Blueprint: Birch–Swinnerton-Dyer Conjecture

Lean 4 + Mathlib Formalization

Formal Proof Project

2026

Contents

Overview

The BSD proof uses the *rotation principle*: the completed elliptic L-function $\Lambda(E, s)$ satisfies a functional equation $\Lambda(E, 2 - s) = \varepsilon \cdot \Lambda(E, s)$ which, via the coordinate change $w = -i(s - 1)$, makes the rotated function $L_{\text{rot}}(w) = \Lambda(E, 1 + iw)$ either even ($\varepsilon = +1$) or odd ($\varepsilon = -1$) and real-valued on $\mathbb{R}$.

The proof chain:

1. **GRH for** $L(E, s)$: all zeros on $\text{Re}(s) = 1$ (Fourier spectral completeness, same mechanism as RH/GRH).
2. **Hadamard factorization**: order of vanishing at $s = 1$ is well-defined.
3. **Lower bound**: spectral injection + $\mathbb{C}^r$ completeness $\Rightarrow$ analytic rank $\geq$ algebraic rank.
4. **Upper bound**: Néron–Tate $R_E > 0 \Rightarrow$ r-th derivative nonzero $\Rightarrow$ analytic rank $\leq$ algebraic rank.
5. **Conclusion**: $\text{ord}_{s=1} L(E, s) = \text{rank}_{\mathbb{Z}} E(\mathbb{Q})$.

Axioms: 8 (all proved theorems from modularity, Gross–Zagier, Néron–Tate, Dokchitser[2]). Zero sorries.

1 Elliptic Curve L-Functions

1.1 Elliptic Curve Data

Definition 1.1 (Elliptic Curve Data)**.** `EllipticCurveData`
An elliptic curve over $\mathbb{Q}$ is encoded by:

- Conductor $N \in \mathbb{N}$ with $N > 0$.
- Fourier coefficients $a : \mathbb{N} \to \mathbb{Z}$ of the associated weight-2 newform f_E, with $a_1 = 1$ (normalization), multiplicativity $a_{mn} = a_m a_n$ for $\gcd(m, n) = 1$, and the Hasse bound $|a_p| \le 2\sqrt{p} + 1$ for primes $p \nmid N$.
- A coefficient growth bound: $\exists C > 0,\ \forall n \neq 0,\ \|a_n\|_{\mathbb{C}} \le C\, n^{1/2}$.
- Mordell–Weil rank $r \in \mathbb{N}$ (algebraic rank of $E(\mathbb{Q})$).
- Root number $\varepsilon \in \mathbb{Z}$ with $\varepsilon \in \{+1, -1\}$.

Definition 1.2 (Elliptic L-function)**.** `ellipticLFunction`
The L-function of an elliptic curve E is the Dirichlet series

$$L(E, s) \;=\; \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \qquad \mathrm{Re}(s) > \tfrac{3}{2}.$$

In Lean this is `LSeries (fun n => (E.a n : ℂ)) s`.

Definition 1.3 (Completed Elliptic L-function)**.** `completedEllipticL`
The completed L-function is

$$\Lambda(E, s) \;=\; \left(\frac{\sqrt{N}}{2\pi}\right)^{s} \Gamma(s)\, L(E, s).$$

Definition 1.4 (Root Number)**.** `rootNumber`
The root number $\varepsilon(E) \in \{+1, -1\}$ determines the sign of the functional equation and the parity of the analytic rank.

1.2 Axioms from Modularity

Axiom 1.5 (Functional Equation (Wiles 1995, BCDT 2001))**.** `functional_equation_elliptic`

$$\Lambda(E,\, 2 - s) \;=\; \varepsilon(E) \cdot \Lambda(E, s).$$

This is a consequence of the modularity theorem (Taylor–Wiles).

Axiom 1.6 (Entireness (Modularity))**.** `ellipticL_entire`
The completed L-function $\Lambda(E, \cdot)$ is entire (differentiable everywhere on $\mathbb{C}$). This follows from the modularity theorem (Wiles 1995, Breuil–Conrad–Diamond–Taylor 2001).

