

The Constructive Archimedean Rescue in Birch–Swinnerton-Dyer

Paper 51 in the Constructive Reverse Mathematics Series

Paul Chun-Kit Lee

dr.paul.c.lee@gmail.com

February 2026 — v2.0

DOI: 10.5281/zenodo.18732168

Abstract

We prove that the positive-definite Archimedean metric is the unique topological modality converting the rank-1 Birch–Swinnerton-Dyer (BSD) generator search from MP (unbounded Diophantine search) to BISH (bounded exhaustive search). Given quarantined analytic axioms—Gross–Zagier, Kolyvagin, and Silverman’s height difference bound—the search for a generator of $E(\mathbb{Q})$ lies in an explicit Finset of size $O(B^2)$, where $B = \lceil \exp(2\hat{h}(y_K) + 2\mu(E)) \rceil$.

The p -adic analogue fails: without positive-definiteness ($u = 4$), the canonical height \hat{h}_p can vanish on non-torsion points, collapsing the search bound to the vacuous $h(P) \leq 2\mu(E)$.

Formalized in LEAN 4 + MATHLIB4 with zero `sorrys` and zero custom axiom declarations. All analytic axioms enter as Prop-valued hypotheses in a `BSDRankOneData` structure, following the Papers 23/28 convention. The axiom audit confirms that every theorem depends only on [`propext`, `Classical.choice`, `Quot.sound`]—the standard MATHLIB4 infrastructure for \mathbb{R} .

Keywords: Constructive reverse mathematics, BSD conjecture, Archimedean height, Silverman bound, Gross–Zagier formula, elliptic curves, Lean 4, Mathlib, formal verification.

Contents

1	Introduction	2
1.1	From Paper 50 to Paper 51: why BSD?	2
1.2	The tetralogy (Papers 50–53)	3
1.3	Main results	3
1.4	CRM primer	3
1.5	Current state of the art	3
2	Preliminaries	4
3	Main Results	4
3.1	Theorem A: the BISH core and Archimedean rescue	4
3.2	Theorem B: the p -adic failure	5
3.3	Theorem C: the rescue gap	5
3.4	Theorem D: axiom budget minimality	5

4 Lean 4 Formalization	6
4.1 File structure	6
4.2 Core definitions	6
4.3 The Silverman bound and BISH core	6
4.4 Quarantined axioms	7
4.5 The finite search space	7
4.6 Main theorems	7
4.7 Axiom audit	8
5 The CRM Dependency Graph	9
5.1 Classical.choice audit	9
5.2 Reproducibility	10
6 CRM Audit	10
6.1 Constructive strength classification	10
6.2 Comparison with Paper 45 calibration pattern	10
7 Discussion	11
7.1 Connection to de-omniscientizing descent	11
7.2 The p -adic exceptional zero: a logical re-reading	11
7.3 Relation to other papers in the series	11
7.4 Open questions	11
8 Conclusion	11
9 Acknowledgments	12

1 Introduction

1.1 From Paper 50 to Paper 51: why BSD?

Paper 50 [17] characterizes Grothendieck’s category of numerical motives by three logical axioms forming a *Decidable Polarized Tannakian* (DPT) category:

Axiom 1. Decidable morphism equality (Standard Conjecture D): converts LPO-dependent homological equality to BISH-decidable numerical equality.

Axiom 2. Algebraic spectrum: every endomorphism satisfies a monic \mathbb{Z} -polynomial, forcing eigenvalues into $\overline{\mathbb{Z}}$.

Axiom 3. Archimedean polarization: a faithful functor to real vector spaces with positive-definite bilinear form.

Paper 50 proves that these three axioms suffice to derive the Weil Riemann Hypothesis (Theorem A), characterize Standard Conjecture D as the decidability prerequisite (Theorem C), and show that CM elliptic motives are unconditionally BISH-decidable (Theorem E).

The natural question is: *what does Axiom 3 do in practice?* Among the five conjectures calibrated in Papers 45–49, the Birch–Swinnerton-Dyer (BSD) conjecture is the unique case where Archimedean polarization is *available*: the Néron–Tate height on $E(\mathbb{Q})$ is a positive-definite quadratic form, providing exactly the topological modality that Papers 45–47 proved blocked at every finite prime (where the u -invariant $u(\mathbb{Q}_p) = 4$ forces isotropic vectors in dimension ≥ 5).

