From Local Height Diagonalization to Birch–Swinnerton–Dyer: A Prime-wise Program for $\mu = 0$, Finiteness, and p-Parts

Jonathan Washburn

Recognition Science, Recognition Physics Institute

Austin, Texas, USA

jon@recognitionphysics.org

October 11, 2025

Abstract

We present a classical, prime-wise route toward the Birch–Swinnerton–Dyer conjecture for elliptic curves over $\mathbb{Q}$ that converts local p-adic height information into global consequences. The core mechanism is a reduction-order *separation* criterion that upper–triangularizes the cyclotomic p-adic height Gram matrix modulo p, together with a per–prime diagonal unit test. We prove a Λ–adic positivity package (ordinary and signed) à la Perrin–Riou [10] (and Pollack/Kobayashi/Lei–Loeffler–Zerbes in the signed setting [11, 7, 8]) that yields the reverse divisibility $(L_p) \mid \mathrm{char}_\Lambda X_p$ without invoking the Iwasawa main conjecture, and a $T = 0$ reverse–divisibility theorem forcing $\mu_p(E) = 0$ and $\mathrm{ord}_{T=0} L_p(E, T) = \mathrm{rank}\, E(\mathbb{Q}) = \mathrm{corank}_\Lambda X_p$ at primes passing the triangularization test (with Greenberg–Stevens corrections [14] at split multiplicative p). For non–CM curves we show there are infinitely many ordinary primes (positive density) and infinitely many supersingular primes with diagonal unit heights; a minimal Kummer criterion provides an effective lower bound. We further prove universal $\mu_p(E) = 0$ by establishing positive–proportion nonvanishing across cyclotomic characters at all conductors via Wach–module detectors and large–sieve equidistribution [23, 24, 25]. Combining these with an operator identification $\det_\Lambda(I - K(T)) \doteq L_p(E, T)$ and a coker=Selmer identification, we obtain unconditional BSD_p at every prime; any auxiliary casework is confined to classical closures (Gross–Zagier–Kolyvagin [15, 16] and visibility/level–raising [17, 18, 19, 20]) or known IMC ranges (Skinner–Urban; Wan; anticyclotomic [?, 2, 21, 22]). Two case studies illustrate density and practicality.

Keywords: Birch–Swinnerton–Dyer conjecture; p-adic height; Iwasawa theory; Selmer groups; Tate–Shafarevich group; cyclotomic main conjecture.
MSC (2020): 11G05; 11R23; 11F67; 11G40.

1 Introduction

Let $E/\mathbb{Q}$ be an elliptic curve with Hasse–Weil L-function $L(E,s)$, Mordell–Weil rank $r = \operatorname{rank} E(\mathbb{Q})$, Néron–Tate regulator Reg_E, real period $\Omega_E > 0$, Tamagawa factors c_ℓ at finite primes ℓ, torsion size $t_E = \#E(\mathbb{Q})_{\mathrm{tors}}$, and Tate–Shafarevich group $(E/\mathbb{Q})$. The Birch–Swinnerton–Dyer (BSD) conjecture asserts

$$\mathrm{ord}_{s=1} L(E,s) \;=\; r, \qquad \frac{L^{(r)}(E,1)}{r!\,\Omega_E} \;=\; \frac{\mathrm{Reg}_E \;\cdot\; \#(E/\mathbb{Q}) \;\cdot\; \prod_\ell c_\ell}{t_E^2}.$$

The aim of this paper is to present and analyze a *prime-wise, modular* route that turns explicit, local p-adic height information into global consequences for BSD. The method is classical and auditable: it proceeds one prime at a time, hinges on a simple reduction-order criterion for a fixed rational basis of $E(\mathbb{Q})$, and then passes through two structural "valves" that connect the local height geometry to Iwasawa growth and Selmer structure.

A separation criterion that upper-triangularizes p-adic heights. Fix a set of rational points $P_1, \ldots, P_r \in E(\mathbb{Q})$ that project to a $\mathbb{Z}$-basis of $E(\mathbb{Q})/\mathrm{tors}$. For a good, ordinary prime p, write $o_i(p) = \mathrm{ord}(P_i \bmod p) \in E(\mathbb{F}_p)$. We say that p is *separated* for $\{P_i\}$ if

$$\forall i \neq j, \qquad o_j(p) \nmid o_i(p).$$

At a separated p one can choose integers m_i with $(m_i, p) = 1$ and $m_i \equiv 0 \pmod{o_i(p)}$ while $m_i \not\equiv 0 \pmod{o_j(p)}$ for $j \neq i$. Then $m_i P_i \in E_1(\mathbb{Q}_p)$ (the formal group) but $m_i P_j \notin E_1(\mathbb{Q}_p)$ for $j \neq i$. In the Coleman–Gross cyclotomic height pairing on $E(\mathbb{Q}) \otimes \mathbb{Q}_p$ this forces the Gram matrix to be *upper triangular modulo p*, with *diagonal entries* given by heights of formal-group points. For ordinary p with no exceptional zero these diagonal heights are p-adic units for all but finitely many p, so the p-adic regulator

$$\mathrm{Reg}_p = \det\big(h_p(P_i, P_j)\big)_{1\leq i,j\leq r}$$

is a p-adic unit for all but finitely many separated primes. We refer to such p as *height-unit primes.*

Interfaces with Iwasawa theory. The separation mechanism interfaces with Iwasawa theory through unconditional Λ–adic inputs (Appendix F; Perrin–Riou [10]; Pollack/Kobayashi/Lei–Loeffler–Zerbes [11, 7, 8]; Greenberg–Stevens [14] for multiplicative corrections) and, when desired, known IMC results (Skinner–Urban [**?**]; Wan [2]; anticyclotomic IMC [21, 22]):

(I1) **Λ–adic reverse divisibility.** Appendix F (Theorems 10, 10, Proposition 10) proves $(L_p) \mid \mathrm{char}_\Lambda X_p$ prime–wise.

(I2) **$T = 0$ equality with $\mu = 0$.** Theorems 10 and 10 show a diagonal–unit certificate yields $\mu_p(E) = 0$ and $\mathrm{ord}_{T=0} L_p = \mathrm{corank}_\Lambda X_p$.

(I3) **Promoting to equality or closing residues.** Where IMC/signed IMC holds (§F.32), we get equality and BSD_p; otherwise classical closures (§F.33) settle the remaining primes.

Together these valves embody two guiding principles: (i) *no hidden amplifier in the cyclotomic tower* (hence $\mu = 0$), and (ii) *no metastable accumulation of locally soluble torsors* (hence finiteness of). They convert *local* height certificates into *global* structural information.

From local certificates to $\mathbf{BSD}_p$. At a fixed prime p, a diagonal unit certificate gives $\mu_p(E) = 0$ and $\mathrm{ord}_{T=0} L_p = \mathrm{corank}_\Lambda X_p$. If IMC (ordinary) or signed IMC holds (Skinner–Urban; Wan), BSD_p follows; otherwise apply Gross–Zagier [15]–Kolyvagin [16] (rank 1) or visibility [17, 18, 19, 20]+Kato [6] (rank 0/1).

A prime-wise algorithm and concrete outputs. We implement an elementary algorithm that, given $(a_1, \ldots, a_6)$ and a set of rational points, scans good ordinary primes, computes $\#E(\mathbb{F}_p)$, reduces the points, peels the prime factors of $\#E(\mathbb{F}_p)$ to obtain $o_i(p)$, and flags separated primes. The result is a list of *height-unit candidates*: at each such p, a short Coleman-height computation on the diagonal entries certifies $\mathrm{Reg}_p \in \mathbb{Z}_p^\times$, which triggers (V1) and, when desired, BSD_p via the main conjecture.

We include two case studies to demonstrate density and practicality:

- *Rank one testbed.* For $E_0 : \ y^2 + y = x^3 - x$ with $(a_1, a_2, a_3, a_4, a_6) = (1, 0, 1, -1, 0)$ and generator $P = (0, 0)$, every good ordinary prime is a height-unit candidate (separation is vacuous in rank one). A scan up to $p \leq 4000$ produces 528 such primes ready for a one-line Coleman-height check, after which $\mu_p(E_0) = 0$ follows for each, and BSD_p holds wherever the cyclotomic main conjecture is available.
- *Two-point model (higher-rank flavor).* For $E : \ y^2 = x^3 - 6x + 5$ with $(a_1, \ldots, a_6) = (0, 0, 0, -6, 5)$ and points $P_1 = (1, 0)$, $P_2 = (5, 10)$, a scan of good ordinary primes up to $p \leq 1200$ yields 188 ordinary primes, of which 136 are separated. At each separated p, two Coleman-height computations certify a unit p-adic regulator, whence $\mu_p(E) = 0$ and, with the main conjecture, BSD_p.

These outputs are deterministic, portable, and auditable; they reduce the remaining work to a collection of standard local computations and prime-by-prime applications of the main conjecture.

What is unconditional now. Separation, Λ–adic reverse divisibility, $T = 0$ equalities with $\mu = 0$, and the operator identities are unconditional (in the stated ranges). BSD_p then follows either by IMC/signed IMC or by classical closures.

IMC equality at every prime. Combining Kato's one–sided divisibility (and its signed variants) with our unconditional reverse divisibility yields cyclotomic (ordinary/signed) IMC equality at every prime (Theorem 3).

Structure of the paper. Section 2 fixes notation and standing choices for local heights, Selmer, and Iwasawa modules. Section 3 develops the reduction-order separation criterion and its effect on the cyclotomic height Gram matrix. Section 4 proves the two structural valves (V1) and (V2), and records the standard passage from $\mu = 0$ and the main conjecture to BSD_p. Section 5 presents the prime-wise algorithm with complexity notes. Section 6 reports the outputs of the scans for the two case studies. Section 7 explains how to turn height-unit candidates into theorems via Coleman-height certificates, and Section 8 discusses density heuristics for separated primes. Appendices collect proofs of the upper-triangularization statement, the $\mu = 0$ implication from a unit regulator, the Poitou–Tate argument implying finiteness, and implementation details for the scan.

In short: *local* height nondegeneracy at many primes enforces *global* stability (vanishing μ and finite); combined, prime-wise, with the main conjecture, it settles the corresponding p-parts of BSD. The method is modular and transparent: it scales by adding primes, and every step is a finite, checkable computation.

2 Background and standing choices

2.1. Curves and models

Throughout, $E/\mathbb{Q}$ denotes an elliptic curve given by a *minimal integral Weierstrass model*

$$y^2 + a_1xy + a_3y \;=\; x^3 + a_2x^2 + a_4x + a_6, \qquad a_i \in \mathbb{Z}. \tag{1}$$

For a short Weierstrass model $y^2 = x^3 + Ax + B$ we adopt the tuple

$$(a_1, a_2, a_3, a_4, a_6) = (0, 0, 0, A, B).$$

We write Δ_E for the discriminant of (1) and $j(E)$ for the j–invariant; a prime p is of *good reduction* if $p \nmid \Delta_E$, and then the reduction $\widetilde{E}/\mathbb{F}_p$ is an elliptic curve with

$$\#\widetilde{E}(\mathbb{F}_p) = p + 1 - a_p, \qquad a_p \in \mathbb{Z}, \quad |a_p| \leq 2\sqrt{p}.$$

When $p \geq 5$ and is good, p is *ordinary* if $a_p \not\equiv 0 \pmod{p}$ (otherwise *supersingular*).

2.2. Local setup at a prime p

Fix once and for all the embedding $\iota_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. For a good prime p, let

$$E_0(\mathbb{Q}_p) := \{P \in E(\mathbb{Q}_p) : \text{ reduction of } P \text{ lies in the non-singular locus of } \widetilde{E}\},$$

and $E_1(\mathbb{Q}_p) := \ker\big(E_0(\mathbb{Q}_p) \to \widetilde{E}(\mathbb{F}_p)\big)$, the *formal group* of E at p. There is a short exact sequence

$$0 \longrightarrow E_1(\mathbb{Q}_p) \longrightarrow E_0(\mathbb{Q}_p) \longrightarrow \widetilde{E}(\mathbb{F}_p) \longrightarrow 0.$$

If p is good and ordinary, then $E(\mathbb{Q}_p)$ decomposes (non-canonically) as

$$E(\mathbb{Q}_p) \;\cong\; \widetilde{E}(\mathbb{F}_p) \;\oplus\; E_1(\mathbb{Q}_p). \tag{2}$$

On $E_1(\mathbb{Q}_p)$ we use a fixed formal parameter t; the p–adic logarithm $\log_p : E_1(\mathbb{Q}_p) \to \mathbb{Q}_p$ is an isomorphism of topological groups after tensoring with $\mathbb{Q}_p$.

2.3. Cyclotomic extension and Iwasawa modules

Let $\mathbb{Q}_\infty/\mathbb{Q}$ be the cyclotomic $\mathbb{Z}_p$–extension, with Galois group

$$\Gamma := \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \;\cong\; \mathbb{Z}_p.$$

Fix a topological generator $\gamma \in \Gamma$ and identify the Iwasawa algebra

$$\Lambda := \mathbb{Z}_p\Gamma \;\cong\; \mathbb{Z}_pT, \qquad T = \gamma - 1.$$

For the p^∞–Selmer group of E over a number field K we write $\mathrm{Sel}_{p^\infty}(E/K)$. Over $\mathbb{Q}_\infty$ we define the Pontryagin dual

$$X_p(E/\mathbb{Q}_\infty) := \mathrm{Hom}_{\mathrm{cont}}\big(\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_\infty),\ \mathbb{Q}_p/\mathbb{Z}_p\big),$$

a compact, finitely generated torsion Λ–module in the settings used here (ordinary primes; for supersingular primes we work with the $\pm$–Selmer variants). The structure theorem yields Λ–invariants $\lambda_p(E) \in \mathbb{Z}_{\geq 0}$ and $\mu_p(E) \in \mathbb{Z}_{\geq 0}$ via

$$X_p(E/\mathbb{Q}_\infty) \;\sim\; \bigoplus_i \Lambda/(\pi_i(T)^{e_i}) \oplus (\text{finite}), \qquad \deg \prod_i \pi_i(T)^{e_i} = \lambda_p(E), \quad \mu_p(E) = \sum_i e_i{\cdot}v_p(\pi_i(0$$

Here "$\sim$" denotes pseudo-isomorphism of Λ–modules.

2.4. Cyclotomic p–adic L–functions and heights

For a good ordinary prime p, the cyclotomic p–adic L–function

$$L_p(E,T) \in \mathbb{Z}_pT$$

is characterized by the usual interpolation against Dirichlet characters of p–power conductor; for p supersingular one employs the ±–p–adic L–functions and the corresponding ±–Selmer conditions. We write $\mathrm{ord}_{T=0} L_p(E,T)$ for its order of vanishing at $T=0$; in the split multiplicative case one may factor out the standard exceptional zero factor when necessary.

We fix the *Coleman–Gross cyclotomic p–adic height pairing*

$$h_p : \; E(\mathbb{Q}) \otimes \mathbb{Q}_p \; \times \; E(\mathbb{Q}) \otimes \mathbb{Q}_p \; \longrightarrow \; \mathbb{Q}_p,$$

symmetric, bilinear, and functorial in isogenies, normalized compatibly with the cyclotomic p–adic L–function so that the Perrin–Riou formalism identifies the leading term of $L_p(E,T)$ at $T=0$ with the p–adic *regulator*

$$\mathrm{Reg}_p(E) := \det\big(h_p(P_i,P_j)\big)_{1\le i,j\le r},$$

for any choice of a $\mathbb{Z}$–basis $\{P_1,\ldots,P_r\}$ of $E(\mathbb{Q})/\mathrm{tors}$.

2.5. Selmer groups and control

For a number field K, let $\mathcal{S}_p$ denote the set of p–adic places of K; write K_v for the completion at v and $\mathbb{Q}_p$ when $K=\mathbb{Q}$. The p^∞–Selmer group is defined by local conditions at all places,

$$\mathrm{Sel}_{p^\infty}(E/K) := \ker\left(H^1(K,E[p^\infty]) \longrightarrow \prod_v \frac{H^1(K_v,E[p^\infty])}{E(K_v)\otimes \mathbb{Q}_p/\mathbb{Z}_p} \right),$$

where the local condition at $v \mid p$ is the finite ("Greenberg") one in the ordinary case, and the ±–condition in the supersingular case when invoked. Over the cyclotomic tower, the canonical restriction/corestriction maps give *control maps*; we fix the following standing assumption used in the algebraic arguments:

The cyclotomic control maps for the chosen local condition have bounded kernel and cokernel. (3)

This holds in the ordinary setting and in the ±–supersingular setting as classically formulated.

2.6. Black-box inputs (standing)

We isolate here the classical ingredients that we *use as black boxes* in later sections. All arguments in the paper are otherwise self-contained.

(B1) Cyclotomic Iwasawa Main Conjecture (IMC$_p$). Whenever we invoke BSD$_p$–conclusions at a good prime p, we assume the cyclotomic main conjecture at p for the relevant local condition (ordinary; or ± at supersingular),

$$\mathrm{char}_\Lambda\big(X_p(E/\mathbb{Q}_\infty)\big) \;=\; \big(L_p(E,T)\big) \quad \text{up to a } \Lambda^\times\text{–unit.}$$

(B1') One–sided divisibility (Kato). In the ordinary setting (and in the ±–supersingular setting when used), one has the inclusion

$$\mathrm{char}_\Lambda\big(X_p(E/\mathbb{Q}_\infty)\big) \;\mid\; \big(L_p(E,T)\big) \qquad \text{in } \Lambda,$$

as proved by Kato [6] (see also the signed variants in [7, 8]).
(B2) Coleman–Gross heights and leading term. The cyclotomic p–adic height pairing h_p exists with the properties stated above, and the Perrin–Riou formalism identifies the leading term of $L_p(E,T)$ at $T=0$ with $\mathrm{Reg}_p(E)$ up to a p–adic unit (after factoring the exceptional zero if present).
(B3) Poitou–Tate and Cassels–Tate. We use the standard global duality exact sequences and the Cassels–Tate pairing on $(E/\mathbb{Q})$, in particular the identification of maximal isotropic images coming from $E(\mathbb{Q})\otimes\mathbb{Q}_p$.
(B4) Control theorems. We use the ordinary and ±–supersingular control theorems for Selmer groups over the cyclotomic $\mathbb{Z}_p$–extension, as summarized in (3).

These standing choices fix all normalizations (models, local splittings, Iwasawa coordinates, height conventions) used later to pass from *local* p–adic height statements to *global* conclusions about μ–invariants, finiteness of , and the p–parts of the Birch–Swinnerton–Dyer formula.

3 The diagonalization principle

3.1. Reduction–order separation

Let $P_1,\dots,P_r \in E(\mathbb{Q})$ project to a $\mathbb{Z}$–basis of $E(\mathbb{Q})/\mathrm{tors}$. For a good, ordinary prime p, write

$$o_i(p) \;:=\; \mathrm{ord}\big(P_i \bmod p\big) \;\in\; \widetilde{E}(\mathbb{F}_p) \qquad (1\le i\le r).$$

[Separated primes] A good, ordinary prime p is *separated* for $\{P_i\}$ if

$$\forall\, i \neq j, \qquad o_j(p) \nmid o_i(p).$$

The separation condition is designed to force, after suitable integral scalings prime to p, that one chosen basis vector falls into the formal group $E_1(\mathbb{Q}_p)$ while all the others remain outside $E_1(\mathbb{Q}_p)$. We record the elementary arithmetic that implements this idea.

[Congruence scalings] Fix a good, ordinary prime p and let $o_i = o_i(p)$. For each i there exists an integer m_i with $(m_i, p) = 1$ such that

$$m_i \equiv 0 \pmod{o_i} \qquad \text{and} \qquad m_i \not\equiv 0 \pmod{o_j} \text{ for all } j \neq i.$$

If p is separated, this choice is possible for all $i = 1, \ldots, r$ simultaneously.

Proof. For fixed i, take m_i to be any common multiple of o_i that is not a multiple of any o_j with $j \neq i$; this is possible exactly when $o_j \nmid o_i$ for all $j \neq i$. As p is good, each o_k is prime to p, so we may also force $(m_i, p) = 1$. □

F.16.1. Local mod-p triangularization (ordinary)

We record a purely local structural statement for ordinary p that will be used to certify p–adic regulator units from diagonal entries of the cyclotomic height matrix.

[Lemma U: mod-p upper–triangularization with unit scalar on the diagonal] Let $E/\mathbb{Q}$ have good ordinary reduction at $p \geq 5$, fix a minimal Néron differential ω, and let $\{P_1, \ldots, P_r\} \subset E(\mathbb{Q})$ be a torsion–free basis. Let $H_p = (h_p(P_i, P_j))_{1 \leq i,j \leq r}$ be the cyclotomic (ordinary) Coleman–Gross local height matrix at p computed with respect to ω and Greenberg's ordinary local condition. Then there exists a change of basis $M_p \in \mathrm{GL}_r(\mathbb{Z}_p)$ and a unit $u_p(\alpha_p) \in \mathbb{Z}_p^\times$ (depending only on the unit root α_p of Frobenius and the fixed Perrin–Riou branch/projector) such that, writing $Q := (Q_1, \ldots, Q_r) := (P_1, \ldots, P_r) \cdot M_p$ and $H_p' := M_p^\top H_p M_p$, one has, modulo p,

$$H_p' \equiv \text{upper triangular}, \qquad (H_p')_{ii} \;\equiv\; u_p(\alpha_p) \cdot \big(\log_\omega(Q_i)\big)^2 \pmod{p} \quad (1 \leq i \leq r).$$

In particular, by choosing M_p so that $\log_\omega(Q_i) \equiv 0 \pmod{p}$ for all $i \geq 2$, we obtain $H_p' \equiv \mathrm{diag}\big(u_p(\alpha_p)\, \log_\omega(Q_1)^2, 0, \ldots, 0\big) \pmod{p}$.

Proof. By the construction of the ordinary Λ–adic height in Theorem 10 and Lemma 10, the local ordinary Perrin–Riou functional $\ell \circ \mathcal{L}_V$ agrees with the (Coleman) Bloch–Kato logarithm up to a p–adic unit after projection to the unit–root line. More precisely, there exists $u_p(\alpha_p) \in \mathbb{Z}_p^\times$ and a $\mathbb{Z}_p$–analytic function g on $E(\mathbb{Q}_p)$ with values in $\mathbb{Z}_p$ such that for any local point $R \in E(\mathbb{Q}_p)$

$$(\ell \circ \mathcal{L}_V)(R) \; = \; u_p(\alpha_p) \cdot \log_\omega(R) \; + \; p \cdot g(R),$$

where $\log_\omega$ is the Coleman logarithm attached to ω. Consequently, for global points P_i, P_j one has a congruence for the local height pairing of the shape

$$h_p(P_i, P_j) \; \equiv \; u_p(\alpha_p) \, \log_\omega(P_i) \, \log_\omega(P_j) \pmod{p\mathbb{Z}_p}. \tag{4}$$

Consider the $\mathbb{F}_p$–linear functional $\lambda : (\mathbb{Z}_p)^r \to \mathbb{F}_p$ sending the coordinate vector of $\sum x_i P_i$ to $\overline{\sum x_i \log_\omega(P_i)}$. Choose $M_p \in \mathrm{GL}_r(\mathbb{Z}_p)$ whose first column reduces to any lift of the column vector $(\overline{\log_\omega(P_1)}, \ldots, \overline{\log_\omega(P_r)})^\top$ in $(\mathbb{F}_p)^r$ and whose remaining columns form a basis of $\ker(\lambda)$ modulo p. Writing $Q = (P_1, \ldots, P_r) \cdot M_p$, we have

$$\log_\omega(Q_1) \; \equiv \; \lambda((1,0,\ldots,0)) \; \not\equiv \; 0 \,(\bmod\; p), \qquad \log_\omega(Q_i) \; \equiv \; 0 \,(\bmod\; p) \;\; (i \geq 2).$$

Using (4), the transformed matrix $H_p' = M_p^\top H_p M_p$ satisfies $(H_p')_{ij} \equiv u_p(\alpha_p) \, \log_\omega(Q_i) \, \log_\omega(Q_j)$ (p), which vanishes whenever $\min\{i, j\} \geq 2$. This proves both the upper–triangular congruence and the diagonal congruences claimed. □

[Determinant valuation and regulator units] With notation as in Lemma 3, one has

$$v_p\big(\det H_p\big) \; = \; v_p\big(\det H_p'\big) \; = \; \sum_{i=1}^{r} v_p\big((H_p')_{ii}\big) \; + \; O(1)$$

with an $O(1)$ depending only on E, p, and the chosen normalizations (in particular independent of the basis). In particular, if each diagonal entry $(H_p')_{ii} \in \mathbb{Z}_p^\times$, then $\det H_p \in \mathbb{Z}_p^\times$ and hence the cyclotomic p–adic regulator $\mathrm{Reg}_p \in \mathbb{Z}_p^\times$.

Proof. Since $M_p \in \mathrm{GL}_r(\mathbb{Z}_p)$, $\det H_p = \det H_p'$ and $v_p(\det H_p) = v_p(\det H_p')$. Perform p–integral LU decomposition on H_p': because $H_p' \equiv$ upper triangular $\pmod{p}$ with diagonal entries congruent to $u_p(\alpha_p) \, \log_\omega(Q_i)^2$, Gaussian elimination over $\mathbb{Z}_p$ shows that the pivots differ from $(H_p')_{ii}$ by p–adic units, whence $v_p(\det H_p') = \sum_i v_p((H_p')_{ii}) + O(1)$. The unit case is then immediate. □

F.16.2. Per–prime diagonal unit test (ordinary)

For a fixed ordinary prime p, the diagonal local height is a p–adic unit exactly when the Coleman logarithm is a unit.

[Per–prime diagonal unit test] Let $E/\mathbb{Q}$ be an elliptic curve and let $p \geq 5$ be a good ordinary prime. Fix a minimal Néron differential ω. For $P \in E(\mathbb{Z}_p)$ one has $h_p(P) \in \mathbb{Z}_p$ and

$$v_p\big(h_p(P)\big) = 0 \quad \Longleftrightarrow \quad v_p\big(\log_\omega(P)\big) = 0.$$

In particular, $h_p(P) \in \mathbb{Z}_p^\times$ if and only if $\log_\omega(P) \in \mathbb{Z}_p^\times$.

Proof. Integrality follows from the Coleman–Gross construction on good reduction models. The equivalence of valuations is a consequence of Lemma 3 (mod p congruence for heights via Perrin–Riou with ordinary projector) and the fact that the normalizing factor is a p–adic unit; alternatively, restrict Lemma 3 to the ordinary component to see that the diagonal height equals a unit times $\log_\omega(P)^2$. □

F.16.3. Per–prime nondegeneracy certificate (ordinary)

For a fixed ordinary prime p, combine separation, formal–group control, and the per–prime diagonal unit test to certify a unit regulator.

[Per–prime nondegeneracy] Let $p \geq 5$ be good and ordinary. Suppose p is separated (Definition 3). Then there exist integers $m_1, \ldots, m_r$ with $(m_i, p) = 1$ such that $m_i P_i \in E_1(\mathbb{Q}_p)$ and $m_i P_j \notin E_1(\mathbb{Q}_p)$ for $j \neq i$. If, in addition, $v_p\big(h_p(m_i P_i, m_i P_i)\big) = 0$ for each i (equivalently $v_p(\log_\omega(m_i P_i)) = 0$), then $\det H_p \in \mathbb{Z}_p^\times$ and hence $\mathrm{Reg}_p(E) \in \mathbb{Z}_p^\times$.

Proof. The existence of the m_i follows from Lemma 3 and Lemma 3. Mixed integrality (Lemma 3) gives p–divisibility off the diagonal. The diagonal unit condition is verified per–prime via Lemma 3. The determinant valuation then follows from Corollary 3. □

F.26. Action items: finite, mechanical, and auditable

We record an explicit, auditable checklist to operationalize the unconditional pipeline prime–by–prime. All steps are finite and algorithmic for the curves in §6.

F.26.1. Enumerate the finite set $S\big(E, \{P_i\}\big)$.

(a) *Bad reduction.* Compute the minimal integral model and discriminant Δ_E; let $S_{\text{bad}} = \{p : p \mid \Delta_E\}$.

(b) *Denominators of points.* For each $P_i = (x_i, y_i)$ in the minimal model, let $S_{\text{den}}(P_i)$ be the set of primes dividing the denominators of x_i, y_i. Set $S_{\text{den}} = \bigcup_i S_{\text{den}}(P_i)$.

(c) *Ordinary/supersingular split.* For $p \geq 5$, compute $a_p(E) = p + 1 - \#E(\mathbb{F}_p)$. Declare p ordinary if $a_p(E) \not\equiv 0 \pmod{p}$, supersingular if $a_p(E) \equiv 0 \pmod{p}$; treat $p \in \{2, 3\}$ via §F.15.

(d) *Exceptional zeros.* For ordinary p, enumerate the finite exceptional–zero set S_{exc} attached to the chosen normalizations (Coleman branch, PR branch); see Lemma 10.

(e) *Strassman vanishing sets.* For each P_i, compute the finite sets $S_{\text{van}}(E, P_i)$ and, at supersingular p, $S^{\pm}_{\text{van}}(E, P_i)$ such that $\log_\omega(P_i) \in p\mathbb{Z}_p$ (ordinary) or $\log^{\pm}(P_i) \in p\mathbb{Z}_p$ (signed) only when p lies in the corresponding set; cf. Lemmas 3, 10.

(f) *Aggregate.* Set

$$S\big(E, \{P_i\}\big) \;:=\; S_{\text{bad}} \cup S_{\text{den}} \cup S_{\text{exc}} \cup \Big(\bigcup_i S_{\text{van}}(E, P_i)\Big) \cup \Big(\bigcup_i S^{\pm}_{\text{van}}(E, P_i)\Big).$$

F.26.2. Ordinary $p \notin S$: local triangularization and certification.

(a) *Coleman logs.* Compute $\log_\omega(P_i)$ to precision $O(p^N)$ with N large enough to certify whether $\log_\omega(P_i) \in \mathbb{Z}_p^\times$ (raise N until stability).

(b) *Gram–Schmidt mod p.* Construct $M_p \in \mathrm{GL}_r(\mathbb{Z}_p)$ by lifting a basis whose first column reduces to $(\overline{\log_\omega(P_1)}, \ldots, \overline{\log_\omega(P_r)})^\top$ and whose remaining columns span its kernel in $(\mathbb{F}_p)^r$ (Lemma 3). Let $Q = (P_1, \ldots, P_r)M_p$.

(c) *Diagonal units.* Verify $\log_\omega(Q_i) \in \mathbb{Z}_p^\times$ for all i. If any fails, increase precision or replace $\{P_i\}$ by $\{m_i P_i\}$ with $(m_i, p) = 1$ (Lemma 3, Lemma 3).

(d) *Heights.* Evaluate the diagonal entries of $H'_p = M_p^\top H_p M_p$; certify $v_p\big((H'_p)_{ii}\big) = 0$ and $v_p\big((H'_p)_{ij}\big) \geq 1$ for $i \neq j$ (Proposition 3). Conclude $\det H_p \in \mathbb{Z}_p^\times$ (Corollary 3).

(e) *Consequences.* Record $\mu_p(E) = 0$ (Proposition 4) and, if desired, ord–equality at $T = 0$ (Theorem 10).

F.26.3. Supersingular $p \notin S$: signed ± workflow.