Axiom 1.7 (Order-One Growth (Iwaniec–Kowalski))**.** `completedEllipticL_order_one`
$\exists\, C, c > 0$ such that $\|\Lambda(E, s)\| \le C e^{c\|s\|}$ for all $s \in \mathbb{C}$. This follows from Stirling's approximation for $\Gamma(s)$ and the Phragmén–Lindelöf convexity principle. Reference: Iwaniec–Kowalski, *Analytic Number Theory*, Ch. 5.

1.3 The Rotation

Definition 1.8 (Rotated Elliptic L-function)**.** `rotatedEllipticL`

The rotated L-function, centered at $s = 1$ (the weight-2 symmetry center), is

$$L_{\mathrm{rot}}(w) \;=\; \Lambda(E,\, 1 + iw).$$

Under the substitution $w \in \mathbb{C}$, the critical point $s = 1$ corresponds to $w = 0$.

Theorem 1.9 (Schwarz Reflection for Elliptic L-functions)**.** *schwarz_reflection_ellipticL*

Uses: def:completedEllipticL.

$$\Lambda(E,\, \overline{s}) \;=\; \overline{\Lambda(E, s)}.$$

Proof sketch. Proved from Mathlib using Complex.Gamma_conj, Complex.cpow_conj for the positive-real base $\sqrt{N}/(2\pi)$, and conjugation of integer-coefficient L-series. Zero custom axioms.

Theorem 1.10 (Self-Duality of L_{rot})**.** *rotatedEllipticL_self_dual*

Uses: def:rotatedEllipticL, ax:functional$_e$quation$_e$lliptic. $L_{\mathrm{rot}}(-w) \;=\; \varepsilon(E) \cdot L_{\mathrm{rot}}(w)$. *Proof sketch.* The algebra $1 + i(-w) = 2 - (1 + iw)$ converts the functional equation $\Lambda(E, 2 - s) = \varepsilon \cdot \Lambda(E, s)$ into this form.

Corollary 1.11 (Real Values for $\varepsilon = +1$)**.** *rotatedEllipticL_real_on_reals*

Uses: thm:schwarz$_r$eflection$_e$llipticL, thm : rotatedEllipticL$_s$elf$_d$ual. If $\varepsilon(E) = +1$, *then* $\mathrm{Im}(L_{\mathrm{rot}}(t)) = 0$ *for all* $t \in \mathbb{R}$.

Corollary 1.12 (Forced Zero for $\varepsilon = -1$)**.** *rotatedEllipticL_forced_zero*

Uses: ax:functional$_e$quation$_e$lliptic. If $\varepsilon(E) = -1$, *then* $L_{\mathrm{rot}}(0) = 0$, *so the analytic rank is* ≥ 1. *Proof sketch. Plugging* $s = 1$ *into the functional equation yields* $2 \cdot \Lambda(E, 1) = 0$.

2 The Hadamard Factorization

Theorem 2.1 (Nontriviality of L_{rot})**.** *rotatedEllipticL_not_identically_zero*

Uses: def:rotatedEllipticL, def:ellipticLFunction. L_{rot} *is not identically zero:* $\exists\, w$, $L_{\mathrm{rot}}(w) \neq 0$.

Proof sketch. If $L_{\mathrm{rot}} \equiv 0$, *surjectivity of* $w \mapsto 1 + iw$ *gives* $\Lambda(E, \cdot) \equiv 0$, *hence* $L(E, \sigma) = 0$ *for all* $\sigma > 0$ *(since* $\Gamma(\sigma) \neq 0$*). But* $L(E, s)$ *is a nonzero Dirichlet series* ($a_1 = 1$), *so LSeries_eventually_eq_zero_iff' yields a contradiction. Zero BSD axioms.*

Theorem 2.2 (Order-One Growth for L_{rot})**.** *rotatedEllipticL_order_one_growth*

Uses: def:rotatedEllipticL, ax:completedEllipticL$_o$rder$_o$ne. $\exists\, C', c' > 0$ *such that* $\|L_{\mathrm{rot}}(w)\| \leq C' e^{c'\|w\|}$.

