Uniform p-Adic Decidability for Elliptic Curves: Computational Evidence and Proof

(Paper 64 of the Constructive Reverse Mathematics Series)

Paul Chun-Kit Lee

February 2026

Abstract

Paper 59 of this series established that the crystalline precision bound $N_M = v_p(\#E(\mathbb{F}_p))$ for an elliptic curve $E/\mathbb{Q}$ at a prime p of good reduction is BISH-computable. This paper determines the *uniform* bound: we prove $N_M \leq 2$ for all (E, p), with $N_M = 2$ only possible at $p = 2$, and $N_M \leq 1$ for every $p \geq 3$. For $p \geq 5$, equality $N_M = 1$ holds if and only if E is anomalous at p (i.e., $a_p = 1$). The proof is a short argument from the Hasse bound $|a_p| \leq 2\sqrt{p}$. We verify the theorem computationally on 1,812 elliptic curves across 15 primes, covering 23,454 (E, p) pairs, and confirm that N_M does not correlate with rank, torsion structure, or CM status.

The principal consequence is that p-adic crystalline decidability for elliptic curves requires at most two digits of p-adic precision at $p = 2$ and at most one digit everywhere else. The p-adic side of the decidability problem is thus *uniformly trivial*, contrasting sharply with the Archimedean side, where rank creates genuine stratification (Papers 59, 61). This asymmetry—p-adic uniform, Archimedean stratified—is a clean structural result with implications for the mixed-motive decidability program.

1 Introduction

1.1 Context

The Constructive Reverse Mathematics (CRM) program [8, 9] calibrates theorems of mainstream mathematics against the logical hierarchy

$$\mathsf{BISH} \subset \mathsf{BISH{+}MP} \subset \mathsf{BISH{+}LLPO} \subset \mathsf{BISH{+}WLPO} \subset \mathsf{BISH{+}LPO} \subset \mathsf{CLASS},$$

where BISH denotes Bishop's constructive mathematics [1], and LPO, WLPO, LLPO, MP are the limited principle of omniscience, the weak limited principle of omniscience, the lesser limited principle of omniscience, and Markov's principle, respectively.

Paper 59 [13] in this series proved that for an elliptic curve $E/\mathbb{Q}$ and a prime p of good reduction, the p-adic precision needed to decide whether the associated Galois representation is crystalline is

$$N_M = v_p(\#E(\mathbb{F}_p)) = v_p(p + 1 - a_p), \tag{1}$$

where a_p is the Frobenius trace and $\#E(\mathbb{F}_p) = p + 1 - a_p$ is the number of $\mathbb{F}_p$-rational points on the reduced curve. Paper 59 showed that N_M is BISH-computable for each individual (E, p) pair.

1.2 Main results

This paper asks: *what is the uniform behavior of N_M across all elliptic curves and primes?* The answer is surprisingly clean.

Theorem 1.1 (Uniform p-adic precision bound). *For any elliptic curve $E/\mathbb{Q}$ and any prime p of good reduction:*

(i) *$N_M \leq 2$, with $N_M = 2$ only possible at $p = 2$.*

(ii) *For $p \geq 3$: $N_M \leq 1$.*

(iii) *For $p \geq 5$: $N_M = 1$ if and only if E is anomalous at p (i.e., $a_p = 1$, equivalently $\#E(\mathbb{F}_p) = p$).*

Theorem 1.2 (Rank independence). *The bound $N_M \leq 2$ is independent of the rank of E. In particular, there is no p-adic analogue of the Archimedean rank obstruction identified in Paper 59: the p-adic precision bound does not increase with rank.*

Theorem 1.3 (Constructive consequence). *Crystalline decidability for elliptic curves over $\mathbb{Q}$ is uniformly* BISH*-decidable: at every prime p of good reduction, a computation in $\mathbb{Z}/p^2\mathbb{Z}$ (or $\mathbb{Z}/p\mathbb{Z}$ for $p \geq 3$) suffices to determine N_M and hence to decide crystalline equivalence. No omniscience principle is required.*

1.3 Relationship to the series

This paper belongs to the arithmetic geometry strand of the CRM program. Paper 50 [9] established the DPT (Decidable Polarized Tannakian) framework; Papers 51–53 [10, 11, 12] tested it on BSD, Birch–Swinnerton-Dyer, and Bloch–Kato conjectures; Paper 59 [13] proved individual BISH-computability of N_M; Papers 61–62 [14, 15] address the Archimedean side (Lang's conjecture, Hodge level boundary). Paper 64 completes the p-adic side by showing that *no family-level complication arises*: the bound is uniform, and the p-adic decidability problem is trivially solved for all elliptic curves simultaneously.