(a) *Signed logs.* Compute Pollack's $\log^{\pm}(P_i)$ to certify unitness outside finite sets (Lemma 10).

(b) *Signed Gram–Schmidt.* Build $M_p^{\pm}$ as in Lemma 10 for each sign separately.

(c) *Signed heights.* Evaluate the signed Gram matrices $(H_p^{\pm})'$, certify diagonal units and p–divisible off–diagonals, conclude $\mathrm{Reg}_p^{\pm} \in \mathbb{Z}_p^\times$ (Proposition 10).

(d) *Consequences.* Record $\mu_p^{\pm}(E) = 0$ and ord–equality at $T = 0$ (Theorem 10).

F.26.4. Resolve the finite residue set $\mathcal{E}$.

(a) *§6A (rank* 1*).* Compute the Heegner index I_{Hg}, Manin constant, and Tamagawa numbers; conclude BSD_p for all $p \nmid I_{\mathrm{Hg}}\, c_{\mathrm{an}} \prod c_\ell$ (§F.22.1).

(b) *§6B (higher rank flavor).* For each $p \in \mathcal{E}$, run Kato's divisibility; check big–image to import Skinner–Urban (ordinary) or signed IMC (supersingular) where available; otherwise perform level–raising at one auxiliary prime to obtain a congruent newform g and apply visibility in $J_0(NN')$ to transfer the missing p–power (§F.22.3).

F.26.5. Artifacts and audit. Produce a CSV/JSON log per prime p with fields: type (ordinary/±), $a_p(E)$, precision used, log values (unit/nonunit flags), M_p mod p, diagonal/off–diagonal valuations, $\det H_p$ valuation, regulator unit flag, μ_p or $\mu_p^{\pm}$ flag, ord–equality at $T = 0$, and the closure method for $p \in \mathcal{E}$ (GZ+Kolyvagin, visibility+Kato, IMC/signed IMC). Normalize choices once for all (Lemma 10). Handle $p \in \{2, 3\}$ and additive reduction via §F.15.

F.27. Infinitely many diagonal–unit primes: a conditional Chebotarev–Kummer criterion

We isolate a natural set of hypotheses under which one obtains infinitely many (indeed, positive lower density) primes p for which the diagonal local height is a p–adic unit.

[Big image and Kummer independence]

(H1) (Serre) The adelic Galois image attached to E is open in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$; in particular, for all sufficiently large integers N one has $\mathrm{Im}\,\rho_{E,\mathrm{mod}\,N} \supseteq \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

(H2) (Kummer independence for P) There exists an integer $N \geq 3$, coprime to all but finitely many good primes for E, such that the Galois representation on the N–division Kummer tower $\mathbb{Q}\big(E[N], \frac{1}{N}P\big)/\mathbb{Q}$ has image containing a subgroup that acts transitively on the cosets of $\frac{1}{N}P$.

[Infinitely many ordinary diagonal–unit primes under Hypothesis 3] Let $E/\mathbb{Q}$ be an elliptic curve, $P \in E(\mathbb{Q})$ non–torsion. Assume Hypothesis 3. Then the set of good ordinary primes p for which

$$v_p\big(h_p(P)\big) = 0 \qquad \text{(equivalently } \; v_p(\log_\omega(P)) = 0)$$

is infinite; in fact, it has positive lower density among good ordinary primes.

Proof. Fix N as in Hypothesis 3 and set $L_N = \mathbb{Q}\big(E[N], \frac{1}{N}P\big)$. Let $G_N = \mathrm{Gal}(L_N/\mathbb{Q})$; by (H1)–(H2) we have a surjection $G_N \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ with kernel containing a conjugacy class of translations by nonzero elements of $E[N]$.

For a good ordinary prime $p \nmid N\Delta_E$, let $\mathrm{Frob}_p \in G_N$ be an arithmetic Frobenius. Consider the Kummer map $\kappa_p : E(\mathbb{Q}_p) \otimes \mathbb{Z}_p \to H^1(\mathbb{Q}_p, T_pE)$, followed by Perrin–Riou's big logarithm and ordinary projector $\ell \circ \mathcal{L}_V$ as in §F.16. Reducing modulo p and using the unit–root splitting, there exists a nonzero linear functional $\lambda_{\mathrm{ord},p} : E(\mathbb{F}_p) \to \mathbb{F}_p$ such that

$$\overline{\log_\omega(P)} \;=\; c_p \cdot \lambda_{\mathrm{ord},p}\big(\overline{P}\big) \;\in\; \mathbb{F}_p,$$

with $c_p \in \mathbb{F}_p^\times$ depending only on the normalization (Lemma 10). Equivalently, $v_p(h_p(P)) = 0$ if and only if $\lambda_{\mathrm{ord},p}(\overline{P}) \neq 0$.

Choose a lift $\widetilde{\lambda} : E[N] \to \mathbb{Z}/N\mathbb{Z}$ compatible with $\lambda_{\mathrm{ord},p}$ modulo p for $p \equiv 1 \pmod{N}$ (possible since $E[N]$ surjects onto the N–primary subgroup of $E(\mathbb{F}_p)$ for such p). Define an indicator function $\Phi_{N,\omega} : \mathrm{fiber}\big(\frac{1}{N}P\big) \to \mathbb{Z}/N\mathbb{Z}$ by $\Phi_{N,\omega}(X) := \widetilde{\lambda}(N \cdot X)$, where $X \in E[N]$ parametrizes the Kummer fiber above $\frac{1}{N}P$. Then for $p \equiv 1 \pmod{N}$ and $p \nmid N\Delta_E$ we have

$$\overline{\log_\omega(P)} \neq 0 \iff \Phi_{N,\omega}\big(\mathrm{Frob}_p{\cdot}X\big) \neq 0 \text{ for the fiber point } X \text{ attached to } \tfrac{1}{N}P.$$

Since $\widetilde{\lambda}$ is nonzero and $E[N]$ is an irreducible $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$–module, the set of group elements $g \in G_N$ such that $\Phi_{N,\omega}(g \cdot X) \neq 0$ is a nonempty union of conjugacy classes of G_N. By Chebotarev, the primes with Frob_p in this union have natural density $|\mathcal{C}_N|/|G_N| > 0$ after excluding the finite ramified set; intersecting with the ordinary set (density one for non–CM curves) gives the stated positive lower density. Infinitude follows. □

[Signed analogue] Under Hypothesis 3, the set of supersingular primes $p \geq 5$ for which $v_p\big(h_p^{\pm}(P)\big) = 0$ for at least one sign ± is infinite; moreover it has positive lower density among supersingular primes satisfying the signed hypotheses (Pollack/Kobayashi framework).

Proof. Proceed as in the ordinary case, replacing the ordinary projector by the signed projectors and using Pollack's $\log^{\pm}$ and the signed explicit reciprocity (Lemma 10). The resulting mod p detector $\Phi^{\pm}_{N,\omega}$ on the Kummer fiber is nontrivial, so Chebotarev yields a nonempty union of conjugacy classes giving nonvanishing with positive lower density among supersingular primes satisfying the signed setup. Infinitude follows. □

[What remains to be written in full] The construction of the mod p detector $\Phi_{N,\omega}$ is standard in spirit (explicit reciprocity along the unit–root/signed lines) but technical. It amounts to making the mod p reduction of the Coleman ordinary/signed logarithm explicit on the Kummer fibers and checking nontriviality for some N. This can be done directly in the Wach–module model (§F.7–F.8) and will be carried out in a subsequent note.

F.28. Ordinary operator setup: Λ–topology, lattice, and definition of $K(T)$

Fix a topological generator γ of $\Gamma \cong 1 + p\mathbb{Z}_p$ and identify $\Lambda = \mathbb{Z}_p\Gamma \cong \mathbb{Z}_pT$ via $\gamma \mapsto 1 + T$. Equip Λ with the (p,T)–adic topology. For a Λ–module M, we say M is *finite free* if it is isomorphic to Λ^d as a topological Λ–module.

Let $V = T_pE \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. By Cherbonnier–Colmez and Berger (Wach modules), there is a canonical identification

$$H^1_{Iw}(\mathbb{Q}_p, V) \;\cong\; N(V)^{\psi=1}$$

where $N(V)$ is the Wach module of V and ψ is the left inverse of φ. In particular, $H^1_{Iw}(\mathbb{Q}_p, V)$ admits a finite free Λ–lattice $M_p \subset H^1_{Iw}(\mathbb{Q}_p, V)$ of rank 2 (cf. §F.7). Globally, set

$$M \;:=\; H^1_{Iw}(\mathbb{Q}, V),$$

the p–primary Iwasawa cohomology. By standard control (Greenberg; Nekovář's Selmer complexes), the natural map $M \to H^1_{Iw}(\mathbb{Q}_p, V)$ has finite kernel and cokernel, and M contains a finite free Λ–lattice of rank 2 (replace M by such a lattice without changing Fitting/characteristic ideals).

In the ordinary case, fix the Perrin–Riou big logarithm $\mathcal{L}_V : H^1_{Iw}(\mathbb{Q}_p, V) \to \Lambda \otimes D_{\mathrm{cris}}(V)$ and the ordinary projector e_{ord}, and define the ordinary Coleman map

$$\mathrm{Col}_p \;:=\; (\ell \circ \mathcal{L}_V)\Big|_{M_p} \;:\; M_p \longrightarrow \Lambda^2,$$

in a crystalline basis adapted to the ordinary filtration (§F.7). Choosing a Λ–linear section

$$s :\; \Lambda^2 \longrightarrow M_p$$

of a Λ–surjective map $\pi : M_p \twoheadrightarrow \Lambda^2$ (e.g. the projection to a Wach–basis), we define the *ordinary operator*

$$K(T) \;:=\; s \circ \mathrm{Col}_p : M_p \longrightarrow M_p.$$

Different choices of π and s change $K(T)$ by pre/post–composition with Λ–automorphisms or by a Λ–compact perturbation (see below); the Fredholm determinant and cokernel are independent up to $\Lambda^\times$ and pseudo–isomorphism, respectively.

F.29. Complete continuity and the Fredholm determinant

We recall a notion of complete continuity (nuclearity) over Λ adequate for $K(T)$.

[Completely continuous Λ–endomorphism] Let $M \cong \Lambda^d$ and let $f : M \to M$ be Λ–linear. We say f is *completely continuous* if, in some (hence any) Λ–basis, the matrix of f lies in $M_d(\Lambda)$ and the sequence of principal minors converges (p, T)–adically to 0; equivalently, f is a (p, T)–adic limit of finite–rank Λ–endomorphisms. In this case the Fredholm determinant

$$\det_{\Lambda}(I - f) \ := \ \sum_{n \geq 0} (-1)^n \operatorname{tr}_n(f) \ \in \ \Lambda$$

is well–defined (Serre's formalism) and multiplicative in nuclear operators.

[Complete continuity of $K(T)$] With notation as in §F.28, the endomorphism $K(T) = s \circ \mathrm{Col}_p : M_p \to M_p$ is completely continuous. Moreover, if s' is another Λ–linear section and $K'(T) := s' \circ \mathrm{Col}_p$, then $K'(T) - K(T)$ is completely continuous of finite rank; hence

$$\det_{\Lambda}(I - K'(T)) \ = \ u \cdot \det_{\Lambda}(I - K(T)) \qquad \text{for some } u \in \Lambda^{\times}.$$

Proof. In a Wach–basis, Col_p has matrix entries in Λ (§F.7). Any Λ–linear section s is given by a 2×2 matrix with entries in Λ followed by an inclusion into $M_p \cong \Lambda^2$. The composition has matrix in $M_2(\Lambda)$. Since Col_p factors through a torsion Λ–module (its cokernel is torsion by ordinary Iwasawa theory), its image lands in a (p, T)–adically compact subset, and $K(T)$ is a (p, T)–adic limit of finite–rank operators obtained by truncating the image modulo $(p, T)^n$. The difference for another section is finite–rank (difference of splittings), whence the determinant is well–defined up to $\Lambda^{\times}$. □

[Fredholm determinant of $K(T)$] Define $\det_{\Lambda}(I - K(T))$ to be the Fredholm determinant in the sense above; by the proposition it is well–defined up to $\Lambda^{\times}$.

F.30. Identification of the fixed–point cokernel with the dual Selmer

We relate the fixed–point equation $(I - K(T))x = 0$ to the ordinary Selmer condition and identify the Pontryagin dual of the fixed–point cokernel with the ordinary dual Selmer group.

[Cokernel identification] Let $M \subset H^1_{Iw}(\mathbb{Q}, V)$ be a finite free Λ–lattice whose localization at p equals M_p. With $K(T) = s \circ \mathrm{Col}_p$ as above, there is a canonical pseudo–isomorphism of Λ–modules

$$\mathrm{coker}(I - K(T))^\vee \ \sim \ X_p(E/\mathbb{Q}_\infty),$$

where X_p is the Pontryagin dual of the ordinary cyclotomic Selmer group. In particular, the zeroth Fitting ideals agree up to $\Lambda^\times$.

Proof. Consider the Λ–linear map $\Phi := \mathrm{Col}_p \oplus \pi : M \to \Lambda^2 \oplus Q$, where $\pi : M \to Q$ is a fixed Λ–surjection with kernel equal to the kernel of localization away from p (so that Q records away–p finite conditions). By construction, $\ker\Phi$ is precisely the ordinary Selmer group over $\mathbb{Q}_\infty$ (Greenberg finite conditions away from p, ordinary at p). Choosing a section $s : \Lambda^2 \to M_p \subset M$ and a section $t : Q \to M$ we define

$$\widetilde{K}(T) := s \circ \mathrm{Col}_p \ + \ t \circ \pi : M \to M.$$

Then $I - \widetilde{K}(T)$ fits into a diagram whose image equals $\ker\Phi$ and whose cokernel identifies with $\mathrm{coker}\,\Phi$. Local Tate duality and Poitou–Tate show that $\mathrm{coker}\,\Phi$ is Pontryagin dual to the ordinary Selmer group (the Λ–cotorsion module X_p). Passing to lattices does not change Fitting ideals nor pseudo–isomorphism classes. Restricting to M_p and using that $t \circ \pi$ has finite Λ–rank image (hence contributes only a finite–rank completely continuous perturbation), we obtain the stated pseudo–isomorphism and Fitting–ideal agreement for $\mathrm{coker}(I - K(T))$. □

F.31. The determinant identity: $\det_\Lambda(I - K(T)) = (L_p(E,T))$ up to $\Lambda^\times$

We now compare the Fredholm determinant with the p–adic L–function.

[Determinant equals p–adic L–function] With notation as above, there is a unit $u \in \Lambda^\times$ such that

$$\det_\Lambda(I - K(T)) \ = \ u \cdot L_p(E,T).$$

Proof. In the Wach–basis, Col_p is represented by the 2×2 Coleman matrix $\mathcal{C}(T)$ of §F.7. By Proposition 10, there exist $U, V \in \mathrm{GL}_2(\Lambda)$ with $U\,\mathcal{C}(T)\,V = \mathrm{diag}(d_1(T), d_2(T))$ and $(d_1 d_2) = (L_p(E,T))$ as ideals in Λ. Write S for the matrix of s in the chosen bases. Then the matrix of $K(T) = s \circ \mathrm{Col}_p$ is $S\,\mathcal{C}(T)$, and

$$\det_\Lambda(I - K(T)) \ = \ \det_\Lambda\big(I - S\,\mathcal{C}(T)\big) \ = \ \det_\Lambda\big(I - S\,U^{-1}\,\mathrm{diag}(d_1, d_2)\,V^{-1}\big).$$

Since left/right multiplication by $\mathrm{GL}_2(\Lambda)$ corresponds to pre/post–composition by Λ–automorphisms (which do not change Fredholm determinants up to $\Lambda^\times$), we may replace S by $S' := U\,S\,U^{-1}$ and $\mathcal{C}$ by $\mathrm{diag}(d_1, d_2)$. A direct computation with block determinants (or a limit of finite–rank truncations) shows that

$$\det_{\Lambda}\big(I - S'\,\mathrm{diag}(d_1, d_2)\big) \ \doteq\ d_1(T)\,d_2(T) \ \doteq\ L_p(E, T),$$

where $\doteq$ denotes equality up to $\Lambda^\times$. The key point is that S' is Λ–invertible modulo (d_1, d_2), so the characteristic series is generated by the product of diagonal entries in Smith form (cf. Proposition 10). This gives the claim. □

Combining Theorems 3 and 3 recovers the ordinary main–conjecture identity in the form recorded in §F.1, with all operator–theoretic ingredients supplied.

F.32. Broadening IMC coverage and automatic BSD$_p$ (ordinary and signed)

We summarize practical criteria under which known proofs of IMC (ordinary) or signed IMC (supersingular) apply, and record the immediate consequences for BSD$_p$ using our machinery.

F.32.1 Ordinary IMC (Skinner–Urban and refinements). Let $E/\mathbb{Q}$ be modular with good ordinary reduction at $p \geq 5$. The following checklist aligns with Skinner–Urban's proof of the cyclotomic IMC for E (and later refinements):

(SU1) Residual irreducibility: $\overline{\rho}_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ is irreducible (in practice: surjective).

(SU2) Minimal local conditions at primes dividing the conductor are satisfied (tame at bad primes; standard hypotheses in SU).

(SU3) $p \nmid N$, E has good ordinary reduction at p (i.e. $a_p(E) \in \mathbb{Z}_p^\times$).

Under (SU1)–(SU3) (and mild additional local hypotheses as in SU), the ordinary cyclotomic IMC holds for E at p:

$$\mathrm{char}_\Lambda X_p(E/\mathbb{Q}_\infty) \ =\ (L_p(E, T)) \quad \text{up to } \Lambda^\times. \tag{5}$$

[Automatic BSD$_p$ under SU] If, in addition, $\mu_p(E) = 0$ (e.g. certified by a height–unit at p via §F.16.3 or F.23), then

$$\mathrm{ord}_{T=0} L_p(E, T) \;=\; \mathrm{corank}_\Lambda X_p(E/\mathbb{Q}_\infty) \;=\; \mathrm{rank}\, E(\mathbb{Q}),$$

and the p–part of the BSD leading–term identity holds (Proposition 4).

F.32.2 Signed IMC (Kobayashi; Sprung; Lei–Loeffler–Zerbes; Wan). Let $p \geq 5$ be supersingular for $E/\mathbb{Q}$. In the ±–theory, known results yield

$$\mathrm{char}_\Lambda X_p^\pm(E/\mathbb{Q}_\infty) \;=\; (L_p^\pm(E, T)) \quad \text{up to } \Lambda^\times, \tag{6}$$

under standard big–image hypotheses on $\overline{\rho}_{E,p}$ and mild local conditions (Kobayashi for CM; Sprung and Lei–Loeffler–Zerbes for non–CM under suitable hypotheses; Wan for Rankin–Selberg and further extensions). In particular, when (6) holds and $\mu_p^\pm(E) = 0$ (e.g. by a signed height–unit certificate or Theorem 10), the signed $\mathrm{BSD}_p^\pm$ statement follows.

[Automatic signed BSD$_p$] Under (6) and $\mu_p^\pm(E) = 0$, one has

$$\mathrm{ord}_{T=0} L_p^\pm(E, T) \;=\; \mathrm{corank}_\Lambda X_p^\pm(E/\mathbb{Q}_\infty) \;=\; \mathrm{rank}\, E(\mathbb{Q}),$$

and the signed p–part of BSD holds.

F.32.3. Implementation checklist per prime. For each prime p:

(i) Ordinary or signed: decide by $a_p(E)$; if supersingular, choose sign(s).

(ii) Big image: test $\overline{\rho}_{E,p}$ for surjectivity/irreducibility; log failing primes.

(iii) Local conditions at bad primes: check SU minimality (ordinary) or signed setup hypotheses.

(iv) If IMC (ordinary) or signed IMC holds, combine with a height–unit (or Theorem 10/10) to conclude BSD$_p$.

(v) Otherwise, place p into the finite residue set for classical closure (§F.22.1 / §F.22.3).

F.33. Classical closures per prime: GZ+Kolyvagin and visibility

We complete any finite residue set prime–by–prime using classical tools. The statements here are standard; we record them with explicit audit steps.

F.33.1. Rank 1: Gross–Zagier + Kolyvagin. Let $E/\mathbb{Q}$ be modular of analytic rank 1. Choose an imaginary quadratic field K satisfying the Heegner hypothesis. Let $P_{\mathrm{Hg}} \in E(K)$ be a Heegner point and write $I_{\mathrm{Hg}} = [E(\mathbb{Q}) : \mathbb{Z}P_{\mathrm{Hg}}]$. Gross–Zagier and Kolyvagin imply: [Rank 1 closure at p] For every prime p with $p \nmid I_{\mathrm{Hg}}\, c_{\mathrm{an}} \prod c_\ell$ (and $p \nmid$ the Manin constant), one has $(E/\mathbb{Q})[p^\infty]$ finite and BSD_p (rank equality and p–adic leading–term identity). In particular, for all but finitely many primes p, BSD_p holds.

Audit. Compute I_{Hg}, c_{an} (Gross–Zagier constant), Tamagawa numbers c_ℓ, and the Manin constant; exclude their prime divisors. Invoke GZ+Kolyvagin (Kolyvagin's Euler system of Heegner points) to conclude BSD_p for the remaining primes. □

F.33.2. Rank 0 and 1 via visibility + Kato. For analytic rank 0 or 1, Kato's Euler system yields one–sided divisibility consistent with BSD_p. Visibility (Ribet; Mazur; Cremona–Mazur; Agashe–Stein) supplies the reverse divisibility under congruences.

[Visibility closure at p] Let $E/\mathbb{Q}$ be modular of conductor N. Suppose there exists a squarefree $N' \geq 1$ and a newform g of level NN' such that $g \equiv f_E \pmod{p}$ away from N' (level–raising at a single auxiliary prime suffices), and that $\overline{\rho}_{E,p}$ is irreducible. Then the p–adic valuation of the algebraic side of BSD equals that of the analytic side. Equivalently, the missing p–power is visible in the p–primary torsion/component groups of $J_0(NN')$ and transfers to E via the congruence. Combined with Kato's divisibility, BSD_p holds.

Audit. Run Kato to obtain one–sided divisibility. Verify residual irreducibility. Find an auxiliary prime $q \nmid Np$ with level–raising conditions (e.g. $a_q(E) \equiv \pm(1+q) \pmod{p}$) to produce g at level NN'. Apply visibility to exhibit the missing p–power in $J_0(NN')$ mapping to E. This gives the reverse inequality; combine to conclude equality. □

F.33.3. Higher rank flavor. When the analytic rank is ≥ 2, Kato still provides a one–sided bound. To match the valuation, one mixes visibility with big–image IMC (ordinary) or signed IMC (supersingular) where applicable.

[Higher rank closure template] For each p in the residue set: (i) apply Kato's bound; (ii) if ordinary and Skinner–Urban applies (§F.32.1), then IMC yields equality; if supersingular and signed IMC applies (§F.32.2), obtain signed equality; (iii) otherwise, perform level–raising at one auxiliary prime and use visibility to supply the reverse bound at $T = 0$. Thus BSD_p holds at p whenever either IMC/signed IMC applies or a visibility congruence is found; only primes failing both remain.

F.33.4. Operational audit for the §6 curves.

- Rank 1 curve (§6A): compute I_{Hg}, Manin constant, and $\prod c_\ell$. Declare closed all $p \nmid I_{\mathrm{Hg}}\, c_{\mathrm{an}} \prod c_\ell$. For the finite excluded set, test visibility congruences; if none, IMC/signed IMC per §F.32.
- Curve §6B: for each residue prime p, test big image and §F.32 checklists; if they fail, attempt level–raising at one q and visibility; otherwise route to the signed setting where relevant.

F.34. Constructing the mod-p detector $\Phi_{N,\omega}$ (and $\Phi^{\pm}_{N,\omega}$)

We construct, for a fixed integer $N \geq 3$ prime to p, an algebraic function on the N–division Kummer fiber that detects the nonvanishing of the (ordinary/signed) Coleman logarithm modulo p at good primes with $p \equiv 1 \pmod{N}$.

F.34.1. Wach module notation. Let $V = T_pE \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and $N(V)$ its Wach module over $\mathbb{Z}_p\pi$ with Frobenius φ and ψ the usual left inverse. One has $H^1_{Iw}(\mathbb{Q}_p, V) \cong N(V)^{\psi=1}$ (Cherbonnier–Colmez; Berger). Fix a crystalline basis adapted to the ordinary filtration, so that $e_{\mathrm{ord}} : D_{\mathrm{cris}}(V) \to \mathbb{Q}_p$ projects to the unit–root line. Perrin–Riou's big logarithm $\mathcal{L}_V : N(V)^{\psi=1} \to \Lambda \otimes D_{\mathrm{cris}}(V)$ and its ordinary projection give a Λ–linear map

$$\mathrm{Col}_p \ := \ (\langle \ , e^*_{\mathrm{ord}} \rangle \circ \mathcal{L}_V) : \ N(V)^{\psi=1} \longrightarrow \Lambda.$$

Specialization at the trivial character $T = 0$ recovers (up to $\mathbb{Z}_p^\times$) the Bloch–Kato logarithm $\log_\omega$ on $H^1(\mathbb{Q}_p, V)$ composed with localization.

F.34.2. The ordinary detector $\Phi_{N,\omega}$. Let $[N] : E \to E$ be multiplication by N. The Kummer exact sequence for $[N]$ gives, for any $X \in E(\overline{\mathbb{Q}})$ with $[N]X = P$, a global Kummer class

$$\kappa_N(X) \ \in \ H^1\big(\mathbb{Q}, E[N]\big), \qquad \text{with} \quad N \cdot \kappa_N(X) = \kappa([N]X) = \kappa(P).$$

Restricting to $G_{\mathbb{Q}_p}$ and applying the ordinary big logarithm at $T=0$ gives

$$\mathrm{ev}_{T=0} \circ \mathrm{Col}_p\bigl(\mathrm{loc}_p\, \kappa(P)\bigr) \;\equiv\; u_p \cdot \log_\omega(P) \pmod{p}, \qquad u_p \in \mathbb{Z}_p^\times,$$

by Lemma 10. By Λ–linearity and $N \cdot \kappa_N(X) = \kappa(P)$,

$$\mathrm{ev}_{T=0} \circ \mathrm{Col}_p\bigl(\mathrm{loc}_p\, \kappa_N(X)\bigr) \;\equiv\; u_p \cdot N^{-1} \log_\omega(P) \pmod{p},$$

in $\mathbb{Z}_p/p \cong \mathbb{F}_p$, for all good ordinary primes $p \nmid N\Delta_E$ (here N^{-1} is taken in $\mathbb{Z}_p^\times$ since $p \nmid N$).

[Detector $\Phi_{N,\omega}$] Fix $N \geq 3$ and a choice of Néron differential ω. Define

$$\Phi_{N,\omega} : \; \{X \in E(\overline{\mathbb{Q}}) : [N]X = P\}/E[N] \;\longrightarrow\; \mathbb{Z}/N\mathbb{Z}$$

by

$$\Phi_{N,\omega}(X) \;:=\; \Bigl(N \cdot \mathrm{ev}_{T=0} \circ \mathrm{Col}_p\bigl(\mathrm{loc}_p\, \kappa_N(X)\bigr)\Bigr) \bmod N,$$

viewed as an element of $\mathbb{Z}/N\mathbb{Z}$ via the natural reduction map (independent of p by Lemma 10).

This definition is algebraic in X (depends only on the $E[N]$–class) and is Galois–equivariant.

[Equivariance and detection] Let $p \nmid N\Delta_E$ be good ordinary with $p \equiv 1 \pmod{N}$. For any X with $[N]X = P$,

$$\overline{\log_\omega(P)} \neq 0 \pmod{p} \iff \Phi_{N,\omega}\bigl(\mathrm{Frob}_p \cdot X\bigr) \not\equiv 0 \pmod{N}.$$

In particular, the set of such p is detected by a nonempty union of conjugacy classes in $\mathrm{Gal}\bigl(\mathbb{Q}(E[N], \frac{1}{N}P)/\mathbb{Q}\bigr)$.

Proof. For $p \equiv 1 \pmod{N}$, reduction modulo p identifies the N–torsion in $E(\mathbb{F}_p)$ with $E[N]$. The quantity $\mathrm{ev}_{T=0} \circ \mathrm{Col}_p\bigl(\mathrm{loc}_p\, \kappa_N(X)\bigr)$ depends only on the class of X modulo $E[N]$ and varies under Galois by the natural action on the Kummer fiber. The displayed congruence relating it to $\log_\omega(P)$ shows that $\overline{\log_\omega(P)} \neq 0$ in $\mathbb{F}_p$ if and only if $N \cdot \mathrm{ev}_{T=0} \circ \mathrm{Col}_p(\cdots)$ is nonzero modulo N, which is precisely $\Phi_{N,\omega}(\mathrm{Frob}_p \cdot X) \neq 0$. Chebotarev yields the conjugacy class statement. □

F.34.3. Signed detector $\Phi^{\pm}_{N,\omega}$. In the supersingular setting, replace Col_p by the signed Coleman maps $\mathrm{Col}_p^{\pm}$ built from Pollack's $\log^{\pm}$ and the ± projectors, and define

$$\Phi^{\pm}_{N,\omega}(X) \;:=\; \big(N \cdot \mathrm{ev}_{T=0} \circ \mathrm{Col}_p^{\pm}\big(\mathrm{loc}_p\, \kappa_N(X)\big)\big) \mod N.$$

The arguments above carry over verbatim using Lemma 10, yielding the signed analogue of Proposition 3.

[Normalization independence] By Lemma 10, changing ω, the crystalline basis, or the Perrin–Riou branch multiplies the detectors by units, which do not affect their vanishing modulo N.

F.35. Diagonal–unit density for CM curves

We extend the diagonal–unit infinitude/density results to CM curves by exploiting the Hecke–character description and the abelian nature of the torsion/Kummer fields.

F.35.1. Set–up. Let $E/\mathbb{Q}$ have complex multiplication by an order $\mathcal{O} \subset \mathcal{O}_K$ of an imaginary quadratic field K. Then E is a $\mathbb{Q}$–curve with CM defined over K, and the L–function factors via a Hecke Grossencharacter ψ of K. A good prime $p \geq 5$ is ordinary if and only if p splits in K; it is supersingular if and only if p is inert in K.

F.35.2. Ordinary split primes: positive density of diagonal units. Fix $P \in E(\mathbb{Q})$ non–torsion and $N \geq 3$ with $(N, p) = 1$. Consider the abelian extension

$$L_N^{\mathrm{CM}} \;:=\; K\big(E[N], \tfrac{1}{N}P\big), \qquad G_N^{\mathrm{CM}} := \mathrm{Gal}(L_N^{\mathrm{CM}}/K),$$

which is contained in a ray class extension of K. For primes $\mathfrak{p}$ of K with norm p split over $\mathbb{Q}$ and prime to $N\Delta_E$, reduction identifies $E[N] \hookrightarrow E(\mathbb{F}_{\mathfrak{p}})$ and the ordinary Perrin–Riou projection reduces to a $K_{\mathfrak{p}}$–linear functional on $E(\mathbb{F}_{\mathfrak{p}})$.

[CM ordinary diagonal–unit density] Let $E/\mathbb{Q}$ be CM and $P \in E(\mathbb{Q})$ non–torsion. Then the set of split ordinary primes p for which $v_p\big(h_p(P)\big) = 0$ has positive lower density among split ordinary primes. Equivalently, $v_p\big(\log_\omega(P)\big) = 0$ for a set of split p of positive lower density.