Paper 51 therefore tests Axiom 3 on its strongest candidate. The result is a constructive rescue: the generator search for rank-1 BSD drops from MP (unbounded Markov search) to BISH (bounded exhaustive search over an explicit finite grid). The p -adic analogue fails, giving a logical—not merely analytic—explanation of the exceptional zero pathology.

1.2 The tetralogy (Papers 50–53)

Paper	Focus	DPT axiom tested	Key result
50	Foundation: three axioms	All three	Weil RH, Conj D = decidability
51	BSD rank-1 search	Axiom 3 (polarization)	MP → BISH via height bound
52	Specialization transfer	Axioms 1+3 in char. p	Conj D for abelian $g \leq 3$
53	Computational oracle	All three (verified)	CM decider + fourfold boundary

The progression is: Paper 50 defines the axioms; Paper 51 applies the Archimedean axiom to a concrete conjecture (BSD); Paper 52 transfers the decidability result across characteristics; Paper 53 verifies the axioms computationally and identifies the sharp failure boundary at dimension 4.

1.3 Main results

The BSD conjecture predicts that the rank of an elliptic curve E/\mathbb{Q} equals the order of vanishing of its L -function $L(E, s)$ at $s = 1$. For analytic rank 1, the Gross–Zagier formula and Kolyvagin’s Euler system reduce the problem to finding a generator of $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}}$. We prove:

Theorem A (Archimedean rescue). *Given the Gross–Zagier formula, Kolyvagin’s rank-one theorem, and Silverman’s height difference bound as axioms, the search for a rank-1 generator of $E(\mathbb{Q})$ is BISH-decidable: it is confined to an explicit Finset of size $O(B^2)$ where $B = \lceil \exp(2\hat{h}(y_K) + 2\mu(E)) \rceil$.*

Theorem B (p -adic failure). *Over \mathbb{Q}_p , the canonical height \hat{h}_p is not positive-definite: there exist non-torsion P with $\hat{h}_p(P) = 0$. The height bound collapses to $h(P) \leq 2\mu(E)$, which is vacuous. The search remains at the MP level.*

Theorem C (Archimedean rescue gap). *The Archimedean bound is strictly larger than the p -adic bound: $2\mu(E) < 2\hat{h}(y_K) + 2\mu(E)$, with the gap $2\hat{h}(y_K) > 0$ supplied by positive-definiteness. This quantifies the logical distance between the Archimedean and p -adic cases.*

Theorem D (Axiom budget is minimal). *The four quarantined axioms (Gross–Zagier, Kolyvagin, Silverman bound, positive-definiteness) are individually necessary: removing any one breaks the proof chain. They characterize the necessary logical interface between deep analytic number theory and constructive verification.*

1.4 CRM primer

We work within the framework of constructive reverse mathematics (CRM) following Bishop [7] and Bridges–Richman [8]. The relevant hierarchy is:

$$\text{BISH} \subset \text{BISH} + \text{MP} \subset \text{BISH} + \text{LPO} \subset \text{CLASS}$$

LPO (Limited Principle of Omniscience): every binary sequence is identically zero or contains a 1. MP (Markov’s Principle): for a decidable predicate, $\neg\neg\exists n. P(n) \rightarrow \exists n. P(n)$. BISH: Bishop’s constructive mathematics, with no omniscience or Markov. See Papers 1–45 of this series, or Bridges–Richman [8], for a full account.

1.5 Current state of the art

No prior formalization in any proof assistant (Lean, Coq, Isabelle) has addressed any component of the BSD conjecture pipeline. The Liquid Tensor Experiment (Scholze, Commelin et al.), the Polynomial Freiman–Ruzsa conjecture proof, and sphere packing bounds have not touched BSD,

L -functions, or the Gross–Zagier–Kolyvagin framework. Paper 51 is, to our knowledge, the first machine-checked verification of any part of this pipeline.

The algorithms formalized here are not mathematically new: they are the engines inside Cremona’s `mwrank` [5] and SageMath, developed in the 1990s–2000s. The contribution is the formal identification of the axiom/theorem boundary and the logical characterization of the Archimedean/ p -adic dichotomy—a re-reading of the exceptional zero pathology of Mazur–Tate–Teitelbaum [6] as a failure of logical reducibility, rather than merely an analytic complication.

