A blueprint for the Birch and Swinnerton-Dyer conjecture in Lean

数学机械化重点实验室 Seminar

David Ang (洪鼎赐)

University of East Anglia

Tuesday, 13 January 2026

Introduction

Let E_K be an elliptic curve over a number field K.

Conjecture (Birch–Swinnerton-Dyer)

Assume that $L(E_K, s)$ has meromophic continuation at $s = 1$.

1. *The order of vanishing of $L(E_K, s)$ at $s = 1$ is equal to $\mathrm{rk}(E_K)$.*
2. *The group $\text{Ш}(E_K)$ is finite.*
3. *The leading term of $L(E_K, s)$ at $s = 1$ satisfies*

$$\lim_{s \to 1} \frac{L(E_K, s)}{(s-1)^{\mathrm{rk}(E_K)}} = \frac{\Omega(E_K) \cdot \mathrm{Reg}(E_K) \cdot \# \text{Ш}(E_K) \cdot \mathrm{Tam}(E_K)}{\delta_K \cdot \# \mathrm{tor}(E_K)^2},$$

   where δ_K is the absolute discriminant of K.

In this talk, I will describe each of these invariants in detail.

Note that this generalises to abelian varieties over global fields.

Weierstrass equations

An *elliptic curve* E_F over a field F is a smooth projective curve of genus one over F with a distinguished point $\mathcal{O}$ over F.

By the Riemann–Roch theorem, E_F is isomorphic to a curve of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

for some $a_i \in F$ such that $\Delta \neq 0$, and $\mathcal{O}$ is its unique point at infinity.

In `mathlib`, a *Weierstrass curve* over F is a tuple $(a_1, a_2, a_3, a_4, a_6) \in F^5$, and an elliptic curve is a Weierstrass curve such that $\Delta \neq 0$.

A *point* over F is either $\mathcal{O}$ or an affine point $(x, y) \in F^2$ satisfying

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

and a nonsingularity condition.

The group law

With this definition, addition on points is given by explicit rational functions, where associativity is known to be *computationally difficult*: generic associativity is an equality of polynomials with 26,082 terms!

Formalisation (洪–许, 2022)

The type of nonsingular F-points $E_F(F)$ is an abelian group.

It suffices to show that the homomorphism $E_F(F) \to \mathrm{Cl}(F[E_F])$ mapping (x, y) to $[(X - x, Y - y)]$ is injective. If it were not, then there are polynomials $f, g \in F[X]$ such that $(X - x, Y - y) = (f + gY)$. Then

$$\deg(\mathrm{Nm}(f + gY)) = \begin{cases} \max(2\deg(f), 2\deg(g) + 3), \\ \dim_F(F[E_F]/(f + gY)), \end{cases}$$

which give a contradiction.

The Tate module

I attempted to formalise the isomorphism $E_F(F^s)[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ in 2023.

Silverman defines polynomials $\psi_n, \phi_n, \omega_n \in F^s[X, Y]$ and *claims* that there is a computational proof for the multiplication-by-n formula

$$[n](x, y) = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x, y)}{\psi_n^3(x, y)}\right).$$

Computing $\deg(\phi_n) = n^2$ and $\deg(\psi_n^2) = n^2 - 1$, and proving that $(\phi_n, \psi_n^2) = 1$, imply that $\# \ker[n] = n^2$, and the result follows formally.

Formalisation (洪–吴–许, 2026?)

For any $\ell \neq \mathrm{char}(F)$, the ℓ-adic Tate module $T_\ell E_{F^s}$ defines a two-dimensional Galois representation $\rho_{E_F,\ell} : G_F \to \mathrm{GL}(T_\ell E_{F^s})$.

The proof is much trickier than he claims!

The L-function

Let E_K be an elliptic curve over a number field K.

The **Euler factor** of E_K at a finite place v of K is

$$L_v(E_K, s) := \det(1 - \rho_{E_K,\ell}^{\vee I_v}(\phi_v) \cdot q_v^{-s}),$$

where $\ell \nmid q_v$ is any prime number.

The **L-function** of E_K is

$$L(E_K, s) := \prod_{\mathfrak{p}} \frac{1}{L_v(E_K, s)},$$

where the product runs over all finite places v of K.

Assuming an appropriate modularity conjecture for E_K over K, the L-function has analytic continuation to all of $\mathbb{C}$.

Non-archimedean local fields

Let E_F be an elliptic curve over a non-archimedean local field F with normalised valuation v, valuation ring R, and residue field k.