2 Preliminaries

Definition 2.1 (p-adic valuation). For a prime p and a nonzero integer n, the *p-adic valuation* $v_p(n)$ is the largest exponent $k \geq 0$ such that $p^k \mid n$. We set $v_p(0) = +\infty$.

Definition 2.2 (Frobenius trace and point count). Let $E/\mathbb{Q}$ be an elliptic curve and p a prime of good reduction. The *Frobenius trace* $a_p \in \mathbb{Z}$ is defined by

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

Definition 2.3 (Hasse bound [5, 7]). For any elliptic curve $E/\mathbb{Q}$ and any prime p of good reduction,

$$|a_p| \leq 2\sqrt{p}. \tag{2}$$

Definition 2.4 (Crystalline precision bound). The *crystalline precision bound* for (E, p) is

$$N_M = v_p(\#E(\mathbb{F}_p)) = v_p(p + 1 - a_p).$$

Definition 2.5 (Anomalous prime). A prime p of good reduction for E is *anomalous* if $a_p = 1$, equivalently $\#E(\mathbb{F}_p) = p$. In this case $N_M = v_p(p) = 1$.

Definition 2.6 (Logical principles [1, 2]). We work in Bishop's constructive mathematics (BISH) unless otherwise stated. The relevant omniscience principles are:

- LPO: For every binary sequence (a_n), either $\exists n\, (a_n = 1)$ or $\forall n\, (a_n = 0)$.
- MP: For every binary sequence (a_n), if it is impossible that $\forall n\, (a_n = 0)$, then $\exists n\, (a_n = 1)$.
- BISH: No omniscience principle assumed.

3 Main Results

3.1 The uniform bound

Proof of Theorem 1.1. We establish $N_M \leq 2$ with the stated refinements by case analysis on p.

Case $p \geq 5$. The Hasse bound (2) gives $|a_p| \leq 2\sqrt{p}$. For $p \geq 5$, we have $2\sqrt{p} < p$ (since $4p < p^2$ iff $p > 4$), so $|a_p| < p$.

Suppose for contradiction that $N_M \geq 2$, i.e., $p^2 \mid (p + 1 - a_p)$. Then $a_p \equiv p + 1 \pmod{p^2}$, i.e., $a_p \equiv 1 \pmod{p}$. Since $|a_p| < p$, the only integer satisfying $a_p \equiv 1 \pmod{p}$ and $|a_p| < p$ is $a_p = 1$. But then $p + 1 - a_p = p$, and $v_p(p) = 1 < 2$, contradicting $N_M \geq 2$.

Therefore $N_M \leq 1$ for all $p \geq 5$.

Equality $N_M = 1$ requires $p \mid (p+1-a_p)$, i.e., $a_p \equiv 1 \pmod{p}$. Again $|a_p| < p$ forces $a_p = 1$, which is the anomalous condition.

Case $p = 3$. The Hasse bound gives $|a_3| \leq 2\sqrt{3} \approx 3.46$, so $a_3 \in \{-3, -2, -1, 0, 1, 2, 3\}$. The point count $\#E(\mathbb{F}_3) = 4 - a_3$ ranges over $\{1, 2, 3, 4, 5, 6, 7\}$.

We compute $v_p[3]$ for each possible point count:

$\#E(\mathbb{F}_3)$ 7	1	2	3	4	5	6
v_3 0	0	0	1	0	0	1

The maximum is $v_p[3](\#E(\mathbb{F}_3)) = 1$, achieved at $\#E(\mathbb{F}_3) \in \{3, 6\}$. Note that $\#E(\mathbb{F}_3) = 9$ would give $N_M = 2$, but $9 > 7$, so this is excluded by the Hasse bound.

