# On the parity conjecture for elliptic curves

Holly Green

University of Bristol

January 16th, 2024

# Main results

**Theorem (Dokchitser–G.–Konstantinou–Morgan)**

*Assuming Ш is finite, the Birch and Swinnerton-Dyer conjecture correctly predicts the parity of the rank of elliptic curves.*

**Theorem (Dokchitser–G.–Konstantinou–Morgan)**

*Assuming Ш is finite, then for all smooth, projective curves over number fields $X/K$*

$$\mathrm{rank}(\mathrm{Jac}_X) \equiv \sum_{v \text{ place of } K} \Lambda_v(X) \mod 2$$

*where $\Lambda_v \in \mathbb{Z}$ is an explicit invariant computed from curves over local fields.*

Will assume Ш is finite throughout.

# The Birch and Swinnerton-Dyer and parity conjectures

Let $E$ be an elliptic curve over a number field $K$.

**Birch–Swinnerton-Dyer conjecture (i)**

$$\mathrm{rank}(E) = \mathrm{ord}_{s=1} L(E,s)$$

$+$

**Conjectural functional equation**

$$L^*(E,s) = w(E) L^*(E, 2-s)$$

$\Downarrow$

**The parity conjecture**

$$(-1)^{\mathrm{rank}(E)} = w(E) := \prod_{v \text{ place of } K} w_v(E)$$

When $v \mid \infty$, $w_v(E) = -1$. Otherwise,

$$w_v(E) = \begin{cases} +1 & E/K_v \text{ has good reduction,} \\ -1 & E/K_v \text{ has split multiplicative reduction,} \\ +1 & E/K_v \text{ has non-split multiplicative reduction,} \\ \dots & E/K_v \text{ has additive reduction.} \end{cases}$$

# Parity phenomena

If $E$ is semistable, the parity conjecture predicts that

$$(-1)^{\mathrm{rank}(E)} = (-1)^{\#\{v|\infty\} \ + \ \#\{v\nmid\infty,\ E/K_v \text{ split multiplicative}\}}.$$

$E/\mathbb{Q} : y^2 = x^3 - \frac{1}{3}x + \frac{35}{108}$, $\Delta_E = -43$. $E$ has non-split multiplicative reduction at 43

$$\Rightarrow \ \mathrm{rank}(E) \text{ is odd } \ \Rightarrow \ E \text{ has a } \mathbb{Q}\text{-point of infinite order.}$$

If $E/\mathbb{Q}$ is semistable with split multiplicative reduction at 2 then $\mathrm{rank}(E/\mathbb{Q}(\zeta_8))$ is odd.

If $K$ is imaginary quadratic and $E/K$ has everywhere good reduction then $\mathrm{rank}(E/K)$ is odd.
If $L/K$ has even degree then $\mathrm{rank}(E/L)$ is even and

$$\mathrm{rank}(E/K) < \mathrm{rank}(E/L).$$

# Strategy

## Goal 1

Develop an arithmetic analogue of the parity conjecture:

$$(-1)^{\mathrm{rank}(E)} = \prod_v (-1)^{\Lambda_v(E)}.$$

E.g., (Cassels) if $E \to E'$ is an isogeny of degree $d$, then $\Lambda_v(E) = \mathrm{ord}_d(c_v(E)/c_v(E'))$.

## Goal 2

Prove the parity conjecture:

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

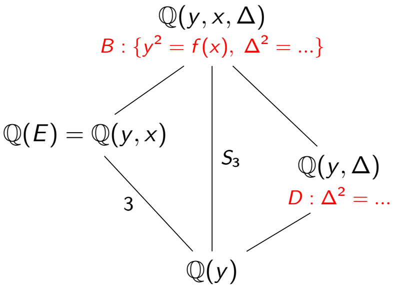
Relate $\Lambda_v(E)$ to $w_v(E)$, i.e. find $H_v \in \{\pm 1\}$ satisfying

$$(-1)^{\Lambda_v(E)} = H_v w_v(E) \qquad \text{and} \qquad \prod_v H_v = +1.$$

**New idea:** Use the arithmetic of covers of curves.

# Taking covers of curves

Let $E/\mathbb{Q} : y^2 = f(x) := x^3 + ax + b$ be an elliptic curve, $a \neq 0$.