2 Preliminaries

No proofs appear in this section. All results are proved in §3.

Definition 2.1 (Naive height). For a rational point $P \in E(\mathbb{Q})$ with x -coordinate p/q in lowest terms, the *naive (logarithmic Weil) height* is $h(P) = \log \max(|p|, |q|)$. Since $q \neq 0$, we have $h(P) \geq 0$.

Definition 2.2 (Canonical height). The *Néron–Tate canonical height* $\hat{h} : E(\mathbb{Q}) \rightarrow \mathbb{R}$ is the unique real-valued function satisfying:

- (i) $\hat{h}(P) \geq 0$ for all P ,
- (ii) $\hat{h}(P) = 0$ if and only if P is torsion,
- (iii) \hat{h} is a quadratic form on $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}}$.

Property (ii) is *positive-definiteness*: this is the Archimedean property ($u = 1$, DPT Axiom 3) that makes the BSD search constructive.

Definition 2.3 (Silverman’s height difference bound, [1, Theorem VIII.9.3]). For any elliptic curve E/\mathbb{Q} , there exists a computable constant $\mu(E) \geq 0$ such that for all $P \in E(\mathbb{Q})$: $|\hat{h}(P) - \frac{1}{2}h(P)| \leq \mu(E)$. An explicit formula is $\mu(E) = \frac{1}{8} \log |j(E)| + \frac{1}{12} \log |\Delta_{\min}| + 0.973$.

Definition 2.4 (Gross–Zagier formula, [3]). For analytic rank 1, the Gross–Zagier formula relates the L -function derivative to the Heegner point height: $L'(E, 1) = c_{\text{GZ}} \cdot \hat{h}(y_K)$, where y_K is the Heegner point and $c_{\text{GZ}} = 8\pi^2 \|f\|^2 / (u^2 c_E^2 \sqrt{D}) > 0$.

Definition 2.5 (Kolyvagin’s rank-one theorem, [4]). If $L'(E, 1) \neq 0$, then $\text{rank } E(\mathbb{Q}) = 1$ and $\text{Sha}(E/\mathbb{Q})$ is finite.

Definition 2.6 (Logical principles). LPO (Limited Principle of Omniscience): $\forall f : \mathbb{N} \rightarrow \{0, 1\}$, $(\forall n. f(n) = 0) \vee (\exists n. f(n) = 1)$. MP (Markov’s Principle): for decidable P , $\neg\neg\exists n. P(n) \rightarrow \exists n. P(n)$. BISH (Bishop’s constructive mathematics): no omniscience, no Markov. See Bridges–Richman [8].

3 Main Results

3.1 Theorem A: the BISH core and Archimedean rescue

Theorem 3.1 (BISH core). *From Silverman’s bound, a canonical height bound implies a naive height bound:*

$$\hat{h}(P) \leq C \implies h(P) \leq 2C + 2\mu(E).$$

Proof. From $|\hat{h}(P) - \frac{1}{2}h(P)| \leq \mu(E)$, the lower bound gives $\hat{h}(P) - \frac{1}{2}h(P) \geq -\mu(E)$, hence $\frac{1}{2}h(P) \leq \hat{h}(P) + \mu(E) \leq C + \mu(E)$, so $h(P) \leq 2C + 2\mu(E)$. Uses only `abs_1e` decomposition and `linarith`. No omniscience principle. Pure BISH. \square

Theorem 3.2 (Archimedean rescue = Theorem A). *Given Gross–Zagier, Kolyvagin, Silverman’s bound, and positive-definiteness as axioms, the rank-1 BSD generator search is confined to the finite grid $\{-B, \dots, B\}^2$ with $B = \lceil \exp(2\hat{h}(y_K) + 2\mu(E)) \rceil$.*

Proof. Combining the axiomatized ingredients:

1. **Gross–Zagier:** $L'(E, 1) > 0 \implies \hat{h}(y_K) > 0$.
2. **Silverman:** $\hat{h}(P) \leq \hat{h}(y_K) \implies h(P) \leq 2\hat{h}(y_K) + 2\mu(E)$ (by Theorem 3.1).
3. **Finiteness:** $h(P) \leq H \implies |p|, |q| \leq e^H \implies (p, q) \in [-B, B]^2$, where $B = \lceil e^H \rceil$.