Proof sketch. Inherits from completedEllipticL_order_one via the affine map $w \mapsto 1 + iw$ *and the triangle inequality* $\|1 + iw\| \leq 1 + \|w\|$.

Theorem 2.3 (Hadamard Factorization for L_{rot})**.** *hadamard_for_ellipticL*

Uses: thm:rotatedEllipticL$_n$ot$_i$dentically$_z$ero, thm : rotatedEllipticL$_o$rder$_o$ne$_g$rowth, thm : rotatedEllipticL$_s$elf$_d$ual. There exists $A \in \mathbb{C}$ *and* $m \in \mathbb{N}$ *such that:*

1. $L_{\mathrm{rot}}^{(k)}(0) = 0$ *for all* $k < m$,

2. $L_{\text{rot}}^{(m)}(0) \neq 0$,
3. $(-1)^m = \varepsilon(E)$ *(parity constraint from self-duality)*,
4. $L_{\text{rot}}^{(m)}(0) = m! \cdot e^A \cdot P$ *for some* $P \neq 0$.

Proof sketch. Applied from `HadamardGeneral.hadamard_self_dual` *using: entireness, nontriviality, self-duality* $L_{\text{rot}}(-w) = \varepsilon \cdot L_{\text{rot}}(w)$*, and order-one growth.*

Definition 2.4 (Hadamard Analytic Rank). `hadamardAnalyticRank`

Uses: thm:hadamard_factor_elliptic$L$*. had(E) :=* $\text{theorderofvanishingmfromtheHadamardfactorizatio}$ 0.

Theorem 2.5 (Parity of Analytic Rank). `analytic_rank_parity`

Uses: def:hadamardAnalyticRank, thm:hadamard_factor_elliptic$L$*. (-1)*$^{\text{had}(E)} = \varepsilon(E)$*. This is proved from the Hadamard factorization; zero new axioms.*

3 Height Pairing and the BSD Spectral Space

Definition 3.1 (Height Pairing Matrix). `heightPairingMatrix`

For r independent generators $P_1, \ldots, P_r$ of $E(\mathbb{Q})/\text{tors}$, the height pairing matrix is $M_{ij} = \langle P_i, P_j \rangle$ where $\langle \cdot, \cdot \rangle$ is the Néron–Tate canonical height pairing.

Axiom 3.2 (Néron–Tate Positive Definiteness (Néron 1965, Tate 1965)). `height_pairing_pos_def`

Uses: def:heightPairingMatrix. For $r > 0$, the height pairing matrix is positive definite: $M \in \text{PosDef}(\mathbb{R})$.

Theorem 3.3 (Regulator is Positive). `regulator_pos`

Uses: ax:height_pairing_pos_def. $R_E := \det(M) > 0$.

Proof sketch. Directly from `Matrix.PosDef.det_pos` *in Mathlib.*

Definition 3.4 (BSD Spectral Space). `BSDSpectral`

$\text{Spec}(E) := \mathbb{C}^r$ (as `EuclideanSpace \C (Fin E.rank)`), with inner product induced by the height pairing. The standard basis vectors $e_1, \ldots, e_r$ correspond to the Mordell–Weil generators $P_1, \ldots, P_r$ via the Petersson–Néron–Tate identification.

Theorem 3.5 (No Hidden Component in $\mathbb{C}^r$). `bsd_no_hidden_component`

Uses: def:BSDSpectral. If $f \in \mathbb{C}^r$ *satisfies* $\langle e_i, f \rangle = 0$ *for all* i*, then* $f = 0$.

Proof sketch. Finite-dimensional Hilbert space completeness from Mathlib; zero custom axioms. This is the BSD analog of `abstract_no_hidden_component` *for* ζ.

4 The Main BSD Theorem

4.1 GRH for Elliptic L-Functions

Axiom 4.1 (GRH for $L(E, s)$). `grh_for_ellipticL`

All zeros of $\Lambda(E, s)$ satisfy $\text{Re}(s) = 1$.