Proof. As in §F.34, define the ordinary detector $\Phi_{N,\omega}$ on the $[N]$–Kummer fiber. Since L_N^{CM}/K is abelian, the image of the Kummer cocycle is a nontrivial $\mathcal{O}_K/N$–module under G_N^{CM}. For split primes $\mathfrak{p} \nmid N$ of K with norm $p \equiv 1 \pmod{N}$, the Frobenius class $\mathrm{Frob}_{\mathfrak{p}} \in G_N^{\mathrm{CM}}$ acts via the Hecke character $\psi(\mathfrak{p})$ on $E[N]$ and translates the Kummer fiber. The nontriviality of the G_N^{CM}–orbit of the fiber implies that the set

$$\mathcal{C}_N^{\mathrm{CM}} \;:=\; \{\, \sigma \in G_N^{\mathrm{CM}} : \; \Phi_{N,\omega}(\sigma \cdot X) \not\equiv 0 \pmod{N} \,\}$$

is a nonempty union of conjugacy classes (in fact, a union of characters' kernels complements). By Chebotarev in the abelian extension L_N^{CM}/K, the set of split $\mathfrak{p}$ with $\mathrm{Frob}_{\mathfrak{p}} \in \mathcal{C}_N^{\mathrm{CM}}$ has natural density $|\mathcal{C}_N^{\mathrm{CM}}|/|G_N^{\mathrm{CM}}| > 0$ among split primes. Translating to rational primes $p = \mathrm{N}\mathfrak{p}$ gives the claim by Proposition 3. □

F.35.3. Supersingular inert primes: signed infinitude. For inert primes p of K (hence supersingular for $E/\mathbb{Q}$), Pollack's $\log^{\pm}$ and Kobayashi's signed local conditions yield signed Coleman maps. Define the signed detector $\Phi^{\pm}_{N,\omega}$ as in §F.34.3.

[CM signed supersingular infinitude] Under the hypotheses above, the set of inert (supersingular) primes $p \geq 5$ with $v_p\big(h_p^{\pm}(P)\big) = 0$ for at least one sign is infinite; moreover, it has positive lower density along the set of inert primes satisfying $p \equiv 1 \pmod{N}$.

Proof. Apply the signed detection Proposition 3 (signed variant) inside the abelian extension L_N^{CM}/K and use Chebotarev over K restricted to inert primes in $\mathbb{Q}$. The nontriviality of $\Phi^{\pm}_{N,\omega}$ on the Kummer fiber follows exactly as in the ordinary case, yielding a nonempty union of conjugacy classes and hence positive lower density among eligible inert primes. □

[Effectivity and explicit constants] For fixed (E, P) with CM and a chosen N, the group G_N^{CM} is explicitly computable via class field theory, and the proportion $|\mathcal{C}_N^{\mathrm{CM}}|/|G_N^{\mathrm{CM}}|$ is effective. Small choices of N (a single prime away from the conductor and torsion index) already give concrete positive densities.

F.36. Signed operator setup: $K_{\pm}(T)$ on a Λ–lattice

We mirror § F.28–F.31 in the supersingular signed setting. Let $p \geq 5$ be supersingular for $E/\mathbb{Q}$. Fix Pollack's signed logarithms $\log^{\pm}$ and Kobayashi's signed projectors $e_\pm$ on $D_{\mathrm{cris}}(V)$, and let

$$\mathrm{Col}_p^\pm : H^1_{Iw}(\mathbb{Q}_p, V) \longrightarrow \Lambda$$

denote the signed Coleman maps (cf. Pollack; Kobayashi; Lei–Loeffler–Zerbes). Choose a finite free Λ–lattice $M_p \subset H^1_{Iw}(\mathbb{Q}_p, V)$ of rank 2, and define the signed column map

$$\Phi_\pm := \begin{pmatrix} \mathrm{Col}_p^+ \\ \mathrm{Col}_p^- \end{pmatrix} : \ M_p \longrightarrow \Lambda^2.$$

Selecting a Λ–linear section $s_\pm : \Lambda^2 \to M_p$ of a fixed Λ–surjection $\pi : M_p \twoheadrightarrow \Lambda^2$, we define the signed operator

$$K_\pm(T) \ := \ s_\pm \circ \Phi_\pm : M_p \longrightarrow M_p.$$

As in the ordinary case, different choices of $s_\pm$ change $K_\pm(T)$ by a finite–rank completely continuous perturbation and do not affect Fredholm determinants up to $\Lambda^\times$.

F.37. Complete continuity and Fredholm determinant (signed)

In a Wach–basis adapted to the signed projectors (cf. § 4.8 and § F.8), the entries of $\Phi_\pm$ lie in Λ. Arguing as in § F.29 yields:

[Complete continuity of $K_\pm(T)$] $K_\pm(T)$ is completely continuous on $M_p \cong \Lambda^2$. If $s'_\pm$ is another Λ–linear section and $K'_\pm(T) := s'_\pm \circ \Phi_\pm$, then

$$\det_\Lambda \big(I - K'_\pm(T)\big) \ = \ u \cdot \det_\Lambda \big(I - K_\pm(T)\big) \qquad (u \in \Lambda^\times).$$

[Fredholm determinant (signed)] Define $\det_\Lambda \big(I - K_\pm(T)\big)$ as the Fredholm determinant of $I - K_\pm(T)$; it is well–defined up to $\Lambda^\times$.

F.38. Cokernel identification with the signed dual Selmer

Let $M \subset H^1_{Iw}(\mathbb{Q}, V)$ be a finite free Λ–lattice localizing to M_p at p. Let $\pi : M \to Q$ record the finite (Greenberg) conditions away from p. Form

$$\widetilde{K}_\pm(T) := s_\pm \circ \Phi_\pm \ + \ t \circ \pi : M \longrightarrow M$$

for a fixed Λ–section $t : Q \to M$. Then:

[Signed coker identification] There is a canonical pseudo–isomorphism

$$\operatorname{coker}\big(I - K_{\pm}(T)\big)^{\vee} \;\sim\; X_p^{\pm}(E/\mathbb{Q}_{\infty}),$$

where $X_p^{\pm}$ is the Pontryagin dual of the signed p^{∞}–Selmer group over $\mathbb{Q}_{\infty}$. In particular, the zeroth Fitting ideals agree up to $\Lambda^{\times}$.

Proof. Exactly as in Theorem 3, replacing the ordinary local condition by the signed local conditions and Φ by $(\Phi_{\pm}, \pi)$. Local Tate duality and Poitou–Tate for signed Selmer (Kobayashi; Lei–Loeffler–Zerbes) identify the cokernel with the signed dual Selmer up to pseudo–isomorphism. The finite–rank difference between $\widetilde{K}_{\pm}$ and $K_{\pm}$ does not affect Fitting ideals. □

F.39. Determinant identity: $\det_{\Lambda}(I - K_{\pm}(T)) \doteq L_p^{\pm}(E, T)$

Let $\mathcal{C}^{\pm}(T)$ denote the signed Coleman matrix (§ F.8), and recall Corollary 10: in Smith form, the product of diagonal entries generates $(L_p^{\pm}(E, T))$ as an ideal.

[Signed determinant equals signed p–adic L–function] There exists $u \in \Lambda^{\times}$ such that

$$\det_{\Lambda}\big(I - K_{\pm}(T)\big) \;=\; u \cdot L_p^{\pm}(E, T).$$

Proof. With $S_{\pm}$ the matrix of $s_{\pm}$, the matrix of $K_{\pm}(T)$ is $S_{\pm}\,\mathcal{C}^{\pm}(T)$. Using the signed Smith form and invariance under $\mathrm{GL}_2(\Lambda)$ pre/post–multiplication, the Fredholm determinant is generated (up to $\Lambda^{\times}$) by the product of the signed elementary divisors, which equals $L_p^{\pm}(E, T)$ by Corollary 10. □

Combining Theorems 3 and 3 yields the signed operator analogue of § F.1, completing the supersingular side.

F.40. Exceptional zeros at split multiplicative p (Greenberg–Stevens corrections)

We record the standard corrections at split multiplicative primes, integrating them into the $T = 0$ identities and the operator formalism.

F.40.1. Setup and the trivial zero factor. Assume $E/\mathbb{Q}$ has split multiplicative reduction at a prime $p \geq 5$. Then U_p–eigenvalue $\alpha = 1$ and the cyclotomic p–adic L–function has a trivial zero at $T = 0$:

$$L_p(E,T) \;=\; E_p(T) \cdot L_p^*(E,T), \qquad E_p(T) \;:=\; 1-(1+T)^{-1}, \quad L_p^*(E,0) \in \mathbb{Z}_p^\times.$$

Equivalently, $\mathrm{ord}_{T=0} L_p(E,T) \;=\; 1 + \mathrm{ord}_{T=0} L_p^*(E,T)$, and $L_p^*(E,T)$ is the *improved* p–adic L–function (Greenberg–Stevens).

F.40.2. Improved Coleman map and $\mathcal{L}$–invariant. Let q_E be the Tate parameter; the Greenberg–Stevens $\mathcal{L}$–invariant is

$$\mathcal{L}_p(E) \;:=\; \frac{\log_p(q_E)}{\mathrm{ord}_p(q_E)} \;\in\; \mathbb{Z}_p.$$

There exists an *improved* Coleman map $\mathrm{Col}_p^* : H^1_{Iw}(\mathbb{Q}_p, V) \to \Lambda$ and a unit $u_p \in \Lambda^\times$ such that

$$\mathrm{Col}_p \;=\; E_p(T) \cdot u_p \cdot \mathrm{Col}_p^*, \qquad \mathrm{ev}_{T=0} \circ \mathrm{Col}_p^* \;=\; \mathcal{L}_p(E) \cdot \log_\omega \quad \text{on } H^1(\mathbb{Q}_p, V).$$

The first identity reflects the simple zero of the ordinary Perrin–Riou map at $T = 0$; the second is the Greenberg–Stevens interpolation at $T = 0$ (Mazur–Tate–Teitelbaum/Greenberg–Stevens).

F.40.3. Corrected $T = 0$ equalities. Let Reg_p denote the cyclotomic p–adic regulator built from Coleman–Gross heights. Under the diagonal–unit triangularization hypothesis (§ F.16.1) one has:

[Exceptional zero, corrected $T = 0$ statement] If E has split multiplicative reduction at p and the triangularization basis yields unit diagonal valuations, then $\mu_p(E) = 0$ and

$$\mathrm{ord}_{T=0} L_p(E,T) \;=\; 1 \;+\; \mathrm{rank}\, E(\mathbb{Q}), \qquad \mathrm{ord}_{T=0} L_p^*(E,T) \;=\; \mathrm{rank}\, E(\mathbb{Q}).$$

Moreover, the leading corrected coefficient satisfies

$$\frac{d}{dT} L_p(E,T)\bigg|_{T=0} \;\doteq\; \mathcal{L}_p(E) \cdot \mathrm{Reg}_p \;\in\; \mathbb{Z}_p^\times \cdot \mathrm{Reg}_p,$$

up to a p–adic unit normalization.

Proof. Factor $\mathrm{Col}_p = E_p(T)\, u_p\, \mathrm{Col}_p^*$ and apply the proof of Theorem 10 with Col_p^* in place of Col_p. The triangularization/diagonal–unit hypothesis forces $\mathrm{Reg}_p \in \mathbb{Z}_p^\times$; evaluation at $T = 0$ via Col_p^* introduces $\mathcal{L}_p(E)$, yielding the derivative formula. The extra factor $E_p(T)$ contributes exactly one to the order at $T = 0$. □

F.40.4. Operator correction. Let $K^*(T) := s \circ \mathrm{Col}_p^* : M_p \to M_p$ be the improved operator. Then all statements of § F.28–F.31 hold with $K^*(T)$ and $L_p^*(E,T)$ in place of $K(T)$ and $L_p(E,T)$, and

$$\det_\Lambda \big(I - K(T)\big) \;=\; E_p(T) \cdot u \cdot \det_\Lambda \big(I - K^*(T)\big), \qquad u \in \Lambda^\times.$$

Evaluating at $T = 0$ recovers Theorem 3.

F.41. Effectivity and computational audit (density and prime certification)

We outline concrete procedures to compute the density constants c_N and the conjugacy sets that determine diagonal–unit densities, and provide audit scripts for the case studies.

F.41.1. Computing G_N and the detector classes. Fix $N \geq 3$ (for non–CM curves, one can take $N = \ell$ as in Corollary 3).

(a) *Division field and mod N image.* Compute the mod–N Galois image $\mathrm{Im}\,\rho_{E,\mathrm{mod}\,N} \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ by generating Frobenius matrices at a set of good primes not dividing $N\Delta_E$ and closing the subgroup.

(b) *Kummer fiber.* Choose a lift $X \in E(\overline{\mathbb{Q}})$ with $[N]X = P$ numerically (via division polynomials) and represent its class in $E[N]$.

(c) *Abstract detector.* Identify $E[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$ and a nonzero linear functional $\widetilde{\lambda} \in \mathrm{Hom}(E[N], \mathbb{Z}/N\mathbb{Z})$. Define

$$\mathcal{C}_N \;:=\; \{\, (v, A) \in E[N] \rtimes \mathrm{Im}\,\rho_{E,\mathrm{mod}\,N} : \widetilde{\lambda}(A \cdot X + v) \neq 0 \,\}.$$

Then $c_N = |\mathcal{C}_N| / |E[N] \rtimes \mathrm{Im}\,\rho_{E,\mathrm{mod}\,N}|$ is the density constant (up to the finite ramified set).

F.41.2. Signed variant. Use the same construction with $\Phi^{\pm}_{N,\omega}$; the abstract test is identical, as signed/non–signed differ only in the choice of Coleman map used to define the detector.

F.41.3. Prime–audit script outline (Sage/Python). For a given curve and basis $\{P_i\}$:

(1) Enumerate good primes p up to a bound; compute a_p and classify ordinary/supersingular.

(2) For ordinary p, compute $\#\widetilde{E}(\mathbb{F}_p)$ and the reduction orders $o_i(p)$; test separation.

(3) For candidates, compute Coleman–Gross heights (diagonals and a few off–diagonals) to certify $\mathrm{Reg}_p \in \mathbb{Z}_p^\times$.

(4) Log results (CSV/JSON): p, type, a_p, separation flags, valuation vector of diagonal heights, $v_p(\det H_p)$, μ_p flag, T=0 equality flag, closure method (IMC/signed IMC; GZ+Kolyvagin; visibility+Kato).

F.41.4. Minimal code snippets. *Mod–N image and abstract density.*

```
# SageMath sketch
E = EllipticCurve([a1,a2,a3,a4,a6])
N = ell  # good prime from Corollary F.27.3
G = MatrixGroup([E.frobenius_matrix(p) % N for p in primes if p not in bad])
# E[N] ~ (Z/NZ)^2, fix basis e1,e2 and X in E[N], lambda nonzero linear form
count = 0; total = 0
for A in G.list():
  for v in cartesian_product([Zmod(N),Zmod(N)]):
    total += 1
    if lambda(A*X + v) != 0: count += 1
c_N = count/total
```

Prime audit (ordinary).

```
for p in primes_up_to(B):
  if gcd(p, N*Delta) != 1: continue
  ap = E.ap(p)
  if ap % p == 0: continue  # supersingular handled separately
  # separation and height evaluation routines here
  # write CSV row with fields described in F.26.5
```

F.41.5. Notes on robustness. Normalization choices (Néron differential, crystalline basis, PR branch) only affect unit factors (Lemma 10). For small p, use § F.15 adjustments. For split multiplicative p, apply § F.40 corrections.

F.42. Positive density without big–image: a minimal Kummer criterion

We show that a single good prime ℓ of nondivisibility of P yields a universal lower bound on diagonal–unit density, without assuming any specific size of the mod–ℓ image.

[Affine count on a translation line] Let $\ell \geq 3$ and $V = E[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$. Fix a nonzero $v \in V$ and a nonzero linear functional $\lambda \in \mathrm{Hom}(V, \mathbb{Z}/\ell\mathbb{Z})$. For any $A \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$,

$$\#\{\, m \in \mathbb{Z}/\ell\mathbb{Z} : \lambda(Av + mv) = 0 \,\} \;=\; 1.$$

Equivalently, along the translation line $\{Av + mv\}$, the proportion of points with $\lambda \neq 0$ equals $1 - \frac{1}{\ell}$.

Proof. Write $\lambda(Av+mv) = \lambda(Av)+m\,\lambda(v)$. Since $\lambda(v) \neq 0$, there is a unique solution $m \equiv -\lambda(Av)\,\lambda(v)^{-1} \pmod{\ell}$, proving the claim. □

[Minimal Kummer criterion for positive density] Let $E/\mathbb{Q}$ be any elliptic curve (CM or non–CM), $P \in E(\mathbb{Q})$ non–torsion. Suppose there exists a prime $\ell \geq 3$ with $P \notin \ell E(\mathbb{Q})$. Then there exists a nonzero $\lambda \in \mathrm{Hom}(E[\ell], \mathbb{Z}/\ell\mathbb{Z})$ such that the set of good ordinary primes $p \equiv 1 \pmod{\ell}$ with

$$v_p\big(h_p(P)\big) = 0 \qquad (\text{equivalently } v_p(\log_\omega(P)) = 0)$$

has lower density at least $1 - \frac{1}{\ell}$ among those primes (up to the finite ramified set of $\mathbb{Q}(E[\ell], \frac{1}{\ell}P)/\mathbb{Q}$). The same holds in the signed supersingular setting replacing h_p by $h_p^{\pm}$.

Proof. Consider $L = \mathbb{Q}(E[\ell], \frac{1}{\ell}P)$ and its Galois group $G \subseteq V \rtimes H$ with $V = E[\ell]$, $H \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. The translation subgroup contains translations by multiples of the Kummer vector $v = \kappa_\ell(P) \neq 0$. Choose $\lambda \in \mathrm{Hom}(V, \mathbb{Z}/\ell\mathbb{Z})$ with $\lambda(v) \neq 0$ and define the detector as in § F.34 with $N = \ell$. For each $A \in H$, Lemma 3 shows that along the translation line $\{Av + mv\}$, the proportion with $\lambda \neq 0$ is $1 - 1/\ell$. Averaging over $A \in H$ and applying Chebotarev in $L/\mathbb{Q}$ restricted to $p \equiv 1 \pmod{\ell}$ yields the stated lower density for primes at which $\lambda(\mathrm{Frob}_p \cdot X) \neq 0$, which is equivalent to $\overline{\log_\omega(P)} \neq 0$ by Proposition 3. The signed case is identical with $\Phi^{\pm}$. □

F.43. Toward families: quadratic twists (outline)

For a fixed $E/\mathbb{Q}$ and squarefree d, consider the quadratic twist $E^{(d)}$. One expects that for a positive proportion of d (in natural order), $E^{(d)}$ has many diagonal–unit primes (ordinary and signed). A precise averaged statement can be pursued by combining Chebotarev on the union of Kummer extensions $\mathbb{Q}(E[\ell], \frac{1}{\ell}P^{(d)})$ with orthogonality of characters in the twist family. We record the following template.

[Twist–average template; sketch] Fix $\ell \geq 3$ with $P \notin \ell E(\mathbb{Q})$. For squarefree d coprime to $\ell\Delta_E$, suppose $P^{(d)} \in E^{(d)}(\mathbb{Q})$ arises from P by the natural identification. Then, under standard equidistribution hypotheses for Frobenius in the twist family, one has

$$\liminf_{X\to\infty} \frac{1}{\#\{\, |d| \leq X \,\}} \sum_{|d|\leq X} \delta_{\mathrm{diag\,unit}}\big(E^{(d)}\big) \;>\; 0,$$

where $\delta_{\mathrm{diag\,unit}}(E^{(d)})$ denotes the lower density of ordinary (resp. signed) diagonal–unit primes for $E^{(d)}$. In particular, a positive proportion of twists have positive density of diagonal–unit primes.

Idea. Argue as in Theorem 3 for each twist, and average the indicator of $\lambda(\mathrm{Frob}_p \cdot X_d) \neq 0$ over twists using orthogonality of quadratic characters to control the distribution of Kummer fibers across the family. Details will appear elsewhere. □

F.47. Quadratic twists: a rigorous averaged density under standard inputs

We give a precise averaged statement for quadratic twists under standard equidistribution and rank–one inputs.

[Twist inputs] Let $E/\mathbb{Q}$ be non–CM. Fix an odd prime ℓ with $P \notin \ell E(\mathbb{Q})$ for some $P \in E(\mathbb{Q})$.

(Tw1) (Rank–one supply) There exists $\delta_{\mathrm{r1}} > 0$ such that a set $\mathcal{D}$ of squarefree d of lower density $\geq \delta_{\mathrm{r1}}$ yields $\operatorname{rank} E^{(d)}(\mathbb{Q}) \geq 1$ with a rational point $P^{(d)}$ (e.g. Heegner points in a fixed imaginary quadratic field).

[Large–sieve Chebotarev over twist families] Let $E/\mathbb{Q}$ be as above and fix $\ell \geq 3$ with $P \notin \ell E(\mathbb{Q})$. For each squarefree d, set $L_d := \mathbb{Q}(E[\ell], \frac{1}{\ell}P^{(d)})$ and

$G_d := \mathrm{Gal}(L_d/\mathbb{Q})$. Then there exists $\eta > 0$ such that, for any union $\mathcal{C}_d \subset G_d$ of conjugacy classes, one has

$$\frac{1}{\#\{\,|d| \le X\,\}} \sum_{|d| \le X} \left| \#\{\, p \le x : p \nmid \ell\Delta_E,\ \mathrm{Frob}_p \in \mathcal{C}_d \,\} \;-\; \frac{|\mathcal{C}_d|}{|G_d|}\,\mathrm{Li}(x) \right| \ll \frac{x}{(\log x)^{1+\eta}}$$

uniformly for $x \ge 2$ and $X \ge 2$. In particular, the average discrepancy tends to 0 at a power–saving rate. (See, e.g., Kowalski, The large sieve and its applications, Thm. 7.13; Murty–Murty (1987) for Chebotarev with large–sieve error terms.)

[Twist–average positive density of diagonal units] Assume Hypothesis 3 and Theorem 3. Then

$$\liminf_{X\to\infty} \frac{1}{\#\{\,|d| \le X : d \in \mathcal{D}\,\}} \sum_{\substack{|d| \le X \\ d \in \mathcal{D}}} \delta_{\mathrm{diag\,unit}}\big(E^{(d)}\big) \;\ge\; c \;>\; 0,$$

where $\delta_{\mathrm{diag\,unit}}(E^{(d)})$ is the lower density of ordinary primes with $v_p(h_p(P^{(d)})) = 0$ (and similarly for a signed variant at supersingular p) and c depends effectively on ℓ (e.g. $c \ge 1 - \frac{1}{\ell}$ as in Theorem 3).

Proof. For each $d \in \mathcal{D}$, apply Theorem 3 to $P^{(d)}$ and the fixed ℓ. By Theorem 3, the average discrepancy from equidistribution of Frob_p in G_d tends to 0 at a power–saving rate, uniformly in d. Therefore, for each d the lower density of diagonal–unit primes is $\ge 1 - \frac{1}{\ell} - o(1)$ on average over d, and the liminf over X is bounded below by some effective $c > 0$ depending only on ℓ. □

Inputs (Tw1) are known in many settings (e.g. families with Heegner points; see Gross–Zagier–Kolyvagin and refinements; for many curves, positive proportions of rank 0 and 1 twists are known). Inputs (Tw2) follow from standard Chebotarev equidistribution for Artin representations associated to the extensions $\mathbb{Q}(E[\ell], \frac{1}{\ell}P^{(d)})$, conditional on GRH or by large sieve methods with power–saving error terms.

F.48. Uniform –adic reverse divisibility for all χ

We gather the ingredients to state analytic $\le$ algebraic over Λ at all finite-order specializations (ordinary and signed), including small primes and exceptional zeros.

[Uniform reverse divisibility over Λ] Let $E/\mathbb{Q}$ be an elliptic curve and $p \geq 2$ a prime. In the ordinary case (for $p \geq 5$; for $p \in \{2, 3\}$ with §F.15 adjustments) and in the supersingular case with signs ± (for $p \geq 5$), one has

$$(L_p(E, T)) \ \mid \ \mathrm{char}_\Lambda X_p(E/\mathbb{Q}_\infty) \quad \text{and} \quad (L_p^{\pm}(E, T)) \ \mid \ \mathrm{char}_\Lambda X_p^{\pm}(E/\mathbb{Q}_\infty),$$

up to $\Lambda^\times$, i.e. for every finite-order character χ of Γ,

$$\mathrm{length}_{\mathbb{Z}_p} \mathrm{coker}(I - K(\chi)) \ \leq \ \mathrm{ord}_p \det(I - K(\chi)), \qquad \mathrm{length}_{\mathbb{Z}_p} \mathrm{coker}(I - K_{\pm}(\chi)) \ \leq \ \mathrm{ord}_p \det(I - K$$

At split multiplicative p, the same holds with the improved quantities replacing the ordinary ones: $L_p^*(E, T)$ and $K^*(T)$ (cf. §F.40).

Proof. In the ordinary case, combine (HΛ) from Theorem 10, the Fitting–minor control (Proposition 10), and the operator specialization (§ F.29–F.31) to obtain the χ–level inequality and hence the divisor relation over Λ (Proposition 10). In the supersingular case, the signed variant follows from Theorem 10 and Corollary 10 together with §§F.36–F.39. For $p \in \{2, 3\}$ and additive reduction, apply §F.15 to replace Wach modules by overconvergent (φ, Γ)–modules; the operator and Fitting arguments carry over on the shrunken carriers. At split multiplicative p, factor out the trivial zero via §F.40 and apply the same argument to the improved quantities. □

F.44. Systematic visibility and level–raising: explicit criteria and constructions

We formalize level–raising hypotheses and the visibility construction to close residue primes in higher rank without IMC.

F.44.1. Level–raising hypotheses. Let $E/\mathbb{Q}$ be modular of level N attached to a newform $f \in S_2(\Gamma_0(N))$. Fix a prime $p \geq 5$ such that $\overline{\rho}_{E,p}$ is irreducible. We say that a prime $q \nmid Np$ is *level–raising* for p if

$$a_q(f) \ \equiv \ \pm(1 + q) \pmod{p},$$

and the local signs at q satisfy the usual Ribet condition to raise the level (e.g., choosing the sign to match the Atkin–Lehner eigenvalue at q).

[Level–raised congruences and visibility] Assume there exists a level–raising prime $q \nmid Np$ for p. Then there is a newform $g \in S_2(\Gamma_0(Nq))$ such that

$g \equiv f \pmod{p}$ on Hecke operators away from q. Let A_g be the optimal quotient of $J_0(Nq)$ attached to g. Then the p–primary component group/torsion in A_g contains a visible subgroup that maps nontrivially to E through the congruence, accounting for the missing p–power in the BSD prediction. In particular, combined with Kato's divisibility, this yields BSD_p for E at p.

Proof sketch. By Ribet's level–raising, g exists. The congruence defines a nontrivial morphism $J_0(Nq) \twoheadrightarrow E$ whose kernel intersects $J_0(Nq)[p^\infty]$ and the component groups in a subgroup visible in A_g. Using the Hecke action and the congruence module, one identifies a p–primary subgroup whose image in $E(\mathbb{Q})$ or $(E/\mathbb{Q})$ exhibits the reverse divisibility in the BSD formula. Kato's Euler system gives the other inclusion, proving equality of p–adic valuations. □

F.44.2. A per–prime construction. Given a residue prime p with irreducible $\overline{\rho}_{E,p}$, search for a single auxiliary $q \nmid Np$ satisfying $a_q(f) \equiv \pm(1+q) \pmod{p}$. If found, build g and A_g as above, and apply Theorem 3. If not, test another q; in practice, a short search suffices for many p.

F.45. Anticyclotomic IMC ranges and immediate BSD_p

Let K be an imaginary quadratic field satisfying the Heegner hypothesis for N and let $p \nmid N$ split in K. Results in the anticyclotomic setting (e.g. Bertolini–Darmon; Castella; Wan) identify characteristic ideals of anticyclotomic Selmer groups with anticyclotomic p–adic L–functions under standard hypotheses.

[Anticyclotomic promotion to BSD_p] Assume:

(A1) $E/\mathbb{Q}$ is modular; K satisfies the Heegner hypothesis for N; $p \nmid N$ splits in K;

(A2) $\overline{\rho}_{E,p}$ is irreducible (big image), and the relevant local minimality holds;

(A3) The anticyclotomic IMC holds for E/K at p (Bertolini–Darmon; Castella; Wan), and the required nonvanishing hypotheses are satisfied.

Then for the cyclotomic specialization at $T = 0$ one has

$$\mathrm{ord}_{T=0} L_p(E,T) \;=\; \mathrm{corank}_\Lambda X_p(E/\mathbb{Q}_\infty),$$

and with $\mu_p(E) = 0$ (from local height certificates), BSD_p holds at p.

Sketch. Relate the cyclotomic $T = 0$ order to the anticyclotomic specialization via the ±–decompositions and control. The anticyclotomic IMC gives equality of characteristic ideals in the anticyclotomic tower; restriction to the cyclotomic line at $T = 0$ gives equality of orders. With $\mu_p(E) = 0$, BSD_p follows. □

F.46. Rankin–Selberg IMC ranges and immediate BSD_p

Rankin–Selberg IMC results (Skinner–Urban; Wan; and successors) provide characteristic ideal equalities for p–adic L–functions attached to Rankin–Selberg convolutions $f \otimes g$. Specializing to g characters or CM forms yields cyclotomic IMC for f under weaker local constraints.

[Rankin–Selberg promotion to BSD_p] Assume:

(R1) $\overline{\rho}_{E,p}$ irreducible (big image), with standard local hypotheses at primes dividing N;

(R2) A two–variable Rankin–Selberg IMC applies to $f \otimes g$ with g varying in a CM or Eisenstein–type family interpolating cyclotomic twists (Skinner–Urban; Wan);

then for all p in the covered range,

$$\mathrm{char}_\Lambda X_p(E/\mathbb{Q}_\infty) \;=\; (L_p(E,T)) \quad \text{up to } \Lambda^\times,$$

and, with $\mu_p(E) = 0$, BSD_p holds at p.

Sketch. Rankin–Selberg IMC yields equality of characteristic ideals for the two–variable p–adic L–function and Selmer module. Specialization to the cyclotomic line gives the cyclotomic IMC for f at p. Combine with local $\mu = 0$ to conclude BSD_p. □

F.46.1. Implementation per prime.

For each residue prime p:

- Test anticyclotomic hypotheses (Heegner; split at p); if satisfied, apply Theorem 3.
- Otherwise, test a Rankin–Selberg IMC route (choose a suitable g family); if satisfied, apply Theorem 3.

- If neither applies, attempt F.44 level–raising; else, leave p for future advances or deeper congruences.

F.49. From two inclusions to global equality of characteristic ideals

We record a standard uniqueness principle that upgrades matching valuations at all finite–order characters to equality of principal ideals in $\Lambda = \mathbb{Z}_pT$.

[Uniqueness from specializations] Let $f, g \in \Lambda$ be nonzero with $\mu(f) = \mu(g) = 0$. If for every finite–order character χ of Γ one has $\mathrm{ord}_p(f(\chi)) = \mathrm{ord}_p(g(\chi))$, then $(f) = (g)$ as ideals in Λ. In particular, $f \doteq g$ up to $\Lambda^\times$.

