Parity of ranks of elliptic curves

Holly Green

University College London

March 2nd, 2022

Main results

Theorem (G., Maistret)

Let K be a number field. Let E_1, E_2 be elliptic curves over K such that $E_1[2] \cong E_2[2]$ as Galois modules. Assuming finiteness of Ш, the Birch and Swinnerton-Dyer conjecture correctly predicts the parity of the rank of E_1 iff it correctly predicts the parity of the rank of E_2.

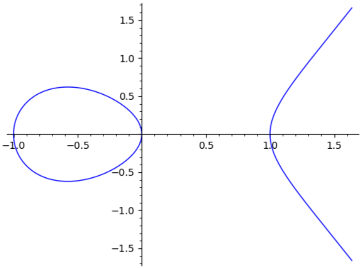
In particular, BSD correctly predicts the parity of the rank of $E_1 \times E_2$.

Theorem

Let p be a prime. Let K be a totally real field. The p-Parity Conjecture holds for all elliptic curves over K.

Elliptic curves

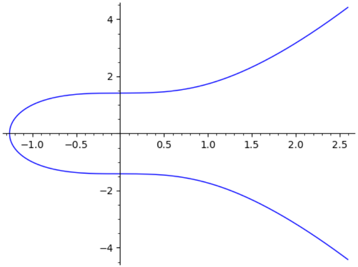
$$y^2 = x^3 - x$$



$\mathbb{Q}$-points: $(0,0)$, $(\pm 1, 0)$, ∞.

This is all of them.

$$y^2 = x^3 + 2$$



$\mathbb{Q}$-points: $(-1, \pm 1)$, ∞.

There are infinitely many of them.

Ranks of elliptic curves

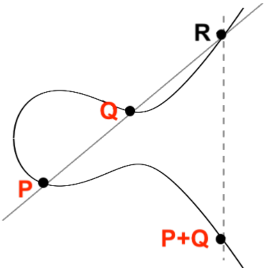
Let $E/\mathbb{Q}$ be an elliptic curve. The $\mathbb{Q}$-points on E form an abelian group.

Theorem (Mordell–Weil)

There is some $r \in \mathbb{N}$ and a finite group T such that $E(\mathbb{Q}) \cong \mathbb{Z}^r \times T$.

- $E : y^2 = x^3 - x, \qquad E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
- $E : y^2 = x^3 + 2, \qquad E(\mathbb{Q}) \cong \langle(-1, 1)\rangle \cong \mathbb{Z}$

Notation: write $\mathrm{rank}(E) := r$ and $E(\mathbb{Q})_{\mathrm{tors}} := T$.



Conjecture (Birch and Swinnerton-Dyer I)

Assuming $L(E, s)$ has an analytic continuation to $\mathbb{C}$, $\mathrm{rank}(E) = \mathrm{ord}_{s=1} L(E, s)$.

The Parity Conjecture

Let $E/\mathbb{Q}$ be an elliptic curve.

Conjecture

The completed L-function $L^*(E,s)$ satisfies

$$L^*(E,s) = w(E)L^*(E,2-s), \quad w(E) \in \{\pm 1\}.$$

Consequently,

$$(-1)^{\mathrm{ord}_{s=1} L(E,s)} = w(E) := w_\infty(E) \cdot \prod_p w_p(E).$$

Conjecture (Birch and Swinnerton-Dyer I)

Assuming $L(E,s)$ has an analytic continuation to $\mathbb{C}$, $\mathrm{rank}(E) = \mathrm{ord}_{s=1} L(E,s)$.

Conjecture (The Parity Conjecture)

$$(-1)^{\mathrm{rank}(E)} = w(E) := w_\infty(E) \cdot \prod_p w_p(E).$$

Example

Conjecture (The Parity Conjecture)

$$(-1)^{\mathrm{rank}(E)} = w(E) := w_\infty(E) \cdot \prod_p w_p(E).$$

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

$$w_\infty(E) = -1, \quad w_p(E) = \begin{cases} +1 & \bar{f}(x) \text{ has no repeated roots } (p \text{ odd}) \\ -1 & \bar{f}(x) = (x-\alpha)^2(x-\beta) \text{ and } \bar{\alpha} - \bar{\beta} = \square \ (p \text{ odd}) \\ +1 & \bar{f}(x) = (x-\alpha)^2(x-\beta) \text{ and } \bar{\alpha} - \bar{\beta} \neq \square \ (p \text{ odd}) \\ \ldots \end{cases}$$

Let $f(x) = x^3 + 4x^2 - 80x + 400$, $\Delta_f = -2^8 \cdot 5^3 \cdot 11 \cdot 13$.

$$w(E) = w_\infty(E) w_2(E) w_5(E) w_{11}(E) w_{13}(E) = (-1)(+1)(-1)(+1)(-1) = -1.$$

PC says that E has **odd** rank $\Rightarrow$ E has infinitely many rational points.