By the valuative criterion for properness, there is a *reduction map*

$$\widetilde{(\cdot)} : E_F \xleftarrow{\sim} E_R \twoheadrightarrow E_k,$$

which induces a map on points $E_F(F) \to \widetilde{E_F}(k)$.

Note that this generalises to the fraction field F of a Bézout domain R with $k := R/m$ for any maximal ideal m of R.

Say that E_F is *minimal* if $v(\Delta) \in \mathbb{N}$ is minimal subject to $a_i \in R$. Any elliptic curve over F is isomorphic to one that is minimal.

If E_K is an elliptic curve over a number field K with $\mathrm{Cl}(K) = 1$, then E_K is isomorphic to an elliptic curve that is minimal everywhere.

Reduction types

Say that E_F is

- *good* if $\widetilde{E_F}$ is elliptic,
- *split multiplicative* if $\widetilde{E_F}$ is nodal with tangent over k,
- *non-split multiplicative* if $\widetilde{E_F}$ is nodal with tangent not over k, and
- *additive* if $\widetilde{E_F}$ is cuspidal.

Let E_K be an elliptic curve over a number field K. Then

$$L_v(E_K, s) = \begin{cases} 1 - a_v q_v^{-s} + q_v^{1-2s} & \text{if } E_{K_v} \text{ is good,} \\ 1 - q_v^{-s} & \text{if } E_{K_v} \text{ is split multiplicative,} \\ 1 + q_v^{-s} & \text{if } E_{K_v} \text{ is non-split multiplicative,} \\ 1 & \text{if } E_{K_v} \text{ is additive,} \end{cases}$$

where $a_v := 1 + q_v - \#\widetilde{E_{K_v}}(k_v)$ is the trace of Frobenius of E_K at v.

Tamagawa numbers

The **Tamagawa number** of E_F is

$$\mathrm{Tam}(E_F) := [E_F(F) : E_F^0(F)],$$

where $E_F^0(F)$ is the subgroup of $E_F(F)$ with nonsingular reduction.

Let E_K be an elliptic curve over a number field K, and let

$$\omega := \frac{\mathrm{d}x}{2y + a_1x + a_3}.$$

For each place v of K, let ω_v be a non-zero invariant differential of a minimal elliptic curve isomorphic to E_{K_v}. Then its **Tamagawa number** is

$$\mathrm{Tam}(E_K) := \prod_v \mathrm{Tam}(E_{K_v}) \cdot \left|\frac{\omega_v}{\omega}\right|_v,$$

where the product runs over all finite places v of K.

Complex fields

Let $E_{\mathbb{C}}$ be an elliptic curve over $\mathbb{C}$ given by $y^2 = x^3 + Ax + B$.

There is a $\mathbb{C}$-lattice $\Lambda_{A,B}$ that is unique up to homothety such that

$$\begin{array}{rcl} \mathbb{C}/\Lambda_{A,B} & \longrightarrow & E_{\mathbb{C}}(\mathbb{C}) \\ z & \longmapsto & (\wp(z), \frac{1}{2}\wp'(z)) \end{array}$$

is an isomorphism of complex Lie groups.

The **period** of $E_{\mathbb{C}}$ is

$$\Omega(E_{\mathbb{C}}) := \int_{\mathbb{C}/\Lambda_{A,B}} 2\mathrm{d}x\mathrm{d}y = \int_{E_{\mathbb{C}}(\mathbb{C})} \omega \wedge \overline{\omega},$$

which is just the area of $\Lambda_{A,B}$.

See Silverman's *Advanced Topics in the Arithmetic of Elliptic Curves*.

Real fields

Let $E_{\mathbb{R}}$ be an elliptic curve over $\mathbb{R}$. Then there is an isomorphism

$$E_{\mathbb{R}}(\mathbb{R}) \cong \begin{cases} S^1 & \text{if } \Delta < 0 \\ S^1 \oplus C_2 & \text{if } \Delta > 0 \end{cases}$$

of real Lie groups.

The **period** of $E_{\mathbb{R}}$ is

$$\Omega(E_{\mathbb{R}}) := \int_{E_{\mathbb{R}}(\mathbb{R})} \omega.$$

If E_K is an elliptic curve over a number field K, its **period** is

$$\Omega(E_K) := \prod_v \Omega(E_{K_v}),$$

where the product runs over all infinite places v of K.

The Mordell–Weil theorem

Let E_K be an elliptic curve over a number field K.