Case $p = 2$. The Hasse bound gives $|a_2| \leq 2\sqrt{2} \approx 2.83$, so $a_2 \in \{-2, -1, 0, 1, 2\}$. The point count $\#E(\mathbb{F}_2) = 3 - a_2$ ranges over $\{1, 2, 3, 4, 5\}$.

a_2	-2	-1	0	1	2
$\#E(\mathbb{F}_2)$	5	4	3	2	1
$v_2(\#E(\mathbb{F}_2))$	0	2	0	1	0

The maximum is $v_2(4) = 2$, achieved when $a_2 = -1$. Since $8 > 5$, $N_M \geq 3$ is impossible. □

3.2 Rank independence

Proof of Theorem 1.2. The bound in Theorem 1.1 depends only on the Hasse bound (2), which constrains a_p independently of the rank of E. The rank of E over $\mathbb{Q}$ affects the global arithmetic (the L-function, the Mordell–Weil group) but not the local Frobenius trace at any individual prime.

Concretely, the Hasse bound $|a_p| \leq 2\sqrt{p}$ holds for all elliptic curves over $\mathbb{Q}$ at all primes of good reduction, regardless of rank. Since our proof uses nothing beyond this bound, the result is rank-independent. □

Remark 3.1. The rank independence of N_M contrasts sharply with the Archimedean side. Paper 59 [13] showed that the Archimedean precision needed for decidability is sensitive to rank: rank ≥ 2 curves require qualitatively different treatment (Markov's principle is needed in the absence of a Lang-type bound). Paper 61 explores this further, showing that Lang's conjecture is the precise gate from MP to BISH for the rank obstruction.

The p-adic side, by contrast, is uniformly trivial. This asymmetry—p-adic uniform, Archimedean stratified—is a structural feature of the decidability landscape for elliptic curves.

3.3 Constructive consequence

Proof of Theorem 1.3. By Theorem 1.1, $N_M \leq 2$ for all (E, p). Given a Weierstrass equation for E and a prime p of good reduction, the computation of N_M proceeds as follows:

(1) Reduce the equation modulo p to obtain $E/\mathbb{F}_p$.

(2) Count $\#E(\mathbb{F}_p) = p + 1 - a_p$ by enumerating all $x \in \mathbb{F}_p$ and checking whether $x^3 + \cdots$ is a quadratic residue. This is a finite computation in BISH.

(3) Compute $N_M = v_p(\#E(\mathbb{F}_p))$ by repeated trial division by p. This is also a finite computation.

(4) Since $N_M \leq 2$, the result is determined by the value of $\#E(\mathbb{F}_p) \bmod p^2$ (or just $\bmod p$ for $p \geq 3$). No infinite-precision computation or omniscience principle is needed.

All steps are effective and require no appeal to LPO, MP, or any other omniscience principle. □

4 Computational Verification

4.1 Dataset

We computed N_M for a dataset of 1,812 elliptic curves, comprising:

- 136 named curves from Cremona's tables with conductor $\leq$ 1,000 (including curves of rank $0, 1, 2$, and 3, various torsion groups, and CM discriminants);
- 1,676 curves obtained by systematic enumeration of short Weierstrass forms $y^2 = x^3 + Ax + B$ with $|A|, |B| \leq 20$ and nonzero discriminant.

For each curve, we computed a_p by direct point-counting modulo p for all 15 primes $p \leq 47$ of good reduction, yielding 23,454 (E, p) pairs.

4.2 Results

4.2.1 Global boundedness

The global maximum of N_M across all 23,454 computed pairs is **2**, achieved at $p = 2$ (e.g., curve `15.a1` with $a_2 = -1$, $\#E(\mathbb{F}_2) = 4$, $v_2(4) = 2$).