Current status

Let K be a number field. Let E/K be an elliptic curve.

Conjecture (The Parity Conjecture)

$$(-1)^{\mathrm{rank}(E/K)} = w(E/K) := \prod_v w_v(E/K).$$

Under the assumption that $\#\text{Ш}(E/K)$ is finite, certain cases have been proved:

- $K = \mathbb{Q}$ (Monsky)
- E admits an ℓ-isogeny (Dokchitser–Dokchitser, Česnavičius)
- K is a totally real field (Dokchitser–Dokchitser, Nekovář)
- true for $y^2 = f(x)$ iff true for $y^2 = df(x)$, for $d \in K^\times$ (Kramer–Tunnell)
- true for E_1 iff true for E_2, when $E_1, E_2/K$ and $E_1[2] \cong E_2[2]$ (G., Maistret)

Strategy: proving Parity Conjecture for $E_1[2] \cong E_2[2]$

Theorem (G., Maistret)

Let E_1, E_2 be elliptic curves over $\mathbb{Q}$ such that $E_1[2] \cong E_2[2]$ as Galois modules. Assuming finiteness of Ш, the Parity Conjecture holds for E_1 iff it holds for E_2.

- Reword the assumption on the 2-torsion
- Exhibit an isogeny
- Compute the parity of the rank
- Write this as a product of local terms, then compare to local root numbers

The 2-torsion assumption

Let $E_1, E_2/\mathbb{Q}$ have $E_1[2] \cong E_2[2]$ as Galois-modules.

E.g. $E_1 : y^2 = x^3 - 2$ and $E_2 : y^2 = x^3 - 4$, both cubics have s.f. $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$.

Lemma

There exists $f(x) = x^3 + ax^2 + bx + c$, separable, with $c \neq 0$, such that $E_1 \cong E : y^2 = f(x)$ and E_2 is a quadratic twist of

$$E' : y^2 = x^3 + bx^2 + acx + c^2.$$

Our goal follows from:

Theorem

Let $f(x), E, E'$ be as above. Assuming finiteness of Ш, the Parity Conjecture holds for E iff it holds for E'.

$$(-1)^{\mathrm{rank}(E)+\mathrm{rank}(E')} = w(E)w(E').$$

Strategy: proving Parity Conjecture for $E_1[2] \cong E_2[2]$

Theorem (G., Maistret)

Let E_1, E_2 be elliptic curves over $\mathbb{Q}$ such that $E_1[2] \cong E_2[2]$ as Galois modules. Assuming finiteness of Ш, the Parity Conjecture holds for E_1 iff it holds for E_2.

- Reword the assumption on the 2-torsion
  - It is enough to show that PC holds for E iff E'
- Exhibit an isogeny
- Compute the parity of the rank
- Write this as a product of local terms, then compare to local root numbers

Exhibiting an isogeny

Let $f(x) = x^3 + ax^2 + bx + c$ $(c \neq 0)$. Define

$$E : y^2 = f(x), \qquad E' : y^2 = x^3 + bx^2 + acx + c^2.$$

Define a *genus 2* curve

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

We associate to C an *abelian variety* $\mathrm{Jac}\, C$.

Lemma

There's a $(2,2)$*-isogeny*

$$\phi : E \times E' \to \mathrm{Jac}\, C.$$

Strategy: proving Parity Conjecture for $E_1[2] \cong E_2[2]$

Theorem (G., Maistret)

Let E_1, E_2 be elliptic curves over $\mathbb{Q}$ such that $E_1[2] \cong E_2[2]$ as Galois modules. Assuming finiteness of Ш, the Parity Conjecture holds for E_1 iff it holds for E_2.

- Reword the assumption on the 2-torsion
  - It is enough to show that PC holds for E iff E'
- Exhibit an isogeny
  - There's a $(2, 2)$-isogeny $\phi : E \times E' \to \mathrm{Jac}\, C$
- Compute the parity of the rank
- Write this as a product of local terms, then compare to local root numbers

Computing the parity of the rank

Conjecture (Birch and Swinnerton-Dyer II)

$$\lim_{s=1}\frac{L(E,s)}{(s-1)^r}=\frac{\#\text{Ш}(E)\cdot\Omega(E)\cdot\mathrm{Reg}(E)\cdot\prod_p c_p(E)}{\#E(\mathbb{Q})^2_{\mathrm{tors}}}=:\mathrm{BSD}(E)$$