$$D : \Delta^2 = \mathrm{Disc}_x(f(x) - y^2)$$
$$= -27y^4 + 54by^2 - (4a^3 + 27b^2).$$

**Theorem**

*Let $Y/\mathbb{Q}$ be curve and $G \leq \mathrm{Aut}_{\mathbb{Q}}(Y)$ finite.*

- $\mathbb{Q}(Y)^G = \mathbb{Q}(Y/G)$,
- $\Omega^1(Y)^G = \Omega^1(Y/G)$,
- $(\mathrm{Jac}_Y(\mathbb{Q}) \otimes \mathbb{Q})^G = \mathrm{Jac}_{Y/G}(\mathbb{Q}) \otimes \mathbb{Q}$.

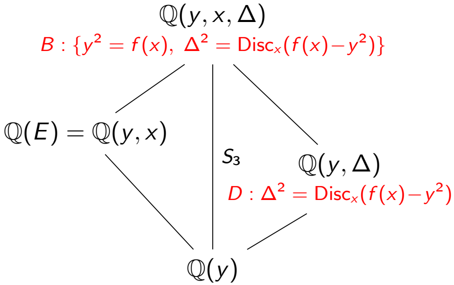
**Example: $B$ has genus 3**

$\Omega^1(B) = \mathbb{1}^{\oplus s} \oplus \epsilon^{\oplus t} \oplus \rho^{\oplus u} \Rightarrow B$ has genus $s + t + 2u$.

$$s = \dim \Omega^1(B)^{S_3} = \dim \Omega^1(\mathbb{P}^1) = 0, \qquad s + t = \dim \Omega^1(B)^{C_3} = \dim \Omega^1(D) = 1,$$
$$s + u = \dim \Omega^1(B)^{C_2} = \dim \Omega^1(E) = 1.$$

# Exhibiting isogenies

Let $E/\mathbb{Q} : y^2 = f(x) := x^3 + ax + b$ be an elliptic curve, $a \neq 0$.




## Theorem (Kani–Rosen)

*Let $Y/\mathbb{Q}$ be a curve and $G \leq \mathrm{Aut}_{\mathbb{Q}}(Y)$ finite. Suppose that $\bigoplus_i \mathbb{C}[G/H_i] \cong \bigoplus_j \mathbb{C}[G/H'_j]$ for some $H_i, H'_j \leq G$. Then there's an isogeny*

$$\prod_i \mathrm{Jac}_{Y/H_i} \longrightarrow \prod_j \mathrm{Jac}_{Y/H'_j}.$$

## Example: there's an isogeny $E \times E \times \mathrm{Jac}_D \to \mathrm{Jac}_B$

$$\mathbb{C}[S_3/1] = \mathbb{1} \oplus \epsilon \oplus \rho^{\oplus 2}, \quad \mathbb{C}[S_3/C_2] = \mathbb{1} \oplus \rho, \quad \mathbb{C}[S_3/C_3] = \mathbb{1} \oplus \epsilon, \quad \mathbb{C}[S_3/S_3] = \mathbb{1}.$$

$\Longrightarrow$ there's an isogeny $\mathrm{Jac}_{B/C_2} \times \mathrm{Jac}_{B/C_2} \times \mathrm{Jac}_{B/C_3} \to \mathrm{Jac}_{B/1} \times \mathrm{Jac}_{B/S_3} \times \mathrm{Jac}_{B/S_3}$.

$$\begin{array}{cccccc} \mathrm{Jac}_{B/C_2} & \mathrm{Jac}_{B/C_2} & \mathrm{Jac}_{B/C_3} & \mathrm{Jac}_{B/1} & \mathrm{Jac}_{B/S_3} & \mathrm{Jac}_{B/S_3} \\ \parallel & \parallel & \parallel & \parallel & \parallel & \parallel \\ E & E & \mathrm{Jac}_D & \mathrm{Jac}_B & 0 & 0 \end{array}$$