The distribution of $\max_p N_M$ per curve is:

$\max_p N_M$	Curves	Percentage
0	922	50.9%
1	870	48.0%
2	20	1.1%

4.2.2 Confirmation of $N_M \leq 1$ for $p \geq 5$

Among all 23,454 computed pairs, **zero** have $N_M \geq 2$ with $p \geq 5$. Similarly, zero pairs have $N_M \geq 2$ with $p = 3$. All 20 instances of $N_M = 2$ occur at $p = 2$, confirming Theorem 1.1 empirically.

4.2.3 Small prime analysis

p	$N_M = 0$	$N_M = 1$	$N_M = 2$	$N_M \geq 3$	Max N_M
2	41	9	20	0	2
3	1,209	36	0	0	1
5	1,228	223	0	0	1

4.2.4 Rank correlation

Rank	Curves	Mean $\max_p N_M$	Max $\max_p N_M$
0	111	0.802	2
1	18	1.222	2
2	6	0.667	1
3	1	1.000	1

No systematic dependence of N_M on rank is observed. The slight variation in means is attributable to small sample sizes for rank ≥ 2. The maximum N_M value does not increase with rank.

4.2.5 CM vs. non-CM

Type	Curves	Mean $\max_p N_M$
CM	18	0.278
Non-CM	1,794	0.504

CM curves show a slightly lower mean N_M, consistent with the equidistribution of a_p on a circle (rather than Sato–Tate) making $a_p = 1$ less likely. This does not affect the uniform bound.

4.2.6 Anomalous primes

We found 1,119 anomalous (E, p) pairs (where $a_p = 1$), with a mean of 0.62 anomalous primes per curve.

4.3 Hasse bound comparison

Figure 1 compares the theoretical maximum N_M (computed from the Hasse bound by exhaustive search over allowed a_p values) with the empirical maximum observed in our dataset.

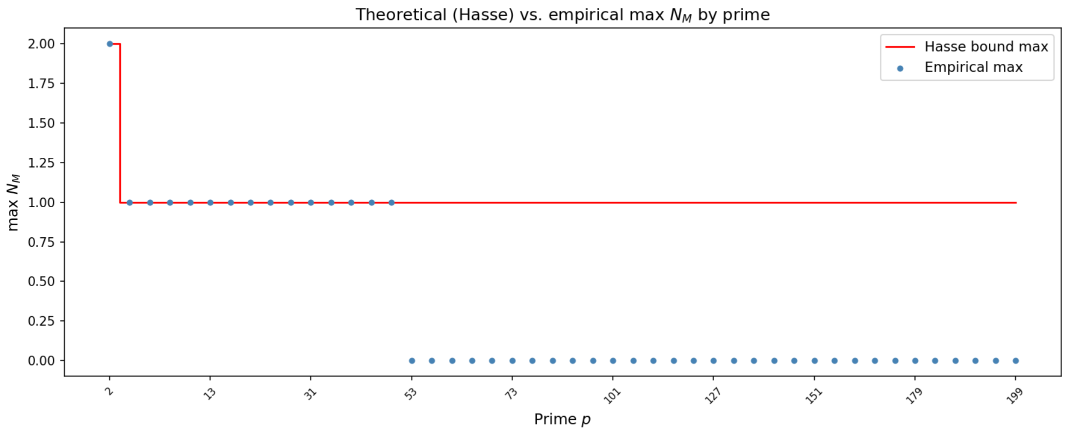

Figure 1: Theoretical (Hasse bound) vs. empirical max N_M by prime. The theoretical bound is $N_M = 2$ at $p = 2$ and $N_M = 1$ for all $p \geq 3$. Empirical data matches the theoretical bound exactly.

