Introduction to root numbers and the parity conjecture

Holly Green

University College London

November 15th, 2022

Overview and notation

- Motivation
- What are root numbers?
- Parity phenomena

Notation

- E is an elliptic curve
- K is a number field
- $\mathcal{K}$ is a local field, e.g. $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}_p$ or K_v (v a place of K)

Motivation

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

Birch and Swinnerton-Dyer conjecture

Assuming that $L(E,s)$ has an analytic continuation to $\mathbb{C}$,

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

Conjectural functional equation

Assuming that $L(E,s)$ has an analytic continuation to $\mathbb{C}$,

$$L(E,s) = w(E)L(E,2-s) \times (\text{stuff}), \qquad w(E) \in \{\pm 1\}.$$

The sign in the functional equation is conjectured to be the *global root number*:

Definition (Global root number)

$$w(E/K) = \prod_{v \text{ place of } K} w(E/K_v).$$

Local root numbers

Let $\mathcal{K}$ be a local field (i.e. $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}_p$).

For characters (David)

Let χ be a 1-dimensional continuous ℓ-adic representation over $\mathcal{K}$. The local root number $w(\chi, \psi, dx)$ (w.r.t. ψ and dx) is defined in terms of ϵ-factors:

$$\epsilon(\chi, \psi, dx) = \frac{\chi(\pi_{\mathcal{K}}^{n(\psi)})}{||\pi_{\mathcal{K}}^{n(\psi)}||} \int_{\mathcal{O}_{\mathcal{K}}} dx \qquad \text{and} \qquad w(\chi, \psi, dx) = \frac{\epsilon(\chi, \psi, dx)}{|\epsilon(\chi, \psi, dx)|}.$$

For representations (Jamie)

Let ρ be a finite dimensional representation continuous ℓ-adic representation over $\mathcal{K}$. Extend the definition of ϵ-factors so that various properties are satisfied (multiplicativity, inductivity, ...), then define $w(\rho, \psi, dx)$ as above.

To define the root number of an elliptic curve $E/\mathcal{K}$, need to associate to it a representation.

Local root numbers for abelian varieties

Let $E/\mathcal{K}$ then $E[\ell^n] \cong (\mathbb{Z}/\ell^n\mathbb{Z})^2$. Write $E[\ell] = \langle P_1, Q_1 \rangle$. For $n \geq 2$, find $\langle P_n, Q_n \rangle = E[\ell^n]$ with

$$\ell P_n = P_{n-1}, \qquad \ell Q_n = Q_{n-1}.$$

For $g \in G_\mathcal{K}$, $g(P_n) = (a_1 + ... + a_n \ell^{n-1})P_n + (b_1 + ... + b_n \ell^{n-1})Q_n$ and $g(Q_n) = \dots$

Then $\rho_{E/\mathcal{K}} : G_\mathcal{K} \to \mathrm{GL}_2(\mathbb{Q}_\ell)$ is the ℓ-adic representation of $E/\mathcal{K}$.

For general $A/\mathcal{K}$, $A[\ell^n] \cong (\mathbb{Z}/\ell^n\mathbb{Z})^{2 \dim A}$. Similarly we get $\rho_{A/\mathcal{K}} : G_\mathcal{K} \to \mathrm{GL}_{2 \dim A}(\mathbb{Q}_\ell)$.

- **Last week:** Yuan told us that $\rho_{E/\mathcal{K}}$ is independent of ℓ

$$w(E/\mathcal{K}) := w(\rho^*_{E/\mathcal{K}}, \psi, dx)$$

- $w(E/\mathcal{K})$ is independent of ψ and dx
- $w(E/\mathcal{K}) \in \{\pm 1\}$
- $w(E/\mathcal{K}) = -1$ when $\mathcal{K}$ is Archimedean, (more generally $w(A/\mathcal{K}) = (-1)^{\dim A}$).

Computing root numbers

Recall that the global root number is $w(E/K) = \prod_v w(E/K_v)$.