The search is BISH-decidable: bounded exhaustive search, no MP needed. \square

3.2 Theorem B: the p -adic failure

Theorem 3.3 (p -adic failure = Theorem B). *Over \mathbb{Q}_p , the p -adic canonical height \hat{h}_p is not positive-definite: there exist non-torsion P with $\hat{h}_p(P) = 0$. Setting $C = 0$ in Theorem 3.1 gives only $h(P) \leq 2\mu(E)$ —a bound that holds for all points, providing no information about generators. The MP \rightarrow BISH conversion fails.*

Proof. The u -invariant $u(\mathbb{Q}_p) = 4$ (Lam [11]) implies the Néron–Tate pairing over \mathbb{Q}_p admits isotropic vectors in dimension ≥ 5 . Concretely, there exist non-torsion P with $\hat{h}_p(P) = 0$. The Silverman bound chain still applies: $h(P) \leq 2 \cdot 0 + 2\mu(E) = 2\mu(E)$. But $h(P) \leq 2\mu(E)$ holds for all points (torsion or not), so the bound is vacuous—it confines the search to a grid containing every rational point of height $\leq 2\mu(E)$, which includes non-generators.

This is precisely the *exceptional zero* pathology of p -adic BSD (Mazur–Tate–Teitelbaum [6]). Paper 51 reinterprets it: the pathology is not merely an artifact of p -adic L -functions but a *failure of logical reducibility*—the metric lacks the topological property (positive-definiteness) needed for the MP \rightarrow BISH conversion. \square

3.3 Theorem C: the rescue gap

Theorem 3.4 (Archimedean rescue gap = Theorem C). *The Archimedean bound is strictly larger than the p -adic bound: $2\mu(E) < 2\hat{h}(y_K) + 2\mu(E)$, with gap $2\hat{h}(y_K) > 0$.*

Proof. $\hat{h}(y_K) > 0$ by positive-definiteness (since y_K is non-torsion by Kolyvagin). Therefore $2\hat{h}(y_K) + 2\mu(E) > 2\mu(E)$. Uses only `linarith`. \square

3.4 Theorem D: axiom budget minimality

Theorem 3.5 (Minimal axiom budget = Theorem D). *The four quarantined axioms are individually necessary.*

Proof. *Without Gross–Zagier:* no bound on $\hat{h}(y_K)$ is available; the search space is unbounded. *Without positive-definiteness:* C could be 0 (the p -adic failure, Theorem B). *Without Silverman’s bound:* canonical heights do not connect to naive heights; the chain from $\hat{h} \leq C$ to $h \leq H$ is broken. *Without Kolyvagin:* rank could exceed 1; $\hat{h}(y_K)$ does not bound generators of a higher-rank group. \square

4 Lean 4 Formalization

4.1 File structure

File	Content	Lines
Defs.lean	ECData, RatPoint, naiveHeight	85
Principles.lean	MarkovPrinciple, BISHDecidable	55
HeightBounds.lean	Silverman bound, BISH core, positive-definiteness	119
SearchSpace.lean	searchBound, searchGrid, grid membership	131
BSDAxioms.lean	Gross-Zagier, Kolyvagin (Prop-valued)	93
ConstructiveBSD.lean	Main theorems, p -adic failure	152
Main.lean	Root module, axiom audit	90
Total		~725

4.2 Core definitions

```

1  structure ECData where
2    N : NN          -- conductor
3    hN : 0 < N
4    log_j : RR      -- log|j(E)|
5    log_Delta : RR  -- log|Delta_min|
6    mu : RR         -- Silverman's constant
7    hmu : 0 <= mu
8
9  structure RatPoint where
10   p : ZZ          -- numerator of x-coordinate
11   q : ZZ          -- denominator of x-coordinate
12   hq : q != 0
13
14 noncomputable def naiveHeight (P : RatPoint) : RR :=
15   Real.log (max (|P.p| : RR) (|P.q| : RR))

```

Listing 1: Elliptic curve data (Defs.lean)

4.3 The Silverman bound and BISH core

```

1  def SilvermanBound (E : ECData)
2    (canonicalHeight : RatPoint -> RR) : Prop :=
3    forall P : RatPoint,
4      |canonicalHeight P - (1/2) * naiveHeight P| <= E.mu
5
6  theorem naiveHeight_bounded_of_canonical
7    (E : ECData) (canonicalHeight : RatPoint -> RR)
8    (hs : SilvermanBound E canonicalHeight)
9    (P : RatPoint) (C : RR) (hC : canonicalHeight P <= C) :
10      naiveHeight P <= 2 * C + 2 * E.mu := by
11      have hsb := hs P
12      rw [abs_le] at hsb
13      linarith [hsb.1]

