Étude 3: The Birch and Swinnerton-Dyer Conjecture via Hypostructure

0. Introduction

Conjecture 0.1 (Birch and Swinnerton-Dyer). Let $E/\mathbb{Q}$ be an elliptic curve. Then: 1. $\mathrm{ord}_{s=1}L(E,s) = \text{rank } E(\mathbb{Q})$ 2. $\lim_{s\to 1}\frac{L(E,s)}{(s-1)^r} = \frac{\Omega_E\cdot\mathrm{Reg}_E\cdot\prod_p c_p\cdot|\ (E/\mathbb{Q})|}{|E(\mathbb{Q})_{\text{tors}}|^2}$

We construct a hypostructure on the moduli of elliptic curves and interpret BSD through the structural axioms and metatheorems.

---

1. Elliptic Curves: Algebraic Setup

1.1 Basic Definitions

Definition 1.1.1. An elliptic curve over $\mathbb{Q}$ is a smooth projective curve E of genus 1 with a specified rational point $O \in E(\mathbb{Q})$.

Definition 1.1.2. Every elliptic curve over $\mathbb{Q}$ has a Weierstrass model:

$$E: y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}, \quad \Delta := -16(4a^3 + 27b^2) \neq 0$$

Definition 1.1.3. The conductor N_E is defined by:

$$N_E := \prod_{p|\Delta} p^{f_p}$$

where $f_p \in \{1, 2\}$ for $p \geq 5$, with specific formulas for $p = 2, 3$.

Definition 1.1.4. The Mordell-Weil group $E(\mathbb{Q})$ is the group of rational points with the chord-tangent law. By the Mordell-Weil theorem:

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}}$$

where $r = \text{rank } E(\mathbb{Q}) \geq 0$ and $E(\mathbb{Q})_{\text{tors}}$ is finite.

1.2 The L-Function

Definition 1.2.1. For a prime $p \nmid N_E$, define:

$$a_p := p + 1 - |E(\mathbb{F}_p)|$$

where $E(\mathbb{F}_p)$ is the reduction of E modulo p.

Definition 1.2.2. The Hasse-Weil L-function is:

$$L(E,s) := \prod_{p\nmid N_E}\frac{1}{1 - a_p p^{-s} + p^{1-2s}}\prod_{p|N_E}\frac{1}{1 - a_p p^{-s}}$$

for $\mathrm{Re}(s) > 3/2$.

Theorem 1.2.3 (Modularity, Wiles et al.). $L(E,s)$ extends to an entire function satisfying the functional equation:

$$\Lambda(E,s) := N_E^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s) = w_E\Lambda(E,2-s)$$

where $w_E = \pm 1$ is the root number.

---

2. The Hypostructure Data

2.1 State Space

Definition 2.1.1. The moduli stack of elliptic curves over $\mathbb{Q}$ is:

$$\mathcal{M}_{1,1}(\mathbb{Q}) := [\mathrm{Ell}/\mathrm{Isom}]$$

We work with a rigidification: fix a level structure or work with isomorphism classes.

Definition 2.1.2. The state space is:

$$X := \{(E, P_1, \dots, P_r) : E/\mathbb{Q} \text{ elliptic}, P_i \in E(\mathbb{Q}) \text{ independent}\}/\sim$$

where $\sim$ is isomorphism respecting the points.

Definition 2.1.3. Alternatively, use the height-graded space:

$$X_H := \{E/\mathbb{Q} : h(E) \leq H\}$$

where $h(E)$ is the Faltings height or naive height.

2.2 Height Functional

Definition 2.2.1. The Néron-Tate height on $E(\mathbb{Q})$ is:

$$\hat{h} : E(\mathbb{Q}) \to \mathbb{R}_{\geq 0}$$

defined by $\hat{h}(P) := \lim_{n\to\infty} \frac{h([2^n]P)}{4^n}$ where h is the naive height.

Proposition 2.2.2. The Néron-Tate height satisfies: 1. $\hat{h}([n]P) = n^2\hat{h}(P)$ 2. $\hat{h}(P) = 0 \Leftrightarrow P \in E(\mathbb{Q})_{\text{tors}}$ 3. $\hat{h}$ extends to a positive definite quadratic form on $E(\mathbb{Q}) \otimes \mathbb{R}$

Definition 2.2.3. The regulator is:

$$\mathrm{Reg}_E := \det(\langle P_i, P_j\rangle)_{1\leq i,j\leq r}$$

where $\langle P, Q\rangle := \frac{1}{2}(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q))$ is the Néron-Tate pairing and $\{P_1, \dots, P_r\}$ is a basis for $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}}$.