Elliptic curves (Sven)

Let E/K be a semistable elliptic curve over a number field. It turns out that,

$$w(E/K) = (-1)^{m_K + u_K}$$

- $m_K = \#\{\text{primes where } E \text{ has split multiplicative reduction}\}$,
- $u_K = \#\{\text{infinite places}\}$.

When E/K is not semistable, we have Rohrlich's theorem.

Abelian varieties (Lilybelle)

- Formulae for twisted root numbers
- Analogue of Rohrlich's theorem for tame abelian varieties
- Cluster picture machinery for tame hyperelliptic curves

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

Birch and Swinnerton-Dyer conjecture

Assuming that $L(E,s)$ has an analytic continuation to $\mathbb{C}$,

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

Conjectural functional equation

Assuming that $L(E,s)$ has an analytic continuation to $\mathbb{C}$,

$$L(E,s) = w(E/K)L(E,2-s) \times (\text{stuff}), \qquad w(E/K) \in \{\pm 1\}.$$

Rephrased: $(-1)^{\mathrm{ord}_{s=1} L(E,s)} = w(E/K)$.

The Parity Conjecture

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

Parity Phenomena

- Predicting the existence of points of infinite order
- Rational abelian varieties have even rank over $\mathbb{Q}(i, \sqrt{17})$
- An elliptic curve with infinitely many $\mathbb{Q}(\sqrt[3]{n})$ points
- An elliptic curve whose rank grows in all even degree extensions
- Goldfeld's conjecture cannot hold when $K \neq \mathbb{Q}$
- ... (see Lilybelle and Vladimir's paper!)

Predicting the existence of points of infinite order

The Parity Conjecture

$$(-1)^{\mathrm{rank}(A/K)} = w(A/K) = \prod_{v \text{ place of } K} w(A/K_v).$$

Consequently, if $w(A/K) = -1$ then $\mathrm{rank}(A/K) \geq 1$!

If E/K is semistable then

$$w(E/K) = (-1)^{m_K + u_K},$$

where $m_K = \#\{\text{primes where } E \text{ has split multiplicative reduction}\}$, $u_K = \#\{\text{infinite places}\}$.

Let $E/\mathbb{Q} : y^2 - 23y = x^3 - 99997x^2 - 17x + 42$, $\Delta_E = 17 \cdot 655943686625481101$. Then $m_{\mathbb{Q}} = 0$ and $u_{\mathbb{Q}} = 1$. The parity conjecture says

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

Therefore E has a $\mathbb{Q}$-point of infinite order. Magma can't compute this!

Rational abelian varieties have even rank over $\mathbb{Q}(i, \sqrt{17})$

Let $A/\mathbb{Q}$ be an abelian variety and $K = \mathbb{Q}(i, \sqrt{17})$.

Fact

Each $p \in \mathbb{Z}$ splits into an even number, n_p, of primes in $\mathcal{O}_K$.

E.g. 2 splits in $\mathbb{Q}(\sqrt{17})$ and ramifies in $\mathbb{Q}(i)$ & $\mathbb{Q}(\sqrt{-17})$. In $\mathcal{O}_K$ we have $2 = \mathfrak{p}_1^2\mathfrak{p}_2^2$.

Fact

If $\mathfrak{p}_1, \mathfrak{p}_2 | p \in \mathbb{Z}$, then $w(A/K_{\mathfrak{p}_1}) = w(A/K_{\mathfrak{p}_2})$.

The parity conjecture says

$$(-1)^{\mathrm{rank}(A/K)} = \prod_v w(A/K_v) = w(A/\mathbb{C})^2 \cdot \prod_{p \in \mathbb{Z}} \left(\prod_{\mathfrak{p}|p} w(A/K_{\mathfrak{p}}) \right) = \prod_{\substack{p \in \mathbb{Z} \\ \text{fix } \mathfrak{p}|p}} w(A/K_{\mathfrak{p}})^{n_p} = +1.$$

Therefore $\mathrm{rank}(A/K)$ is even for any abelian variety $A/\mathbb{Q}$.

