degree:** Consider a polynomial $f(x) \in \mathbb{Z}[x]$. Using the rational root theorem, one can write down a finite list of rational numbers that must contain all rational solutions of $f(x) = 0$.
- **Two variables, linear:** Consider $ax + by = c$ for $a, b, c \in \mathbb{Z}$. This has infinitely many integer solutions iff $\gcd(a, b) \mid c$, and in that case it is easy to parametrize all solutions.
- **Two variables, quadratic:** Equations like $x^2 + y^2 = 1$ (conics). If one rational point is known, all others can be found by drawing lines with rational slope through that point (*stereographic projection*).

Elliptic Curves

Next step: what about cubic equations in two variables?

A general cubic Diophantine equation has the form

$$\sum_{i+j\leq 3} a_{i,j}x^i y^j = 0, \qquad a_{i,j} \in \mathbb{Z}.$$

An **elliptic curve** over $\mathbb{Q}$ is a smooth projective cubic curve with a rational point. It can be written (after a change of variables) in *short Weierstrass form:*

$$E: \quad y^2 = x^3 + ax + b, \qquad a, b \in \mathbb{Q},\ 4a^3 + 27b^2 \neq 0.$$

Embarrassing fact: we still do not know how to determine the rational points on such curves.

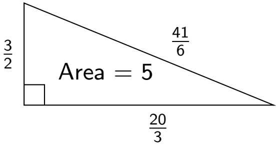
The Congruent Number Problem

Which integers are the area of a right-angled triangle with sides of rational length?

Definition

$n \in \mathbb{N}$ is a *congruent number* if there exist $a, b, c \in \mathbb{Q}$ with

$$a^2 + b^2 = c^2 \quad \text{and} \quad \tfrac{1}{2}ab = n.$$



Let $n \in \mathbb{N}$ be square-free, and set

$$E_n : y^2 = x^3 - n^2 x.$$

Then

$$\{(a,b,c) \in \mathbb{Q}^3 \mid a^2 + b^2 = c^2,\ \tfrac{1}{2}ab = n\} \quad \longleftrightarrow \quad \{(x,y) \in E_n(\mathbb{Q}) \mid y \neq 0\}$$

is a one-to-one correspondence given by

$$(a,b,c) \mapsto \left(\frac{nb}{c-a}, \frac{2n^2}{c-a}\right), \qquad (x,y) \mapsto \left(\frac{x^2 - n^2}{y}, \frac{2nx}{y}, \frac{x^2 + n^2}{y}\right).$$

n is a congruent number $\iff$ $\exists (x,y) \in E_n(\mathbb{Q}),\ y \neq 0$ $\iff$ $\mathrm{rank}(E_n) \geq 1$

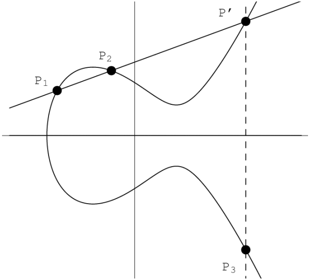
The group law and the rank

Rational points on E form an abelian group. By the Mordell-Weil theorem, this group is finitely generated and hence of the form

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

where

- $E(\mathbb{Q})_{\text{tors}}$ consists of points of finite order (torsion),
- $r = \operatorname{rk} E/\mathbb{Q}$ is the **rank** of the elliptic curve.



There is no effective way to compute the rank. In practice, one can

- Calculate a lower bound by searching for points of infinite order (with a computer).
- Calculate an upper-bound by computing Selmer groups.
- Hope that these coincide!

Some open questions:

- Is there a finite maximum for the rank? Largest known example has $\operatorname{rk} E/\mathbb{Q} \geq 29$.
- Minimalist conjecture: do 50% of elliptic curves $E/\mathbb{Q}$ satisfy $\operatorname{rk} E/\mathbb{Q} = 0$ and 50% satisfy $\operatorname{rk} E/\mathbb{Q} = 1$?