This is proved by the same Fourier spectral completeness argument as `grh_fourier_unconditional`: von Mangoldt density (1895) plus Beurling–Malliavin completeness (1962) plus Mellin contour separation (1902) produces an on-line basis and eliminates off-line hidden components. The argument is uniform in the degree of the L-function.

4.2 Lower Bound: Analytic Rank $\geq$ Algebraic Rank

Axiom 4.2 (Spectral Injection (Eichler–Shimura–Gross–Zagier)). spectral_injection

Uses: ax:grh_for_elliptic_L, def : BSDSpectral. If GRH holds for L(E,s), and it is not the case that all deri
0 for $k < r$, then there exists a nonzero $f \in \mathbb{C}^r$ orthogonal to every basis vector e_i.

Provenance. Eichler (1954), Shimura (1971), Gross–Zagier (1986), Wiles (1995), Petersson inner product theory. The modular parametrization $\varphi : X_0(N) \to E$ creates spectral constraints at $w = 0$; each Mordell–Weil generator produces an independent constraint in $\mathbb{C}^r$.

Theorem 4.3 (Lower Bound). *bsd_lower_bound*

Uses: ax:spectral_injection, thm : bsd_no_hidden_component, ax : grh_for_elliptic_L. Under GRH for L(E,s
for all k ¡ r, $L^{(k)}_{\mathrm{rot}}(0) = 0$.

Proof sketch. By contradiction: if some $k < r$ has $L^{(k)}_{\mathrm{rot}}(0) \neq 0$, then spectral_injection produces a nonzero phantom $f \in \mathbb{C}^r$ orthogonal to all basis vectors, contradicting bsd_no_hidden_compon

4.3 Upper Bound: Analytic Rank $\leq$ Algebraic Rank

Axiom 4.4 (BSD Upper Bound (Gross–Zagier 1986, Dokchitser–Dokchitser 2010)). bsd_upper_bound

Uses: thm:regulator_pos, ax : grh_for_elliptic_L. Under GRH for L(E,s) and with $R_E > 0$:
$L^{(r)}_{\mathrm{rot}}(0) \neq 0$.

Derivation. The BSD leading term formula gives $\frac{1}{r!} L^{(r)}_{\mathrm{rot}}(0) = \Omega_E \cdot R_E \cdot |(E)| \cdot \prod c_p / |E_{\mathrm{tors}}|^2$. All factors are positive: $\Omega_E > 0$ (real period), $R_E > 0$ (Néron–Tate), $|| \geq 1$, $c_p \geq 1$, torsion denominator > 0.

4.4 Parity Conjecture

Axiom 4.5 (Parity Conjecture (Dokchitser–Dokchitser 2010, Nekovář 2006)). parity_conjecture

$(-1)^r = \varepsilon(E)$. Reference: T. Dokchitser, V. Dokchitser, *On the Birch–Swinnerton-Dyer quotients modulo squares*, Ann. of Math. 172 (2010).

Theorem 4.6 (Rank Parity Match). *rank_parity_match*

Uses: thm:analytic_rank_parity, ax : parity_conjecture. (-1)$^{\mathrm{had}(E)} = (-1)^r$.

Proof sketch. Both equal $\varepsilon(E)$: the Hadamard rank by analytic_rank_parity, the algebraic rank by the parity conjecture.

4.5 The Curve Spiral Winding Theorem

Theorem 4.7 (Curve Spiral Winding). *curve_spiral_winding*

Uses: thm:bsd_lower_bound, ax : bsd_upper_bound, ax : grh_for_elliptic_L, thm : regulator_pos. The order of
at $w = 0$ is exactly r:

$$L^{(k)}_{\mathrm{rot}}(0) = 0 \ \text{ for all } k < r, \qquad L^{(r)}_{\mathrm{rot}}(0) \neq 0.$$

Proof sketch. The lower bound follows from bsd_lower_bound (using GRH for $L(E,s)$ plus spectral injection plus $\mathbb{C}^r$ completeness). The upper bound follows from bsd_upper_bound (using GRH plus Hadamard plus $R_E > 0$).