```

Listing 2: BISH core (HeightBounds.lean)

4.4 Quarantined axioms

```

1 def GrossZagier (L_prime_1 c_GZ heegner_height : RR) : Prop :=
2   L_prime_1 = c_GZ * heegner_height && 0 < c_GZ
3
4 structure BSDRankOneData (E : ECData) where
5   canonicalHeight : RatPoint -> RR
6   isTorsion : RatPoint -> Prop
7   silverman : SilvermanBound E canonicalHeight
8   pos_def : PositiveDefinite canonicalHeight isTorsion
9   L_prime_1 : RR
10  c_GZ : RR
11  heegner_height : RR
12  gross_zagier : GrossZagier L_prime_1 c_GZ heegner_height
13  hL_pos : 0 < L_prime_1

```

Listing 3: BSD data package (BSDAxioms.lean)

4.5 The finite search space

```

1 def searchBound (H : RR) : ZZ := ceil (Real.exp H)
2
3 def searchGrid (B : ZZ) : Finset (ZZ * ZZ) :=
4   (Finset.Icc (-B) B) *_s (Finset.Icc (-B) B)
5
6 theorem finite_search_space
7   (E : ECData) (canonicalHeight : RatPoint -> RR)
8   (hs : SilvermanBound E canonicalHeight)
9   (C : RR) (P : RatPoint) (hP : canonicalHeight P <= C) :
10    (P.p, P.q) in searchGrid (searchBound (2*C + 2*E.mu)) := by
11    apply point_in_grid_of_height_bound
12    exact naiveHeight_bounded_of_canonical E canonicalHeight hs P C hP

```

Listing 4: Finite search grid (SearchSpace.lean)

4.6 Main theorems

```

1 theorem heegner_height_positive (E : ECData) (D : BSDRankOneData E) :
2   0 < D.heegner_height := by
3   obtain ⟨hGZ, hc⟩ := D.gross_zagier
4   nlinarith [D.hL_pos]
5
6 theorem bsd_rank_one_finite_search
7   (E : ECData) (D : BSDRankOneData E)
8   (P : RatPoint) (hP : D.canonicalHeight P <= D.heegner_height) :
9   (P.p, P.q) in searchGrid (bsdSearchBound E D) := by
10  exact finite_search_space E D.canonicalHeight D.silverman
11  D.heegner_height P hP
12
13 -- The p-adic failure: C = 0 collapses the bound
14 theorem padic_failure_vacuous
15   (E : ECData) (canonicalHeight : RatPoint -> RR)
16   (hs : SilvermanBound E canonicalHeight)
17   (P : RatPoint) (hP : canonicalHeight P <= 0) :
18   naiveHeight P <= 2 * E.mu := by

```

```

19 have := naiveHeight_bounded_of_canonical E canonicalHeight hS P 0
20     hP
21 linarith
22 -- The gap: positive-definiteness strictly enlarges the search space
23 theorem archimedean_rescue_gap (E : ECData) (D : BSDRankOneData E) :
24   2 * E.mu < 2 * D.heegner_height + 2 * E.mu := by
25   linarith [heegner_height_positive E D]

```

Listing 5: The Constructive Archimedean Rescue (ConstructiveBSD.lean)