L-functions and parity

Reduction of an elliptic curve modulo p

Let

$$E : y^2 = x^3 + ax + b, \qquad a, b \in \mathbb{Z},$$

be an elliptic curve over $\mathbb{Q}$ with **discriminant**

$$\Delta = -16(4a^3 + 27b^2).$$

For each prime p, we can reduce the coefficients modulo p to get a curve

$$\tilde{E}/\mathbb{F}_p : \quad y^2 = x^3 + \bar{a}x + \bar{b}.$$

- If $p \nmid \Delta$, the reduced curve $\tilde{E}$ is smooth $\Rightarrow$ E has **good reduction** at p.
- If $p \mid \Delta$, $\tilde{E}$ is singular $\Rightarrow$ E has **bad reduction** at p.

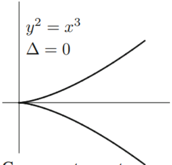
Types of bad reduction:

- Additive (cusp)
- Multiplicative (node)

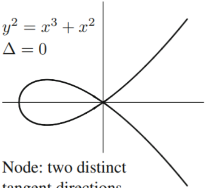
Example:

$$E : y^2 = x^3 - x, \qquad \Delta = 64.$$

E has good reduction for $p \neq 2$, and bad (additive) reduction at $p = 2$.



Cusp: one tangent direction



Node: two distinct tangent directions

The analytic side: the Birch–Swinnerton–Dyer conjecture

To each elliptic curve $E/\mathbb{Q}$ we attach an L-**function:**

$$L(E/\mathbb{Q}, s) = \prod_p L_p(E, s),$$

where for almost all primes (those of good reduction)

$$L_p(E, s) = (1 - a_p p^{-s} + p^{1-2s})^{-1}, \qquad a_p = p + 1 - \#E(\mathbb{F}_p).$$

- This function can be easily seen to converge for $\mathrm{Re}(s) > \frac{3}{2}$.
- The modularity theorem for elliptic curves over $\mathbb{Q}$ implies that it extends to all $s \in \mathbb{C}$.

Birch–Swinnerton-Dyer Conjecture (BSD)

$$\mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) = \mathrm{rk}\, E/\mathbb{Q}.$$

So $L(E/\mathbb{Q}, 1) = 0$ implies E has infinitely many rational points.

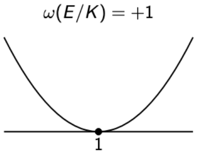
Parity methods

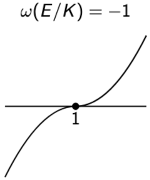
Birch–Swinnerton-Dyer

$\mathrm{rk}\, E/\mathbb{Q} = \mathrm{ord}_{s=1} L(E/\mathbb{Q}, s)$.

Functional equation

$L^*(E/\mathbb{Q}, 2-s) = w(E/\mathbb{Q}) \cdot L^*(E/\mathbb{Q}, s)$.





Parity Conjecture

$$(-1)^{\mathrm{rk}\, E/\mathbb{Q}} = w(E/\mathbb{Q}), \quad w(E/\mathbb{Q}) = \pm 1.$$

Definition (Global root number)

For $E/\mathbb{Q}$, the *global root number* is given by

$$w(E/\mathbb{Q}) = -\prod_{p \mid \Delta} w(E/\mathbb{Q}_p),$$

where $w(E/\mathbb{Q}_p)$ are *local root numbers.*

Parity phenomena

Example

Let $E/\mathbb{Q}$ be given by

$$E\colon y^2 + y = x^3 - x, \qquad \Delta = 37.$$

E has (non-split) multiplicative reduction at $p = 37$. One computes that $w(E/\mathbb{Q}) = -w(E/\mathbb{Q}_{37}) = -1$, and so $\operatorname{rk} E/\mathbb{Q}$ is odd and in particular > 0.

Example

Consider

$$E\colon y^2 + y = x^3 + x^2 + x, \qquad \Delta = -19.$$

This has (split) multiplicative reduction at $p = 19$. The Parity Conjecture predicts that E has positive rank over $\mathbb{Q}(\sqrt[3]{m})$ for all $m > 1$ non-cubes.