Definition 2.2.4. The height functional on X is:

$$\Phi(E, P_1, \dots, P_r) := \mathrm{Reg}_E = \det(\langle P_i, P_j\rangle)$$

2.3 Dissipation and Dynamics

Remark 2.3.1. Elliptic curves do not have a natural "flow" in the PDE sense. The dynamics arise from: 1. Descent (reducing modulo primes) 2. Isogeny (maps between curves) 3. Galois action on $\bar{\mathbb{Q}}$-points

Definition 2.3.2. The p-descent map:

$$\delta_p : E(\mathbb{Q})/pE(\mathbb{Q}) \to H^1(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), E[p])$$

measures the failure of divisibility.

Definition 2.3.3. The Selmer group is:

$$\mathrm{Sel}_p(E/\mathbb{Q}) := \ker\left(H^1(\mathbb{Q}, E[p]) \to \prod_v H^1(\mathbb{Q}_v, E)\right)$$

Definition 2.3.4. The Tate-Shafarevich group is:

$$(E/\mathbb{Q}) := \ker\left(H^1(\mathbb{Q}, E) \to \prod_v H^1(\mathbb{Q}_v, E)\right)$$

Proposition 2.3.5. There is an exact sequence:

$$0 \to E(\mathbb{Q})/pE(\mathbb{Q}) \to \mathrm{Sel}_p(E/\mathbb{Q}) \to \ (E/\mathbb{Q})[p] \to 0$$

---

3. Verification of Axioms

3.1 Axiom C (Compactness)

Theorem 3.1.1 (Mordell-Weil). $E(\mathbb{Q})$ is finitely generated.

Theorem 3.1.2 (Northcott). For any $B > 0$:

$$|\{P \in E(\mathbb{Q}) : \hat{h}(P) \leq B\}| < \infty$$

Corollary 3.1.3 (Axiom C). The set $\{(E, P) : h(E) \leq H, \hat{h}(P) \leq B\}$ is finite.

Proof. Northcott's theorem applied fiber by fiber over the finite set of curves with bounded height. □

3.2 Axiom D (Dissipation)

Definition 3.2.1. Define the "dissipation" as the defect of the rank:

$$\mathfrak{D}(E) := \dim_{\mathbb{F}_p} \mathrm{Sel}_p(E/\mathbb{Q}) - \mathrm{rank}\ E(\mathbb{Q})$$

Proposition 3.2.2. $\mathfrak{D}(E) \geq 0$ with equality iff $\ (E/\mathbb{Q})[p] = 0$.

Remark 3.2.3. This is not a true "dissipation" in the dynamical sense but captures the obstruction to perfect descent.

3.3 Axiom Cap (Capacity) via Theorem 9.126

Theorem 9.126 (Arithmetic Height Barrier). For elliptic curves, the height satisfies:

$$\hat{h}(P) \geq c(\epsilon) N_E^{-\epsilon}$$

for all $P \in E(\mathbb{Q}) \quad E(\mathbb{Q})_{\text{tors}}$ and any $\epsilon > 0$.

Corollary 3.3.1. Points cannot accumulate at height zero (capacity barrier for the singular set $\hat{h} = 0$).

3.4 Axiom TB (Topological Background)

Definition 3.4.1. The topological sectors for $E/\mathbb{Q}$ are: 1. Root number $w_E = \pm 1$ (parity of rank) 2. Torsion structure $E(\mathbb{Q})_{\text{tors}}$ 3. Conductor N_E (level)

Theorem 3.4.2 (Parity Conjecture, Nekovář, Dokchitser^2).

$$(-1)^{\text{rank } E(\mathbb{Q})} = w_E$$

Corollary 3.4.3. The sector $w_E = +1$ forces even rank; $w_E = -1$ forces odd rank.

---

4. The BSD Formula as Height-Dissipation Balance

4.1 The Analytic Side

Definition 4.1.1. The order of vanishing:

$$r_{an} := \text{ord}_{s=1} L(E, s)$$

Definition 4.1.2. The leading coefficient:

$$L^*(E, 1) := \lim_{s \to 1} \frac{L(E, s)}{(s-1)^{r_{an}}}$$

4.2 The Algebraic Side

Definition 4.2.1. The algebraic rank:

$$r_{alg} := \text{rank } E(\mathbb{Q})$$

Definition 4.2.2. The BSD invariant:

$$\mathcal{B}(E) := \frac{\Omega_E \cdot \text{Reg}_E \cdot \prod_p c_p \cdot | \ (E/\mathbb{Q})|}{|E(\mathbb{Q})_{\text{tors}}|^2}$$

where: - $\Omega_E = \int_{E(\mathbb{R})} |\omega|$ is the real period - $c_p = [E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)]$ are Tamagawa numbers

4.3 BSD as Structural Balance

Conjecture 4.3.1 (BSD Rank). $r_{an} = r_{alg}$.

Interpretation. The "height" (regulator) equals the "L-function order" (analytic obstruction).