- (Cassels–Tate) $\mathrm{BSD}(E\times E')=\mathrm{BSD}(\mathrm{Jac}\,C)$

$$\frac{\mathrm{Reg}(E)\cdot\mathrm{Reg}(E')}{\mathrm{Reg}(\mathrm{Jac}\,C)}=\frac{\#\text{Ш}(\mathrm{Jac}\,C)\cdot\Omega(\mathrm{Jac}\,C)\cdot\prod_p c_p(\mathrm{Jac}\,C)}{\Omega(E)\cdot\Omega(E')\cdot\prod_p c_p(E)c_p(E')}\cdot\square_{\mathbb{Q}}$$

- LHS $=2^{\mathrm{rank}(E)+\mathrm{rank}(E')}\cdot\square_{\mathbb{Q}}$
- (Poonen–Stoll) $\#\text{Ш}(\mathrm{Jac}\,C)=d_\infty(C)\cdot\prod_p d_p(C)\cdot\square_{\mathbb{Q}}$

$$2^{\mathrm{rank}(E)+\mathrm{rank}(E')}=\frac{\Omega(\mathrm{Jac}\,C)d_\infty(C)}{\Omega(E)\Omega(E')}\cdot\prod_p\frac{c_p(\mathrm{Jac}\,C)d_p(C)}{c_p(E)c_p(E')}\cdot\square_{\mathbb{Q}}$$

Example

$$2^{\mathrm{rank}(E)+\mathrm{rank}(E')} = \frac{\Omega(\mathrm{Jac}\, C) d_\infty(C)}{\Omega(E)\Omega(E')} \cdot \prod_p \frac{c_p(\mathrm{Jac}\, C) d_p(C)}{c_p(E) c_p(E')} \cdot \square_{\mathbb{Q}}$$

Let $f(x) = x^3 - 2x + 1$. Then

$$E : y^2 = f(x), \qquad E' : y^2 = x^3 - 2x^2 + 1, \qquad C : y^2 = f(x^2)$$

(these are 40.a3, 20.a3, 800.a.409600.1). The local data is:

$$\begin{array}{llll} \Omega(\mathrm{Jac}\, C) = 16.77\ldots & d_\infty(C) = 1 & \Omega(E) = 5.93\ldots & \Omega(E') = 5.65\ldots \\ c_2(\mathrm{Jac}\, C) = 12 & d_2(C) = 1 & c_2(E) = 2 & c_2(E') = 3 \\ c_5(\mathrm{Jac}\, C) = 1 & d_5(C) = 1 & c_5(E) = 1 & c_5(E') = 1 \end{array}$$

Therefore, $2^{\mathrm{rank}(E)+\mathrm{rank}(E')} = (\frac{1}{2}) \cdot (2) \cdot (1) \cdot \square_{\mathbb{Q}} \Rightarrow \mathrm{rank}(E) \equiv \mathrm{rank}(E') \bmod 2.$

Strategy: proving Parity Conjecture for $E_1[2] \cong E_2[2]$

Theorem (G., Maistret)

Let E_1, E_2 be elliptic curves over $\mathbb{Q}$ such that $E_1[2] \cong E_2[2]$ as Galois modules. Assuming finiteness of Ш, the Parity Conjecture holds for E_1 iff it holds for E_2.

- Reword the assumption on the 2-torsion
  - It is enough to show that PC holds for E iff E'
- Exhibit an isogeny
  - There's a $(2, 2)$-isogeny $\phi : E \times E' \to \mathrm{Jac}\, C$
- Compute the parity of the rank
  - Cassels + regulator result + Poonen–Stoll
- Write this as a product of local terms, then compare to local root numbers

Comparison to the Parity Conjecture

Recall, the Parity Conjecture says that $(-1)^{\text{rank}(E)} = w(E)$. We are aiming to show:

$$(-1)^{\text{rank}(E)+\text{rank}(E')} = w(E)w(E') := w_\infty(E)w_\infty(E') \cdot \prod_p w_p(E)w_p(E').$$

So far

$$2^{\text{rank}(E)+\text{rank}(E')} = \frac{\Omega(\text{Jac } C)d_\infty(C)}{\Omega(E)\Omega(E')} \cdot \prod_p \frac{c_p(\text{Jac } C)d_p(C)}{c_p(E)c_p(E')} \cdot \square_{\mathbb{Q}}$$

Theorem (G., Maistret)

$$(-1)^{\text{rank}(E)+\text{rank}(E')} = \lambda_\infty \cdot \prod_p \lambda_p \qquad \begin{cases} \lambda_\infty = (-1)^{\text{ord}_2\left(\frac{\Omega(\text{Jac } C)d_\infty(C)}{\Omega(E)\Omega(E')}\right)} \\ \lambda_p = (-1)^{\text{ord}_2\left(\frac{c_p(\text{Jac } C)d_p(C)}{c_p(E)c_p(E')}\right)} \end{cases}$$

Does $\lambda_\infty = w_\infty(E)w_\infty(E')$ and $\lambda_p = w_p(E)w_p(E')$?