# Isogeny invariance of BSD

**Birch–Swinnerton-Dyer conjecture (ii)**

$$\frac{L^{(r_E)}(E,1)}{r_E!} = \mathrm{BSD}_E := \frac{\#\text{Ш}_E \cdot \mathrm{Reg}_E \cdot C_E}{\#E(\mathbb{Q})^2_{\mathrm{tors}}}$$

**Theorem (Cassels–Tate)**

*The BSD coefficient is invariant under isogeny.*

Apply to the isogeny $E \times E \times \mathrm{Jac}_D \to \mathrm{Jac}_B$.

$$\square \cdot 3^{\mathrm{rank}(E)+\mathrm{rank}(\mathrm{Jac}_D)} = \frac{\mathrm{Reg}_{\mathrm{Jac}_B}}{\mathrm{Reg}_E^2\ \mathrm{Reg}_{\mathrm{Jac}_D}} = \frac{\#\mathrm{Jac}_B(\mathbb{Q})^2_{\mathrm{tors}}}{\#E(\mathbb{Q})^4_{\mathrm{tors}}\ \#\mathrm{Jac}_D(\mathbb{Q})^2_{\mathrm{tors}}} \cdot \frac{\#\text{Ш}_E^2\ \#\text{Ш}_{\mathrm{Jac}_D}}{\#\text{Ш}_{\mathrm{Jac}_B}} \cdot \frac{C_E^2\ C_{\mathrm{Jac}_D}}{C_{\mathrm{Jac}_B}} = \square \cdot \frac{C_E^2\ C_{\mathrm{Jac}_D}}{C_{\mathrm{Jac}_B}}$$

**Theorem**

*Assuming that* $\text{Ш}_E[3^\infty]$ *and* $\text{Ш}_{\mathrm{Jac}_D}[3^\infty]$ *are finite,*

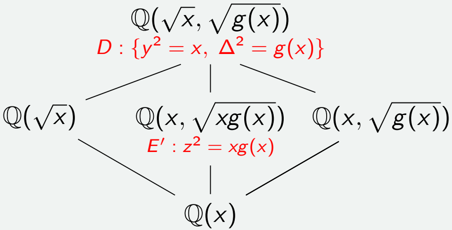
$$\mathrm{rank}(E) + \mathrm{rank}(\mathrm{Jac}_D) \equiv \sum_v \mathrm{ord}_3\left(\frac{c_v(E)^2 c_v(\mathrm{Jac}_D)}{c_v(\mathrm{Jac}_B)}\right) \mod 2.$$

Let $E : y^2 = x^3 - \frac{1}{3}x + \frac{35}{108} \Rightarrow \mathrm{Jac}_D : y^2 = x^3 - \frac{35}{4}x^2 + x$ $\quad (\Delta_E = -43,\ \Delta_{\mathrm{Jac}_D} = 3^3 \cdot 43)$

$v = 3$, $v = 43$, $v = \infty$

$$\mathrm{rank}(E) + \mathrm{rank}(\mathrm{Jac}_D) \equiv \mathrm{ord}_3\left(\frac{1^2 \cdot 3}{3}\right) + \mathrm{ord}_3\left(\frac{1^2 \cdot 1}{1}\right) + \mathrm{ord}_3\left(\frac{5.46\ldots^2 \cdot 2.14\ldots}{21.26\ldots}\right) \equiv 1 \mod 2.$$

# An arithmetic analogue of the parity conjecture

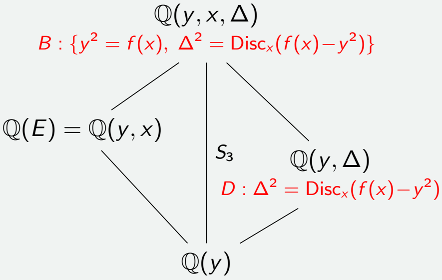



Suppose $g(x)$ is quadratic.