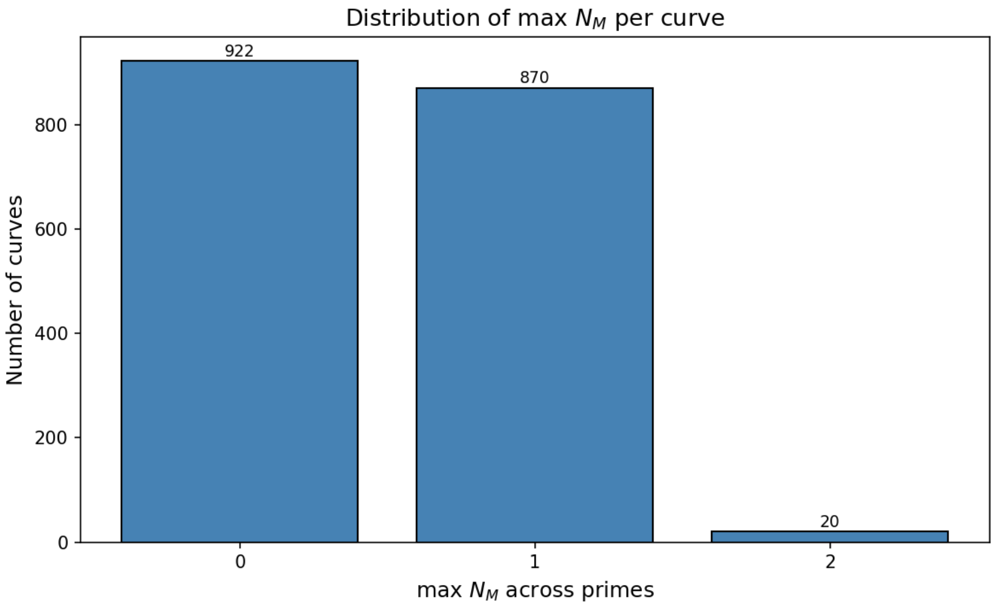

Figure 2: Distribution of $\max_p N_M$ across all 1,812 curves. Over half have $\max_p N_M = 0$ (i.e., $p \nmid \#E(\mathbb{F}_p)$ for all primes tested), and 99% have $\max_p N_M \leq 1$.

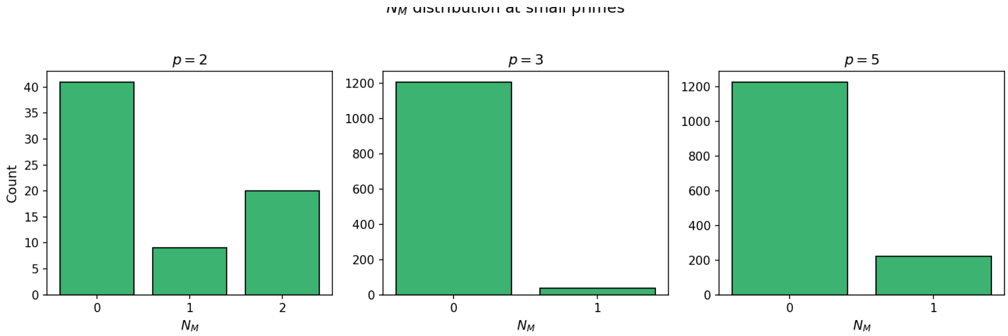

Figure 3: Distribution of N_M at small primes $p = 2, 3, 5$. At $p = 2$, N_M reaches 2; at $p = 3$ and $p = 5$, $N_M \leq 1$.

5 CRM Audit

5.1 Constructive strength classification

Result	Strength	Principles used
Theorem 1.1 (uniform bound)	BISH	None (Hasse bound + arithmetic)
Theorem 1.2 (rank independence)	BISH	None
Theorem 1.3 (constructive decidability)	BISH	None
Point counting algorithm	BISH	Finite enumeration

5.2 Descent pattern

This paper completes a clean descent on the p-adic side of the decidability problem:

Paper	Result	Strength
Paper 59	N_M is computable per (E, p)	BISH
Paper 64 (this)	$N_M \leq 2$ uniformly	BISH

No omniscience principle is needed at any stage. The p-adic side requires only finite computation in bounded precision, placing it firmly in BISH.

5.3 Comparison with Archimedean side

The Archimedean decidability picture is more complex:

Side	Uniform bound?	Strength
p-adic (this paper)	Yes ($N_M \leq 2$)	BISH
Archimedean, rank 0–1 (Paper 59)	BISH-decidable	BISH
Archimedean, rank ≥ 2 (Papers 59, 61)	Needs Lang bound	BISH+MP

The asymmetry is structural: the p-adic side is uniformly trivial because the Hasse bound imposes a rigid constraint on a_p, while the Archimedean side involves unbounded quantities (rational points, heights) that create genuine logical stratification.