An elliptic curve with infinitely many $\mathbb{Q}(\sqrt[3]{n})$ points

Let $E : y^2 + y = x^3 + x^2 + x$, $\Delta_E = 19$. $E/\mathbb{Q}$ has split multiplicative reduction at 19, so

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

In fact $\mathrm{rank}(E/\mathbb{Q}) = 0$. What about $E/\mathbb{Q}(\sqrt[3]{n})$?

- If $19 \nmid n$, then look at $x^3 - n$. If $\bar{n}$ is a cube in $\mathbb{F}_{19}$ then $19 = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, else $19 = \mathfrak{p}$.
- If $n = 19^\alpha c$. Write $\sqrt[3]{n} = \prod_{i=1}^{k} \mathfrak{p}_i^{n_i} \implies 19^\alpha = \prod_{i=1}^{k_0} \mathfrak{p}_i^{3n_i} \implies 19 = \mathfrak{p}_1^3$.

Fact

If E has split multiplicative reduction at p then it has split multiplicative reduction at $\mathfrak{p}|p$.

Therefore, $m_{\mathbb{Q}(\sqrt[3]{n})}$ is odd and $u_{\mathbb{Q}(\sqrt[3]{n})} = 2$, so

$$(-1)^{\mathrm{rank}(E/\mathbb{Q}(\sqrt[3]{n}))} = w(E/\mathbb{Q}(\sqrt[3]{n})) = -1.$$

E has infinitely many $\mathbb{Q}(\sqrt[3]{n})$-rational points!

An elliptic curve whose rank grows across even degree extensions

Let $K = \mathbb{Q}(\sqrt{-643})$, $\lambda = \frac{1}{2}(1+\sqrt{-643})$ and

$$E/K : y^2 + xy + (\lambda+1)\,y = x^3 + \lambda x^2 + (-\lambda - 60)\,x - 8\lambda + 78.$$

E/K has everywhere good reduction so $m_K = 0$ and $u_K = 1$. Therefore

$$w(E/K) = -1 \quad \Rightarrow \quad \text{rank}(E/K) \text{ is odd.}$$

Now let L/K be an even degree extension, $m_L = 0$ and u_L is even. Therefore

$$w(E/L) = +1 \quad \Rightarrow \quad \text{rank}(E/L) \text{ is even.}$$

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

Goldfeld's conjecture

Let $E : y^2 + y = x^3 - x^2$, $\Delta_E = -11$. $E/\mathbb{Q}$ has split mult. reduction at 11 $\Rightarrow w(E/\mathbb{Q}) = +1$.

Fact

Let $d \in K^\times/(K^\times)^2$. Then $w(E_d/K) = w(E/K)w(E/K(\sqrt{d}))$.

$w(E_d/\mathbb{Q}) = w(E/\mathbb{Q}(\sqrt{d}))$ are equally distributed.

Goldfeld's conjecture

$$\operatorname{rank}(E_d/\mathbb{Q}) = \begin{cases} 0 & \text{for 50\% of } d \in \mathbb{Q}^\times \bmod \square \\ 1 & \text{for 50\% of } d \in \mathbb{Q}^\times \bmod \square \end{cases}$$

Now let $K = \mathbb{Q}(\sqrt{-643})$, $\lambda = \frac{1}{2}(1 + \sqrt{-643})$.

$$E/K : y^2 + xy + (\lambda + 1)\, y = x^3 + \lambda x^2 + (-\lambda - 60)\, x - 8\lambda + 78$$

has good reduction so $w(E/K) = -1$ and $w(E/K(\sqrt{d})) = +1 \Rightarrow w(E_d/K) = -1$.

An analogue of Goldfeld's conjecture can't be true when $K \neq \mathbb{Q}$!

Thank you for your attention!