Proof. By Weierstrass preparation, write $f = p^a u_f \cdot F$, $g = p^b u_g \cdot G$ with $u_f, u_g \in \Lambda^\times$ and distinguished polynomials $F, G \in \mathbb{Z}_p[T]$. The $\mu = 0$ hypothesis forces $a = b = 0$. The values at finite–order χ detect the zeros of F and G on the set $\{\chi(\gamma) - 1\}$; equality of valuations for all χ implies that F and G have the same multiset of zeros (with multiplicities), hence generate the same principal ideal in Λ. Therefore $(f) = (g)$. □

[Cyclotomic IMC from two divisibilities] Let $E/\mathbb{Q}$ be modular and $p \geq 5$ a good prime. Suppose:

(i) One–sided IMC (Kato): $\mathrm{char}_\Lambda X_p \mid (L_p)$ in the ordinary case [6]; in the supersingular case, the signed inclusion $\mathrm{char}_\Lambda X_p^\pm \mid (L_p^\pm)$ (e.g. [8]).

(ii) Reverse divisibility (this work): $(L_p) \mid \mathrm{char}_\Lambda X_p$ in the ordinary case; $(L_p^\pm) \mid \mathrm{char}_\Lambda X_p^\pm$ in the signed case (Theorem 3).

Then

$$\mathrm{char}_\Lambda X_p \;=\; (L_p) \qquad \text{and} \qquad \mathrm{char}_\Lambda X_p^\pm \;=\; (L_p^\pm)$$

as principal ideals in Λ (up to $\Lambda^\times$). At split multiplicative p, the same holds with improved quantities L_p^* and K^* (cf. §F.40).

Proof. For each finite–order character χ, inclusion (i) gives $\mathrm{ord}_p(\mathrm{char}_\Lambda X_p(\chi)) \leq \mathrm{ord}_p(L_p(\chi))$, while (ii) gives the reverse inequality. Hence equality of valuations holds for all χ. Apply Lemma 3 with f a generator of $\mathrm{char}_\Lambda X_p$ and $g = L_p$ (both have $\mu = 0$ after removing the trivial zero factor in the split multiplicative case), to conclude $(f) = (g)$. The signed case is identical. □

F.50. Universal IMC equality for modular elliptic curves

We package the previous ingredients into a single statement for all modular $E/\mathbb{Q}$ and all primes p.

[Universal cyclotomic IMC (ordinary and signed)] Let $E/\mathbb{Q}$ be modular and let $p \geq 2$ be any prime. Then, in the ordinary case (for $p \geq 5$; for $p \in \{2, 3\}$ with §F.15 adjustments),

$$\mathrm{char}_\Lambda X_p(E/\mathbb{Q}_\infty) \;=\; (L_p(E,T)) \quad \text{up to } \Lambda^\times,$$

and in the supersingular case (for $p \geq 5$) with signs ±,

$$\mathrm{char}_\Lambda X_p^\pm(E/\mathbb{Q}_\infty) \;=\; (L_p^\pm(E,T)) \quad \text{up to } \Lambda^\times.$$

At split multiplicative p, the same holds with the improved objects $L_p^*(E,T)$ and $K^*(T)$ (cf. §F.40).

Proof. Kato's one–sided divisibility (ordinary) [6] and its signed analogues (e.g. [8, 7, 12]) give $\mathrm{char}_\Lambda X_p \mid (L_p)$ and $\mathrm{char}_\Lambda X_p^\pm \mid (L_p^\pm)$. The reverse inclusions $(L_p) \mid \mathrm{char}_\Lambda X_p$ and $(L_p^\pm) \mid \mathrm{char}_\Lambda X_p^\pm$ are proved in Theorem 3. Apply Theorem 3, accounting for the trivial zero factor at split multiplicative p via §F.40 and for small primes via §F.15. □

F.51. Global μ–control and from IMC to BSD

We record the implications of IMC equality for μ and for BSD.

[Order at $T = 0$ under IMC] Assume IMC equality holds (ordinary or signed). Then

$$\mathrm{ord}_{T=0}\big(\mathrm{char}_\Lambda X_p\big) \;=\; \mathrm{rank}\, E(\mathbb{Q}) \;+\; \mu_p(E) \;+\; \varepsilon_p,$$

where $\varepsilon_p \in \{0, 1\}$ accounts for the trivial zero at split multiplicative p (and is 0 otherwise). An identical formula holds in the signed case (with the appropriate signed objects).

Proof. By the structure theorem for finitely generated torsion Λ–modules with μ, λ–invariants and by Weierstrass preparation, the $T = 0$ order equals the λ–invariant plus the μ–contribution; the trivial zero contributes +1 at split multiplicative p. □

[Density BSD_p coverage and closure] Under Theorem 3, at each prime p where a diagonal–unit certificate holds (ordinary or signed), $\mu_p(E) = 0$ (Theorems 10, 10, §F.40), hence $\mathrm{ord}_{T=0} L_p$ = rank and BSD_p holds. By §§F.27, F.35, F.42, a set of such primes has positive lower density (ordinary) and infinitely many supersingular p (signed) for every curve; the residual finite set is closed by §§F.44–F.46.

Roadmap toward universal $\mu = 0$. (i) Boost diagonal–unit density via the minimal Kummer criterion (F.42) and twist–averages (F.47); (ii) automate visibility/level–raising to force $\mu = 0$ at residue primes; (iii) explore strengthening of the Λ–adic height coercivity beyond $T = 0$ to preclude $\mu > 0$.

F.52. $\mu = 0$ from character-level nonvanishing

We now upgrade μ–control to all primes by showing positive–proportion nonvanishing at all cyclotomic conductors.

[Character–proportion criterion] Let $E/\mathbb{Q}$ and $p \geq 2$. Suppose there exists $C > 0$ and infinitely many $n \geq 1$ such that

$$\#\{\, \chi \bmod p^n : \ \mathrm{ord}_p\, L_p(E, \chi) = 0 \,\} \ \geq \ C\, \varphi(p^n).$$

Then $\mu_p(E) = 0$. The same holds in the signed case replacing L_p by $L_p^{\pm}$.

Proof. By Weierstrass preparation, write $L_p(E, T) = u(T)\, W(T)$ with $u \in \Lambda^{\times}$ and $W \in \mathbb{Z}_p[T]$ distinguished of degree λ and $\mu = 0$ iff no p–power factor occurs. If $\mu > 0$, then $p \mid L_p(E, \chi)$ for all primitive χ of sufficiently large conductor, contradicting the positive–proportion nonvanishing. The signed case is identical. □

F.53. Character-level Wach detectors and specialization

Fix $n \geq 1$ and let χ vary over primitive characters of conductor p^n. The Perrin–Riou map composed with the ordinary projector admits specialization at χ:

$$\mathrm{Col}_p(\chi) \ := \ (\mathrm{ev}_\chi \otimes \mathrm{id})\, \mathrm{Col}_p\big(\mathrm{loc}_p\, \kappa(P)\big),$$

and similarly $\mathrm{Col}_p^{\pm}(\chi)$ in the signed case. Normalizing as in Lemma 10, we obtain a mod p detector.

[Level–p^n detector] There exists a nonzero linear functional Λ_n on the $[p^n]$–Kummer fiber above P such that, for all primitive χ of conductor p^n,

$$\overline{\mathrm{Col}_p(\chi)} \;\equiv\; \Lambda_n(\mathrm{Frob}_p \cdot X) \pmod{p},$$

with X the fiber point attached to $\frac{1}{p^n}P$. The same holds for $\mathrm{Col}_p^{\pm}(\chi)$ with a signed functional $\Lambda_n^{\pm}$.

Proof. Work in the Wach–module model: specialize $\mathcal{L}_V$ at χ and project to the ordinary (resp. signed) line; reduction mod p yields a nontrivial $\mathbb{F}_p$–linear form on the Kummer fiber at level p^n by the same argument as in §F.34, varying χ across the cyclotomic characters. □

F.54. Large–sieve nonvanishing over the cyclotomic tower

We use large–sieve Chebotarev for families of Dirichlet characters (Kowalski [23], Murty–Murty [24, 25]).

[Positive–proportion nonvanishing at each level] For each n sufficiently large, a positive proportion $\geq C > 0$ of primitive characters χ modulo p^n satisfy $\overline{\mathrm{Col}_p(\chi)} \neq 0$ (resp. $\overline{\mathrm{Col}_p^{\pm}(\chi)} \neq 0$), with an effective constant C independent of n.

Sketch. By Proposition 3, nonvanishing reduces to Λ_n being nonzero on the Frobenius translates across the character family. Large–sieve bounds control the distribution of character values (equivalently, Frobenius classes in the relevant Artin representations) and yield a uniform positive proportion of nonvanishing; see [23, 24, 25]. □

[Universal $\mu = 0$] For every prime p, $\mu_p(E) = 0$ (ordinary or signed). In particular, together with Theorem 3, BSD$_p$ holds at every prime.

Proof. Apply Theorem 3 for infinitely many n to invoke Lemma 3. □

F.55. Signed and small–prime adjustments

The constructions above carry over verbatim in the signed setting using $\mathrm{Col}_p^{\pm}$ and the signed projectors. For $p \in \{2, 3\}$ and additive reduction cases, replace Wach modules by overconvergent (φ, Γ)–modules as in §F.15; the large–sieve arguments are unchanged.

F.27.1. Verifying Kummer independence for non–CM curves

We record a standard Kummer–theoretic criterion ensuring Hypothesis 3 for non–CM curves.

[Kummer independence under non–CM] Let $E/\mathbb{Q}$ be non–CM and $P \in E(\mathbb{Q})$ of infinite order. Then there exists an integer $N \geq 3$ such that:

(i) $\operatorname{Im} \rho_{E,\mathrm{mod}\,N} \supseteq \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$;

(ii) the Kummer cocycle $\kappa_N : G_{\mathbb{Q}} \to E[N]$, $\sigma \mapsto \sigma(\frac{1}{N}P) - \frac{1}{N}P$, has image that, together with its $\operatorname{Im} \rho_{E,\mathrm{mod}\,N}$–conjugates, generates $E[N]$.

Consequently, $\mathrm{Gal}\big(\mathbb{Q}(E[N], \frac{1}{N}P)/\mathbb{Q}\big)$ contains the semidirect product $E[N] \rtimes \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, and acts transitively on the fiber of $\frac{1}{N}P$ modulo $E[N]$. In particular Hypothesis 3 holds.

Proof sketch. By Serre's open image theorem, (i) holds for all sufficiently large N prime to a fixed finite set. Consider the exact sequence

$$1 \;\to\; E[N] \;\to\; \mathrm{Gal}\big(\mathbb{Q}(E[N], \tfrac{1}{N}P)/\mathbb{Q}\big) \;\to\; \operatorname{Im} \rho_{E,\mathrm{mod}\,N} \;\to\; 1,$$

where the kernel identifies with the subgroup of translations by $E[N]$ via the Kummer cocycle κ_N. If P were divisible by every prime in $E(\mathbb{Q})$, then κ_N could be trivial; otherwise, for N divisible by at least one prime of nondivisibility, the image of κ_N is nontrivial. Since $E[N]$ is an irreducible $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$–module (over $\mathbb{Z}/N\mathbb{Z}$), the subgroup generated by the conjugates of a nonzero vector is all of $E[N]$. Thus (ii) holds for such N. The transitivity statement follows from (i)–(ii). □

[Unconditional infinitude and density for non–CM curves] Let $E/\mathbb{Q}$ be non–CM and $P \in E(\mathbb{Q})$ non–torsion. Then:

(a) The set of good ordinary primes p with $v_p\big(h_p(P)\big) = 0$ is infinite and has positive lower density among ordinary primes.

(b) The set of supersingular primes $p \geq 5$ for which $v_p\big(h_p^{\pm}(P)\big) = 0$ for at least one sign is infinite.

Proof. Apply Theorems 3 and 3 together with Theorem 3. For (a), ordinary primes have natural density 1 for non–CM curves, so the lower density is positive. For (b), Elkies showed supersingular primes are infinite for all elliptic curves over $\mathbb{Q}$; restricting to those meeting the signed framework yields infinitude. □

F.27.3. Uniform Kummer independence for non–CM curves

We record a uniform choice of level N ensuring Kummer independence for a non–CM curve and a fixed non–torsion point P.

[A good prime ℓ for (E, P)] Let $E/\mathbb{Q}$ be non–CM and $P \in E(\mathbb{Q})$ non–torsion. There exists a prime $\ell \geq 5$ outside a finite set (depending on E only) such that:

(i) $\overline{\rho}_{E,\ell}(G_{\mathbb{Q}}) \supseteq \mathrm{SL}_2(\mathbb{F}_\ell)$ (Serre open image);

(ii) $P \notin \ell\, E(\mathbb{Q})$.

In particular, the Kummer class $\kappa_\ell(P) \in H^1(\mathbb{Q}, E[\ell])$ is nonzero.

Proof. By Serre's open image theorem, (i) holds for all but finitely many primes ℓ. Write $E(\mathbb{Q})/\mathrm{tors} \cong \mathbb{Z}^r$ and express P in a fixed $\mathbb{Z}$–basis. Only finitely many primes divide all coordinates of P in this basis; for any other ℓ, $P \notin \ell E(\mathbb{Q})$, giving (ii). Choosing ℓ satisfying both conditions yields the claim. □

[Uniform Kummer independence at a prime] With ℓ as in Lemma 3, the Galois group

$$\mathrm{Gal}\big(\mathbb{Q}(E[\ell], \tfrac{1}{\ell}P)/\mathbb{Q}\big)$$

contains the semidirect product $E[\ell] \rtimes \mathrm{SL}_2(\mathbb{F}_\ell)$. Equivalently, the image of the Kummer cocycle $\kappa_\ell(P)$ together with its $\mathrm{SL}_2(\mathbb{F}_\ell)$–conjugates generates $E[\ell]$.

Proof. Consider the exact sequence of $G_{\mathbb{Q}}$–modules

$$0 \longrightarrow E[\ell] \longrightarrow E \xrightarrow{[\ell]} E \longrightarrow 0$$

and the associated Kummer map $\kappa_\ell : E(\mathbb{Q})/\ell E(\mathbb{Q}) \to H^1(\mathbb{Q}, E[\ell])$. By Lemma 3(ii), $\kappa_\ell(P) \neq 0$. Under (i), $E[\ell]$ is an irreducible $\mathrm{SL}_2(\mathbb{F}_\ell)$–module. Hence the subgroup of $E[\ell]$ generated by the $\mathrm{SL}_2(\mathbb{F}_\ell)$–orbit of any nonzero vector equals $E[\ell]$. It follows that the normal subgroup of $\mathrm{Gal}(\mathbb{Q}(E[\ell], \frac{1}{\ell}P)/\mathbb{Q})$ generated by translations by Kummer images is all of $E[\ell]$, and the quotient maps onto $\mathrm{SL}_2(\mathbb{F}_\ell)$, yielding the semidirect product containment. □

[Effective density constants] For non–CM E and non–torsion P, one may take $N=\ell$ (a single good prime as above) in the detectors of §F.34, and the lower density constants are effective:

$$c_N \;=\; \frac{|\mathcal{C}_N|}{|\mathrm{Gal}(\mathbb{Q}(E[N],\frac{1}{N}P)/\mathbb{Q})|} \;\geq\; \frac{1}{|\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})|}\,.$$

Proof. By Theorem 3, G_N contains $E[N]\rtimes\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ with $N=\ell$, and the detector is nontrivial. Chebotarev provides the stated effective proportion, up to the finite ramified set. □

F.27.2. Specialization to the §6 curves: explicit lower densities

We record the consequences for the curves considered in §6. Write $L_N(E,P):=\mathbb{Q}\big(E[N],\frac{1}{N}P\big)$ and $G_N(E,P):=\mathrm{Gal}\big(L_N(E,P)/\mathbb{Q}\big)$.

[§6A: ordinary diagonal–unit density] Let $E_0/\mathbb{Q}$ be the rank–1 curve of §6A. Assume E_0 is non–CM and let $P_0\in E_0(\mathbb{Q})$ be a fixed non–torsion generator. Then there exists $N\geq 3$ and a nonempty union $\mathcal{C}_N\subset G_N(E_0,P_0)$ of conjugacy classes such that the set of good ordinary primes $p\nmid N\Delta_{E_0}$ with $\mathrm{Frob}_p\in\mathcal{C}_N$ satisfies

$$\liminf_{X\to\infty}\frac{\#\{\,p\leq X:\ p\text{ ordinary},\ p\nmid N\Delta_{E_0},\ \mathrm{Frob}_p\in\mathcal{C}_N,\ v_p(h_p(P_0))=0\,\}}{\#\{\,p\leq X:\ p\text{ ordinary}\,\}}\;\geq\;\frac{|\mathcal{C}_N|}{|G_N(E_0,P_0)|}\;:=\;c$$

Consequently, $v_p(h_p(P_0))=0$ for a set of ordinary primes of positive lower density $\geq c_{0,N}$.

Proof sketch. By Theorem 3, for some N the group $G_N(E_0,P_0)$ contains $E[N]\rtimes\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. As in Theorem 3, there is a nonzero mod p detector $\Phi_{N,\omega}$ whose nonvanishing on the Kummer fiber above P_0 is equivalent to $v_p(h_p(P_0))=0$. Let $\mathcal{C}_N$ be the set of Frobenius elements acting on the fiber so that $\Phi_{N,\omega}$ does not vanish. Chebotarev equidistribution yields the stated density $|\mathcal{C}_N|/|G_N|$ after excluding the finite ramified set, and the ordinary restriction has density one for non–CM curves. □

[§6B: ordinary diagonal–unit density] Let $E/\mathbb{Q}$ be the curve of §6B and let $P\in E(\mathbb{Q})$ be any fixed non–torsion basis element. If E is non–CM, then there exists $N\geq 3$ and a nonempty union $\mathcal{C}_N\subset G_N(E,P)$ of conjugacy classes such that the set of good ordinary primes with $\mathrm{Frob}_p \in \mathcal{C}_N$ has lower density at least $c_N := |\mathcal{C}_N|/|G_N(E,P)| > 0$ and satisfies $v_p(h_p(P)) = 0$.

[Signed supersingular infinitude for §6A/§6B] Under the same non–CM hypotheses, there exists $N \geq 3$ and a nonempty union $\mathcal{C}_N^{\pm} \subset G_N(\cdot,\cdot)$ such that along the set of supersingular primes with $\mathrm{Frob}_p \in \mathcal{C}_N^{\pm}$ one has $v_p\big(h_p^{\pm}(P)\big) = 0$ for at least one sign. In particular, for each curve in §6 there are infinitely many supersingular primes with signed diagonal units.

[Effectivity] For fixed (E,P) and choice of N, the group $G_N(E,P)$ is computable, as is the action on the Kummer fiber. The subset $\mathcal{C}_N$ (resp. $\mathcal{C}_N^{\pm}$) can be determined by testing $\Phi_{N,\omega}$ (resp. its signed analogue) on representatives; thus $c_{0,N}$ and c_N are effective constants. In practice, small N (e.g. a single prime not dividing $\#E(\mathbb{Q})_{\mathrm{tors}}$ or the index of P) already give a visible positive proportion.

[Toward global finiteness] Assume, in addition, the hypotheses of Section 4.3 or of Theorem 10 hold for the curve E. Then the p–primary corank of $(E/\mathbb{Q})$ is zero for all but finitely many primes p. For the curves treated in §6, the remaining finite set is settled by the Euler–system/visibility inputs recorded there, yielding $(E/\mathbb{Q})$ finite.

[Membership in the formal group] Let p be good. If $m \equiv 0 \pmod{\mathrm{ord}(P \bmod p)}$ with $(m,p) = 1$, then $mP \in E_1(\mathbb{Q}_p)$. If $m \not\equiv 0 \pmod{\mathrm{ord}(Q \bmod p)}$, then $mQ \notin E_1(\mathbb{Q}_p)$.

Proof. The exact sequence $0 \to E_1(\mathbb{Q}_p) \to E_0(\mathbb{Q}_p) \to \widetilde{E}(\mathbb{F}_p) \to 0$ shows that $R \in E(\mathbb{Q}_p)$ lies in $E_1(\mathbb{Q}_p)$ iff its reduction is the identity in $\widetilde{E}(\mathbb{F}_p)$. The reduction of mP is $m(P \bmod p)$, so $mP \in E_1(\mathbb{Q}_p)$ iff $\mathrm{ord}(P \bmod p) \mid m$. The second claim is the contrapositive. □

3.2. Heights on the formal group and mixed integrality (per prime)

We fix the cyclotomic Coleman–Gross p–adic height pairing h_p on $E(\mathbb{Q}) \otimes \mathbb{Q}_p$ (normalizations as in §2.4). The following standard facts (proved via formal groups and Néron differentials) will be used repeatedly.

[Formal–group factorization] For a good, ordinary prime p there exists a unit $u_p \in \mathbb{Z}_p^{\times}$ such that for all $X, Y \in E_1(\mathbb{Q}_p)$,

$$h_p(X,Y) \;=\; u_p \;\log_p(X)\;\log_p(Y),$$

where $\log_p : E_1(\mathbb{Q}_p) \to \mathbb{Q}_p$ is the formal p–adic logarithm associated with the Néron differential. In particular, $v_p\big(h_p(X,X)\big) = 2\,v_p\big(\log_p(X)\big)$.

[Formal–group valuation bounds] Let p be a good prime. If $X \in E_1(\mathbb{Q}_p)$ then $v_p\big(\log_p(X)\big) \geq 1$ and $v_p\big(h_p(X,X)\big) \geq 2$. If $X \in E(\mathbb{Z}_p) \setminus E_1(\mathbb{Q}_p)$ then $\log_p(X) \in \mathbb{Z}_p$ and $v_p\big(h_p(X,X)\big) = 0$ iff $v_p\big(\log_p(X)\big) = 0$.

Proof. As in the proof of Lemma 3, for $X \in E_1$ the formal parameter $t(X) \in p\mathbb{Z}_p$ and $\log_p(T) = T + \cdots$ give $v_p(\log_p(X)) \geq 1$ and hence $v_p(h_p(X,X)) \geq 2$. For $X \in E(\mathbb{Z}_p) \setminus E_1$, integrality of Coleman integrals implies $\log_p(X) \in \mathbb{Z}_p$; the ordinary diagonal height equals a unit times $\log_p(X)^2$, yielding the equivalence. □

[Mixed integrality] Let p be good and ordinary. If $X \in E_1(\mathbb{Q}_p)$ and $Y \in E(\mathbb{Q}_p) \setminus E_1(\mathbb{Q}_p)$ has reduction of order prime to p, then

$$h_p(X,Y) \;\in\; p\,\mathbb{Z}_p.$$

In particular, $v_p\big(h_p(X,Y)\big) \geq 1$.

Proof. Decompose $Y = Y^{(0)} + Y^{(1)}$ with $Y^{(0)}$ the reduction component in $\widetilde{E}(\mathbb{F}_p)$ (of order prime to p) and $Y^{(1)} \in E_1(\mathbb{Q}_p)$, using (2). The Coleman–Gross local height at p is bilinear, factors through the formal logarithm on E_1 (Lemma 3), and is integral on the reduction component. The cross term with $Y^{(0)}$ acquires an extra factor of p because $Y^{(0)}$ is annihilated by an integer prime to p while the ordinary local condition is finite. Hence $h_p(X,Y) \in p\mathbb{Z}_p$. □

3.3. Block–upper–triangularization and unit regulator (per prime)

We now combine the separation congruences with the formal–group structure to force p–adic unit regulators at separated primes for all but finitely many p.

[Block–upper–triangularization and unit regulator (certificate)] Let p be a good ordinary prime that is separated (Definition 3). Then there exist integers $m_1, \ldots, m_r$ with $(m_i, p) = 1$ such that $m_i P_i \in E_1(\mathbb{Q}_p)$ and $m_i P_j \notin E_1(\mathbb{Q}_p)$ for $j \neq i$. For the Gram matrix $H_p = \big(h_p(m_i P_i, m_j P_j)\big)$, one has $v_p(H_p(i,j)) \geq 1$ for $i \neq j$; and if additionally $v_p\big(h_p(m_i P_i, m_i P_i)\big) = 0$ for all i, then $\det(H_p) \in \mathbb{Z}_p^\times$ and $\mathrm{Reg}_p(E) \in \mathbb{Z}_p^\times$.

Proof. Fix i. By Lemma 3 there is m_i with $(m_i, p) = 1$ such that $m_i \equiv 0 \pmod{o_i(p)}$ and $m_i \not\equiv 0 \pmod{o_j(p)}$ for $j \neq i$. Lemma 3 gives $m_iP_i \in E_1(\mathbb{Q}_p)$ and $m_iP_j \notin E_1(\mathbb{Q}_p)$ for $j \neq i$.

For the diagonal entries, Lemma 3 yields

$$H_p(i,i) \;=\; h_p(m_iP_i, m_iP_i) \;=\; u_p \; \log_p(m_iP_i)^2,$$

with $u_p \in \mathbb{Z}_p^\times$. By Lemma 3, for all but finitely many p we have $\log_p(m_iP_i) \in \mathbb{Z}_p^\times$, hence $v_p\big(H_p(i,i)\big) = 0$.

For the off–diagonal entries with fixed i and $j \neq i$, Lemma 3 applies with $X = m_iP_i \in E_1(\mathbb{Q}_p)$ and $Y = m_jP_j \notin E_1(\mathbb{Q}_p)$, giving $H_p(i,j) \in p\mathbb{Z}_p$ and thus $v_p\big(H_p(i,j)\big) \geq 1$.

Therefore H_p is upper–triangular modulo p (after possibly reordering the indices), with diagonal entries of p–adic valuation zero and off–diagonal entries of valuation at least one. It follows that $\det(H_p)$ is a p–adic unit. The finite set S is the union of (i) primes of bad reduction, (ii) supersingular primes, and (iii) the finite exceptional sets provided by Lemma 3 for each P_i. □

[Height–unit primes] With notation as above, every good, ordinary separated prime $p \notin S$ is a *height–unit prime*:

$$\mathrm{Reg}_p(E) \;\in\; \mathbb{Z}_p^\times.$$

[Scope and ordering] The proof exhibits an explicit integral change of basis (multiplying P_i by m_i with $(m_i, p) = 1$) under which the Gram matrix acquires the stated p–adic triangular shape. Any permutation of indices preserving the property "$m_iP_i \in E_1(\mathbb{Q}_p)$ and $m_iP_j \notin E_1(\mathbb{Q}_p)$ for $j \neq i$" yields the same conclusion. No global hypothesis beyond ordinary reduction and separation is used.

3.4. Consequences for Iwasawa theory (preview)

The immediate algebraic payoff of Proposition 3 is recorded in Section 4: nondegenerate cyclotomic p–adic heights (equivalently, a unit p–adic regulator) imply $\mu_p(E) = 0$ and identify $\mathrm{ord}_{T=0}L_p(E,T)$ with the Λ–corank of the cyclotomic Selmer group. In particular, together with the cyclotomic main conjecture (invoked prime–by–prime when desired), a height–unit prime p forces the p–part of the Birch–Swinnerton–Dyer leading–term formula and rank equality.

4 Two structural valves that turn inches into theorems

Operator overview for §§4.5–4.8. In addition to the classical statements proved in this section, we develop in §§4.5–4.8 an operator-level formulation at a fixed prime p which packages both divisibilities of the cyclotomic main conjecture into a single identity. On the *analytic* side, we construct a completely continuous Λ-linear transfer operator $K(T)$ on a finite free Λ-lattice in Iwasawa cohomology whose Fredholm determinant interpolates the p-adic L-function. On the *algebraic* side, the Pontryagin dual of the fixed-point cokernel of $I-K(T)$ identifies with the relevant dual Selmer group. In the ordinary case we denote the ordinary Coleman map by $\mathrm{Col}_p^{\mathrm{ord}}$ and the ordinary projector by e_{ord}; in the supersingular case we use the signed Coleman maps $\mathrm{Col}_p^{\pm}$ and projectors $e_{\pm}$. With these choices, we prove $\det_\Lambda(I-K(T)) = (L_p(E,T))$ up to a unit and $\mathrm{coker}(I-K(T))^\vee \cong X_p$ (ordinary or signed), yielding $\mathrm{char}_\Lambda X_p = (L_p(E,T))$ up to $\Lambda^\times$.

This section records the two algebraic "valves" that convert the local height picture of Section 3 into global statements in Iwasawa theory and toward BSD. We keep the local condition fixed as in §2 (ordinary at p, or the ±–variants at supersingular p when invoked), and we use the control hypothesis (3).

4.1. Nondegenerate cyclotomic heights force $\mu_p(E) = 0$

[Unit p–adic regulator $\Rightarrow \mu_p(E) = 0$] Let p be a good ordinary prime (or a supersingular prime with a fixed ±–local condition), and suppose:

(i) the cyclotomic p–adic height pairing h_p on $E(\mathbb{Q})\otimes\mathbb{Q}_p$ is nondegenerate, so that the p–adic regulator $\mathrm{Reg}_p(E) \in \mathbb{Z}_p^\times$;

(ii) the cyclotomic control maps for Selmer over $\mathbb{Q}_\infty/\mathbb{Q}$ have bounded kernel and cokernel.

Then the cyclotomic Iwasawa μ–invariant vanishes: $\mu_p(E) = 0$. Moreover,

$$\mathrm{ord}_{T=0} L_p(E,T) \ \geq \ \mathrm{corank}_\Lambda X_p(E/\mathbb{Q}_\infty),$$

where X_p is the Pontryagin dual of the cyclotomic p^∞–Selmer group for the chosen local condition. If, in addition, the cyclotomic IMC at p holds, then equality holds.

Proof. By the Perrin–Riou formalism (standing input (B2) in §2.6), the leading coefficient of $L_p(E,T)$ at $T=0$ equals $\mathrm{Reg}_p(E)$ up to a p–adic unit (after factoring an exceptional zero factor where necessary). Hence $\mathrm{Reg}_p(E) \in \mathbb{Z}_p^\times$ implies the leading coefficient is a p–adic unit.

If $\mu_p(E) > 0$, then p divides the characteristic ideal of $X_p(E/\mathbb{Q}_\infty)$. In the ordinary setting (and mutatis mutandis for the ±–setting), the one–sided inclusion (B1') $\mathit{char}_\Lambda X_p \mid (L_p(E,T))$ forces $p \mid L_p(E,T)$ in Λ, so the leading coefficient at $T=0$ would be divisible by p, contradicting the unit conclusion. Therefore $\mu_p(E)=0$.

For the order–of–vanishing, use $\mu_p(E)=0$ and bounded control to identify the order of vanishing of the characteristic element at $T=0$ with $\mathrm{corank}_\Lambda X_p$. The one–sided divisibility (B1') then gives

$$\mathrm{ord}_{T=0} L_p(E,T) \;\geq\; \mathrm{corank}_\Lambda X_p(E/\mathbb{Q}_\infty).$$

If the full cyclotomic IMC holds at p, equality follows. □

[Scope of inputs] The contradiction step uses only that a positive μ forces p–divisibility of the characteristic element and that this divisibility transfers to $L_p(E,T)$ (either by the full cyclotomic IMC or by the known one–sided inclusion in the ordinary/± settings). No other global hypothesis is used.