Conjecture 4.3.2 (BSD Formula). $L^*(E, 1) = \mathcal{B}(E)$.

Interpretation. The leading coefficient balances: - Ω_E: archimedean contribution (real points) - Reg_E: height contribution (Mordell-Weil lattice) - $\prod c_p$: local contributions (bad reduction) - $| \ |$: global obstruction (failure of local-global) - $|E_{\mathrm{tors}}|^2$: torsion contribution

---

5. Invocation of Metatheorems

5.1 Theorem 9.22 (Symplectic Transmission)

Application. The Cassels-Tate pairing:

$$(E/\mathbb{Q}) \times \ (E/\mathbb{Q}) \to \mathbb{Q}/\mathbb{Z}$$

is alternating. Hence $| \ |$ is a perfect square (if finite).

Corollary 5.1.1. The BSD formula involves $| \ |$, not $| \ |^{1/2}$.

5.2 Theorem 9.50 (Galois-Monodromy Lock)

Application. The Galois representation:

$$\rho_{E,\ell} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$$

has image constrained by monodromy. By Serre's theorem, the image is "large" for non-CM curves.

Corollary 5.2.1. The L-function $L(E, s)$ is determined by Galois-theoretic data.

5.3 Theorem 9.126 (Arithmetic Height Barrier)

Application. The Néron-Tate height provides a positive definite form on $E(\mathbb{Q}) \otimes \mathbb{R}$. The regulator $\mathrm{Reg}_E > 0$ for $r > 0$.

Corollary 5.3.1. The BSD formula makes sense: $\mathrm{Reg}_E \neq 0$ when $r > 0$.

5.4 Theorem 9.18 (Gap Quantization)

Application. The rank $r \in \mathbb{Z}_{\geq 0}$ is discrete. There is no "fractional rank."

Corollary 5.4.1. The order of vanishing r_{an} is also an integer, consistent with $r_{an} = r_{alg}$.

5.5 Theorem 18.4.1 (Arithmetic Isomorphism)

Application. The BSD conjecture instantiates the Hypostructure via:

Hypostructure	BSD Instantiation
State space X	$E(\mathbb{Q})$
Height Φ	Néron-Tate $\hat{h}$
Axiom C	Mordell-Weil (finite generation)
Obstruction $\mathcal{O}$	Tate-Shafarevich
Axiom 9.22	Cassels-Tate pairing

---

6. Known Cases of BSD

6.1 Rank 0

Theorem 6.1.1 (Coates-Wiles [CW77]). If E has complex multiplication by $\mathcal{O}_K$ and $L(E,1) \neq 0$, then $E(\mathbb{Q})$ is finite.

Theorem 6.1.2 (Gross-Zagier, Kolyvagin [GZ86, K90]). If $\text{ord}_{s=1} L(E,s) = 0$, then rank $E(\mathbb{Q}) = 0$ and $(E/\mathbb{Q})$ is finite.

6.2 Rank 1

Theorem 6.2.1 (Gross-Zagier [GZ86]). If $\text{ord}_{s=1} L(E,s) = 1$, then:

$$L'(E,1) = \frac{\Omega_E \cdot \hat{h}(P_{GZ})}{\sqrt{|\Delta_K|}} \cdot \text{(period factor)}$$

where P_{GZ} is a Heegner point.

Theorem 6.2.2 (Kolyvagin [K90]). If $\text{ord}_{s=1} L(E,s) = 1$, then rank $E(\mathbb{Q}) = 1$ and is finite.

6.3 Higher Rank

Open Problem 6.3.1. For $\text{ord}_{s=1} L(E,s) \geq 2$, the BSD conjecture is open.

Remark 6.3.2. No method currently produces points when the analytic rank is ≥ 2.

---

7. The Selmer-Sha Exact Sequence

7.1 The Fundamental Sequence

Theorem 7.1.1. For each prime p, there is an exact sequence:

$$0 \to E(\mathbb{Q})/pE(\mathbb{Q}) \to \text{Sel}_p(E/\mathbb{Q}) \to \ (E/\mathbb{Q})[p] \to 0$$

Corollary 7.1.2.

$$\dim_{\mathbb{F}_p} \mathrm{Sel}_p(E/\mathbb{Q}) = r + \dim_{\mathbb{F}_p} E(\mathbb{Q})[p] + \dim_{\mathbb{F}_p} \ [p]$$

7.2 Structural Interpretation

Definition 7.2.1. The p-Selmer rank is:

$$s_p(E) := \dim_{\mathbb{F}_p} \mathrm{Sel}_p(E/\mathbb{Q})$$

Proposition 7.2.2. $s_p(E) \geq r$ with equality modulo contributions from torsion and .

Interpretation. The Selmer group is computable (local conditions), while $E(\mathbb{Q})$ and   are global. Descent computes s_p and bounds r.