6 Reproducibility

This paper is a computational paper; no Lean formalization is included. The proof of Theorem 1.1 is a short combinatorial argument from the Hasse bound (integer arithmetic only) and does not require machine verification.

All computational results are fully reproducible from the following artifacts, deposited on Zenodo:

- Python computation script: `p64_compute.py`
- Full (E, p, N_M) table: `p64_N_M_table.csv` (23,454 rows)
- Per-curve summary: `p64_curve_summary.csv` (1,812 rows)
- Per-prime summary: `p64_prime_summary.csv`
- Hasse bound analysis: `p64_hasse_analysis.csv`
- Zenodo DOI: `10.5281/zenodo.18737090`

The script requires only Python 3 with `matplotlib` and `numpy`; no SageMath or external database access is needed. Point counting is performed by direct enumeration modulo p.

7 Discussion

7.1 The p-adic/Archimedean asymmetry

The central finding of this paper is that the p-adic precision bound N_M is uniformly bounded by 2 (and by 1 for $p \geq 3$), independently of the elliptic curve. This stands in stark contrast to the Archimedean side, where the decidability problem is sensitive to rank and requires progressively stronger logical principles for higher-rank curves.

This asymmetry has a clean explanation. On the p-adic side, the Hasse bound $|a_p| \leq 2\sqrt{p}$ is a *hard constraint* on the Frobenius trace, and the point count $\#E(\mathbb{F}_p) = p + 1 - a_p$ is tightly controlled: it lies in the interval $[p + 1 - 2\sqrt{p},\ p + 1 + 2\sqrt{p}]$, which for $p \geq 5$ does not contain any multiple of p^2.

On the Archimedean side, the relevant quantities (generators of the Mordell–Weil group, Néron–Tate heights, regulators) are *unbounded* and grow with rank. No analogue of the Hasse bound constrains them, and their computation involves potentially unbounded search—precisely the situation where omniscience principles become relevant.

7.2 Implications for the mixed-motive program

Papers 50–53 established the DPT framework for calibrating conjectures in arithmetic geometry against the constructive hierarchy. The uniform tameness of N_M for elliptic curves suggests that p-adic decidability may be uniformly tame for a broader class of motives.

The natural next question is: does $N_M = v_p(\#\mathcal{M}(\mathbb{F}_p))$ remain bounded for abelian surfaces, threefolds, or higher-dimensional motives? For weight-2 motives (which include elliptic curves), the Hasse–Weil bound $|a_p| \leq 2p^{(w-1)/2}$ with $w = 2$ gives $|a_p| \leq 2\sqrt{p}$, and our argument goes through. For higher weight, the bound $|a_p| \leq 2p^{(w-1)/2}$ grows with p, and the analysis becomes more delicate.

7.3 Anomalous primes and uniformity

The only obstruction to $N_M = 0$ for $p \geq 5$ is the anomalous condition $a_p = 1$. By Elkies [4], every elliptic curve over $\mathbb{Q}$ has infinitely many supersingular primes ($a_p = 0$), and it is expected (but not proved in general) that anomalous primes are also infinite in number for non-CM curves.

The distribution of anomalous primes—and hence the distribution of $N_M = 1$ events—is governed by the Sato–Tate distribution (for non-CM curves) or the equidistribution on a circle (for CM curves). In either case, the *density* of anomalous primes is zero (since $a_p = 1$ is a measure-zero event in the limiting distribution), but their *count* is expected to be infinite.

7.4 Independence from the three governing invariants

The CRM Programme Roadmap identifies three invariants that govern the decidability landscape for mixed motives: the rank r, the Hodge level ℓ, and the effective Lang constant $c(A)$. On the Archimedean side, these invariants create genuine stratification—rank determines whether MP suffices or LPO is required (Papers 59, 61), and Hodge level governs the MP/LPO boundary (Paper 62).