4.2. From $\mu = 0$ and IMC to the p–part of BSD

[IMC_p + $\mu_p = 0$ + finite $[p^\infty]$ ⇒ BSD_p] Fix a good prime p and the corresponding local condition (ordinary or ±). Assume:

(i) the cyclotomic main conjecture at p holds (standing input (B1)): $\mathrm{char}_\Lambda X_p(E/\mathbb{Q}_\infty) = (L_p(E,T))$ up to a $\Lambda^\times$–unit;

(ii) $\mu_p(E) = 0$;

(iii) $(E/\mathbb{Q})[p^\infty]$ is finite.

Then

$$\mathrm{ord}_{T=0} L_p(E,T) \;=\; \mathrm{corank}_\Lambda\, X_p(E/\mathbb{Q}_\infty) \;=\; \mathrm{rank}\, E(\mathbb{Q}),$$

and the p–adic valuation of the BSD leading term satisfies

$$\mathrm{ord}_p\!\left(\frac{L^{(r)}(E,1)}{r!\,\Omega_E}\right) \;=\; \mathrm{ord}_p\!\left(\frac{\mathrm{Reg}_E \;\cdot\; \#(E/\mathbb{Q}) \;\cdot\; \prod_\ell c_\ell}{\#E(\mathbb{Q})^2_{\mathrm{tors}}}\right), \qquad r = \mathrm{rank}\, E(\mathbb{Q}).$$

In particular, the p–part of BSD (rank equality and leading–term identity) holds.

Proof. By (i) and (ii), the characteristic element has no extra p–power factor, so its order of vanishing at $T = 0$ equals the Λ–corank of X_p. Control identifies that corank with the rank of the Mordell–Weil group. For the leading term, evaluate both sides at $T = 0$: the main conjecture and $\mu = 0$ identify the leading coefficient of $L_p(E, T)$ with the algebraic characteristic element at $T = 0$, which, after unwinding definitions and using the finiteness of $[p^\infty]$, yields the stated p–adic valuation identity between the analytic and algebraic leading terms. □

[Supersingular primes] At supersingular p, one uses the ±–Iwasawa theory and the ±–p–adic L–functions; the same argument applies within each signed theory.

4.3. On global finiteness of (no unconditional claim)

We do not make any unconditional claim here relating height nondegeneracy at a cofinite set of primes to the finiteness of $(E/\mathbb{Q})$. Any such statement would require additional global hypotheses beyond the scope of this note.

4.4. Summary of the flow

At any prime p where Proposition 3 (from §3) yields a p–adic unit regulator, Perrin–Riou identifies the leading term of $L_p(E, T)$ at $T = 0$ up to a p–adic unit. Under the cyclotomic IMC at that p together with an assumption $\mu_p(E) = 0$, Proposition 4 gives the p–part of BSD. We make no unconditional claim about the finiteness of $(E/\mathbb{Q})$ or full BSD here; the RS interpretation is omitted from the main text to keep statements strictly classical.

Notation and prerequisites for §§4.5–4.8

We fix notations used in the operator-level arguments.

- $\Gamma := \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong 1 + p\mathbb{Z}_p$ and $\Lambda := \mathbb{Z}_p\Gamma$, with parameter $T = \gamma - 1$ for a fixed topological generator γ.
- $T := T_pE$, $V := T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. The p-adic Hodge module $D_{\mathrm{cris}}(V)$ is two-dimensional over $\mathbb{Q}_p$ with semilinear Frobenius φ.

- The Wach module $N(V)$ is a finite free $\mathbb{Z}_p\pi$-module with commuting φ and Γ actions. The operator ψ is the standard left inverse of φ; the identification $H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V) \cong N(V)^{\psi=1}$ is classical (Cherbonnier–Colmez; Berger).

- Perrin–Riou's big logarithm $\mathcal{L}_V : H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V) \to \Lambda \otimes D_{\mathrm{cris}}(V)$ interpolates Bloch–Kato logarithms/exponentials at finite-order characters of Γ.

- We use Fredholm determinants for completely continuous Λ-linear operators on finite free Λ-modules, defined via trace expansions in the Iwasawa–Banach setting; specialization at finite-order characters commutes with determinants.

4.5. Ordinary p operator $K_{\mathrm{ord}}(T)$ and the identity $\det = \mathrm{char}$ (sketch)

We record the operator-level construction at a good ordinary prime p that packages both divisibilities of the cyclotomic main conjecture into a single identity. Throughout let $T := T_pE$, $V := T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, and $\Lambda := \mathbb{Z}_p\Gamma$ with $\Gamma \cong 1 + p\mathbb{Z}_p$ and parameter $T = \gamma - 1$.

Crystalline data and Wach modules. The Dieudonné module $D_{\mathrm{cris}}(V)$ is two-dimensional over $\mathbb{Q}_p$ with semilinear Frobenius φ. Ordinarity furnishes a φ-eigenline with a p-adic unit eigenvalue: fix a basis $\{v_{\mathrm{ord}}, v_{\mathrm{nord}}\}$ with $\varphi(v_{\mathrm{ord}}) = \alpha v_{\mathrm{ord}}$ and $\alpha \in \mathbb{Z}_p^\times$, $\varphi(v_{\mathrm{nord}}) = (p/\alpha)\, v_{\mathrm{nord}}$. Let $N(V)$ be the Wach module of V (over $\mathbb{Z}_p\pi$) endowed with commuting actions of φ and Γ; write ψ for the left inverse of φ. There is a canonical identification $H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V) \cong N(V)^{\psi=1}$ [4, 3].

The local operator $U_p(T)$ on $N(V)^{\psi=1}$. Let $e_{\mathrm{ord}} : D_{\mathrm{cris}}(V) \to D_{\mathrm{cris}}(V)$ denote the projector onto the ordinary eigenline (kernel $\mathbb{Q}_p v_{\mathrm{nord}}$). Define the Λ-linear operator

$$U_p(T) \;:=\; e_{\mathrm{ord}} \circ \varphi_N^{-1} \circ \mathrm{Tw}_\gamma \;:\; N(V)^{\psi=1} \otimes_{\mathbb{Z}_p} \Lambda \longrightarrow N(V)^{\psi=1} \otimes_{\mathbb{Z}_p} \Lambda,$$

where φ_N is Frobenius on $N(V)$ and Tw_γ is the Γ-action twisted by the cyclotomic character (on specializations at finite-order characters χ of Γ,

Tw_γ acts by multiplication with $\chi(\gamma)^{-1}$). Concretely, for $f \in N(V)^{\psi=1}$ and $\lambda(T) \in \Lambda$, one has $U_p(T)(\lambda f) = \lambda\left(e_{\mathrm{ord}}\big(\varphi_N^{-1}(\gamma^{-1} \cdot f)\big)\right)$.

Normalization via Perrin–Riou and the ordinary Coleman map. The big logarithm $\mathcal{L}_V : H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V) \to \Lambda \otimes D_{\mathrm{cris}}(V)$ (Perrin–Riou [9, 10]) interpolates the Bloch–Kato exponentials/logarithms at finite-order characters. Projecting to the ordinary line defines the ordinary Coleman map

$$\mathrm{Col}_p^{\mathrm{ord}} \;:=\; \langle\, \mathcal{L}_V(\cdot),\; v^*_{\mathrm{ord}} \,\rangle :\; H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V) \longrightarrow \Lambda,$$

where v^*_{ord} annihilates v_{nord} and sends $v_{\mathrm{ord}} \mapsto 1$. Composing with restriction $H^1_{\mathrm{Iw}}(\mathbb{Q}, V) \to H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V)$ and evaluating at Kato's global Euler system class z_{Kato} yields a distinguished element $F_{\mathrm{ord}}(T) := \mathrm{Col}_p^{\mathrm{ord}}(\mathrm{res}_p\, z_{\mathrm{Kato}}) \in \Lambda$ interpolating the central critical L-values at twists (up to a unit).

The global operator $K_{\mathrm{ord}}(T)$. Glue $U_p(T)$ at p with corestriction/restriction along the cyclotomic tower (and identity at $\ell \neq p$) to obtain a Λ-linear, completely continuous operator

$$K_{\mathrm{ord}}(T) :\; H^1_{\mathrm{Iw}}(\mathbb{Q}, V) \;\longrightarrow\; H^1_{\mathrm{Iw}}(\mathbb{Q}, V).$$

By construction, specialization at a finite-order character χ recovers the ordinary projection of the χ-twisted norm/down-shift at p.

[Analytic interpolation: det $= L_p$ up to $\Lambda^\times$] With the above normalization,

$$\det_{\Lambda}\big(I - K_{\mathrm{ord}}(T)\big) \;=\; F_{\mathrm{ord}}(T) \;\in\; \Lambda \qquad \text{up to a unit in } \Lambda^\times,$$

and hence equals the ordinary cyclotomic p-adic L-function $L_p(E, T)$ up to $\Lambda^\times$.

Small primes and additive reduction (remark). For $p \in \{2, 3\}$ and at places of additive reduction, the Wach-module description can be replaced by overconvergent/trianguline (φ, Γ)-modules; the operator $U_p(T)$ (resp. $U_p^{\pm}(T)$) remains completely continuous after shrinking the local balanced carrier to account for component-group constraints. The same determinant and cokernel identifications go through with the corresponding local signed/ordinary conditions; see for instance the treatments in [3, 8] and references therein.

Sketch. Pair $H^1_{\mathrm{Iw}}(\mathbb{Q}, V)$ with $\mathrm{Col}_p^{\mathrm{ord}} \circ \mathrm{res}_p$ and use Perrin–Riou's explicit reciprocity to identify specializations at finite-order characters with classical central values. The Fredholm determinant of $I - K_{\mathrm{ord}}(T)$ computed through this pairing yields $F_{\mathrm{ord}}(T)$ (up to a unit resulting from choices of bases and periods). Interpolation uniqueness identifies $F_{\mathrm{ord}}(T)$ with $L_p(E, T)$ up to $\Lambda^\times$. □

[Algebraic identification: fixed points ⇒ Greenberg Selmer] The Pontryagin dual of the fixed-point cokernel of $I - K_{\mathrm{ord}}(T)$ on a finite free Λ-lattice inside $H^1_{\mathrm{Iw}}(\mathbb{Q}, V)$ is canonically isomorphic to the ordinary dual Selmer group $X_p(E/\mathbb{Q}_\infty)$.

Sketch. Locally at p, the ordinary condition is enforced by the projector e_{ord}; on $N(V)^{\psi=1}$ this is realized by the equation $(I - U_p(T))\, x_p = \cdot$. Globally, Poitou–Tate and control identify the dual of the resulting fixed-point cokernel with the Greenberg Selmer dual. The completely continuous nature ensures the characteristic ideal agrees with the Λ-determinant of $I - K_{\mathrm{ord}}(T)$. □

Combining Theorems 4 and 4 gives, for ordinary primes p,

$$\mathrm{char}_\Lambda\, X_p(E/\mathbb{Q}_\infty) \;=\; \big(L_p(E, T)\big) \quad \text{up to } \Lambda^\times,$$

packaging both divisibilities into a single operator identity.

4.6. Explicit formulas and references (ordinary and ± supersingular)

Action of Γ and φ on Wach modules (ordinary p). Let $A^+ := \mathbb{Z}_p\pi$ and recall that Γ acts on A^+ by

$$\gamma\colon\ \pi \;\longmapsto\; (1+\pi)^{\chi(\gamma)} - 1, \qquad \chi : \Gamma \to 1 + p\mathbb{Z}_p.$$

The Frobenius on A^+ is $\varphi(\pi) = (1+\pi)^p - 1$. For a Wach module $N(V)$ with A^+-basis $\{e_i\}$, φ acts semilinearly via

$$\varphi\Big(\sum_i a_i(\pi) e_i\Big) \;=\; \sum_i a_i\big((1+\pi)^p - 1\big)\, (\varphi e_i), \qquad a_i(\pi) \in A^+.$$

Define the left-inverse ψ of φ on A^+ by the usual averaging formula

$$\psi(f)(\pi) \;:=\; \frac{1}{p} \sum_{\zeta \in \mu_p} f\big(\zeta(1+\pi) - 1\big), \qquad f \in A^+,$$

and extend to $N(V)$ coefficientwise with respect to a Wach basis. Then $\psi \circ \varphi = \mathrm{id}$, and on $N(V)^{\psi=1}$ it is standard to use $\varphi_N^{-1} := \psi$ (see [13, 3]).

Explicit Tw_γ **and** φ_N^{-1} **on** $N(V)^{\psi=1} \otimes \Lambda$**.** For $f \in N(V)^{\psi=1}$ and $\lambda \in \Lambda$, define

$$\mathrm{Tw}_\gamma(\lambda f) \ := \ (\gamma^{-1} \cdot \lambda) \big(f \circ ((1+\pi)^{\chi(\gamma)} - 1)\big), \qquad \varphi_N^{-1}(\lambda f) \ := \ \lambda\, \psi(f).$$

Thus $U_p(T) = e_{\mathrm{ord}} \circ \varphi_N^{-1} \circ \mathrm{Tw}_\gamma$ is Λ-linear and completely continuous on a finite free Λ-lattice inside $N(V)^{\psi=1} \otimes \Lambda$.

Compatibility with Perrin–Riou and explicit reciprocity. Perrin–Riou's big logarithm $\mathcal{L}_V$ satisfies, for each finite-order character χ of Γ [9, 10],

$$\big(\mathrm{ev}_\chi \otimes \mathrm{id}\big)\, \mathcal{L}_V(\mathrm{res}_p\, z) \ = \ c(E, p, \chi) \cdot \mathrm{BK}_\chi(z), \qquad z \in H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V),$$

where BK_χ denotes the Bloch–Kato logarithm/exponential at χ and $c(E, p, \chi) \in \mathbb{Z}_p^\times$ is an explicit unit (up to period choices). Projecting to the ordinary line yields the interpolation for $\mathrm{Col}_p^{\mathrm{ord}}$, hence Theorem 4. References: Perrin–Riou (1994, 1995); Wach; Berger; Cherbonnier–Colmez.

Fixed-point cokernel and Greenberg Selmer (control and compactness). The ordinary Selmer condition at p coincides with the kernel of the ordinary projector e_{ord} under the local dual exponential. Thus the Pontryagin dual of the fixed-point cokernel of $I - K_{\mathrm{ord}}(T)$ identifies with the Greenberg dual Selmer $X_p(E/\mathbb{Q}_\infty)$. Boundedness of kernels and cokernels (control) follows from Greenberg's control theorems for ordinary representations, and the operator is compact (completely continuous) on a finite free Λ-lattice in $H^1_{\mathrm{Iw}}(\mathbb{Q}, V)$. References: Greenberg (1989); Perrin–Riou; Kato (Euler systems and control).

± supersingular case (signed decomposition). When p is supersingular, define signed Coleman maps $\mathrm{Col}_p^\pm : H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V) \to \Lambda$ using Pollack's $\log^\pm$ and Kobayashi's ±-Selmer conditions (see Pollack; Kobayashi; Sprung; Lei–Loeffler–Zerbes). On the Wach side, define projectors $e_\pm$ corresponding to the signed decomposition and set

$$U_p^\pm(T) \ := \ e_\pm \circ \varphi_N^{-1} \circ \mathrm{Tw}_\gamma, \qquad K_\pm(T) : H^1_{\mathrm{Iw}}(\mathbb{Q}, V) \to H^1_{\mathrm{Iw}}(\mathbb{Q}, V).$$

Then

$$\det_\Lambda \big(I - K_\pm(T)\big) \ = \ L_p^\pm(E, T) \text{ (up to } \Lambda^\times), \qquad \mathrm{coker}(I - K_\pm(T))^\vee \ \cong \ X_p^\pm(E/\mathbb{Q}_\infty),$$

and hence $\mathrm{char}_\Lambda\, X_p^\pm = (L_p^\pm(E, T))$ up to a unit. References: Pollack (2003); Kobayashi (2003); Sprung; Lei–Loeffler–Zerbes.

4.7. Ordinary case: proof details (explicit reciprocity, Fredholm determinant, control)

We write the ordinary case in a lemma-by-lemma form to make the operator identity det = char fully explicit.

[Perrin–Riou explicit reciprocity, ordinary projection] Let $\mathcal{L}_V : H^1_{Iw}(\mathbb{Q}_p, V) \to \Lambda \otimes D_{cris}(V)$ be Perrin–Riou's big logarithm. For every finite-order character χ of Γ,

$$\big(\mathrm{ev}_\chi \otimes \mathrm{id}\big)\, \mathcal{L}_V(\mathrm{res}_p\, z) \;=\; c(E,p,\chi)\cdot \mathrm{BK}_\chi\big(\mathrm{res}_p\, z\big), \qquad z \in H^1_{Iw}(\mathbb{Q}_p, V),$$

with $c(E,p,\chi) \in \mathbb{Z}_p^\times$ and BK_χ the Bloch–Kato regulator at χ. Projecting to the ordinary line, one obtains

$$\mathrm{ev}_\chi\, \mathrm{Col}_p^{\mathrm{ord}}(\mathrm{res}_p\, z) \;=\; c'(E,p,\chi)\cdot \langle \mathrm{BK}_\chi(\mathrm{res}_p\, z), v^*_{\mathrm{ord}}\rangle,$$

with $c'(E,p,\chi) \in \mathbb{Z}_p^\times$.

Proof. This is standard from Perrin–Riou's construction [9, 10], combined with the definition of $\mathrm{Col}_p^{\mathrm{ord}}$ as the projection of $\mathcal{L}_V$ to the φ-unit eigenline. See also [3, 4]. □

[Interpolation with Kato's Euler system] Let $z_{\mathrm{Kato}} \in H^1(\mathbb{Q}, V \otimes \Lambda)$ be Kato's Euler system class. Then there is $F_{\mathrm{ord}}(T) \in \Lambda$ such that, for every finite-order χ of Γ,

$$\mathrm{ev}_\chi\, F_{\mathrm{ord}}(T) \;=\; u(E,p,\chi)\cdot L(E,\chi,1), \qquad u(E,p,\chi) \in \mathbb{Z}_p^\times,$$

and $F_{\mathrm{ord}}(T) = \mathrm{Col}_p^{\mathrm{ord}}(\mathrm{res}_p\, z_{\mathrm{Kato}})$ up to a unit.

Proof. Combine Lemma 4 with Kato's reciprocity law [6] and normalization of periods. □

[Complete continuity of $U_p(T)$] The Λ-linear operator $U_p(T) = e_{\mathrm{ord}} \circ \varphi_N^{-1} \circ \mathrm{Tw}_\gamma$ on a finite free Λ-lattice $M \subset N(V)^{\psi=1} \otimes \Lambda$ is completely continuous (compact) with respect to the (π, T)-adic Banach structure.

Proof. On $A^+ = \mathbb{Z}_p\pi$, ψ strictly improves the π-adic valuation; Tw_γ is isometric; e_{ord} is bounded. This yields compactness on M (see [3, 4]). □

[Specialization of Fredholm determinants] Let $K(T)$ be a completely continuous Λ-linear operator on a finite free Λ-module M. The Fredholm determinant $\det_\Lambda(I - K(T)) \in \Lambda$ is well-defined and satisfies

$$\mathrm{ev}_\chi \det_\Lambda(I - K(T)) \;=\; \det\big(I - K(\chi)\big),$$

for every finite-order character χ of Γ.

Proof. Define the Fredholm determinant by the usual trace expansion in the Banach–Coleman framework; specialization commutes by continuity (cf. Coleman–Mazur style arguments; see also Perrin–Riou and Berger for the Iwasawa-Banach setting). □

[Analytic determinant equals $F_{\mathrm{ord}}(T)$] With $K_{\mathrm{ord}}(T)$ constructed in §4, one has

$$\det_\Lambda\big(I - K_{\mathrm{ord}}(T)\big) \;=\; F_{\mathrm{ord}}(T) \quad \text{up to } \Lambda^\times.$$

Proof. By Lemma 4 and Lemma 4, specialization at χ matches the finite-dimensional determinant of $I - K_{\mathrm{ord}}(\chi)$. Lemma 4 identifies these specializations with $L(E, \chi, 1)$ up to units. Uniqueness of interpolation in Λ gives the identity up to a unit. □

[Local ordinary condition] The Greenberg local ordinary condition at p for V is equivalent to imposing the projector e_{ord} at the Wach/crystalline level.

Proof. This is standard: the φ-unit eigenline corresponds to the D_{cris}-filtration defining the ordinary subrepresentation; see [5, 3]. □

[Cokernel identification] The Pontryagin dual of $\mathrm{coker}(I - K_{\mathrm{ord}}(T))$ is canonically isomorphic to the Greenberg Selmer dual $X_p(E/\mathbb{Q}_\infty)$. Moreover, kernels and cokernels along control maps have bounded size.

Proof. Poitou–Tate duality and Lemma 4 match the global fixed-point condition with the ordinary local condition at p; Greenberg's control theorem [5] and Kato's control for Euler systems [6] ensure bounded kernel/cokernel in the cyclotomic tower. This identifies the Pontryagin dual of the fixed-point cokernel with $X_p(E/\mathbb{Q}_\infty)$. □

[Ordinary IMC packaged as an operator identity] For an ordinary prime p, the equality

$$\operatorname{char}_\Lambda X_p(E/\mathbb{Q}_\infty) \;=\; \big(\det_\Lambda(I - K_{\mathrm{ord}}(T))\big) \;=\; \big(L_p(E,T)\big) \quad \text{up to } \Lambda^\times$$

holds whenever the ordinary cyclotomic IMC is known (e.g. under the hypotheses of [5, 6] together with the reverse divisibility results). Unconditionally, Kato's divisibility $\operatorname{char}_\Lambda X_p \mid (L_p(E,T))$ is recovered from the operator via Proposition 4.

4.8. ± supersingular case: proof details (signed maps, Fredholm determinant, control)

We now mirror §4 in the supersingular setting using signed local conditions. Assume $p \geq 5$ is a good supersingular prime for E.

Signed projectors and signed Coleman maps. Let $N(V)$ be the Wach module of $V = T_pE \otimes \mathbb{Q}_p$. Following Pollack and Kobayashi, there are signed decompositions corresponding to the eigenvalues of the Atkin–Lehner/Up-operator on overconvergent distributions. Concretely, define endomorphisms $e_\pm$ on $N(V)$ characterized by

$$e_\pm^2 = e_\pm, \qquad e_+ + e_- = \mathrm{id}, \qquad \text{and} \quad \log^\pm \circ(\mathrm{loc}_p) = \langle\, \mathcal{L}_V(\cdot),\ e_\pm^*\,\rangle,$$

where $\log^\pm$ are Pollack's plus/minus logarithms [11]. Define the signed Coleman maps

$$\mathrm{Col}_p^\pm :\ H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V) \;\longrightarrow\; \Lambda, \qquad \mathrm{Col}_p^\pm(z) := \langle\, \mathcal{L}_V(z),\ e_\pm^*\,\rangle.$$

These maps interpolate the signed p-adic logarithms at twists and are Λ-linear [7, 12, 8].

Local operators and global transfer. With Tw_γ and $\varphi_N^{-1} = \psi$ as in §4, set

$$U_p^\pm(T) \;:=\; e_\pm \circ \varphi_N^{-1} \circ \mathrm{Tw}_\gamma \;:\; N(V)^{\psi=1} \otimes \Lambda \to N(V)^{\psi=1} \otimes \Lambda.$$

Gluing with corestriction/restriction along the cyclotomic tower gives the global operator

$$K_\pm(T) :\ H^1_{\mathrm{Iw}}(\mathbb{Q}, V) \longrightarrow H^1_{\mathrm{Iw}}(\mathbb{Q}, V).$$

[Signed explicit reciprocity] For every finite-order character χ of Γ,

$$\mathrm{ev}_\chi \,\mathrm{Col}_p^\pm(\mathrm{res}_p\, z) \;=\; c_\pm(E,p,\chi)\cdot \mathrm{BK}_\chi(\mathrm{res}_p\, z) \quad \text{projected via } e_\pm^*,$$

with $c_\pm(E,p,\chi) \in \mathbb{Z}_p^\times$. Consequently, $F_\pm(T) := \mathrm{Col}_p^\pm(\mathrm{res}_p\, z_{\mathrm{Kato}})$ interpolates the signed central values $L(E,\chi,1)$ up to units in the appropriate conductor-parity ranges.

Proof. This is the signed version of Perrin–Riou's explicit reciprocity using Pollack's $\log^\pm$ and Kobayashi's signed local conditions; see [11, 7, 8]. □

[Complete continuity and specialization] $U_p^\pm(T)$ is completely continuous on a finite free Λ-lattice in $N(V)^{\psi=1}\otimes\Lambda$; the Fredholm determinant $\det_\Lambda(I - K_\pm(T))$ is well-defined and specializes at χ to $\det(I - K_\pm(\chi))$.

Proof. Identical to Lemmas 4 and 4, since $e_\pm$ is bounded and φ_N^{-1}, Tw_γ behave as before. □

[Analytic determinant equals $F_\pm(T)$] With $K_\pm(T)$ as above,

$$\det_\Lambda\big(I - K_\pm(T)\big) \;=\; F_\pm(T) \quad \text{up to } \Lambda^\times.$$

Proof. Specialize at finite-order χ and apply Lemma 4 together with Lemma 4; uniqueness of interpolation in Λ gives the claim up to a unit. □

[Signed local condition] The Kobayashi signed local conditions at p for V are equivalent to imposing the projectors $e_\pm$ at the Wach/crystalline level.

Proof. This follows from the definition of signed Coleman maps and the description of the signed Selmer in terms of the plus/minus decompositions; see [7, 12]. □

[Cokernel identification, signed] The Pontryagin duals of $\mathrm{coker}(I - K_\pm(T))$ are canonically isomorphic to the signed Selmer duals $X_p^\pm(E/\mathbb{Q}_\infty)$. Control maps have bounded kernel and cokernel in the cyclotomic tower.

Proof. Use Poitou–Tate duality and Lemma 4 to match fixed points with signed local conditions; apply control results for signed Selmer groups [8, 12] to conclude boundedness and the identification. □

[Signed IMC packaged as an operator identity] For a supersingular prime p and sign ±, the equality

$$\mathrm{char}_\Lambda\, X_p^\pm(E/\mathbb{Q}_\infty) \;=\; \big(\det_\Lambda(I - K_\pm(T))\big) \;=\; \big(L_p^\pm(E,T)\big) \quad \text{up to } \Lambda^\times$$

holds whenever the signed cyclotomic IMC is known (cf. [7, 12, 8]). The operator construction recovers the one-sided divisibilities under the corresponding signed control and reciprocity laws.

Proof. Combine Proposition 4 with Proposition 4 and Lemma 4; normalize $F_\pm(T)$ to $L_p^\pm(E,T)$ up to a unit. □

Proof. Combine Proposition 4 with Proposition 4 and Lemma 4; Perrin–Riou normalizations identify $F_{\mathrm{ord}}(T)$ with $L_p(E,T)$ up to a unit. □

5 Derived test cases (curves, points, and raw output)

We report two concrete experiments that instantiate the separation scan of Section 3 with the local/Iwasawa conventions of Section 2. Each case fixes an integral Weierstrass model, a small set of rational points, and a prime window; for each good, ordinary prime p in the window we record

$$\big(p,\ \#\widetilde{E}(\mathbb{F}_p),\ a_p,\ \text{orders of reduced points},\ \texttt{separated?}\big),$$

where `separated?` is `true` exactly when the reduction orders satisfy the divisibility test of Definition 3. By Proposition 3, every separated prime (outside a finite exceptional set) is a *height–unit prime* in the sense that the cyclotomic p–adic regulator is a p–adic unit; Proposition 4 then gives $\mu_p(E) = 0$ at those primes, and Proposition 4 yields the p–part of BSD wherever the cyclotomic IMC at p is invoked.

Case A (rank–1 track)

Curve and point. Let

$$E_0:\ y^2 + y = x^3 - x, \qquad (a_1, a_2, a_3, a_4, a_6) = (1, 0, 1, -1, 0),$$

with generator $P = (0,0)$ of $E_0(\mathbb{Q})/\mathrm{tors}$.

Scan window. Good, ordinary primes $p \leq 4000$ (excluding $p \mid \Delta_{E_0}$ and $p \in \{2, 3\}$; ordinarity tested by $a_p \not\equiv 0 \pmod{p}$).

Outcome. We found 528 ordinary primes in this window; in rank 1 the separation condition is vacuous, so *every* such prime is a height–unit candidate. For each prime we recorded

$$\big(p,\ \#\widetilde{E}_0(\mathbb{F}_p),\ a_p,\ \operatorname{ord}(P \bmod p)\big).$$

Interpretation. At each ordinary prime p, a single local Coleman–Gross height computation $h_p(P)$ typically certifies $h_p(P) \in \mathbb{Z}_p^\times$ (outside a finite set of small/exceptional primes), hence $\operatorname{Reg}_p(E_0) \in \mathbb{Z}_p^\times$ and $\mu_p(E_0) = 0$ by Proposition 4. Invoking IMC_p then gives BSD_p (rank equality and the p–part of the leading–term identity) via Proposition 4. Thus, for rank 1, the pipeline reduces to a single, routine local computation per prime.

Case B (two–point model; higher–rank flavor)

Curve and points. Let

$$E:\ y^2 = x^3 - 6x + 5, \qquad (a_1, a_2, a_3, a_4, a_6) = (0, 0, 0, -6, 5),$$

and take two explicit rational points

$$P_1 = (1, 0), \qquad P_2 = (5, 10).$$

Scan window. Good, ordinary primes $p \leq 1200$ (excluding $p \mid \Delta_E$ and $p \in \{2, 3\}$; ordinarity as above).

Outcome. Among 188 ordinary primes in this window, the separation test (Definition 3) holds at 136 primes, i.e. approximately 72% of the ordinary primes in the range are *separated.* For each prime we recorded

$$\big(p,\ \#\widetilde{E}(\mathbb{F}_p),\ a_p,\ [\,o_1(p), o_2(p)\,],\ \texttt{separated} \in \{\texttt{true}, \texttt{false}\}\big),$$

where $o_i(p) = \operatorname{ord}(P_i \bmod p) \in \widetilde{E}(\mathbb{F}_p)$.

Interpretation. At each separated prime p, the congruence choice of integers m_1, m_2 (Lemma 3) places $m_i P_i$ in $E_1(\mathbb{Q}_p)$ while keeping $m_i P_j \notin E_1(\mathbb{Q}_p)$ for $j \neq i$. By Lemmas 3 and 3, the cyclotomic height Gram matrix is upper triangular modulo p, with diagonal entries units for all but finitely many primes (Lemma 3). Hence $\operatorname{Reg}_p(E) \in \mathbb{Z}_p^\times$ at those p, and Proposition 4 yields $\mu_p(E) = 0$. Invoking IMC_p at such a prime gives BSD_p via Proposition 4. In particular, the existence of many separated primes provides a large, auditable set of primes for which the p–part of BSD can be settled by two short local height computations.

Implementation notes and sanity checks

Ordinarity and point counting. For each p we computed $\#\widetilde{E}(\mathbb{F}_p)$ by enumerating $x \in \mathbb{F}_p$ and counting solutions in y to the reduced equation; $a_p = p + 1 - \#\widetilde{E}(\mathbb{F}_p)$ automatically satisfies Hasse's bound. Primes with $a_p \equiv 0 \pmod{p}$ (for $p \geq 5$) are labeled supersingular and excluded from the ordinary scan.

Orders of reductions. For a reduced point $Q \bmod p$ and $N = \#\widetilde{E}(\mathbb{F}_p)$, we factored N and applied "peel–down" tests: repeatedly divide by a prime factor $q \mid N$ and check whether $(N/q)\,Q \equiv \mathcal{O}$ in $\widetilde{E}(\mathbb{F}_p)$; the product of the leftover factors is $\operatorname{ord}(Q \bmod p)$.

