Local-global methods for elliptic curves

Holly Green

University of Bristol

May 27th, 2026

Overview

1. Elliptic curves
2. The Birch and Swinnerton-Dyer conjecture
3. Using 'local' information to control 'global' data

Global: $\mathbb{Q}$
Hard

Local: $\mathbb{R}$, $\mathbb{F}_p$
Accessible

4. Results

Solving polynomial equations

Goal: Describe the rational solutions to $f(x, y) = 0$.

$y - 2x + 1 = 0$	$x = t,\ y = 2t - 1$ for $t \in \mathbb{Q}$	very easy
$x^2 + y^2 - 1 = 0$	$x = \frac{2t}{1+t^2},\ y = \frac{1-t^2}{1+t^2}$ for $t \in \mathbb{Q}$	easy
$x^2 + y^2 - 3 = 0$	no rational solutions	easy
$x^3 - y^2 - x + 1 = 0$	$x = 0, y = \pm 1, \quad x = 1, y = \pm 1, \quad ???$	hard!

Quadratics satisfy the Hasse principle:

Theorem (Hasse–Minkowski, 1920s)

Let f be a homogeneous quadratic equation. Then,

$$f \text{ has a } \mathbb{Q} \text{ solution} \iff f \text{ has an } \mathbb{R} \text{ solution and } f \bmod p^k \text{ has a solution for all primes } p \text{ and all } k \geq 1.$$

Cubics don't satisfy the Hasse principle ☹, but not all is lost!

Elliptic curves

Fix a cubic $f(x) \in \mathbb{Q}[x]$ with $\mathrm{Disc}(f) \neq 0$. Consider

$$E : y^2 = f(x).$$

An **elliptic curve** is the graph of such an equation.

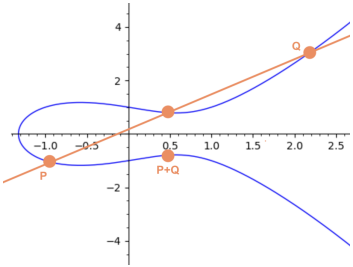
Solutions to the equation $\rightsquigarrow$ points on the curve.

Theorem (Mordell, 1922)

$E(\mathbb{Q})$ is a finitely generated abelian group, i.e.,

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\mathrm{tors}} \oplus \mathbb{Z}^{r_E}$$

for some finite group $E(\mathbb{Q})_{\mathrm{tors}}$ and $r_E \in \mathbb{N}$.



$E : y^2 = x^3 - x + 1$

Have $E(\mathbb{Q})_{\mathrm{tors}} = 1$, $r_E = 1$.

In particular, $E(\mathbb{Q}) = \mathbb{Z} \cdot (1, 1)$.

$E(\mathbb{Q})_{\mathrm{tors}}$ is well studied:

Theorem (Mazur, 1977)

There are 15 possibilities for $E(\mathbb{Q})_{\mathrm{tors}}$.

Much less is known about r_E...

- Is r_E bounded/unbounded?
- An algorithm to compute r_E for all curves?

Relating $E(\mathbb{Q})$ to $E(\mathbb{F}_p)$

Key question: What information does $E(\mathbb{F}_p)$ give us about $E(\mathbb{Q})$?

- A naïve counting argument gives:

$$\#E(\mathbb{F}_p) \approx p + 1.$$

- Hasse (1933) proved:

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

- Birch and Swinnerton-Dyer (1960s) observed:

There's a constant C_E such that:

$$\prod_{p \leq X} \frac{\#E(\mathbb{F}_p)}{p} \sim C_E \log(X)^{r_E} \text{ as } X \to \infty.$$

Definition (L-function attached to E)

$$L(E,s) \text{ “=” } \prod_p \frac{1}{1 + a_p p^{-s} + p^{1-2s}}$$

is a complex analytic function defined when $\mathrm{Re}(s) > \frac{3}{2}$.

Note that,

$$L(E,1) \text{ “=” } \prod_p \frac{p}{\#E(\mathbb{F}_p)}.$$

The Birch and Swinnerton-Dyer conjecture

Let E be an elliptic curve. Then $E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^{r_E}$.

Conjecture (Birch–Swinnerton-Dyer I)

0. $L(E,s)$ has an analytic continuation to $\mathbb{C}$,
1. $r_E = \text{ord}_{s=1} L(E,s)$.

If BSD is true, then there is an algorithm to compute r_E and $E(\mathbb{Q})$!

Current status

0. follows from the modularity theorem (2001),
1. known to hold:
   - when $\text{ord}_{s=1} L(E,s) \leq 1$ (2001),
   - *modulo 2 (2010),
   - for $>66\,\%$ of all elliptic curves (2014).

Conjecture (Birch–Swinnerton-Dyer II)

$L(E,s) = C_E(s-1)^{r_E} +$ *higher order terms* where,

$$C_E = \frac{\text{Reg}_E \cdot \#Ш_E \cdot \Omega_E \cdot \prod_p c_{p,E}}{\#E(\mathbb{Q})^2_{\text{tors}}}.$$

Current status:
- Some progress when $\text{ord}_{s=1} L(E,s) \leq 1$.
- When $\text{ord}_{s=1} L(E,s) > 1$, don't even know that $\#Ш_E < \infty$...