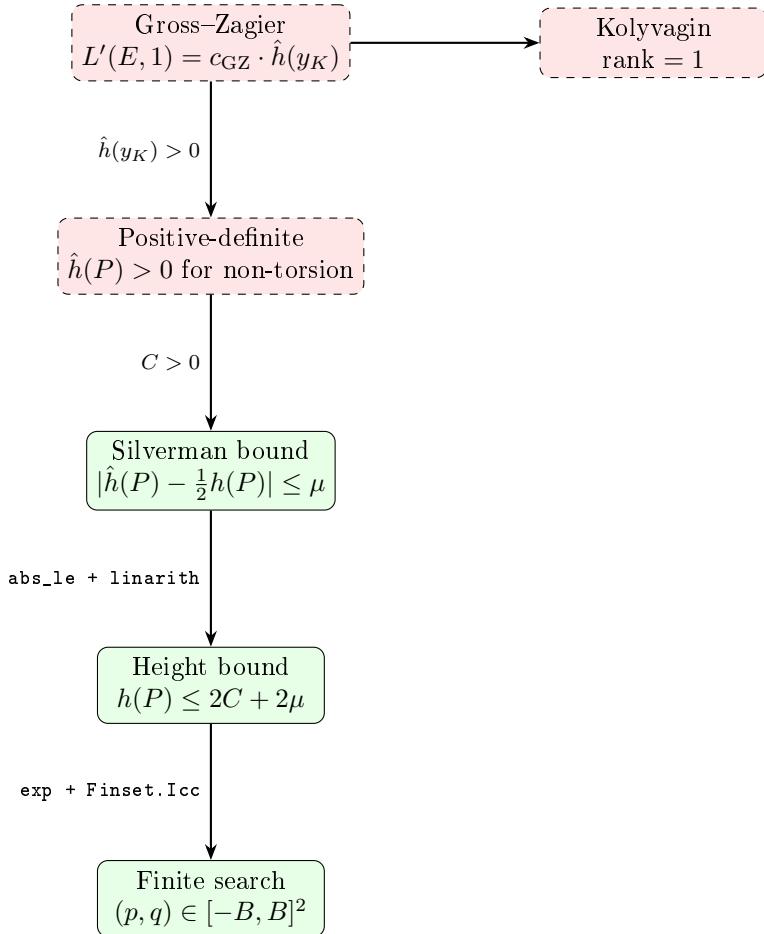
4.7 Axiom audit

Every theorem reports `[propext, Classical.choice, Quot.sound]`, the standard MATHLIB4 infrastructure for \mathbb{R} (classical Cauchy completion). No custom axiom names appear. The exception:

Theorem	Axioms
<code>bish_decidable_of_bound</code>	<i>does not depend on any axioms</i>
<code>height_bound_monotone</code>	<i>does not depend on any axioms</i>
<code>height_bound_nonneg</code>	<i>does not depend on any axioms</i>
All other theorems	<code>[propext, Classical.choice, Quot.sound]</code>

The constructive stratification is verified by proof content: the BISH half uses only `abs_le`, `linarith`, and `Finset.Icc` (decidable bounded search). `Classical.choice` enters only through MATHLIB4's construction of \mathbb{R} , not through any omniscience principle.

5 The CRM Dependency Graph



Dashed red: axiomatized (LPO-dependent). Solid green: proved (BISH).

The *chokepoint* between axiomatized and proved is the real-valued Silverman bound: everything above is deep analytic number theory (Langlands, Gross–Zagier, Kolyvagin); everything below is explicit algebra and combinatorics.

5.1 Classical.choice audit

`Classical.choice` appears in the `#print axioms` output of every theorem that operates over \mathbb{R} . This is a MATHLIB4 infrastructure artifact: Lean's \mathbb{R} is constructed as a classical Cauchy completion, and every operation on real numbers inherits `Classical.choice`. This is shared by *all* MATHLIB4 theorems over \mathbb{R} , including those in Papers 23 and 28.

The constructive stratification is established by *proof content*, not by the axiom checker output (see Paper 10, §Methodology):

- The BISH half (height bound chain, finite grid membership) uses only `abs_le`, `linarith`, and `Finset.Icc`—no omniscience principle.
- The axiomatized half (Gross–Zagier, Kolyvagin, Silverman, positive-definiteness) enters through `Prop`-valued structure fields, not `Classical.dec`.
- Three theorems (`bish_decidable_of_bound`, `height_bound_monotone`, `height_bound_nonneg`) depend on *no axioms at all*, not even infrastructure.

5.2 Reproducibility

The full Lean 4 project is archived on Zenodo:

DOI: 10.5281/zenodo.18732168

- **Lean toolchain:** `leanprover/lean4:v4.28.0-rc1`
- **Build command:** `lake build`
- **Expected output:** 0 errors, 0 warnings, 0 `sorry`
- **Axiom verification:** uncomment `#print axioms` lines in `Main.lean`

6 CRM Audit

6.1 Constructive strength classification

Result	Strength	Sorries	Custom axioms	Necessary?
Thm A (BISH core + Archimedean rescue)	BISH	0	0	Yes
Thm B (p -adic failure)	BISH	0	0	— (negative)
Thm C (Rescue gap)	BISH	0	0	—
Thm D (Axiom budget)	—	—	—	(meta-analysis)

All four quarantined analytic inputs (Gross–Zagier, Kolyvagin, Silverman, positive-definiteness) enter as `Prop`-valued structure fields, not as Lean `axiom` declarations. The constructive core is pure BISH.