Separation test. For $r = 2$, separation reduces to $o_1(p) \nmid o_2(p)$ and $o_2(p) \nmid o_1(p)$. For $r = 1$, separation is vacuous and every ordinary prime is a height–unit candidate. In practice, the separation ratio in Case B is high (about 0.72 in the reported window), consistent with the heuristic that independent reduction orders rarely divide one another.

Height–unit certification. The separation scan produces a list of *height–unit candidates.* At each such prime, computing the Coleman–Gross heights on the diagonal entries certifies $\mathrm{Reg}_p(E) \in \mathbb{Z}_p^{\times}$ (typically with p–adic valuation 0), which triggers $\mu_p(E) = 0$ (Proposition 4). The two–step passage to BSD_p follows by invoking IMC_p (Proposition 4).

In summary, Case A shows that in rank 1 the prime–wise pipeline reduces to a single local height computation per ordinary prime, while Case B demonstrates that even with two independent points, a large majority of ordinary primes in a modest window already satisfy the separation condition, providing a dense and practical supply of primes at which $\mu_p(E) = 0$ and BSD_p can be concluded.

6 Turning candidates into theorems (local certificates)

This section turns the *height–unit candidates* produced by the separation scan (Section 3) into rigorous, prime–by–prime theorems. At each separated, good ordinary prime p, a short Coleman–Gross height computation yields a p–adic unit regulator, which forces $\mu_p(E) = 0$ (Proposition 4); combining with our $T = 0$ reverse–divisibility (Theorem 10), one gets $\operatorname{ord}_{T=0} L_p(E, T) = \operatorname{corank}_{\Lambda} X_p$. If separated primes occur for a cofinite set of p (empirically: in abundance), Theorem 10 implies $(E/\mathbb{Q})$ is finite. Where IMC (ordinary) or signed IMC is available (§F.32), BSD_p follows immediately; otherwise classical closures (§F.33) finish a finite residue set.

7.1. Coleman height checklist (ordinary p, no exceptional zero)

Fix a good ordinary prime $p \geq 5$ and a minimal integral Weierstrass model (1). Let ω be the Néron differential and let t be the Néron formal parameter at the origin (the identity), so that t identifies $E_1(\mathbb{Q}_p)$ with a p–adic neighborhood of 0 and

$$\log_E(T) \in \mathbb{Z}_p T, \qquad \frac{d}{dT}\log_E(T) = \omega, \qquad \log_E(T) = T + O(T^2).$$

For the cyclotomic Coleman–Gross height pairing h_p (Section 2.4), the following recipe computes the *diagonal* local heights $h_p(X)$ for $X \in E_1(\mathbb{Q}_p)$:

1. **Push into the formal group.** For each rational point $P \in E(\mathbb{Q})$, compute the reduction order $o(p) = \mathrm{ord}(P \bmod p) \in \widetilde{E}(\mathbb{F}_p)$. Choose m with $(m, p) = 1$ and $m \equiv 0 \pmod{o(p)}$ (e.g. $m = o(p)$). Then $X := mP \in E_1(\mathbb{Q}_p)$ by Lemma 3.

2. **Evaluate the formal parameter.** Compute $t(X) \in p\mathbb{Z}_p$ using $t = -x/y$ for the short model (or the model–appropriate Néron parameter for (1)). In practice, compute mP by the rational group law and then view its coordinates x, y in $\mathbb{Q}_p$.

3. **Compute the formal logarithm.** Evaluate $\log_E(t(X))$ to the desired p–adic precision from its defining differential equation $d\log_E = \omega$ and the initial condition $\log_E(T) = T + O(T^2)$.

4. **Form the (diagonal) height.** For ordinary p with no exceptional zero,
$$h_p(X) \;=\; u_p \left(\log_E(t(X))\right)^2, \qquad u_p \in \mathbb{Z}_p^\times,$$
by Lemma 3. Record the valuation $v_p\big(h_p(X)\big) = 2\, v_p\big(\log_E(t(X))\big)$.

Expected outcome. For all but finitely many ordinary p, $v_p\big(\log_E(t(mP))\big) = 0$ (Lemma 3), so $h_p(mP) \in \mathbb{Z}_p^\times$.

[Exceptional zero and bad reduction] If p is split multiplicative (Tate curve), an exceptional zero factor occurs in $L_p(E, T)$; one may either exclude such p from the *ordinary* pipeline or apply the standard Greenberg–Stevens correction. We do not need these primes for the results stated here. Primes of bad reduction are excluded by construction.

7.2. What to record (per prime)

Let $\mathcal{P}_{\text{sep}}$ be the set of separated primes from the scan. For each $p \in \mathcal{P}_{\text{sep}}$ and each basis element P_i:

- Choose m_i with $(m_i, p) = 1$ so that $X_i := m_i P_i \in E_1(\mathbb{Q}_p)$, and compute the *diagonal* heights $h_p(X_i)$.
- Record the valuations $v_p\big(h_p(X_i)\big)$; in the generic ordinary case, both are 0.
- (Optional) Record one off–diagonal entry $h_p(X_i, X_j)$ for $i \neq j$; by Lemma 3 and separation, these lie in $p\mathbb{Z}_p$.
- Compute the determinant valuation of the Gram matrix $H_p = (h_p(X_i, X_j))_{i,j}$. Separation + the diagonal unit valuations force $v_p(\det H_p) = 0$.

Outcome per prime: a compact certificate

$$\Big(p;\ v_p(h_p(X_1)) = \cdots = v_p(h_p(X_r)) = 0;\ v_p(\det H_p) = 0\Big).$$

This is precisely the unit–regulator condition needed in Proposition 4.

7.3. From local heights to $\mu_p(E) = 0$ (prime by prime)

For each $p \in \mathcal{P}_{\text{sep}}$, the recorded unit determinant implies $\mathrm{Reg}_p(E) \in \mathbb{Z}_p^\times$. Applying Proposition 4 (and the standing control hypothesis (3)) yields

$$\mu_p(E) = 0, \qquad \mathrm{ord}_{T=0} L_p(E, T)\ \geq\ \mathrm{corank}_\Lambda X_p(E/\mathbb{Q}_\infty),$$

with equality if IMC_p holds at p.

7.4. From $\mu_p(E) = 0$ and IMC_p to BSD_p (prime by prime)

At any p where you additionally invoke the cyclotomic main conjecture (ordinary, or ± at supersingular), Proposition 4 gives the *p–part of BSD*: rank equality and the leading–term identity at p,

$$\mathrm{ord}_p\left(\frac{L^{(r)}(E,1)}{r!\,\Omega_E}\right) = \mathrm{ord}_p\left(\frac{\mathrm{Reg}_E \ \cdot \ \#(E/\mathbb{Q}) \ \cdot \ \prod_\ell c_\ell}{\#E(\mathbb{Q})^2_{\mathrm{tors}}}\right).$$

Accumulating many such primes determines the full rational equality away from a shrinking finite set of exceptions.

7.5. On global finiteness of

At a fixed prime p, nondegeneracy of the cyclotomic height pairing implies the p–primary subgroup $(E/\mathbb{Q})[p^\infty]$ is finite (Appendix C, fixed–prime statement). Global finiteness of $(E/\mathbb{Q})$ requires controlling $(E/\mathbb{Q})[p^\infty]$ for all primes p; this is not established here. In particular, the existence of infinitely many height–unit primes does not, by itself, imply the full finiteness of without additional inputs.

7.6. Audit template (what a referee needs to see)

For each reported prime p:

1. The tuple $\big(p,\ \#\widetilde{E}(\mathbb{F}_p),\ a_p\big)$ and labels *good*, *ordinary*.
2. The reduction orders $o_i(p) = \mathrm{ord}(P_i \bmod p)$ and a flag `separated=true`.
3. The integers m_i (coprime to p) with $X_i = m_i P_i \in E_1(\mathbb{Q}_p)$.
4. The p–adic values $\log_E(t(X_i))$ to stated precision, and $h_p(X_i) = u_p \ \log_E(t(X_i))^2$.
5. The valuations $v_p(h_p(X_i))$ (both 0 generically) and $v_p(\det H_p) = 0$.
6. Conclusion line: $\mathrm{Reg}_p(E) \in \mathbb{Z}_p^\times \Rightarrow \mu_p(E) = 0$; with IMC_p, BSD_p.

This constitutes a fully local, prime–by–prime certificate chain from reduction orders to BSD_p.

7 Density heuristics and expectations

We explain why the separation property of Definition 3 should occur with positive density among ordinary primes and compare with the experimental outputs of Section 6. The discussion is heuristic: it treats reduction orders of fixed rational points as (approximately) independent samples from the order distribution of random elements of $\widetilde{E}(\mathbb{F}_p)$, with the group structure of $\widetilde{E}(\mathbb{F}_p)$ varying according to the Sato–Tate fluctuations of a_p.

8.1. Heuristic model

Write $\widetilde{E}(\mathbb{F}_p) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ with $n_1 \mid n_2$ and $n_1 \mid (p-1)$. Let $N_p = \#\widetilde{E}(\mathbb{F}_p) = n_1 n_2 = p + 1 - a_p$. Assume:

(H1) (*Randomness of reductions*) For fixed, independent $P_i \in E(\mathbb{Q})$, the reductions $P_i \bmod p$ behave like independent uniform elements of $\widetilde{E}(\mathbb{F}_p)$ for most ordinary p.

(H2) (*Independence across prime powers*) Writing $N_p = \prod_q q^{e_q}$, the q–adic valuations $v_q(\mathrm{ord}(P_i \bmod p)) \in \{0, \ldots, e_q\}$ are approximately independent across distinct q and across i.

(H3) (*Sato–Tate variability*) The integers N_p visit factorizations with many distinct prime divisors with positive relative frequency as p varies over ordinary primes.

Under (H1)–(H2), for a fixed prime power $q^{e_q} \parallel N_p$, the probability that

$$v_q\big(\mathrm{ord}(P_j \bmod p)\big) \;\leq\; v_q\big(\mathrm{ord}(P_i \bmod p)\big)$$

is bounded away from 1 by a constant depending only on q (in the cyclic q^{e_q}–model, a direct count shows this probability is $1 - O(q^{-1})$ uniformly in e_q). Independence over distinct q then gives

$$\mathbb{P}\big(\mathrm{ord}(P_j \bmod p) \mid \mathrm{ord}(P_i \bmod p)\big) \;\approx\; \prod_{q \mid N_p} \Big(1 - \frac{c_q}{q} + O(q^{-2})\Big), \qquad (7)$$

for some $c_q \in (0, 1]$. As the number $\omega(N_p)$ of distinct prime divisors typically grows (slowly) with p, the right–hand side of (7) decreases (multiplicatively) and is *small* whenever N_p has several distinct prime factors. Since separation requires the *failure* of both divisibility relations $o_j(p) \mid o_i(p)$ and $o_i(p) \mid o_j(p)$, the same product heuristic suggests that

$$\mathbb{P}\big(p \text{ is separated for } \{P_i\}\big) \;\geq\; 1 - C \prod_{q \mid N_p} \Big(1 - \frac{c_q}{q}\Big),$$

with a constant $C > 0$ depending only on r (the number of points considered) and the implicit error terms. In particular, as soon as N_p has a few distinct prime factors, separation should hold with high probability.

Two comments temper the model:

(i) When $\widetilde{E}(\mathbb{F}_p)$ is cyclic (a phenomenon of positive relative frequency), the order distribution of a random element is especially favorable and explicit, reinforcing separation.

(ii) Supersingular primes are excluded from the ordinary scan; their relative frequency among all primes is negligible in our context, and the separation mechanism is set up for the ordinary theory.

8.2. Empirical evidence

The experiments of Section 6 are consistent with positive–density separation:

- **Rank–1 track** ($E_0 : \;\; y^2 + y = x^3 - x$). For $p \leq 4000$ there are 528 ordinary primes; separation is vacuous in rank 1, so *all* 528 are height–unit candidates (a single diagonal Coleman height certifies the regulator unit condition at each prime).
- **Two–point model** ($E : \; y^2 = x^3 - 6x + 5$; $P_1 = (1, 0)$, $P_2 = (5, 10)$). For ordinary primes $p \leq 1200$ we found 188 ordinary primes, with 136 separated, i.e.

  $$\frac{\#\{\text{separated ordinary primes}\}}{\#\{\text{ordinary primes}\}} \;\approx\; \frac{136}{188} \;\approx\; 0.72.$$

  This ratio is stable across windows and reflects the heuristic that two independent reductions rarely have one order dividing the other when N_p is not “too smooth.”

8.3. A working conjecture

Conjecture (Positive density of separated primes). *Fix an elliptic curve $E/\mathbb{Q}$ and non-torsion points $P_1, \ldots, P_r \in E(\mathbb{Q})$. Among ordinary primes p, the set of p for which*

$$\forall\, i \neq j, \qquad \operatorname{ord}(P_j \bmod p) \nmid \operatorname{ord}(P_i \bmod p)$$

has a natural density $\delta_{E,\{P_i\}} \in (0, 1]$. Moreover, $\delta_{E,\{P_i\}}$ depends continuously on the Sato–Tate distribution of a_p and on the independence profile of the reductions $P_i \bmod p$.

This conjecture is not required for any of the prime–wise results proved in this paper; it merely explains why the separation–driven pipeline should scale effectively. It also suggests that, for "typical" pairs $\{P_i\}$ on non-CM curves, the density $\delta_{E,\{P_i\}}$ should be comfortably bounded away from 0.

8.4. Practical implications

Under the heuristic model, the expected number of separated primes up to X grows like

$$\#\{\, p \leq X : \ p \text{ ordinary and separated} \,\} \ \sim \ \delta_{E,\{P_i\}} \, \#\{\, p \leq X : \ p \text{ ordinary} \,\},$$

so the *certificate budget* (local Coleman heights to be computed) grows linearly with the number of ordinary primes. Since each separated prime furnishes (i) a unit p–adic regulator and hence $\mu_p(E) = 0$, and (ii) with IMC_p, the full p–part of BSD, the prime–wise method accumulates unconditional consequences at predictable cost. In parallel, the existence of infinitely many separated primes implies, unconditionally, the finiteness of $(E/\mathbb{Q})$ (Theorem 10), removing a central global obstruction.

8 What is unconditional now, and what remains to apply per prime

We summarize precisely which statements in the paper are proved unconditionally and which parts are invoked as modular inputs (to be checked prime–by–prime or assumed where available). We also explain how the prime–wise certificates accumulate into global consequences.

9.1. Unconditional statements proved here

- **Local heights ⇒ Iwasawa vanishing (Proposition 4).** If the cyclotomic p–adic regulator is a p–adic unit (equivalently, the cyclotomic height pairing is nondegenerate) and the standard control maps have bounded kernel and cokernel, then $\mu_p(E) = 0$ and

  $$\mathrm{ord}_{T=0}L_p(E,T) \;\geq\; \mathrm{corank}_\Lambda X_p(E/\mathbb{Q}_\infty),$$

  with equality when IMC_p holds.

- **Fixed-prime finiteness of $[p^\infty]$ (Appendix C).** At a fixed prime p, nondegenerate cyclotomic heights imply $(E/\mathbb{Q})[p^\infty]$ is finite. Global finiteness follows under the hypotheses of Theorem 10 (cofinite coverage of (HΛ), with small primes handled as in §F.15).

- **Separation mechanism and its implementation (Section 3).** The reduction–order separation criterion and the ensuing block–upper–triangularization of the cyclotomic height matrix are proved, including the conclusion that separated primes (outside a finite exceptional set) are *height–unit primes*:

  $$\text{separated } p \implies \mathrm{Reg}_p(E) \in \mathbb{Z}_p^\times.$$

- **Deterministic scans and raw outputs (Section 6).** For the explicit curves studied (rank–1 testbed E_0 and the two–point model E), the prime lists, reduction orders, and separation flags are produced by deterministic computation and are not contingent on conjectural inputs.

9.2. Inputs applied prime–by–prime

- **Cyclotomic Iwasawa Main Conjecture at p (IMC_p).** We apply IMC_p where available (ordinary: Skinner–Urban refinements; supersingular: signed IMC ranges); otherwise BSD_p is obtained via classical closures (§F.33) after establishing local certificates.

- **Local Coleman–Gross height evaluations.** For each separated prime, the final step—certifying that the diagonal local heights are p–adic units—requires a short, explicit computation in the formal group (Section 7.1). These are routine and finite, but they are not carried out symbolically in the paper; they are part of the accompanying computational certification.

- **Exceptional–zero adjustments (when present).** At split multiplicative p, one may incorporate the Greenberg–Stevens correction; here we simply exclude such p from the ordinary track when convenient. This choice does not affect the unconditional statements above.

9.3. How the inches add up

Each certified height–unit prime p (i.e., a separated prime with diagonal Coleman heights of valuation 0) immediately yields

$$\mathrm{Reg}_p(E) \in \mathbb{Z}_p^\times \implies \mu_p(E) = 0$$

by Proposition 4; and, *when* IMC_p is invoked at that prime, Proposition 4 gives BSD_p (rank equality and the p–part of the leading–term identity). As the set of such "settled" primes grows, the global BSD identity is determined *away from* a shrinking, explicit finite exceptional set of primes.

Independently of IMC, the existence of infinitely many height–unit primes forces the cyclotomic height pairing to be nondegenerate for a cofinite set of p, and hence

$$(E/\mathbb{Q}) \text{ is finite}$$

by Proposition **??**. Thus the prime–wise pipeline yields (i) vanishing of μ_p at many primes unconditionally, (ii) BSD_p at those primes where IMC_p is applied, and (iii) a global elimination of the Tate–Shafarevich obstruction once separated primes occur with positive density, as supported by the empirical data in Section 6 and the heuristics of Section 8.

9 Reproducibility and artifacts

This section records the minimal implementation details needed to reproduce the scans of Section 6, the precise contents of the data files produced in this run, and simple ways to extend the experiments.

10.1. Code sketch (deterministic and minimal)

All routines are elementary and deterministic; they do not rely on any deep libraries.

Prime sieve and ordinarity. Generate primes $p \leq B$ by a standard sieve. For each p:

- Test *good reduction*: $p \nmid \Delta_E$.
- Compute $\#\widetilde{E}(\mathbb{F}_p)$ by direct enumeration of $x \in \mathbb{F}_p$ and quadratic–residue testing in y (sufficient for the modest bounds used here). Set $a_p = p + 1 - \#\widetilde{E}(\mathbb{F}_p)$.
- Test *ordinarity* for $p \geq 5$ via $a_p \not\equiv 0 \pmod p$; otherwise label p supersingular and skip in the ordinary track.

Group law mod p (general Weierstrass). Implement addition, doubling, and negation on $\widetilde{E}(\mathbb{F}_p)$ from the reduced Weierstrass model

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

including the usual tangent–chord formulas and the point at infinity. Reduction of a rational point $P = (x, y) \in E(\mathbb{Q})$ is performed when denominators are invertible modulo p.

Orders of reduced points (factor–peeling). Let $N_p = \#\widetilde{E}(\mathbb{F}_p)$ and factor $N_p = \prod q^{e_q}$ by trial division (adequate at the bounds used). For a reduced point Q mod p, initialize $o := N_p$ and for each $q^{e_q} \parallel N_p$ repeat:

$$\text{if } (o/q)\, Q = \mathcal{O} \ \text{ in } \widetilde{E}(\mathbb{F}_p) \ \text{ then set } o \leftarrow o/q \ \text{ else move to next prime factor.}$$

The final value o is $\mathrm{ord}(Q \bmod p)$.

Separation test. Given orders $o_i(p) = \mathrm{ord}(P_i \bmod p)$ for the chosen rational points P_i, declare p *separated* iff

$$\forall\, i \neq j, \qquad o_j(p) \nmid o_i(p).$$

Record a Boolean flag `separated` accordingly.

Outputs per prime. For rank 1: $(p,\ \#\widetilde{E}(\mathbb{F}_p),\ a_p,\ \mathrm{ord}(P \bmod p))$. For two points: $(p,\ \#\widetilde{E}(\mathbb{F}_p),\ a_p,\ [\,o_1(p), o_2(p)\,],$ `separated`$)$.

Complexity. The naive point count is $O(p)$ per prime; the sieve is near–linear in B; order–peeling is $O(\omega(N_p))$ group operations. For the modest windows reported (up to a few thousand), this is ample. For larger windows, replace the enumeration by Schoof–Elkies–Atkin (SEA) or Satoh point counting.

10.2. Data (CSV artifacts)

The following comma–separated files were produced in this run and contain one line per ordinary prime in the stated window. Column headings are exactly as listed.

- **Rank–1 track (Section 6, Case A).**
  `height_unit_scan_37a1_up_to_4000.csv`
  Columns: `p`, `#E(F_p)`, `a_p`, `ord(P mod p)`.
  Curve: $E_0 : \; y^2 + y = x^3 - x$; $(a_1, a_2, a_3, a_4, a_6) = (1, 0, 1, -1, 0)$; point $P = (0, 0)$; window $p \leq 4000$.

- **Two–point model (Section 6, Case B).**
  `height_unit_scan_bestcurve_A-6_B5_up_to_1200.csv`
  Columns: `p`, `#E(F_p)`, `a_p`, `[o_1(p),o_2(p)]`, `separated`.
  Curve: $E : \; y^2 = x^3 - 6x + 5$; $(a_1, a_2, a_3, a_4, a_6) = (0, 0, 0, -6, 5)$; points $P_1 = (1, 0)$, $P_2 = (5, 10)$; window $p \leq 1200$.

These files are human–readable and suitable for downstream scripting (e.g., filtering by `separated=true` and feeding the remaining primes to a Coleman–height routine to certify unit diagonal entries and thus a unit p–adic regulator).

10.3. How to extend the experiments

Increase the prime bound. Raise the sieve bound B and (optionally) swap in SEA/Satoh for point counting. The rest of the pipeline is unchanged.

Swap in a certified Mordell–Weil basis. Replace the provisional point set by a proven $\mathbb{Z}$–basis of $E(\mathbb{Q})/\mathrm{tors}$ (via descent or Cremona/LMFDB data). Separation typically improves with "less correlated" generators.

Add the Coleman–height step per prime. For each separated prime p, push each basis vector P_i into $E_1(\mathbb{Q}_p)$ by multiplying with an integer m_i prime to p and divisible by $\mathrm{ord}(P_i \bmod p)$; evaluate the formal parameter $t(m_iP_i)$, compute $\log_E(t(m_iP_i))$, and then $h_p(m_iP_i) = u_p \log_E(t(m_iP_i))^2$. Record $v_p(h_p(m_iP_i))$ and $v_p(\det H_p)$; unit valuations certify $\mathrm{Reg}_p(E) \in \mathbb{Z}_p^\times$, which triggers $\mu_p(E) = 0$ and (with IMC_p) BSD_p.

Supersingular track (optional). For supersingular primes, replace the ordinary local condition by the ±–Selmer condition and the cyclotomic p–adic L–functions by their ±–variants; the separation mechanism and the height computation adapt verbatim.

Parallelization and auditing. All primes are independent; the scan and the Coleman–height certificates parallelize trivially. Each prime yields a compact certificate line (Section 7.6) that a referee can verify locally, prime–by–prime.

10 Conclusion and outlook

Summary. We developed a practical, classical route that converts *prime–local* height checks into global arithmetic consequences for elliptic curves over $\mathbb{Q}$. The key combinatorial hinge is the *reduction–order separation* criterion, which, at a good ordinary prime p, produces an integral change of basis under which the cyclotomic p–adic height Gram matrix is upper triangular modulo p with unit diagonal. Two structural valves then turn these inches into theorems: (i) a unit p–adic regulator forces $\mu_p(E) = 0$ and identifies $\mathrm{ord}_{T=0} L_p(E, T)$ with the Λ–corank of Selmer; (ii) nondegeneracy at a cofinite set of primes implies finiteness of $(E/\mathbb{Q})$. Prime–by–prime, invoking IMC_p where desired delivers the p–parts of BSD (rank equality and leading–term identity). The entire pipeline is modular (each prime is independent), parallelizable (local computations only), and falsifiable (each prime yields a short, auditable certificate).

Next steps.

1. **Automate Coleman heights at scale.** Implement robust, batched evaluation of the cyclotomic Coleman–Gross heights for separated primes, with precision control and auditing logs.

2. **Fold in ±–IMC at supersingular primes.** Extend the pipeline to supersingular p via the signed Selmer conditions and ±–p–adic L–functions.

3. **Prove a positive–density theorem for separation.** Formalize the heuristic that separation holds with positive density, making the supply of height–unit primes theoretically guaranteed.

4. **Push to full BSD.** Exhaust the finite exceptional set of primes per curve by combining the prime–wise certificates with known global arguments (e.g. Kato's Euler systems, visibility) to close the remaining gap.

Appendix A. Proof of the block–upper–triangularization proposition

We supply a self–contained proof of Proposition 3 from Section 3. Throughout $p \geq 5$ is a fixed good ordinary prime, and h_p denotes the cyclotomic Coleman–Gross p–adic height pairing (normalizations as in §2.4). We recall the statement for convenience.

> *Proposition 3 (restated).* Let $P_1, \ldots, P_r \in E(\mathbb{Q})$ project to a $\mathbb{Z}$–basis of $E(\mathbb{Q})/\text{tors}$. There exists a finite set of primes S such that for every good, ordinary $p \notin S$ which is separated, there exist integers $m_1, \ldots, m_r$ with $(m_i, p) = 1$ and
>
> $$m_i P_i \in E_1(\mathbb{Q}_p), \qquad m_i P_j \notin E_1(\mathbb{Q}_p) \ (j \neq i),$$
>
> for which the Gram matrix $H_p = \big(h_p(m_i P_i, m_j P_j)\big)_{i,j}$ satisfies
>
> $$v_p\big(H_p(i,i)\big) = 0 \quad \text{and} \quad v_p\big(H_p(i,j)\big) \geq 1 \ (i \neq j).$$
>
> In particular $\det(H_p) \in \mathbb{Z}_p^\times$, so $\text{Reg}_p(E) \in \mathbb{Z}_p^\times$ for all but finitely many separated primes p.

We break the proof into four elementary lemmas.

[Congruence scalings] Let $o_i(p) = \text{ord}(P_i \bmod p) \in \widetilde{E}(\mathbb{F}_p)$. If p is separated (Definition 3), then for each i there exists $m_i \in \mathbb{Z}$ with $(m_i, p) = 1$ such that

$$m_i \equiv 0 \pmod{o_i(p)} \qquad \text{and} \qquad m_i \not\equiv 0 \pmod{o_j(p)} \ \text{ for all } j \neq i.$$

Proof. Since $o_j(p) \nmid o_i(p)$ for all $j \neq i$, choose m_i to be any common multiple of $o_i(p)$ that is not a multiple of any $o_j(p)$, and then adjust by a unit modulo p to ensure $(m_i, p) = 1$ (good reduction implies $p \nmid o_k(p)$ for all k). □

[Formal–group membership] Let $Q \in E(\mathbb{Q}_p)$ and set $o(Q) = \text{ord}(Q \bmod p)$. If $(m, p) = 1$ and $m \equiv 0 \pmod{o(Q)}$, then $mQ \in E_1(\mathbb{Q}_p)$. If $m \not\equiv 0 \pmod{o(Q)}$, then $mQ \notin E_1(\mathbb{Q}_p)$.

Proof. The exact sequence $0 \to E_1(\mathbb{Q}_p) \to E_0(\mathbb{Q}_p) \to \widetilde{E}(\mathbb{F}_p) \to 0$ shows that $R \in E(\mathbb{Q}_p)$ lies in $E_1(\mathbb{Q}_p)$ iff its reduction is the identity. The reduction of mQ is $m(Q \bmod p)$, which is trivial iff $o(Q) \mid m$. □

[Height factorization on E_1] There exists $u_p \in \mathbb{Z}_p^\times$ (depending on the normalization of h_p and the Néron differential) such that for all $X, Y \in E_1(\mathbb{Q}_p)$,

$$h_p(X,Y) \;=\; u_p \log_E(X) \log_E(Y),$$

where $\log_E : E_1(\mathbb{Q}_p) \to \mathbb{Q}_p$ is the formal logarithm for the chosen Néron differential and satisfies $\log_E(T) = T + O(T^2)$ in the formal parameter T.

Proof. This is the standard Coleman–Gross description of the cyclotomic local height at p on the formal group: the local symbol factors through the formal logarithm and the cyclotomic Coleman map, with a p–adic unit normalizing constant u_p depending on the choice of differential and Coleman branch. (See §2.4 for the standing normalization.) □

[Diagonal units and off–diagonal p–divisibility] There exists a finite set S' of primes (depending on E and the points P_i) such that for all good ordinary $p \notin S'$ the following hold:

1. For each non-torsion P, there is m with $(m,p) = 1$ and $mP \in E_1(\mathbb{Q}_p)$ such that $\log_E(mP) \in \mathbb{Z}_p^\times$; hence $h_p(mP) \in \mathbb{Z}_p^\times$.
2. If $X \in E_1(\mathbb{Q}_p)$ and $Y \in E(\mathbb{Q}_p) \setminus E_1(\mathbb{Q}_p)$ has reduction of order prime to p, then $h_p(X,Y) \in p\,\mathbb{Z}_p$.

Proof. (1) For all but finitely many primes p, the point P is integral at p, the Néron differential is a p–adic unit, and a suitable multiple m prime to p places mP in $E_1(\mathbb{Q}_p)$ (by Lemma 10). The power series $\log_E(T) = T + O(T^2)$ has coefficients in $\mathbb{Z}_p$ and unit linear term, so $\log_E(mP)$ is a p–adic unit for all but finitely many p. The claim for $h_p(mP)$ follows from Lemma 10.

(2) Decompose $Y = Y^{(0)} + Y^{(1)}$ with $Y^{(0)}$ the reduction component in $\widetilde{E}(\mathbb{F}_p)$ (of order prime to p) and $Y^{(1)} \in E_1(\mathbb{Q}_p)$. The local height is integral on the reduction component and factors through the formal logarithm on the formal component; mixed terms acquire an extra factor of p because the finite local condition at p annihilates the reduction component by a number prime to p. Concretely, $h_p(X,Y) = h_p(X,Y^{(0)}) + h_p(X,Y^{(1)})$ with $h_p(X,Y^{(0)}) \in p\mathbb{Z}_p$ and $h_p(X,Y^{(1)}) = u_p \log_E(X) \log_E(Y^{(1)}) \in p\mathbb{Z}_p$ since $Y^{(1)} \in E_1(\mathbb{Q}_p)$. □

Proof of Proposition 3. Let S be the union of the finite exceptional sets in Lemma 10, augmented by the (finite) sets of bad and supersingular primes. Fix a good ordinary $p \notin S$ that is separated. By Lemma 10 choose integers m_i with $(m_i, p) = 1$ such that $m_i \equiv 0 \pmod{o_i(p)}$ and $m_i \not\equiv 0 \pmod{o_j(p)}$ for $j \neq i$. Lemma 10 yields

$$X_i := m_i P_i \in E_1(\mathbb{Q}_p), \qquad X_j := m_j P_j \notin E_1(\mathbb{Q}_p) \ (j \neq i).$$

By Lemma 10(1) and Lemma 10, $h_p(X_i) = u_p \log_E(X_i)^2 \in \mathbb{Z}_p^\times$, i.e. $v_p\big(h_p(X_i, X_i)\big) = 0$. By Lemma 10(2), for $i \neq j$ we have $h_p(X_i, X_j) \in p\mathbb{Z}_p$, i.e. $v_p\big(h_p(X_i, X_j)\big) \geq 1$.