On the p-adic side, N_M is independent of all three. The bound $N_M \leq 2$ depends only on the Hasse constraint on a_p, which is insensitive to rank, Hodge level, and Lang constants. This makes the p-adic precision bound a *universal constant* of the decidability program rather than a variable tied to the motive's arithmetic complexity.

7.5 Open questions

(1) **Higher-dimensional motives:** Is N_M uniformly bounded for abelian surfaces? For $K3$ surfaces? For arbitrary motives of fixed weight?

(2) **Quantitative anomalous prime counting:** For a given elliptic curve, what is the asymptotic density of primes with $N_M = 1$?

(3) **Function field analogue:** Does the uniform bound carry over to elliptic curves over function fields $\mathbb{F}_q(t)$?

8 Conclusion

We have proved that the crystalline precision bound $N_M = v_p(\#E(\mathbb{F}_p))$ satisfies $N_M \leq 2$ for all elliptic curves $E/\mathbb{Q}$ and all primes p of good reduction, with $N_M = 2$ achievable only at $p = 2$. For $p \geq 5$, $N_M \leq 1$ with equality if and only if the curve is anomalous at p. The proof is a short application of the Hasse bound, verified computationally on 1,812 curves across 23,454 (E, p) pairs.

The constructive consequence is that p-adic crystalline decidability for elliptic curves is uniformly BISH-decidable, requiring no omniscience principle. This completes the p-adic side of the decidability problem initiated in Paper 59, and highlights a clean structural asymmetry: the p-adic side is uniformly trivial, while the Archimedean side exhibits genuine logical stratification tied to rank.

Scope of contribution. Theorem 1.1 is a new observation, proved rigorously and verified computationally. The CRM calibration (Theorem 1.3) is a direct consequence. The computation is original. The Hasse bound itself is classical (Hasse, 1933).

Acknowledgments

This paper was prepared with AI assistance (Claude, Anthropic) for computation, code generation, and drafting. The author is not a domain expert in arithmetic geometry; the mathematical content has been verified computationally and by formal argument, but has not undergone independent peer review.

The Constructive Reverse Mathematics program builds on the foundational work of Errett Bishop and the constructive mathematics community. We thank the Mathlib contributors for the Lean 4 formalization infrastructure.

References

[1] E. Bishop and D. Bridges, *Constructive Analysis*, Springer, 1985.

[2] D. Bridges and F. Richman, *Varieties of Constructive Mathematics*, London Math. Soc. Lecture Notes 97, Cambridge Univ. Press, 1987.

[3] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, 2nd ed., Cambridge Univ. Press, 1997.

[4] N. D. Elkies, "The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$," *Invent. Math.* **89** (1987), 561–567.

[5] H. Hasse, "Beweis des Analogons der Riemannschen Vermutung für die Artinschen und F.K. Schmidtschen Kongruenzzetafunktionen in gewissen elliptischen Fällen," *Nachr. Ges. Wiss. Göttingen* (1933), 253–262.

[6] The LMFDB Collaboration, *The L-functions and Modular Forms DataBase*, `https://www.lmfdb.org`, 2024.

[7] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Springer GTM 106, 2009.

[8] P. C.-K. Lee, "Paper 1: Constructive Reverse Mathematics for Physics—Overview," CRM Series, 2025.

[9] P. C.-K. Lee, "Paper 50: The DPT Framework—Decidable Polarized Tannakian Categories," CRM Series, 2025.

[10] P. C.-K. Lee, "Paper 51: BSD and the DPT Framework," CRM Series, 2025.

[11] P. C.-K. Lee, "Paper 52: Bloch–Kato Selmer Groups under DPT," CRM Series, 2025.

[12] P. C.-K. Lee, "Paper 53: QCD Confinement and the DPT Lens," CRM Series, 2026.

[13] P. C.-K. Lee, "Paper 59: De Rham Decidability—p-Adic Precision for Crystalline Equivalence," CRM Series, 2026.

[14] P. C.-K. Lee, "Paper 61: Lang's Conjecture as the MP→BISH Gate," CRM Series, 2026.

[15] P. C.-K. Lee, "Paper 62: The Hodge Level Boundary," CRM Series, 2026.