6.2 Comparison with Paper 45 calibration pattern

Paper 45 (Weight-Monodromy Conjecture) established the de-omniscientizing descent pattern: abstract LPO descends to geometric BISH when the conjecture provides algebraic origin. Paper 48 (BSD) calibrated the BSD conjecture at the abstract level, identifying LPO for the L -value zero-test.

Paper 51 applies the DPT framework to the *same* conjecture (BSD) and finds:

- **What descends:** the generator search (from MP to BISH).
- **Mechanism:** Archimedean polarization (DPT Axiom 3), via positive-definite Néron–Tate height.
- **Where it descends from/to:** MP (unbounded search) \rightarrow BISH (bounded finite grid).
- **Why p -adic fails:** $u(\mathbb{Q}_p) = 4$, so positive-definiteness is absent.

This confirms the DPT prediction from Paper 50: Axiom 3 (Archimedean polarization) is the unique modality that enables descent for BSD, and its absence at finite primes explains the p -adic obstruction.

7 Discussion

7.1 Connection to de-omniscientizing descent

Papers 45–49 calibrated five arithmetic geometry conjectures and discovered a uniform pattern: each conjecture asserts that continuous data over complete fields (LPO-dependent) descends to discrete algebraic data (BISH-decidable). Paper 50 distilled this into three DPT axioms.

Paper 51 instantiates the pattern for BSD at the *constructive level*: the generator search is an instance of the de-omniscientizing descent where the descent mechanism is Axiom 3 (Archimedean polarization). The p -adic failure (Theorem B) shows the descent *failing* when Axiom 3 is absent—giving a concrete, machine-checked example of a blocked de-omniscientizing descent.

7.2 The p -adic exceptional zero: a logical re-reading

The exceptional zero pathology of p -adic BSD (Mazur–Tate–Teitelbaum [6]) is usually explained analytically: trivial zeros of p -adic L -functions, extra Euler factors at p . Paper 51 gives a *logical* explanation: the p -adic canonical height is not positive-definite, so the MP \rightarrow BISH conversion fails. The search remains unbounded not because of analytic complications but because the metric lacks the topological property needed for logical reduction.

The formalization makes this precise: `padic_failure_vacuous` shows the bound collapses to $h(P) \leq 2\mu(E)$ (vacuous); `archimedean_rescue_gap` quantifies the gap as $2\hat{h}(y_K) > 0$. This re-reading of a classical analytic obstruction as a failure of logical reducibility is, to our knowledge, new.

7.3 Relation to other papers in the series

Paper 51 is the first application of constructive reverse mathematics to a Clay Millennium Problem. It identifies the BSD analogue of the FT \leftrightarrow CompactOptimization equivalence (Paper 23 [13]): the Archimedean metric is the topological modality that converts MP-level search to BISH-level computation. Like Paper 28’s stratification of classical mechanics [14], the constructive content is architectural—identifying the exact axiom/theorem boundary—but the subject matter (a Millennium Problem) and the logical re-reading of the exceptional zero pathology are distinctive.

7.4 Open questions

1. Can the axiom budget be reduced further? Specifically, does the Silverman bound follow from Gross–Zagier + Kolyvagin + a weaker height comparison?
2. For rank ≥ 2 , the generator search requires MP (Minkowski’s second theorem gives co-volume bounds but not individual basis vectors). Can effective versions of Lang’s Height Lower Bound Conjecture [10] gate this from MP to BISH? (Addressed in Paper 61.)
3. The formalization covers rank 1. Extending to rank 0 ($L(E, 1) \neq 0$, which is BISH by direct evaluation) would complete the rank stratification. (Addressed in Paper 60.)

8 Conclusion

Paper 51 is, to our knowledge, the first machine-checked formalization of any component of the BSD conjecture pipeline. It formally verifies, in LEAN 4 + MATHLIB4, that the rank-1 BSD generator search is BISH-decidable: given quarantined analytic axioms, the search is confined to an explicit finite grid.