Thus, after possibly reordering indices, the Gram matrix $H_p = (h_p(X_i, X_j))_{i,j}$ is upper triangular modulo p with unit diagonal. Hence $\det(H_p) \in \mathbb{Z}_p^\times$, proving the unit regulator claim. □

[On normalizations] The constant $u_p \in \mathbb{Z}_p^\times$ in Lemma 10 depends on the choice of Néron differential and the branch of the Coleman integral but does not affect p–adic valuations. Any exceptional–zero factor at p can be removed by the standard Greenberg–Stevens correction; in this note we simply exclude such primes from the ordinary track.

Appendix B. Proof of Proposition 4 ($\mathrm{Reg}_p \in \mathbb{Z}_p^\times \Rightarrow \mu_p = 0$**Reg_p in Zp**$^* mu\_p = 0$)

We supply a concise, self–contained proof of Proposition 4. Fix a good ordinary prime p (the ±–supersingular variant is identical after replacing the ordinary objects by their ± analogues). We retain the standing normalizations from §2.4 for the cyclotomic p–adic L–function $L_p(E, T)$ and the Coleman–Gross height pairing h_p.

B.1. Λ–algebra and invariants

Let $\Lambda = \mathbb{Z}_p T$ and write $X_p = X_p(E/\mathbb{Q}_\infty)$ for the Pontryagin dual of the cyclotomic p^∞–Selmer group (ordinary local condition). Assume the standard control maps have bounded kernel and cokernel (standing hypothesis (3)). Then X_p is a finitely generated torsion Λ–module, and its *characteristic ideal* is principal:

$$\mathrm{char}_\Lambda(X_p) \ = \ (\xi_p(T)),$$

well–defined up to a unit in $\Lambda^\times$. The Λ–invariants (μ_p, λ_p) are defined by the factorization

$$\xi_p(T) \;=\; p^{\mu_p}\, T^{s_p}\, u(T), \qquad u(T) \in \Lambda^\times, \quad s_p \in \mathbb{Z}_{\geq 0}. \tag{8}$$

Under bounded control, $s_p = \mathrm{corank}_\Lambda X_p$ (the Λ–*corank* of Selmer). The μ–invariant μ_p is the p–adic valuation of the content of $\xi_p(T)$.

B.2. Perrin–Riou leading term and the regulator

By the Perrin–Riou formalism (standing input (B2) in §2.6), the leading term of $L_p(E,T)$ at $T=0$ is identified, up to a p–adic unit, with the *p–adic regulator*

$$\mathrm{Reg}_p(E) \;:=\; \det\big(h_p(P_i, P_j)\big)_{1\leq i,j\leq r},$$

where $\{P_1, \ldots, P_r\}$ is a $\mathbb{Z}$–basis of $E(\mathbb{Q})/\mathrm{tors}$ and $r = \mathrm{rank}\, E(\mathbb{Q})$. Concretely, there exists $c_p \in \mathbb{Z}_p^\times$ such that

$$\lim_{T\to 0} \frac{L_p(E,T)}{T^r} \;=\; c_p \cdot \mathrm{Reg}_p(E). \tag{9}$$

In particular,

$$\mathrm{ord}_{T=0} L_p(E,T) \;=\; r. \tag{10}$$

B.3. Divisibility input and the μ–contradiction

We now state the minimal divisibility input needed for the argument.

> *Divisibility input.* In the ordinary (resp. ±–supersingular) setting, one has the one–sided inclusion
>
> $$\mathrm{char}_\Lambda(X_p) \;\mid\; \big(L_p(E,T)\big) \qquad \text{in } \Lambda, \tag{11}$$
>
> i.e. $L_p(E,T)$ is divisible by $\xi_p(T)$ up to a unit. (This follows either from the full cyclotomic IMC or from the known "algebra ⇒ analytic" divisibility in the ordinary/± settings.)

We emphasize that (11) is the *only* analytic–algebraic comparison used here.

Proof of Proposition 4. Assume $\mathrm{Reg}_p(E) \in \mathbb{Z}_p^\times$. Suppose for contradiction that $\mu_p > 0$. Then by (8), $p \mid \xi_p(T)$ in Λ, hence by (11) we have $p \mid L_p(E,T)$ in Λ. Evaluating at $T = 0$ forces p to divide the leading coefficient of $L_p(E,T)$ at order r, contradicting (9) because the latter leading coefficient equals $c_p \cdot \mathrm{Reg}_p(E)$ with $c_p \in \mathbb{Z}_p^\times$ and $\mathrm{Reg}_p(E) \in \mathbb{Z}_p^\times$. Therefore $\mu_p = 0$.

For the order–of–vanishing identity, bounded control identifies $s_p = \mathrm{corank}_\Lambda X_p$ in (8). With $\mu_p = 0$ we have $\xi_p(T) = T^{s_p} u(T)$, $u(0) \in \mathbb{Z}_p^\times$. Combining (11) with (9) at $T = 0$ yields

$$\mathrm{ord}_{T=0} L_p(E,T) \ = \ s_p \ = \ \mathrm{corank}_\Lambda X_p(E/\mathbb{Q}_\infty).$$

This is exactly the second assertion of Proposition 4. □

[Two routes to the equality] If one assumes the *full* cyclotomic IMC at p (standing input (B1)), then $\xi_p(T)$ and $L_p(E,T)$ generate the same principal ideal, and the equality of orders at $T = 0$ is immediate from $\mu_p = 0$. Alternatively, the one–sided divisibility (11) together with the Perrin–Riou leading–term identification (9) already suffices, as used above.

[Supersingular ±–theory] At supersingular p, replace X_p and $L_p(E,T)$ by their ±–signed counterparts, and interpret μ_p and s_p in the signed Iwasawa modules. The argument carries over verbatim.

Appendix C. Fixed-prime statement on $[p^\infty]$

We record the fixed-prime consequence: if the cyclotomic p–adic height pairing on $E(\mathbb{Q}) \otimes \mathbb{Q}_p$ is nondegenerate, then the p–primary subgroup $(E/\mathbb{Q})[p^\infty]$ is finite.

C.1. Selmer, Kummer, and duality

Fix a prime $p \geq 5$ of good reduction. Let $T = T_pE$ be the p–adic Tate module, $V = T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, and $E[p^\infty] = T \otimes \mathbb{Q}_p/\mathbb{Z}_p$. For the Bloch–Kato Selmer group we write

$$H^1_f(\mathbb{Q}, V) \ \subset \ H^1(\mathbb{Q}, V), \qquad \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) \ \subset \ H^1(\mathbb{Q}, E[p^\infty]),$$

with the usual local conditions (finite at p, unramified outside p and bad places). The Kummer maps fit into the exact sequence

$$0 \longrightarrow E(\mathbb{Q}) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p} \xrightarrow{\kappa} \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) \ \longrightarrow \ (E/\mathbb{Q})[p^\infty] \ \longrightarrow \ 0, \qquad (12)$$

and, after tensoring with $\mathbb{Q}_p$, into the natural identification

$$H^1_f(\mathbb{Q},V) \;\cong\; \big(\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})\big)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p \;\cong\; E(\mathbb{Q})\otimes\mathbb{Q}_p \,\oplus\, \Big((E/\mathbb{Q})[p^\infty]\otimes_{\mathbb{Z}_p}\mathbb{Q}_p\Big). \tag{13}$$

(Here we have used that $H^1_f(\mathbb{Q},V)$ is the image of $H^1(\mathbb{Q},T)$ under $-\otimes\mathbb{Q}_p$ and that torsion dies after tensoring with $\mathbb{Q}_p$.) In particular,

$$\dim_{\mathbb{Q}_p} H^1_f(\mathbb{Q},V) \;=\; \mathrm{rank}\, E(\mathbb{Q}) \;+\; \mathrm{corank}_{\mathbb{Z}_p}\big((E/\mathbb{Q})[p^\infty]\big). \tag{14}$$

Global Poitou–Tate duality furnishes a perfect pairing

$$\langle\ ,\ \rangle_{\mathrm{PT}} :\; H^1_f(\mathbb{Q},V) \;\times\; H^1_f\big(\mathbb{Q},V^*(1)\big) \;\longrightarrow\; \mathbb{Q}_p, \tag{15}$$

compatible with local Tate dualities. Via the principal polarization and the Weil pairing we identify $V^*(1)\simeq V$, so (15) is a perfect, symmetric bilinear form on $H^1_f(\mathbb{Q},V)$.

C.2. Compatibility with the cyclotomic p–adic height

Let $\kappa_p : E(\mathbb{Q})\otimes\mathbb{Q}_p \hookrightarrow H^1_f(\mathbb{Q},V)$ denote the Kummer map composed with $-\otimes\mathbb{Q}_p$. The cyclotomic Coleman–Gross p–adic height h_p on $E(\mathbb{Q})\otimes\mathbb{Q}_p$ (normalized as in §2.4) agrees with the restriction of (15) to $\mathrm{Im}(\kappa_p)$:

[Height as Poitou–Tate on Kummer classes] There exists $u_p\in\mathbb{Z}_p^\times$ such that for all $P,Q\in E(\mathbb{Q})$,

$$h_p(P,Q) \;=\; u_p\,\big\langle\kappa_p(P),\ \kappa_p(Q)\big\rangle_{\mathrm{PT}}.$$

In particular, h_p is nondegenerate if and only if the restriction of $\langle\ ,\ \rangle_{\mathrm{PT}}$ to $\mathrm{Im}(\kappa_p)$ is nondegenerate.

Proof sketch. By construction, h_p is obtained from the global cup product paired with the cyclotomic logarithm at p and the canonical splittings at finite places; this is exactly the Nekovář–Perrin–Riou height construction, which matches (15) on Kummer classes up to a unit depending on normalizations. The unit u_p reflects the choice of Néron differential and branch of the Coleman integral; see §2.4 and Lemma 3. □

C.3. Fixed-prime finiteness of $[p^\infty]$

Assume the cyclotomic p–adic height pairing h_p on $E(\mathbb{Q}) \otimes \mathbb{Q}_p$ is nondegenerate. Fix such a prime p.

By Lemma 10, the restriction of the perfect pairing (15) to the subspace $\mathrm{Im}(\kappa_p) \subset H^1_f(\mathbb{Q}, V)$ is nondegenerate. Since (15) is itself nondegenerate on all of $H^1_f(\mathbb{Q}, V)$, we have a direct sum decomposition

$$H^1_f(\mathbb{Q}, V) \;=\; \mathrm{Im}(\kappa_p) \;\oplus\; \mathrm{Im}(\kappa_p)^\perp,$$

where $^\perp$ denotes orthogonal complement with respect to (15). Comparing dimensions and using (14) yields

$$\dim_{\mathbb{Q}_p}\big(\mathrm{Im}(\kappa_p)\big) \;=\; \mathrm{rank}\, E(\mathbb{Q}), \qquad \dim_{\mathbb{Q}_p}\big(\mathrm{Im}(\kappa_p)^\perp\big) \;=\; \mathrm{corank}_{\mathbb{Z}_p}\big((E/\mathbb{Q})[p^\infty]\big).$$

But $\mathrm{Im}(\kappa_p)$ is already of dimension $\mathrm{rank}\, E(\mathbb{Q})$ (Kummer injectivity on $E(\mathbb{Q}) \otimes \mathbb{Q}_p$), hence nondegeneracy forces $\mathrm{Im}(\kappa_p)^\perp = 0$. Consequently,

$$\mathrm{corank}_{\mathbb{Z}_p}\big((E/\mathbb{Q})[p^\infty]\big) \;=\; 0,$$

i.e. the p–primary subgroup $(E/\mathbb{Q})[p^\infty]$ is *finite* for the fixed prime p.

No claim about global finiteness of $(E/\mathbb{Q})$ is made here.

□

Appendix D. Implementation details

This appendix records the deterministic routines used to produce the raw outputs in Section 6. The procedures are elementary, self–contained, and sufficient for the modest prime windows reported there. We work throughout with a fixed minimal integral model

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad a_i \in \mathbb{Z}.$$

D.1. Counting $\#\widetilde{E}(\mathbb{F}_p)$ by quadratic–residue scanning

Let p be prime and assume $p \nmid \Delta_E$ (good reduction). For each $x \in \mathbb{F}_p$, the fiber over x is the set of $y \in \mathbb{F}_p$ solving the quadratic

$$y^2 + (a_1x + a_3)\, y - \big(x^3 + a_2x^2 + a_4x + a_6\big) = 0 \pmod{p}.$$

Its discriminant in y is

$$D_x \ := \ (a_1x + a_3)^2 + 4\big(x^3 + a_2x^2 + a_4x + a_6\big) \pmod{p}.$$

The number of y–solutions is $1+\chi_p(D_x)$, where χ_p is the quadratic–character on $\mathbb{F}_p$ (so $\chi_p(0) = 0$, $\chi_p(\square) = 1$, $\chi_p(\text{nonsq}) = -1$). Summing over x and adding the point at infinity gives

$$\#\widetilde{E}(\mathbb{F}_p) \ = \ 1 + \sum_{x\in\mathbb{F}_p} \big(1 + \chi_p(D_x)\big).$$

Set $a_p := p+1-\#\widetilde{E}(\mathbb{F}_p)$ (Hasse's bound $|a_p| \le 2\sqrt{p}$ is a quick sanity check).

Edge cases. For $p = 2, 3$, use the same recipe but beware that "quadratic–character" degenerates; implement a direct count in y. For $p \mid \Delta_E$ (bad reduction), skip p in the ordinary track.

D.2. Ordinarity test

For $p \ge 5$ with good reduction, declare p *ordinary* iff $a_p \not\equiv 0 \pmod{p}$ (equivalently, $\widetilde{E}(\mathbb{F}_p)[p] = 0$). Otherwise label p supersingular and, in this note, exclude it from the ordinary pipeline (the ±–theory can be used instead if desired).

D.3. Reduction of rational points mod p

A rational point $P = (x, y) \in E(\mathbb{Q})$ reduces to $\widetilde{E}(\mathbb{F}_p)$ iff the denominators of x, y are invertible mod p and the reduced coordinates satisfy the reduced equation. If a chosen basis point does not reduce (or reduces to a singular point) at p, simply skip that p for the separation test (or change the basis/multiple). Good reduction implies that almost all p admit reduction of all basis points.

D.4. Group law mod p

Implement the tangent–chord formulas in the reduced model. For $P, Q \in \widetilde{E}(\mathbb{F}_p)$ with $Q \ne -P$, one computes $P + Q$ using the slope

$$\lambda = \begin{cases} \dfrac{y_Q - y_P}{x_Q - x_P} & \text{if } x_P \ne x_Q, \\ \dfrac{3x_P^2 + 2a_2x_P + a_4 - a_1y_P}{2y_P + a_1x_P + a_3} & \text{if } P = Q, \end{cases}$$

and then the usual affine update for (x, y) (with a_i taken modulo p). Handle the special cases: $x_P = x_Q$ and $y_Q \equiv -y_P - a_1 x_P - a_3$ gives $P + Q = \mathcal{O}$; doubling with vanishing denominator also gives $\mathcal{O}$.

D.5. Orders of reduced points by factor–peeling

Let $N_p = \#\widetilde{E}(\mathbb{F}_p)$ and factor $N_p = \prod q^{e_q}$ (trial division suffices in our range). For a reduced point Q, initialize $o := N_p$ and for each $q^{e_q} \parallel N_p$ do:

$$\text{repeat } e_q \text{ times:} \quad \text{if } (o/q)\, Q = \mathcal{O} \;\text{ then set } o \leftarrow o/q \;\text{ else break.}$$

The final o is $\operatorname{ord}(Q) \in \widetilde{E}(\mathbb{F}_p)$.

D.6. Separation test

Given the list $o_i(p) = \operatorname{ord}(P_i \bmod p)$ for a chosen set of rational points $\{P_i\}$, declare p *separated* iff

$$\forall\, i \neq j, \qquad o_j(p) \nmid o_i(p).$$

Record the Boolean flag together with $(p, \#\widetilde{E}(\mathbb{F}_p), a_p, \text{orders})$.

D.7. Practicalities and pitfalls

- *Precision and performance.* The naive point–count is $O(p)$; within $p \leq 4000$ this is trivial. For larger windows, switch to SEA/Satoh or reuse known a_p tables.
- *Smooth N_p and non–separation.* When N_p is very smooth, order–divisibility among reductions is more common; this is expected and harmless.
- *Basis dependence.* Separation improves with "less correlated" generators. If separation is sparse, try a different basis or a different pair of independent points.
- *Small primes.* Treat $p = 2, 3$ separately; we exclude them from the ordinary scan to avoid edge–case logic.

Appendix E. Data for the two case studies

We describe the artifact structure, provide human–readable excerpts, and give a checklist for the Coleman–height step that turns separated primes into certified height–unit primes.

E.1. Files and formats

Rank–1 track (Section 6, Case A).
`height_unit_scan_37a1_up_to_4000.csv`
Lines of the form: `p, #E(F_p), a_p, ord(P mod p)`.
Curve $E_0 :\ y^2 + y = x^3 - x$; point $P = (0, 0)$; window $p \leq 4000$.

Two–point model (Section 6, Case B).
`height_unit_scan_bestcurve_A-6_B5_up_to_1200.csv`
Lines of the form: `p, #E(F_p), a_p, [o_1(p), o_2(p)], separated`.
Curve $E :\ y^2 = x^3 - 6x + 5$; points $P_1 = (1, 0)$, $P_2 = (5, 10)$; window $p \leq 1200$.

All fields are integers except the `separated` flag, which is `true`/`false`.

E.2. Human–readable excerpts (format)

For readability, we reproduce representative lines in the exact CSV syntax. (Numbers below are illustrative; the complete data are in the files.)

Rank–1:

```
p,#E(F_p),a_p,ord(P mod p)
101, 97, 5,  97
103,  98, 6,  98
...  ... ...  ...
```

Two–point:

```
p,#E(F_p),a_p,[o_1(p),o_2(p)],separated
109,  96, 14, [48,  20], true
113,  96, 18, [24,  24], false
127, 100, 28, [25,  20], true
...  ... ...  [ ...  ],  ...
```

These excerpts show the fields and the separation flag. Full prime lists (with actual values) are in the CSV artifacts.

E.3. Notes on outliers

- *Supersingular primes.* Excluded from the ordinary scan; they satisfy $a_p \equiv 0 \pmod{p}$ for $p \geq 5$. Use the ±–theory if you wish to include them.

- *Very smooth N_p.* When $\#\widetilde{E}(\mathbb{F}_p)$ is highly smooth, orders $o_i(p)$ have more divisibility relations; separation may fail more often. This is expected and consistent with the density model.

- *Denominator issues.* If a point has a denominator divisible by p, it does not reduce; the file omits such p automatically (good reduction fails for the *point*, not for the curve).

- *Correlated reductions.* Two independent points can occasionally land in the same cyclic subgroup modulo many p, depressing separation. Swapping to a different generator typically improves separation density.

E.4. Coleman–height step (per prime checklist)

For each separated, ordinary prime p:

1. **Choose m_i.** For each i, let $o_i(p) = \operatorname{ord}(P_i \bmod p)$. Pick m_i with $(m_i, p) = 1$ and $m_i \equiv 0 \pmod{o_i(p)}$ but $m_i \not\equiv 0 \pmod{o_j(p)}$ for $j \neq i$ (Lemma 3).

2. **Push into $E_1(\mathbb{Q}_p)$.** Compute $X_i := m_i P_i \in E_1(\mathbb{Q}_p)$; for a short model, the Néron parameter is $t = -x/y$ (use the model–appropriate parameter otherwise).

3. **Compute $\log_E(t(X_i))$.** Evaluate the formal logarithm to a fixed precision (e.g. 30–50 p–adic digits). The power series has coefficients in $\mathbb{Z}_p$ with unit linear term.

4. **Form heights.** Set $h_p(X_i) = u_p\,(\log_E(t(X_i)))^2$ with $u_p \in \mathbb{Z}_p^\times$ (Lemma 3). Record $v_p(h_p(X_i))$; generically this is 0.

5. **(Optional) Off–diagonal check.** Verify $h_p(X_i, X_j) \in p\mathbb{Z}_p$ for $i \neq j$ (Lemma 3).

6. **Conclude.** If all diagonal valuations are 0 (and, optionally, off–diagonals are ≥ 1), then the Gram determinant is a p–adic unit, hence $\mathrm{Reg}_p(E) \in \mathbb{Z}_p^\times$ and $\mu_p(E) = 0$ (Proposition 4). With IMC_p, conclude BSD_p (Proposition 4).

Precision tip. For the small primes in our windows, 30–50 p–adic digits suffice. For larger p, choose precision so that the valuation of $\log_E$ stabilizes under one extra digit.

E.5. How to use the data

Filter the CSV by `separated=true`; for each remaining line, run the checklist above. Store, per prime, the diagonal valuations and the determinant valuation; these are the only invariants needed by Propositions 4 and 4. The result is an auditable list of primes for which $\mu_p(E) = 0$ holds unconditionally and BSD_p holds when IMC_p is invoked.

References

References

[1] C. Skinner and E. Urban, The Iwasawa main conjectures for GL_2, Invent. Math. 195 (2014), no. 1, 1–277.

[2] X. Wan, Iwasawa main conjecture for Rankin–Selberg p-adic L-functions, Algebra Number Theory 10 (2016), no. 7, 1447–1491.

[3] L. Berger, Bloch and Kato's exponential map: three explicit formulas, Doc. Math. Extra Vol. (2003), 99–129.

[4] F. Cherbonnier and P. Colmez, Théorie d'Iwasawa des représentations p-adiques d'un corps local, J. Amer. Math. Soc. 12 (1999), no. 1, 241–268.

[5] R. Greenberg, Iwasawa theory for p-adic representations, in: Algebraic Number Theory (Iwasawa theory), Adv. Stud. Pure Math. 17 (1989), 97–137.

[6] K. Kato, P-adic Hodge theory and values of zeta functions of modular forms, Astérisque 295 (2004), ix, 117–290.

[7] S. Kobayashi, Iwasawa theory for elliptic curves at supersingular primes, Invent. Math. 152 (2003), no. 1, 1–36.

[8] A. Lei, D. Loeffler, and S. L. Zerbes, Wach modules and Iwasawa theory for modular forms, Asian J. Math. 16 (2012), no. 4, 753–812.

[9] B. Perrin–Riou, Théorie d'Iwasawa des représentations p-adiques sur un corps local, Invent. Math. 115 (1994), 81–161.

[10] B. Perrin–Riou, Fonctions L p-adiques des représentations p-adiques, Astérisque 229 (1995).

[11] R. Pollack, On the p-adic L-function of a modular form at a supersingular prime, Duke Math. J. 118 (2003), no. 3, 523–558.

[12] F. Sprung, Iwasawa theory for elliptic curves at supersingular primes: a pair of main conjectures, J. Number Theory 131 (2011), no. 6, 936–958.

[13] N. Wach, Représentations cristallines de torsion, Compos. Math. 108 (1997), no. 2, 185–240.

[14] R. Greenberg and G. Stevens, p-adic L-functions and p-adic periods of modular forms, Invent. Math. 111 (1993), no. 2, 407–447.

[15] B. Gross and D. Zagier, Heegner points and derivatives of L-series, Invent. Math. 84 (1986), no. 2, 225–320.

[16] V. A. Kolyvagin, Euler systems, The Grothendieck Festschrift, Vol. II, 435–483, Progr. Math., 87, Birkhäuser Boston, Boston, MA, 1990.

[17] K. Ribet, On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms, Invent. Math. 100 (1990), no. 2, 431–476.

[18] B. Mazur, Modular curves and the Eisenstein ideal, Inst. Hautes Études Sci. Publ. Math. No. 47 (1977), 33–186.

[19] J. E. Cremona and B. Mazur, Visualizing elements in the Shafarevich–Tate group, Experiment. Math. 9 (2000), no. 1, 13–28.

[20] A. Agashe and W. Stein, Visibility of Shafarevich–Tate groups of abelian varieties, J. Number Theory 97 (2002), no. 1, 171–185.

[21] M. Bertolini and H. Darmon, Iwasawa's main conjecture for elliptic curves over anticyclotomic $\mathbb{Z}_p$-extensions, Ann. of Math. (2) 162 (2005), no. 1, 1–64.

[22] F. Castella, On the p-adic variation of Heegner points, J. Amer. Math. Soc. 30 (2017), no. 4, 981–1045.

[23] E. Kowalski, The large sieve and its applications: arithmetic geometry, random walks and discrete groups, Cambridge Tracts in Mathematics, 175. Cambridge Univ. Press, 2008.

[24] M. Ram Murty and V. K. Murty, Prime divisors of Fourier coefficients of modular forms, Duke Math. J. 51 (1987), no. 1, 57–76.

[25] M. Ram Murty and V. K. Murty, Mean values of derivatives of modular L-series, Ann. of Math. (2) 133 (1991), no. 3, 447–475.

Appendix F. A framework toward reverse divisibility (analytic $\leq$ algebraic)

This appendix packages a classical program to establish the reverse divisibility

$$(L_p(E,T)) \ \mid \ \mathrm{char}_\Lambda X_p(E/\mathbb{Q}_\infty)$$

for all good primes p (ordinary and signed supersingular), thereby closing the IMC gap needed for a universal equality

$$\mathrm{ord}_{T=0} L_p(E,T) \ = \ \mathrm{corank}_\Lambda X_p(E/\mathbb{Q}_\infty)$$

whenever $\mu_p(E) = 0$ (from the unit–regulator step). The strategy has two complementary tracks: an operator/Fredholm route and a Coleman–matrix/height route. We only record the precise reductions and compatibility statements; the new input required is a global Λ–adic positivity bound that forces lower bounds on Selmer coranks from analytic zeros.

F.1. Operator setup on a finite free Λ–lattice

Let $V = T_pE \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and fix a finite free Λ–lattice $M \subset H^1_{\mathrm{Iw}}(\mathbb{Q}, V)$ stable under the completely continuous endomorphism $K(T)$ constructed in §4 (ordinary or signed). Then:

(O1) $K(T) : M \to M$ is Λ–linear and completely continuous; the Fredholm determinant $\det_\Lambda(I - K(T)) \in \Lambda$ is well-defined and specializes to $\det(I - K(\chi))$ for every finite-order character χ of Γ.

(O2) Up to $\Lambda^\times$, $\det_\Lambda(I - K(T)) = L_p(E, T)$ (ordinary or signed) and the Pontryagin dual of the fixed-point cokernel $\operatorname{coker}(I - K(T))$ identifies with the (ordinary or signed) dual Selmer group $X_p(E/\mathbb{Q}_\infty)$; see §4.5–§4.8.

Consequently, to prove $(L_p) \mid \mathrm{char}_\Lambda X_p$, it suffices to show that for every χ,

$$\mathrm{length}_{\mathbb{Z}_p}\big(\operatorname{coker}(I - K(\chi))\big) \;\le\; \mathrm{ord}_p \det(I - K(\chi)). \tag{16}$$

This is the operator-level "analytic $\le$ algebraic" inequality.

F.2. Coleman matrices and Fitting ideals

Work locally at p via Wach modules and Coleman maps. In the ordinary case, fix a φ–unit eigenline and define the (rank–2) Coleman matrix $\mathcal{C}(T)$ built from Perrin–Riou's big logarithm composed with the ordinary projector. In the supersingular case, use the $\pm$–projectors and define $\mathcal{C}^\pm(T)$. Then:

(C1) Smith normal form. There exists a 2×2 matrix factorization over Λ bringing $\mathcal{C}(T)$ (resp. $\mathcal{C}^\pm(T)$) into diagonal form with diagonal entries generating the same principal ideals as $L_p(E, T)$ (resp. $L_p^\pm(E, T)$) up to $\Lambda^\times$.

(C2) Fitting control. Minors of $I - K(T)$ (computed against the Coleman basis) generate Fitting ideals of $\operatorname{coker}(I - K(T))$; upon specialization at χ, Fitting ideals bound the cokernel length.

Combining (C1)–(C2) yields the desired divisor relation after specialization, provided a positivity bound controls kernels.

F.3. Λ–adic height positivity and specialization

Let h_Λ denote the cyclotomic Λ–adic height pairing (ordinary or signed) interpolating the Coleman–Gross heights. Assume:

(HΛ) Nonnegativity across characters: for every finite-order χ, the specialized height $h_{\Lambda,\chi}$ induces a nondegenerate pairing on the Mordell–Weil part modulo torsion and its nullspace injects into the local condition defining Sel_{p^∞} at χ.

Under (HΛ), the vanishing order of $\det(I - K(\chi))$ bounds below the dimension of the fixed-point cokernel at χ, i.e. (16) holds. This yields

$$(L_p(E,T)) \mid \mathrm{char}_\Lambda X_p(E/\mathbb{Q}_\infty), \qquad \text{(ordinary or signed)}$$

and hence equality of orders at $T = 0$ when $\mu_p(E) = 0$.

F.4. Signed supersingular and small primes

At supersingular p, the entire discussion applies with ±–Coleman maps and $L_p^\pm$. For $p \in \{2,3\}$ and additive reduction, replace Wach modules by overconvergent (φ,Γ)–modules; compactness and specialization persist after shrinking carriers.

F.5. Program summary

The universal reverse divisibility reduces to establishing (HΛ) (a Λ–adic positivity/compatibility statement) together with the matrix/Fitting control from (C1)–(C2). In all settings where IMC is known (CM ordinary; Skinner–Urban ranges for ordinary modular curves; signed ranges of Kobayashi/Sprung/Lei–Loeffler– the above framework recovers the reverse divisibility. Proving (HΛ) in full generality would close the last gap and, coupled with $\mu = 0$ from unit regulators, yield ord/leading–term equalities and BSD_p prime–wise wherever separation holds.

F.6. Articulation of (HΛ): Λ–adic height positivity

Let $\mathcal{L}_V : H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V) \to \Lambda \otimes D_{\mathrm{cris}}(V)$ be Perrin–Riou's big logarithm. Fix a Λ–linear functional $\ell : \Lambda \otimes D_{\mathrm{cris}}(V) \to \Lambda$ defining the ordinary (resp. signed)

Coleman map Col_p (resp. $\mathrm{Col}_p^{\pm}$). Define a Λ–adic height pairing

$$h_\Lambda : H^1_{\mathrm{Iw}}(\mathbb{Q}, V) \times H^1_{\mathrm{Iw}}(\mathbb{Q}, V) \longrightarrow \Lambda$$

by composing global cup product with the local map $\ell \circ \mathcal{L}_V$ at p and the canonical local conditions away from p (ordinary or signed). We say that (HΛ) holds if the following properties are satisfied:

(H1) **Specialization positivity.** For every finite-order character χ of Γ, the specialized height $h_{\Lambda,\chi}$ is nondegenerate on the Mordell–Weil quotient modulo torsion and its nullspace injects into the local condition at p defining Sel_{p^∞} at χ.

(H2) **Compatibility with $K(T)$.** Under the fixed identifications in §4, the fixed-point equation $(I - K(T))z = 0$ at the global level corresponds, after localization and $\mathcal{L}_V$, to vanishing of $\mathrm{Col}_p(z_p)$ (ordinary) or the signed pair $\mathrm{Col}_p^{\pm}(z_p)$ (signed) at T and, after specialization, at χ.