There's an isogeny $\mathrm{Jac}_D \to E' \Rightarrow \mathrm{BSD}_{\mathrm{Jac}_D} = \mathrm{BSD}_{E'}$

$$\Rightarrow \square \cdot 2^{\mathrm{rank}(\mathrm{Jac}_D)} = \frac{\mathrm{Reg}_{E'}}{\mathrm{Reg}_{\mathrm{Jac}_D}} = \square \cdot \frac{C_{\mathrm{Jac}_D}}{C_{E'}}$$

$$\Rightarrow \mathrm{rank}(\mathrm{Jac}_D) \equiv \sum_v \mathrm{ord}_2\left(\frac{c_v(\mathrm{Jac}_D)}{c_v(E')}\right) \mod 2.$$




Let $E/\mathbb{Q} : y^2 = x^3 + ax + b$ be an elliptic curve, $a \neq 0$.

Then

$$D : \Delta^2 = -27y^4 + 54by^2 - (4a^3 + 27b^2)$$
$$= g(y^2)$$

and

$$\mathrm{rank}(E) + \mathrm{rank}(\mathrm{Jac}_D) \equiv \sum_v \mathrm{ord}_3\left(\frac{c_v(E)^2 c_v(\mathrm{Jac}_D)}{c_v(\mathrm{Jac}_B)}\right) \mod 2.$$

# An arithmetic analogue of the parity conjecture

**Theorem (Dokchitser–G.–Konstantinou–Morgan)**

*Assume Ш is finite. Let $X/\mathbb{Q}$ be a smooth, projective curve. There is an explicit invariant $\Lambda \in \mathbb{Z}$ computed from curves over local fields such that*

$$\mathrm{rank}(\mathrm{Jac}_X) \equiv \sum_v \Lambda_v(X) \mod 2.$$

E.g., When $E : y^2 = x^3 + ax + b$,

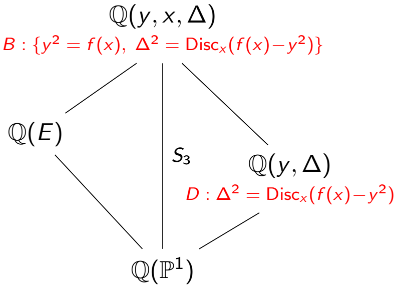
$$\Lambda_v(E) = \mathrm{ord}_3\left(\frac{c_v(E)^2 c_v(\mathrm{Jac}_D)}{c_v(\mathrm{Jac}_B)}\right) + \mathrm{ord}_2\left(\frac{c_v(\mathrm{Jac}_D)}{c_v(E')}\right).$$

**The parity conjecture**

$$(-1)^{\mathrm{rank}(\mathrm{Jac}_X)} = \prod_v w_v(\mathrm{Jac}_X).$$

# Summary

Let $E/\mathbb{Q} : y^2 = f(x) := x^3 + ax + b$ be an elliptic curve, $a \neq 0$.




There's an isogeny $E \times E \times \mathrm{Jac}_D \to \mathrm{Jac}_B$.

**Theorem**

*Assuming* $Ш_E[3^\infty]$, $Ш_{\mathrm{Jac}_D}[3^\infty]$ *are finite,*

$$(-1)^{\mathrm{rank}(E)+\mathrm{rank}(\mathrm{Jac}_D)} = \prod_v (-1)^{\mathrm{ord}_3\left(\frac{c_v(E)^2 c_v(\mathrm{Jac}_D)}{c_v(\mathrm{Jac}_B)}\right)}.$$

**The parity conjecture for $E \times \mathrm{Jac}_D$**

$$(-1)^{\mathrm{rank}(E)+\mathrm{rank}(\mathrm{Jac}_D)} = \prod_v w_v(E) w_v(\mathrm{Jac}_D).$$

**Goal:** Relate $\mathrm{ord}_3\left(\frac{c_v(E)^2 c_v(\mathrm{Jac}_D)}{c_v(\mathrm{Jac}_B)}\right)$ to $w_v(E)w_v(\mathrm{Jac}_D)$.