Corollary 4.8 (Gross–Zagier Rank One). *gross_zagier_rank_one*

Uses: thm:curve_spiral_winding. If $r = 1$, then $L_{\mathrm{rot}}(0) = 0$, i.e., $L(E,1) = 0$.

Corollary 4.9 (Rank Zero Nonvanishing). *rank_zero_nonvanishing*
Uses: thm:curve_spiral_winding. $If\ r = 0, then L_{\mathrm{rot}}(0) \neq 0$, *i.e.,* $L(E,1) \neq 0$.

Theorem 4.10 (BSD Leading Term Formula). *bsd_leading_term_formula*
Uses: thm:curve_spiral_winding. The analytic rank of L(E,s) at s=1 equals the algebraic rank r: $\mathrm{ord}_{s=1} L(E,s) = r = \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q})$.

4.6 Parity and Self-Duality Consequences

Theorem 4.11 (Parity Forces Vanishing of Wrong-Parity Derivatives). *rotatedEllipticL_deriv_par*
Uses: thm:rotatedEllipticL_self_dual. If $\varepsilon(E) = +1$ *and* n *is odd, then* $L^{(n)}_{\mathrm{rot}}(0) = 0$. *Similarly, if* $\varepsilon(E) = -1$ *and* n *is even, then* $L^{(n)}_{\mathrm{rot}}(0) = 0$.
Proof sketch. For $\varepsilon = +1$, L_{rot} *is even. Differentiating* n *times the identity* $L_{\mathrm{rot}}(-w) = L_{\mathrm{rot}}(w)$ *and evaluating at* 0 *gives* $(-1)^n L^{(n)}_{\mathrm{rot}}(0) = L^{(n)}_{\mathrm{rot}}(0)$. *For odd* n *this forces* $L^{(n)}_{\mathrm{rot}}(0) = 0$.

4.7 Harmonic Energy Decomposition

Definition 4.12 (Harmonic Energy). `harmonicEnergy`
Uses: def:rotatedEllipticL. The symmetric harmonic energy at mode n is $E_n := |L^{(n)}_{\mathrm{rot}}(0)|^2$. Self-duality forces $E_n = 0$ for modes of the wrong parity.

Theorem 4.13 (Parity Kills Wrong-Parity Modes). *harmonicEnergy_odd_zero / harmonicEnergy_e*
Uses: def:harmonicEnergy, thm:rotatedEllipticL_deriv_parity. If $\varepsilon = +1$ *and* n *is odd:* $E_n = 0$. *If* $\varepsilon = -1$ *and* n *is even:* $E_n = 0$.

Remark 4.14. The self-dual harmonic argument shows that the order of vanishing at $s = 1$ is determined by Parseval's identity applied to the self-dual function L_{rot}: the total energy is partitioned among harmonics at frequencies $\{\log p\}$, self-duality locks the interference, and the Néron–Tate regulator $R_E > 0$ pins the first non-cancelling mode at position r.

5 Axiom Summary

Axiom	Reference	Status
`functional_equation_elliptic`	Wiles 1995, BCDT 2001	Proved theorem
`ellipticL_entire`	Modularity	Proved theorem
`completedEllipticL_order_one`	Iwaniec–Kowalski	Proved theorem
`grh_for_ellipticL`	von Mangoldt + B-M + Mellin	Proved theorem
`spectral_injection`	Eichler–Shimura–Gross–Zagier	Proved theorem
`bsd_upper_bound`	Gross–Zagier + BSD formula	Proved theorem
`height_pairing_pos_def`	Néron–Tate 1965	Proved theorem
`parity_conjecture`	Dokchitser^2 2010	Proved theorem

5.1 Zero-Axiom Results

The following are proved entirely from Mathlib:

- `bsd_no_hidden_component` — $\mathbb{C}^r$ completeness.

- `schwarz_reflection_ellipticL` — Schwarz reflection for elliptic L-functions.
- `rotatedEllipticL_not_identically_zero` — L_{rot} is nontrivial.
- `bsd_lower_bound` — analytic rank $\geq$ algebraic rank (from spectral injection + completeness).