Example

Theorem (G., Maistret)

$$(-1)^{\mathrm{rank}(E)+\mathrm{rank}(E')} = \lambda_\infty \cdot \prod_p \lambda_p \qquad \begin{cases} \lambda_\infty = (-1)^{\mathrm{ord}_2\left(\frac{\Omega(\mathrm{Jac}\ C)d_\infty(C)}{\Omega(E)\Omega(E')}\right)} \\ \lambda_p = (-1)^{\mathrm{ord}_2\left(\frac{c_p(\mathrm{Jac}\ C)d_p(C)}{c_p(E)c_p(E')}\right)} \end{cases}$$

Does $\lambda_\infty = w_\infty(E)w_\infty(E')$ and $\lambda_p = w_p(E)w_p(E')$? No!

Let $f(x) = x^3 - 2x + 1$.

- $\frac{\Omega(\mathrm{Jac}\ C)d_\infty(C)}{\Omega(E)\Omega(E')} = \frac{1}{2} \Rightarrow \lambda_\infty = -1;\ w_\infty(E)w_\infty(E') = +1$ (not a match)
- $\frac{c_2(\mathrm{Jac}\ C)d_2(C)}{c_2(E)c_2(E')} = 2 \Rightarrow \lambda_2 = -1;\ w_2(E)w_2(E') = -1$ (match)
- $\frac{c_5(\mathrm{Jac}\ C)d_5(C)}{c_5(E)c_5(E')} = 1 \Rightarrow \lambda_5 = 1;\ w_5(E)w_5(E') = -1$ (not a match)

Proving the Parity Conjecture holds for E iff it holds for E'

Recall, $f(x) = x^3 + ax^2 + bx + c$ is separable with $c \neq 0$.

Theorem (G., Maistret)

Let $H_v := (b, -c)_{\mathbb{Q}_v}(-2L, \Delta_f)_{\mathbb{Q}_v}(L, -b)_{\mathbb{Q}_v}$ *where* $L := ab - 9c$ $(v = \infty$ *or* $p)$. *Then*

$$\lambda_\infty = H_\infty \cdot w_\infty(E)w_\infty(E'), \qquad \lambda_p = H_p \cdot w_p(E)w_p(E').$$

In particular $H_\infty \cdot \prod_p H_p = +1$.

Corollary (Parity Conjecture for E iff E')

$$(-1)^{\mathrm{rank}(E)+\mathrm{rank}(E')} = w(E)w(E')$$

Proof.

$$(-1)^{\mathrm{rank}(E)+\mathrm{rank}(E')} = \lambda_\infty \cdot \prod_p \lambda_p = \left(H_\infty \cdot \prod_p H_p\right)\left(w_\infty(E)w_\infty(E') \cdot \prod_p w_p(E)w_p(E')\right).$$

Strategy: proving Parity Conjecture for $E_1[2] \cong E_2[2]$

Theorem (G., Maistret)

Let E_1, E_2 be elliptic curves over $\mathbb{Q}$ such that $E_1[2] \cong E_2[2]$ as Galois modules. Assuming finiteness of Ш, the Parity Conjecture holds for E_1 iff it holds for E_2.

- Reword the assumption on the 2-torsion
  - It is enough to show that PC holds for E iff E'
- Exhibit an isogeny
  - There's a $(2,2)$-isogeny $\phi : E \times E' \to \mathrm{Jac}\, C$
- Compute the parity of the rank
  - Cassels + regulator result + Poonen–Stoll
- Write this as a product of local terms, then compare to local root numbers
  - $(-1)^{\mathrm{rank}(E)+\mathrm{rank}(E')} = \lambda_\infty \cdot \prod_p \lambda_p$
  - $\lambda_v = H_v \cdot w_v(E) w_v(E')$, and consequently $(-1)^{\mathrm{rank}(E)+\mathrm{rank}(E')} = w(E)w(E')$

The p-Parity Conjecture

Conjecture (The p-Parity Conjecture)

$$(-1)^{\mathrm{rank}_p(E/K)} = w(E/K).$$

Theorem (G., Maistret)

Let K be a number field and $E_1, E_2/K$ elliptic curves with $E_1[2] \cong E_2[2]$. The 2-Parity Conjecture holds for E_1 iff it holds for E_2.

Let K be a totally real number field. The p-Parity Conjecture is known for E/K when p is odd, or $p = 2$ and E does not have complex multiplication.

Theorem (G., Maistret)

Let K be a totally real field and E/K a CM elliptic curve. The 2-Parity Conjecture holds for E.

Theorem

Let K be a totally real field and E/K an elliptic curve. The p-Parity Conjecture holds for E.

Thank you for your attention!