# Local comparison

E.g., Let $E : y^2 = x^3 - \frac{1}{3}x + \frac{35}{108} \Rightarrow \mathrm{Jac}_D : y^2 = x^3 - \frac{35}{4}x^2 + x \quad (\Delta_E = -43,\ \Delta_{\mathrm{Jac}_D} = 3^3 \cdot 43)$

| $v$ | $\frac{c_v(E)^2 c_v(\mathrm{Jac}_D)}{c_v(\mathrm{Jac}_B)}$ | $(-1)^{\mathrm{ord}_3\left(\frac{c_v(E)^2 c_v(\mathrm{Jac}_D)}{c_v(\mathrm{Jac}_B)}\right)}$ | $w_v(E)$ | $w_v(\mathrm{Jac}_D)$ |
|---|---|---|---|---|
| $3$ | $\frac{1^2 \cdot 3}{3} = 1$ | $+1$ | $-1$ | $+1$ |
| $43$ | $\frac{1^2 \cdot 1}{1} = 1$ | $+1$ | $+1$ | $+1$ |
| $\infty$ | $\frac{5.46\ldots^2 \cdot 2.14\ldots}{21.26\ldots} = 3$ | $-1$ | $-1$ | $-1$ |
| $p \neq 3, 43$ | $1$ | $+1$ | $+1$ | $+1$ |

## Theorem

*Let $v$ be a place of $\mathbb{Q}$. Then,*

$$(-1)^{\mathrm{ord}_3\left(\frac{c_v(E)^2 c_v(\mathrm{Jac}_D)}{c_v(\mathrm{Jac}_B)}\right)} = \begin{cases} -w_v(E) w_v(\mathrm{Jac}_D) & v = 3 \text{ or } \infty, \\ w_v(E) w_v(\mathrm{Jac}_D) & \text{otherwise.} \end{cases}$$

# Proving the parity conjecture for $E$

$$(-1)^{\mathrm{ord}_3\left(\frac{c_v(E)^2 c_v(\mathrm{Jac}_D)}{c_v(\mathrm{Jac}_B)}\right)} = \begin{cases} -w_v(E)w_v(\mathrm{Jac}_D) & v = 3 \text{ or } \infty, \\ w_v(E)w_v(\mathrm{Jac}_D) & \text{otherwise.} \end{cases}$$

## Theorem

*Let $E/\mathbb{Q}$ be an elliptic curve. Assuming $Ш_E[3^\infty]$, $Ш_{\mathrm{Jac}_D}[3^\infty]$, $Ш_{\mathrm{Jac}_D}[2^\infty]$ are finite, the parity conjecture holds for $E$.*

## Proof.

Write $E : y^2 = x^3 + ax + b$ with $a \neq 0$. Then,

$$(-1)^{\mathrm{rank}(E)+\mathrm{rank}(\mathrm{Jac}_D)} = \prod_v (-1)^{\mathrm{ord}_3\left(\frac{c_v(E)^2 c_v(\mathrm{Jac}_D)}{c_v(\mathrm{Jac}_B)}\right)} = (-1)^2 \prod_v w_v(E)w_v(\mathrm{Jac}_D).$$

Additionally,

$$(-1)^{\mathrm{rank}(\mathrm{Jac}_D)} = \prod_v (-1)^{\mathrm{ord}_2\left(\frac{c_v(\mathrm{Jac}_D)}{c_v(E')}\right)} = \prod_v (3a, -3b)_v (6b, 3\Delta_E)_v w_v(\mathrm{Jac}_D) = \prod_v w_v(\mathrm{Jac}_D).$$

□

# Further applications to the parity conjecture

**Theorem (G.–Maistret)**

*The 2-parity conjecture holds for* $\mathrm{Jac}_C$ *where* $C : y^2 = f(x^2)$ *has genus 2.*

**Theorem (Nekovář, Dokchitser$^2$, G.–Maistret)**

*The* $p$*-parity conjecture holds for elliptic curves over totally real fields.*

**Work in progress (Dokchitser–G.–Morgan)**

*Assume* Ш *is finite. The parity conjecture holds for Jacobians of semistable$^*$ hyperelliptic curves.*

*Thank you for your attention!*