---

8. Iwasawa Theory and p-adic L-functions

8.1 The p-adic Setting

Definition 8.1.1. Let $\mathbb{Q}_\infty = \bigcup_n \mathbb{Q}(\zeta_{p^n})^+$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$.

Definition 8.1.2. The Iwasawa algebra is $\Lambda := \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]] \cong \mathbb{Z}_p[[T]]$.

Definition 8.1.3. The Selmer group over $\mathbb{Q}_\infty$:

$$\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_\infty) := \varinjlim_n \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_n)$$

is a Λ-module.

8.2 Main Conjecture

Theorem 8.2.1 (Kato, Skinner-Urban). Under certain conditions:

$$\mathrm{char}_\Lambda(\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_\infty)^\vee) = (L_p(E))$$

where $L_p(E) \in \Lambda$ is the p-adic L-function.

Interpretation. The “characteristic ideal” equals the “L-function ideal” — an algebraic-analytic correspondence at the level of Λ-modules.

---

9. Connection to Hypostructure Axioms

9.1 Axiom SC (Scaling Structure)

Observation. Under isogeny $\phi : E \to E'$ of degree d:

$$\mathrm{Reg}_{E'} = d^{-r} \cdot |\ker \phi \cap E(\mathbb{Q})|^{-2} \cdot \mathrm{Reg}_E$$

The regulator transforms under isogeny like a height function.

9.2 Axiom LS (Local Stiffness)

Application. The Mordell-Weil lattice $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}}$ with the Néron-Tate pairing is a positive definite lattice. The regulator is the covolume.

Proposition 9.2.1 (Stiffness). For $r \geq 1$:

$$\text{Reg}_E \geq c(r) > 0$$

where $c(r)$ depends only on the rank.

Proof. Hermite's theorem: lattices of rank r have covolume bounded below by a constant depending on r. □

9.3 Axiom Cap (Capacity)

Application. The set of torsion points $E(\mathbb{Q})_{\text{tors}}$ has height zero. By Mazur's theorem, $|E(\mathbb{Q})_{\text{tors}}| \leq 16$.

Proposition 9.3.1. The "singular set" (torsion) has bounded cardinality, hence zero capacity in any reasonable sense.

---

10. Computational Evidence

10.1 Database Verification

Theorem 10.1.1 (Cremona database). For all $E/\mathbb{Q}$ with $N_E \leq 500000$, BSD rank conjecture is verified: $r_{an} = r_{alg}$.

10.2 Formula Verification

Theorem 10.2.1. For all $E/\mathbb{Q}$ with $N_E \leq 5000$ and $r \leq 1$, the BSD formula is numerically verified to high precision.

---

11. Obstructions to BSD

11.1 Finiteness of

Conjecture 11.1.1. $(E/\mathbb{Q})$ is finite for all $E/\mathbb{Q}$.

Remark 11.1.2. This is known for $r \leq 1$ (Kolyvagin) but open for $r \geq 2$.

11.2 Computing

Problem 11.2.1. There is no algorithm proven to compute $|\,|$ in all cases.

Remark 11.2.2. Descent methods compute Selmer groups, giving upper bounds on $|\,|$.

---

12. Conclusion

Theorem 12.1 (Summary). The BSD conjecture fits into the Hypostructure framework via:

Component	Instantiation
State space	Mordell-Weil group $E(\mathbb{Q})$
Height Φ	Néron-Tate height, Regulator
Dissipation	Selmer defect, obstruction
Axiom C	Mordell-Weil theorem
Axiom Cap	Northcott, height gap
Axiom TB	Root number parity
Metatheorem 9.22	Cassels-Tate alternating pairing
Metatheorem 9.126	Height lower bounds

Open. Full BSD (especially for $r \geq 2$) requires new techniques beyond current descent methods.

---

13. References

[CW77] J. Coates, A. Wiles. On the conjecture of Birch and Swinnerton-Dyer. Invent. Math. 39 (1977), 223–251.

[GZ86] B. Gross, D. Zagier. Heegner points and derivatives of L-series. Invent. Math. 84 (1986), 225–320.

[K90] V. Kolyvagin. Euler systems. The Grothendieck Festschrift II, Progr. Math. 87 (1990), 435–483.

[Maz77] B. Mazur. Modular curves and the Eisenstein ideal. Publ. Math. IHÉS 47 (1977), 33–186.

[Sil09] J. Silverman. The Arithmetic of Elliptic Curves. 2nd ed., Springer, 2009.

[SU14] C. Skinner, E. Urban. The Iwasawa main conjectures for GL . Invent. Math. 195 (2014), 1–277.

[Wil95] A. Wiles. Modular elliptic curves and Fermat's Last Theorem. Ann. of Math. 141 (1995), 443–551.