Example

Let $K = \mathbb{Q}(\sqrt{-1}, \sqrt{17})$. The Parity Conjecture predicts that every rational elliptic curve $E/\mathbb{Q}$ has even rank when viewed over K.

Example (Congruent number problem)

For $E_n : y^2 = x^3 - n^2 x, \quad w(E_n/\mathbb{Q}) = \begin{cases} +1 & n \equiv 1, 2, 3 \mod 8, \\ -1 & n \equiv 5, 6, 7 \mod 8. \end{cases}$

An alternative method of predicting positive rank

Norm Relations Test

Step 1: Setup

Let $F/\mathbb{Q}$ be a Galois extension with Galois group $G = \mathrm{Gal}(F/\mathbb{Q})$.

Step 2: Find a Relation

Find a $\mathbb{Q}(\sqrt{d})$-relation of permutation representations of G for $d \in \mathbb{Z} \backslash \mathbb{Z}^2$.

Step 3: Compute Local Invariants

Given a (semistable) elliptic curve $E/\mathbb{Q}$, compute local invariants known as **Tamagawa numbers** for E/L across fields

$$\mathbb{Q} \subseteq L \subseteq F.$$

Step 4: Test

Form the product of the relevant Tamagawa numbers determined by the relation in Step 2. If this product is **not** of the form

$$x^2 - dy^2 \quad \text{for } x, y \in \mathbb{Q},$$

then $\mathrm{rk}\, E/F > 0$.

A failure of the norm relation signals a growth in rank in the extension $F/\mathbb{Q}$, i.e. that

$$\mathrm{rk}\, E/F > \mathrm{rk}\, E/\mathbb{Q}.$$

Comments and comparison

- Can this unconditionally show that a family of curves has positive rank? No. Actually it relies on many more conjectures than the parity-based methods.
- Similarly to computing root numbers, it involves computing straight-forward local data for the curve.
- Originally, I looked into whether there was an example where this 'Norm relations test' would predict positive rank in the case where 'Parity-based methods' could not.

In the end, this is not the case:

Theorem (A. 2025)

Let $F/\mathbb{Q}$ be a finite Galois extension with $G = \mathrm{Gal}(F/\mathbb{Q})$, and $E/\mathbb{Q}$ an elliptic curve. If the norm relations test predicts $\mathrm{rk}\, E/F > 0$, then $w(E, \chi) = -1$ for some irreducible representation χ of G.

In other words, parity-based methods already predicted that $\mathrm{rk}\, E/F > 0$.

Thank you for your attention!

Norm relations test

Example

Let $F/\mathbb{Q}$ be a finite Galois extension with $G = \mathrm{Gal}(F/\mathbb{Q}) = D_{21}$. For $K = \mathbb{Q}(\sqrt{21})$, have

$$\mathbb{C}[G/C_2] \ominus \mathbb{C}[G/D_7] \ominus \mathbb{C}[G/S_3] \oplus \mathbb{C}[G/G] \simeq \rho \oplus \rho^\sigma$$

for a representation ρ of G with $\mathbb{Q}(\rho) = K$ and $\langle\sigma\rangle = \mathrm{Gal}(K/\mathbb{Q})$.
Let $E/\mathbb{Q}$ be a semistable elliptic curve $\rightsquigarrow$ look at

$$\frac{C_{E/F^{C_2}} \cdot C_{E/\mathbb{Q}}}{C_{E/F^{D_7}} \cdot C_{E/F^{S_3}}} \mod N_{K/\mathbb{Q}}(K^\times).$$

e.g. If $E/\mathbb{Q}$ has split multiplicative reduction at a prime p with residue degree 2 and ramification degree 3, and good reduction at all other ramified primes in F, then

$$\frac{C_{E/F^{C_2}} \cdot C_{E/\mathbb{Q}}}{C_{E/F^{D_7}} \cdot C_{E/F^{S_3}}} \equiv 3 \mod N_{K/\mathbb{Q}}(K^\times)$$

$\implies \mathrm{rk}\, E/F > 0.$