Theorem (Mordell–Weil)

$E_K(K)$ is finitely generated.

By the structure theorem of finitely generated abelian groups,

$$E_K(K) \cong \mathrm{tor}(E_K) \oplus \mathbb{Z}^{\mathrm{rk}(E_K)}.$$

where $\mathrm{tor}(E_K)$ is the **torsion subgroup** and $\mathrm{rk}(E_K)$ is the **rank**.

The torsion subgroup can be computed via the reduction map.

The rank is conjecturally the order of vanishing of $L(E_K, s)$ at $s = 1$.

Naïve heights

The proof that $E_K(K)$ is finitely generated reduces to a proof of the *weak Mordell–Weil theorem* that $E_K(K)/n$ is finite and the existence of a *naïve height* $h : E_K(K) \to \mathbb{R}$ satisfying the following.

- For all $Q \in E_K(K)$, there exists $C_1 \in \mathbb{R}$ such that for all $P \in E_K(K)$,
$$h(P+Q) \leq 2h(P) + C_1.$$
- There exists $C_2 \in \mathbb{R}$ such that for all $P \in E_K(K)$,
$$n^2 h(P) \leq h(nP) + C_2.$$
- For all $C_3 \in \mathbb{R}$, the set $\{P \in E_K(K) : h(P) \leq C_3\}$ is finite.

For instance, when $K = \mathbb{Q}$,

$$\begin{array}{cccc} h & : & E_{\mathbb{Q}}(\mathbb{Q}) & \longrightarrow & \mathbb{R} \\ & & (n/d, y) & \longmapsto & \log\max(|n|, |d|) \\ & & \mathcal{O} & \longmapsto & 0 \end{array}.$$

Canonical heights

Any naïve height defines the *canonical height* $\widehat{h} : E_K(K) \to \mathbb{R}$ given by

$$\widehat{h}(P) := \lim_{n\to\infty} \frac{h([2^n]P)}{4^n},$$

which is independent of the choice of naïve height.

This is a quadratic form on $E_K(K)$, with associated bilinear pairing

$$\langle P, Q\rangle := \tfrac{1}{2}(\widehat{h}(P+Q) - \widehat{h}(P) - \widehat{h}(Q)).$$

The **regulator** of E_K is

$$\mathrm{Reg}(E_K) := \left|\det(\langle P_i, P_j\rangle)_{i,j=0}^{\mathrm{rk}(E_K)}\right|,$$

where $\{P_n\}_{n=0}^{\mathrm{rk}(E_K)}$ is any $\mathbb{Z}$-basis of $E_K(K)/\operatorname{tor}(E_K)$.

Galois cohomology

For any field F, multiplication by $n \in \mathbb{Z}$ gives

$$0 \to E_F[n] \to E_F \to E_F \to 0,$$

which induces a long exact sequence that truncates to

$$0 \to E_F(F)/n \to H^1(F, E_F[n]) \to H^1(F, E_F)[n] \to 0.$$

Applying this to $F = K$ and to $F = K_v$ for each place v of K gives

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E_K(K)/n & \longrightarrow & H^1(K, E_K[n]) & \longrightarrow & H^1(K, E_K)[n] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & \overset{\sigma}{\searrow} & \downarrow \tau[n] & & \\
0 & \to & \prod_v E_K(K_v)/n & \to & \prod_v H^1(K_v, E_K[n]) & \to & \prod_v H^1(K_v, E_K)[n] & \to & 0.
\end{array}$$

Note that $H^1(K, E_K[n])$ is not finite in general.

The weak Mordell–Weil theorem

The *n-Selmer group* $\mathrm{Sel}_n(E_K) := \ker\sigma$ and the **Tate–Shafarevich group**

$$Ш(E_K) := \ker\left(\tau : H^1(K, E_K) \to \prod_v H^1(K_v, E_K)\right)$$

fit in a short exact sequence

$$0 \to E_K(K)/n \to \mathrm{Sel}_n(E_K) \to Ш(E_K)[n] \to 0.$$

The weak Mordell–Weil theorem then reduces to showing that

$$\mathrm{Sel}_n(E_K) \subseteq \mathrm{Sel}_n(K, S) \times \mathrm{Sel}_n(K, S),$$

where $\mathrm{Sel}_n(K, S)$ is the n-Selmer group of K unramified outside an explicit finite set S of bad places of K, which is finite since

$$0 \to \mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^n \to \mathrm{Sel}_n(K, S) \to \mathrm{Cl}_S(K)[n] \to 0.$$