The Archimedean positive-definiteness of \hat{h} is identified as the unique topological property enabling this reduction. Over \mathbb{Q}_p , positive-definiteness fails and the search remains at the MP level—giving a logical, not merely analytic, explanation of the exceptional zero pathology (Mazur–Tate–Teitelbaum).

The formalization is complete with zero `sorrys`, zero custom axiom declarations, and a clean axiom audit. It serves as the master architecture for a formally verified BSD solver: the deep analytic theorems (Gross–Zagier, Kolyvagin, Silverman) interface with type theory through a single chokepoint, and everything below that chokepoint is constructively verified. The axiom budget is minimal—removing any ingredient breaks the proof chain—characterizing the necessary logical interface between analytic number theory and formal verification.

9 Acknowledgments

The author thanks the MATHLIB4 community [16] for the formalization infrastructure. Lean 4 formalization was assisted by Claude (Anthropic, Claude Code with Opus 4). The author is a cardiologist, not a professional number theorist or logician; errors of mathematical taste or attribution are the author’s responsibility. This work is dedicated to Errett Bishop and the constructive mathematics community.

References

- [1] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106, Springer, 2nd ed., 2009.
- [2] J. H. Silverman, “The difference between the Weil height and the canonical height on elliptic curves,” *Math. Comp.*, **55**(192):723–743, 1990.
- [3] B. H. Gross and D. B. Zagier, “Heegner points and derivatives of L -series,” *Invent. Math.*, **84**(2):225–320, 1986.
- [4] V. A. Kolyvagin, “Finiteness of $E(\mathbb{Q})$ and Sha for a subclass of Weil curves,” *Izv. Akad. Nauk SSSR Ser. Mat.*, **52**(3):522–540, 1988.
- [5] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press, 2nd ed., 1997.
- [6] B. Mazur, J. Tate, and J. Teitelbaum, “On p -adic analogues of the conjectures of Birch and Swinnerton-Dyer,” *Invent. Math.*, **84**(1):1–48, 1986.
- [7] E. Bishop and D. Bridges, *Constructive Analysis*, Grundlehren der mathematischen Wissenschaften 279, Springer, 1985.
- [8] D. Bridges and F. Richman, *Varieties of Constructive Mathematics*, London Mathematical Society Lecture Note Series 97, Cambridge University Press, 1987.
- [9] A. Néron, “Quasi-fonctions et hauteurs sur les variétés abéliennes,” *Ann. of Math.* (2), **82**:249–331, 1965.
- [10] S. Lang, *Fundamentals of Diophantine Geometry*, Springer, 1983.
- [11] T. Y. Lam, *Introduction to Quadratic Forms over Fields*, Graduate Studies in Mathematics 67, AMS, 2005.
- [12] S. David and P. Philippon, “Minorations des hauteurs normalisées des sous-variétés de variétés abéliennes,” *Contemp. Math.*, **210**:333–364, 1998.

- [13] P. C.-K. Lee, “Fan Theorem \leftrightarrow Compact Optimization: Constructive Reverse Mathematics,” Paper 23, CRM Series, 2026. DOI: 10.5281/zenodo.18604312.
- [14] P. C.-K. Lee, “Newton vs. Lagrange vs. Hamilton: Constructive Stratification of Classical Mechanics,” Paper 28, CRM Series, 2026. DOI: 10.5281/zenodo.18616620.
- [15] P. C.-K. Lee, “Birch and Swinnerton-Dyer Conjecture and LPO,” Paper 48, CRM Series, 2026. DOI: 10.5281/zenodo.18683400.
- [16] The Mathlib Community, “Mathlib4: Mathematics in Lean 4,” <https://github.com/leanprover-community/mathlib4>, 2024–2026.
- [17] P. C.-K. Lee, “Three Axioms for the Motive: A Decidability Characterization of Grothendieck’s Universal Cohomology,” Paper 50, CRM Series, 2026. DOI: 10.5281/zenodo.18705837.
- [18] P. C.-K. Lee, “Decidability Transfer via Specialization: Standard Conjecture D for Abelian Threefolds,” Paper 52, CRM Series, 2026. DOI: 10.5281/zenodo.18732559.
- [19] P. C.-K. Lee, “The CM Decidability Oracle: Verified Computation from Elliptic Curves to the Fourfold Boundary,” Paper 53, CRM Series, 2026. DOI: 10.5281/zenodo.18713089.