The Birch and Swinnerton-Dyer invariants

Conjecture (Birch–Swinnerton-Dyer II)

Let E be an elliptic curve. Then $L(E,s) = C_E(s-1)^{r_E} +$ *higher order terms* where,

$$C_E = \frac{\mathrm{Reg}_E \cdot \#Ш_E \cdot \Omega_E \cdot \prod_p c_{p,E}}{\#E(\mathbb{Q})^2_{\mathrm{tors}}}.$$

Regulator

Write $E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z} \cdot P_1 \oplus \cdots \oplus \mathbb{Z} \cdot P_{r_E}$, then

$$\mathrm{Reg}_E = \det(\langle P_i, P_j \rangle) \in \mathbb{R}$$

is the squared covolume of the lattice.

Tate–Shafarevich group

$Ш_E$ measures the how badly E fails the Hasse principle.

It's only conjectured that $Ш_E$ is finite!
If $Ш_E$ is finite, it has $\square$ order (Cassels).

Real period

$E(\mathbb{C}) \cong$  $\cong \mathbb{C}/\Lambda.$

$$\Omega_E = \mathrm{covol}(\Lambda \cap \mathbb{R}) \times \#\mathrm{Comp}\,(E(\mathbb{R})) \in \mathbb{R}$$

measures the 'length' of E over $\mathbb{R}$.

Tamagawa number at p

$c_{p,E} \in \mathbb{N}$ records how 'bad' E looks modulo p.

- $y^2 = (x-r_1)(x-r_2)(x-r_3) \rightsquigarrow$ good, $c_{p,E} = 1$
- $y^2 = (x-r_1)^2(x-r_2) \rightsquigarrow$ bad
- $y^2 = (x-r_1)^3 \rightsquigarrow$ very bad.

Computing the parity of the rank

An isogeny between elliptic curves is a map preserving their algebraic structure.
Let $\phi : E_1 \to E_2$ be an isogeny and let $d = \#\ker(\phi)$.

Theorem (Cassels, 1965)

Assume that $\#Ш_{E_1}$ is finite. Then,

$$C_{E_1} = C_{E_2}.$$

Lemma

$$\frac{\mathrm{Reg}_{E_1}}{\mathrm{Reg}_{E_2}} = \square \cdot d^{r_{E_1}}$$

$$\implies \quad \square \cdot d^{r_{E_1}} = \frac{\mathrm{Reg}_{E_1}}{\mathrm{Reg}_{E_2}} = \square \cdot \underbrace{\frac{\Omega_{E_2}}{\Omega_{E_1}}}_{\mathbb{R}} \cdot \prod_p \underbrace{\frac{c_{p,E_2}}{c_{p,E_1}}}_{\mathbb{F}_p}$$

Theorem (Birch–Cassels)

Assume that $\#Ш_{E_1}$ is finite and that d is prime. Then,

$$r_{E_1} \equiv \mathrm{ord}_d\left(\frac{\Omega_{E_2}}{\Omega_{E_1}}\right) + \sum_{p \text{ prime}} \mathrm{ord}_d\left(\frac{c_{p,E_2}}{c_{p,E_1}}\right) \mod 2.$$

This is a 'local' recipe for the parity of r_{E_1}!

r_{E_1} odd $\implies r_{E_1} \neq 0$
$\implies E_1(\mathbb{Q})$ is infinite!

Computing the parity of the rank

There's an isogeny $\phi : E_1 \to E_2$ with $\#\ker(\phi) = 2$ when:

$$E_1 : y^2 = \overbrace{x^3 - x^2 - 13x + 22}^{f_1(x)},$$
$$E_2 : y^2 = \underbrace{x^3 - x^2 + 12x + 72}_{f_2(x)}.$$

Theorem (Birch–Cassels)

Assuming $\#Ш_{E_1}$ *is finite,*

$$r_{E_1} \equiv \operatorname{ord}_2\left(\frac{\Omega_{E_2}}{\Omega_{E_1}}\right) + \sum_{p \text{ prime}} \operatorname{ord}_2\left(\frac{c_{p,E_2}}{c_{p,E_1}}\right) \mod 2.$$

$$r_{E_1} \equiv \operatorname{ord}_2\left(\frac{1.9034\ldots}{3.8069\ldots}\right) + \sum_{p \neq 2,3,5} \operatorname{ord}_2\left(\frac{1}{1}\right) + \underbrace{\operatorname{ord}_2\left(\frac{5}{5}\right)}_{p=2} + \underbrace{\operatorname{ord}_2\left(\frac{2}{2}\right)}_{p=3} + \underbrace{\operatorname{ord}_2\left(\frac{2}{2}\right)}_{p=5} = -1$$

p	$f_1(x) \bmod p$	$f_2(x) \bmod p$
$p \neq 2, 3, 5$	distinct roots	distinct roots
$p = 3$	$(x-1)^2(x-2)$	$x^2(x-1)$
$p = 5$	$(x-2)^3$	$(x-2)^3$

r_{E_1} odd $\implies$ $r_{E_1} \neq 0$

$\implies$ $E_1(\mathbb{Q})$ is infinite!

Generalising all of this

Tate later generalised the statement of the Birch and Swinnerton–Dyer conjecture:

$$\text{Elliptic curves} \rightsquigarrow \text{Abelian varieties}$$
$$\mathbb{Q} \rightsquigarrow \text{Number fields}$$

In this setting, much less is known.

- No longer know that the L-function is defined at $s = 1$.
- Have significantly less numerical evidence.
- $\#Ш$ not known to be finite, and we have examples where it is not a square.

Results (assuming $\#Ш$ is finite).
Joint with E. Aylward, V. Dokchitser, A. Konstantinou, A. Morgan

Theorem

The parity of the rank of the Jacobian of a curve can be described explicitly in terms of local data.

Theorem

BSD I holds modulo 2 for:

- *elliptic curves,*
- *Jacobians of hyperelliptic curves*.*

Thank you for your attention!