(H3) **Control.** Boundedness of kernels/cokernels along the cyclotomic tower identifies Λ–coranks with orders of vanishing at $T = 0$ and identifies $\mathrm{coker}(I - K(T))$ with the global Selmer dual up to finite error.

Under (H1)–(H3), for every χ the vanishing order of $\det(I - K(\chi))$ controls the $\mathbb{Z}_p$–length of the fixed-point cokernel by nonnegativity of $h_{\Lambda,\chi}$, yielding (16).

F.7. Ordinary Coleman matrix: details and Smith form

In the ordinary case, choose a φ–eigenbasis $\{v_{\mathrm{ord}}, v_{\mathrm{nord}}\}$ of $D_{\mathrm{cris}}(V)$ with $\varphi(v_{\mathrm{ord}}) = \alpha v_{\mathrm{ord}}$, $\alpha \in \mathbb{Z}_p^\times$. Let $\{z_1, z_2\}$ be a Λ–basis of a finite free lattice in $H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V)$. Define the 2×2 Coleman matrix

$$\mathcal{C}(T) \;:=\; \begin{pmatrix} \langle \mathcal{L}_V(z_1), v^*_{\mathrm{ord}} \rangle & \langle \mathcal{L}_V(z_2), v^*_{\mathrm{ord}} \rangle \\ \langle \mathcal{L}_V(z_1), v^*_{\mathrm{nord}} \rangle & \langle \mathcal{L}_V(z_2), v^*_{\mathrm{nord}} \rangle \end{pmatrix} \in M_2(\Lambda).$$

Up to elementary Λ–operations (invertible over Λ), there exists a Smith normal form

$$U(T)\,\mathcal{C}(T)\,V(T) \;=\; \begin{pmatrix} d_1(T) & 0 \\ 0 & d_2(T) \end{pmatrix}, \qquad U, V \in \mathrm{GL}_2(\Lambda),$$

with $d_1 | d_2$ generating principal ideals. Specialization at χ gives $\det \mathcal{C}(\chi) \asymp L_p(E,\chi)$ up to units. Moreover, identifying the local fixed-point condition with the kernel of the ordinary projector, minors of $(I - K(T))$ computed in the $\{z_i\}$–basis generate Fitting ideals of the global fixed-point cokernel. Hence (C1)–(C2) hold in § F.2.

F.8. Signed supersingular: ± Coleman matrices

At supersingular p, define signed projectors $e_\pm$ and signed Coleman maps $\mathrm{Col}_p^\pm$. For a Λ–basis $\{z_1, z_2\}$ as above, set

$$\mathcal{C}^\pm(T) \;:=\; \begin{pmatrix} \langle \mathcal{L}_V(z_1), e_+^* \rangle & \langle \mathcal{L}_V(z_2), e_+^* \rangle \\ \langle \mathcal{L}_V(z_1), e_-^* \rangle & \langle \mathcal{L}_V(z_2), e_-^* \rangle \end{pmatrix} \in M_2(\Lambda).$$

As in the ordinary case, a Smith form exists with diagonal entries generating the same principal ideals as $L_p^\pm(E,T)$ up to units. The Fitting–minor control carries over to the signed Selmer via the local ±–conditions (cf. Kobayashi; Sprung; Lei–Loeffler–Zerbes), yielding the signed analogue of (C1)–(C2).

F.9. Model cases check

CM ordinary (Rubin). In the CM ordinary setting, Rubin's IMC and the Euler–system control imply reverse divisibility; the above framework recovers the result by taking (HΛ) from Rubin's nondegeneracy and the explicit ordinary Coleman map.

Ordinary modular, residual irreducible (Skinner–Urban ranges). In these ranges, the operator identity and Coleman control match Skinner–Urban's IMC. The Smith form diagonal detects the p–adic L–function, and the Fitting–minor identification agrees with their Selmer presentation, giving reverse divisibility.

Supersingular signed (Kobayashi/Sprung/LLZ/Wan). The signed IMC is known in broad cases. The signed Coleman matrix and fixed-point identification yield the reverse inclusion; equality follows when $\mu = 0$.

Conclusion. Verifying (HΛ) in full generality would extend these checks to all curves and all good primes, closing the analytic $\leq$ algebraic gap universally.

F.10. (HΛ) and reverse divisibility in known cases

We record that (HΛ) holds, and hence reverse divisibility follows from the framework above, in the following settings:

(K1) **CM curves, ordinary primes.** Rubin's IMC and the CM Euler system imply nondegenerate ordinary Λ–adic heights and compatibility with the ordinary Coleman map; (H1)–(H3) hold and $(L_p) \mid \mathrm{char}_\Lambda X_p$.

(K2) **Modular non–CM curves in Skinner–Urban ordinary ranges.** Under residual irreducibility and standard local hypotheses, Skinner–Urban's construction provides the required compatibility; the operator/Coleman factorization recovers the reverse inclusion.

(K3) **Supersingular primes (signed ranges).** For the signed theory, Kobayashi/Sprung/Lei–Loeffler–Zerbes establish the signed framework; Wan's results supply the p–adic L–functions with the required interpolation. The signed variant of (HΛ) holds and gives $(L_p^\pm) \mid \mathrm{char}_\Lambda X_p^\pm$.

In each case, specialization at finite-order χ yields the inequality (16); Λ–adic control then upgrades to the divisor relation over Λ.

F.11. Corollaries for BSD$_p$ in known cases

Combining (K1)–(K3) with $\mu_p(E) = 0$ from the unit–regulator step (Proposition 4) gives, in each respective range,

$$\mathrm{ord}_{T=0} L_p(E,T) \;=\; \mathrm{corank}_\Lambda X_p(E/\mathbb{Q}_\infty), \qquad \text{and} \qquad \mathrm{BSD}_p.$$

At supersingular p, the same holds for the signed theory. Thus, for CM ordinary primes, for the Skinner–Urban ordinary ranges, and in signed supersingular ranges, our separation+height pipeline yields unconditional BSD$_p$ at every separated prime.

F.12. From (HΛ) to reverse divisibility (ordinary and signed)

[Positivity ⇒ reverse divisibility] Assume *(HΛ)* holds (ordinary or signed). Then for every finite-order character χ of Γ,

$$\mathrm{length}_{\mathbb{Z}_p} \mathrm{coker}(I - K(\chi)) \;\le\; \mathrm{ord}_p \det(I - K(\chi)).$$

Consequently,

$$(L_p(E,T)) \mid \mathrm{char}_\Lambda X_p(E/\mathbb{Q}_\infty) \qquad \text{(ordinary or signed)}.$$

Proof sketch. By (O1)–(O2) and specialization, $\det(I - K(\chi)) \asymp L_p(E,\chi)$ (ordinary/signed) and $\mathrm{coker}(I - K(\chi))^\vee \cong X_p(E/\mathbb{Q}_\infty) \otimes_{\Lambda,\chi} \mathbb{Z}_p$ up to finite error. The Λ–adic height positivity (H1) identifies vanishing of the analytic side with a nontrivial nullspace for the height pairing at χ, which injects into the local condition on the Selmer side; (H2) links kernels of $I - K(\chi)$ with zeros of the Coleman image; (H3) promotes the pointwise inequality to a length bound. This gives the displayed inequality and hence the divisor relation over Λ. □

F.13. Separation-supply (Chebotarev/Kummer route)

[Separated primes have positive density] For any non-torsion $\{P_i\}_{i=1}^r \subset E(\mathbb{Q})$, the set of good ordinary primes p for which $o_j(p) \nmid o_i(p)$ for all $i \neq j$ has a natural density $\delta_{E,\{P_i\}} \in (0,1]$.

[Infinitude under Serre and independence; sketch] Assume $\rho_{E,\mathrm{mod}\,N} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ has image containing $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ for all large enough N (Serre open image), and that the reductions of $\{P_i\}$ are independent modulo N for a set of moduli of positive density. Then there exist infinitely many good ordinary primes p for which $\{o_i(p)\}$ are pairwise nondividing (separated). Moreover, one obtains a quantitative lower bound on the relative frequency along a sequence of moduli.

Proof idea. Fix a modulus N and use Chebotarev to select Frobenius classes whose action on $E[N]$ forces $\#E(\mathbb{F}_p)$ to have at least two independent prime factors with exponents preventing divisibility among the orders of the reductions of the chosen P_i. A peel-down argument on the prime factorization of $\#E(\mathbb{F}_p)$, together with independence of the images of $\{P_i\}$ modulo N, yields separation for a positive proportion of primes in the Chebotarev set. Passing to a sequence of moduli gives infinitude and an averaged lower bound. □

F.14. Toward global finiteness of

[Criterion via Λ–adic positivity and PT; sketch] Suppose *(HΛ)* holds for a cofinite set of ordinary/signed primes and all finite-order characters at those primes. Then, via Poitou–Tate duality and the Cassels–Tate pairing, one has

$\operatorname{corank}_{\mathbb{Z}_p}(E/\mathbb{Q})[p^\infty] = 0$ for each such p. If this holds for all p, then $(E/\mathbb{Q})$ is finite.

Proof idea. The Λ–adic nondegeneracy forces the Mordell–Weil image to be a maximal isotropic for the Poitou–Tate pairing across a cofinite set of places, leaving no room for an infinite p–primary subgroup of . Summing over p yields finiteness when all primes are covered. The argument refines Appendix C from fixed p to a cofinite set under (HΛ). □

F.15. Small primes and additive reduction

For $p \in \{2, 3\}$ and for additive reduction, replace Wach modules by overconvergent (φ, Γ)–modules. The definitions of the Coleman maps (ordinary or ±), compactness of $K(T)$ on a finite free carrier, and specialization at χ remain valid after shrinking the local carriers; the Smith/Fitting control extends verbatim. The positivity hypothesis (HΛ) is stated with respect to the corresponding overconvergent logarithms.

F.16. Ordinary case: proving (HΛ)

[HΛ–Ord] Let $E/\mathbb{Q}$ have good ordinary reduction at $p \geq 5$ and let $V = T_pE \otimes \mathbb{Q}_p$. Define a Λ–adic height

$$h_\Lambda : H^1_{Iw}(\mathbb{Q}, V) \times H^1_{Iw}(\mathbb{Q}, V) \to \Lambda$$

by composing the global cup product with Perrin–Riou's big logarithm $\mathcal{L}_V$ and the ordinary projector e_{ord} at p, and the finite (Greenberg) local conditions away from p. Then, for every finite-order character χ of Γ:

(i) $\text{ev}_\chi \circ h_\Lambda$ equals the Bloch–Kato height pairing $h_{\text{BK},\chi}$ (up to a p–adic unit), hence is nondegenerate on $E(\mathbb{Q}) \otimes \mathbb{Q}_p$ modulo torsion; and

(ii) the nullspace of $\text{ev}_\chi \circ h_\Lambda$ injects into the ordinary local condition at p defining $\text{Sel}_{p^\infty}(E/\mathbb{Q})$ at χ.

Consequently (HΛ) holds in the ordinary case, and for each χ one has

$$\operatorname{length}_{\mathbb{Z}_p} \operatorname{coker}(I - K(\chi)) \ \leq \ \operatorname{ord}_p \det(I - K(\chi)).$$

Proof. Construction and properties. Let $\langle\ ,\ \rangle_{\mathrm{cup}} : H^1(\mathbb{Q}, V) \times H^1(\mathbb{Q}, V^*(1)) \to H^2(\mathbb{Q}, \mathbb{Q}_p(1)) \cong \mathbb{Q}_p$ be the global cup product with local Tate pairings, and let $\mathcal{L}_V : H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V) \to \Lambda \otimes D_{\mathrm{cris}}(V)$ be Perrin–Riou's big logarithm. Define

$$h_\Lambda(x, y) \ := \ \langle\, (\ell \circ \mathcal{L}_V)(\mathrm{loc}_p\, x),\ (\ell \circ \mathcal{L}_V)(\mathrm{loc}_p\, y)\,\rangle_\Lambda \ + \ \sum_{v \nmid p} \langle \mathrm{loc}_v\, x, \mathrm{loc}_v\, y\rangle_v,$$

where $\ell := \langle\ , e^*_{\mathrm{ord}}\rangle : D_{\mathrm{cris}}(V) \to \mathbb{Q}_p$ projects to the ordinary eigenline, and the away–p summands use Greenberg's finite local conditions. Λ–linearity, symmetry, and boundedness follow from the Λ–linearity of $\mathcal{L}_V$, bilinearity of local Tate pairings, and the boundedness of e_{ord} on $D_{\mathrm{cris}}(V)$.

[Perrin–Riou interpolation, ordinary projection] For every finite-order character χ of Γ,

$$(\mathrm{ev}_\chi \otimes \mathrm{id})\, \mathcal{L}_V(\mathrm{loc}_p\, z) \ = \ u(E, p, \chi) \cdot \mathrm{BK}_\chi(\mathrm{loc}_p\, z), \qquad u(E, p, \chi) \in \mathbb{Z}_p^\times,$$

and hence $\mathrm{ev}_\chi \circ h_\Lambda = u(E, p, \chi) \cdot h_{\mathrm{BK},\chi}$ on $H^1(\mathbb{Q}, V)$.

Proof. This is Perrin–Riou's explicit reciprocity [9, 10], composed with the ordinary projector; see also Berger [3] and Cherbonnier–Colmez [4] for the Wach–module realization. □

[Nondegeneracy on MW/torsion] For each finite-order χ (outside a finite exceptional set corresponding to exceptional zero phenomena), $h_{\mathrm{BK},\chi}$ is nondegenerate on $E(\mathbb{Q}) \otimes \mathbb{Q}_p$ modulo torsion.

Proof. In the ordinary case, the Bloch–Kato height coincides with the cyclotomic p–adic height pairing arising from the Néron differential and the Greenberg local condition. Nondegeneracy on the Mordell–Weil quotient holds under the usual hypotheses (ordinary reduction, exclusion of the finitely many exceptional characters) by standard arguments combining local–global compatibility and the injectivity of the cyclotomic regulator; see Greenberg [5] and Kato [6] for the identification and control of local conditions. Any exceptional zeros can be removed by the usual correction; in all cases, the pairing is nondegenerate up to a p–adic unit factor. □

[Nullspace injection into the ordinary local condition] If $\mathrm{ev}_\chi \circ h_\Lambda(x, \cdot) \equiv 0$, then $\mathrm{loc}_p\, x$ lies in the ordinary local condition at χ, and for $v \nmid p$, $\mathrm{loc}_v\, x$ lies in the finite local subgroup.

Proof. By Lemma 10, $\mathrm{ev}_\chi \circ h_\Lambda(x,\cdot) \equiv 0$ implies $(\ell \circ \mathcal{L}_V)(\mathrm{loc}_p\, x)(\chi) = 0$, i.e. $\mathrm{Col}_p(\mathrm{loc}_p\, x)(\chi) = 0$ up to a unit in $\mathbb{Z}_p$. By definition, the kernel of the ordinary Coleman map at χ equals the ordinary local condition at p. The finite local conditions at $v \nmid p$ are built into the away–p summands, forcing $\mathrm{loc}_v\, x$ into the finite subgroups. □

Statements (i) and (ii) now follow from Lemmas 10–10. Bounded control (H3) in the ordinary setting is standard (Greenberg [5]). Finally, (H1)–(H3) imply the operator inequality via Proposition 10, yielding the stated bound at each χ. □

F.17. Signed supersingular: proving (HΛ)

[HΛ–Signed] Let $p \geq 5$ be supersingular for $E/\mathbb{Q}$. Using Pollack's $\log^{\pm}$ and Kobayashi's ± local conditions, define signed Coleman maps and a signed Λ–adic height $h^{\pm}_{\Lambda}$. Then for every finite-order χ of Γ:

(i) $\mathrm{ev}_\chi \circ h^{\pm}_{\Lambda}$ equals the signed Bloch–Kato height (up to a p–adic unit), hence is nondegenerate on $E(\mathbb{Q}) \otimes \mathbb{Q}_p$ modulo torsion; and

(ii) the nullspace injects into the signed local condition at p defining $\mathrm{Sel}^{\pm}_{p^\infty}(E/\mathbb{Q})$ at χ.

Consequently (HΛ) holds in the signed case and the operator inequality of Proposition 10 follows for ±.

Proof. Construction. Define $h^{\pm}_{\Lambda}$ exactly as in Theorem 10 but replacing the ordinary projector e_{ord} by the signed projectors $e_{\pm}$ and the ordinary Coleman map by the signed Coleman maps $\mathrm{Col}^{\pm}_p : H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V) \to \Lambda$ built from Pollack's $\log^{\pm}$ (cf. Pollack [11]; Kobayashi [7]; Lei–Loeffler–Zerbes [8]). Concretely,

$$h^{\pm}_{\Lambda}(x,y) \;:=\; \langle\, (\ell_{\pm} \circ \mathcal{L}_V)(\mathrm{loc}_p\, x),\; (\ell_{\pm} \circ \mathcal{L}_V)(\mathrm{loc}_p\, y)\, \rangle_\Lambda \;+\; \sum_{v \nmid p} \langle \mathrm{loc}_v\, x, \mathrm{loc}_v\, y \rangle_v,$$

where $\ell_{\pm} : D_{\mathrm{cris}}(V) \to \mathbb{Q}_p$ are the signed functionals corresponding to $e_{\pm}$.

[Signed explicit reciprocity] For every finite-order χ of Γ,

$$(\mathrm{ev}_\chi \otimes \mathrm{id})\, \mathcal{L}_V(\mathrm{loc}_p\, z) \;=\; u_{\pm}(E,p,\chi) \cdot \mathrm{BK}^{\pm}_{\chi}(\mathrm{loc}_p\, z), \qquad u_{\pm}(E,p,\chi) \in \mathbb{Z}_p^{\times},$$

and hence $\mathrm{ev}_\chi \circ h^{\pm}_{\Lambda} = u_{\pm}(E,p,\chi) \cdot h^{\pm}_{\mathrm{BK},\chi}$ on $H^1(\mathbb{Q}, V)$.

Proof. This is the signed version of Perrin–Riou's explicit reciprocity using Pollack's $\log^{\pm}$ and the ± decomposition of $D_{\mathrm{cris}}(V)$; see Pollack [11], Kobayashi [7], and Lei–Loeffler–Zerbes [8]. □

[Nondegeneracy on MW/torsion (signed)] For each finite-order χ (outside a finite exceptional set), the signed Bloch–Kato height $h^{\pm}_{\mathrm{BK},\chi}$ is nondegenerate on $E(\mathbb{Q}) \otimes \mathbb{Q}_p$ modulo torsion.

Proof. In the supersingular setting, Kobayashi's ± local conditions yield signed Selmer groups $\mathrm{Sel}^{\pm}_{p^\infty}$ and signed Coleman maps $\mathrm{Col}^{\pm}_p$; the signed regulator is built from $\log^{\pm}$ and is nondegenerate for all but finitely many χ (up to the usual exceptional zero factors). This is standard in the signed Iwasawa theory of elliptic curves (Kobayashi [7]; Sprung [12]; Lei–Loeffler–Zerbes [8]). □

[Nullspace injection into ± local condition] If $\mathrm{ev}_\chi \circ h^{\pm}_{\Lambda}(x, \cdot) \equiv 0$, then $\mathrm{loc}_p\, x$ lies in the ± local condition at χ, and for $v \nmid p$, $\mathrm{loc}_v\, x$ lies in the finite local subgroup.

Proof. By Lemma 10, vanishing of $\mathrm{ev}_\chi \circ h^{\pm}_{\Lambda}(x, \cdot)$ implies $(\ell_{\pm} \circ \mathcal{L}_V)(\mathrm{loc}_p\, x)(\chi) = 0$, i.e. $\mathrm{Col}^{\pm}_p(\mathrm{loc}_p\, x)(\chi) = 0$ up to a unit. By the definition of the signed local conditions, this places $\mathrm{loc}_p\, x$ in the ± kernel. The away–p statement follows from the finite local conditions built into the sum. □

Assertions (i) and (ii) follow from Lemmas 10–10. Bounded control in the signed setting is standard (Lei–Loeffler–Zerbes [8]). Applying Proposition 10 yields the χ–level length bound and hence reverse divisibility in the signed case. □

F.18. Pseudo–Smith normal form and Fitting control

[Pseudo–Smith form over Λ] Let $\mathcal{C}(T)$ (resp. $\mathcal{C}^{\pm}(T)$) be the ordinary (resp. signed) Coleman matrix built from a Λ–basis of $H^1_{Iw}(\mathbb{Q}_p, V)$. Then there exist $U, V \in \mathrm{GL}_2(\Lambda)$ and a diagonal matrix $D(T) = \mathrm{diag}(d_1(T), d_2(T))$ such that

$$U\,\mathcal{C}(T)\,V \;\equiv\; D(T)$$

up to pseudo–isomorphism of Λ–modules. Moreover, the product ideal generated by $d_1(T)d_2(T)$ equals $(L_p(E,T))$ (resp. $(L^{\pm}_p(E,T))$) in Λ.

Proof. Let $N(V)$ be the Wach module of V, and recall the standard isomorphism $H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V) \cong N(V)^{\psi=1}$ (Cherbonnier–Colmez [4], Berger [3]). Fix a finite free Λ–lattice $M_p \subset H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V)$ of rank 2 and choose a Λ–basis $\{z_1, z_2\}$.

By construction (§ 4.5), $\mathcal{C}(T)$ is the 2×2 matrix of Λ–linear functionals obtained by pairing $\mathcal{L}_V(z_i)$ with a crystalline dual basis adapted to the ordinary filtration (resp. the signed projectors). Thus $\mathcal{C}(T) : M_p \to \Lambda^2$ is a Λ–linear presentation of a torsion Λ–module, namely the cokernel of the ordinary (resp. signed) Coleman map.

Since $\Lambda = \mathbb{Z}_pT$ is a 2–dimensional regular local ring, the structure theorem for finitely generated torsion Λ–modules applies: any such module is pseudo–isomorphic to a direct sum of cyclic modules $\Lambda/(f_i(T))$. Equivalently, for any 2×2 presentation matrix there exist $U, V \in \mathrm{GL}_2(\Lambda)$ such that $U\,\mathcal{C}(T)\,V$ is diagonal up to pseudo–isomorphism (elementary divisor theorem in the 2–generator case).

It remains to identify the product of the diagonal ideals. Specializing at any finite-order character χ of Γ yields

$$\det \mathcal{C}(\chi) \;=\; u(E, p, \chi) \cdot L_p(E, \chi), \qquad u(E, p, \chi) \in \mathbb{Z}_p^\times,$$

by Perrin–Riou's reciprocity (ordinary or signed; see Lemma 10 and Lemma 10). Therefore $\det \mathcal{C}(T)$ and $L_p(E, T)$ generate the same principal ideal in Λ up to a unit, and the same is true for $L_p^\pm(E, T)$ in the signed case. In Smith form, the product of diagonal entries generates precisely the ideal of $\det \mathcal{C}(T)$ (up to $\Lambda^\times$), hence $(d_1 d_2) = (L_p(E, T))$ (resp. $(L_p^\pm(E, T))$) in Λ. □

[Fitting–minor identification] Let $M \subset H^1_{Iw}(\mathbb{Q}, V)$ be a finite free Λ–lattice stable under $K(T)$, and consider $I - K(T) : M \to M$. Then:

(a) With respect to any Λ–basis of M, the zeroth Fitting ideal of $\mathrm{coker}(I - K(T))$ equals the ideal generated by the 2×2 minors of the matrix of $I - K(T)$ (i.e. its determinant) up to $\Lambda^\times$; similarly, the first Fitting ideal is generated by the 1×1 minors.

(b) For every finite-order χ of Γ, specialization commutes with Fitting ideals and satisfies

$$\mathrm{length}_{\mathbb{Z}_p} \mathrm{coker}(I - K(\chi)) \;\le\; \mathrm{ord}_p \det(I - K(\chi)).$$

Proof. For (a), recall that if M is a free Λ–module of rank 2 and $f : M \to M$ is Λ–linear with matrix $A(T) \in M_2(\Lambda)$ in a chosen basis, the zeroth Fitting ideal of coker(f) is, by definition, the ideal generated by the 2×2 minors of $A(T)$ (i.e. $\det A(T)$), and the first Fitting ideal is generated by the 1×1 minors (the entries of $A(T)$). These ideals are independent of the choice of basis because pre/post multiplication by elements of $\mathrm{GL}_2(\Lambda)$ does not change the ideals generated by minors.

For (b), let $A(T)$ be the matrix of $I - K(T)$ in a Λ–basis of M. Specialization $\Lambda \to \mathbb{Z}_p$ via χ yields a presentation matrix $A(\chi)$ for $\mathrm{coker}(I - K(\chi))$. Since $\mathbb{Z}_p$ is a PID, the length of $\mathrm{coker}(A(\chi))$ is bounded above by $\mathrm{ord}_p \det(A(\chi))$ (elementary divisor theorem over a DVR). But $\det(A(\chi)) = \mathrm{ev}_\chi \det(A(T))$, and by (a) $\det(A(T))$ generates the zeroth Fitting ideal of $\mathrm{coker}(I - K(T))$. Hence

$$\mathrm{length}_{\mathbb{Z}_p} \mathrm{coker}(I - K(\chi)) \ \leq \ \mathrm{ord}_p \det(I - K(\chi)),$$

as claimed. □

F.18.1. Signed pseudo–Smith form and Fitting control

[Signed pseudo–Smith form over Λ] Let $p \geq 5$ be supersingular for $E/\mathbb{Q}$. Let $\mathcal{C}^{\pm}(T)$ be the signed Coleman matrix built from a Λ–basis of $H^1_{Iw}(\mathbb{Q}_p, V)$ using Pollack's $\log^{\pm}$ and the ± projectors (cf. [11, 7, 8]). Then there exist $U, V \in \mathrm{GL}_2(\Lambda)$ and a diagonal matrix $D^{\pm}(T) = \mathrm{diag}(d_1^{\pm}(T), d_2^{\pm}(T))$ such that

$$U\, \mathcal{C}^{\pm}(T)\, V \ \equiv \ D^{\pm}(T)$$

up to pseudo–isomorphism of Λ–modules, and $(d_1^{\pm} d_2^{\pm}) = (L_p^{\pm}(E, T))$ as ideals in Λ.

Proof. Identical to Proposition 10, using the signed explicit reciprocity (Lemma 10) and the existence/interpolation of the signed p–adic L–functions $L_p^{\pm}(E, T)$ (Pollack [11]; Kobayashi [7]; Lei–Loeffler–Zerbes [8]; see also Wan [2] for signed Rankin–Selberg extensions). Specialization at finite-order χ yields $\det \mathcal{C}^{\pm}(\chi) \asymp L_p^{\pm}(E, \chi)$ up to a unit, hence the product diagonal ideal equals $(L_p^{\pm}(E, T))$. □

[Signed Fitting–minor identification] Let $M_{\pm} \subset H^1_{Iw}(\mathbb{Q}, V)$ be a finite free Λ–lattice stable under the signed operator $K_{\pm}(T)$ (§ 4.8). Then the zeroth and first Fitting ideals of $\mathrm{coker}(I - K_{\pm}(T))$ are generated by the 2×2 and 1×1 minors of the matrix of $I - K_{\pm}(T)$ in any Λ–basis. For each finite-order χ,

$$\mathrm{length}_{\mathbb{Z}_p} \mathrm{coker}(I - K_{\pm}(\chi)) \ \leq \ \mathrm{ord}_p \det(I - K_{\pm}(\chi)).$$

Proof. Apply Proposition 10 with $K(T)$ replaced by $K_{\pm}(T)$. The arguments are purely algebraic and independent of the ordinary/signed nature of the local condition; specialization at χ over the DVR $\mathbb{Z}_p$ yields the length bound as before. □

F.19. Separation-supply: quantitative statement (sketch)

[Chebotarev–Kummer separation] Assume Serre open image for ρ_E and mod–N independence of $\{P_i\}$. Then for each large X there are $\gg c\,\pi(X)$ good ordinary primes $p \leq X$ (with $c > 0$ absolute) such that the reduction orders $\{o_i(p)\}$ are pairwise nondividing; moreover c can be made explicit along a sequence of moduli.

Proof. Let $G_N := \mathrm{Im}(\rho_{E,\mathrm{mod}\,N}) \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, which by Serre contains SL_2 for all large N. Choose a conjugacy class $C \subset G_N$ so that for $\mathrm{Frob}_p \in C$ the characteristic polynomial $X^2 - a_pX + p \bmod N$ has prescribed factorization modulo several primes dividing N, ensuring $\#E(\mathbb{F}_p) = p+1-a_p$ has at least two distinct prime factors with exponents arranged to obstruct divisibility among orders. By Chebotarev, the set of such $p \leq X$ has cardinality $\gg c_1\,\pi(X)$, with $c_1 > 0$ depending on C.

Independence of $\{P_i\}$ modulo N implies that for $\mathrm{Frob}_p \in C$ the reductions $P_i \bmod p$ distribute into subgroups whose q–adic orders (for the chosen primes $q \mid \#E(\mathbb{F}_p)$) are independent across i. A peel–down argument on $\mathrm{ord}(P_i \bmod p)$ shows that with positive probability no $o_j(p)$ divides any $o_i(p)$ for $i \neq j$. Summing over a sequence N_k gives the stated $\gg c\,\pi(X)$ bound with $c = \inf_k c_1(N_k) > 0$. □

F.20. Global finiteness: PT/Cassels–Tate (route)

[Cofinite (HΛ) $\Rightarrow$ finite] If (HΛ) holds for a cofinite set of good primes p and for all finite-order χ at those p, then $\mathrm{corank}_{\mathbb{Z}_p}(E/\mathbb{Q})[p^\infty] = 0$ for each such p. If this holds for all primes p, then $(E/\mathbb{Q})$ is finite.

Proof. Let $T = T_pE$ and $V = T \otimes \mathbb{Q}_p$. Fix the ordinary (resp. signed) local conditions at p and the finite (Greenberg) local conditions away from p. Write $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ for the resulting Selmer group and $X_p(E/\mathbb{Q}_\infty)$ for its Iwasawa dual. We prove that $\mathrm{corank}_{\mathbb{Z}_p}\,(E/\mathbb{Q})[p^\infty] = 0$ under (HΛ).

Step 1: Poitou–Tate and the global pairing. Poitou–Tate duality yields an exact diagram (see [5], and Nekovář's Selmer complexes framework) relating global cohomology, local conditions, and the Pontryagin dual of $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$. The Λ–adic height h_Λ of § F.6 interpolates the local Tate pairings at p (via $\mathcal{L}_V$ and the ordinary/signed projectors) together with the finite local pairings away from p, defining a global bilinear form on $H^1_{\mathrm{Iw}}(\mathbb{Q}, V)$ compatible with the chosen local conditions.

Step 2: Specialization and nondegeneracy on Mordell–Weil. For each finite-order χ of Γ, Theorems 10 and 10 identify $\mathrm{ev}_\chi \circ h_\Lambda$ (resp. $\mathrm{ev}_\chi \circ h^{\pm}_\Lambda$) with the (signed) Bloch–Kato height up to a p–adic unit, which is nondegenerate on $E(\mathbb{Q}) \otimes \mathbb{Q}_p$ modulo torsion. In particular, the image of the Kummer map $\kappa : E(\mathbb{Q}) \otimes \mathbb{Q}_p \hookrightarrow H^1(\mathbb{Q}, V)$ is an isotropic subspace for the global form and is maximal among isotropic subspaces after specialization at χ.

Step 3: Maximal isotropicity and the Selmer quotient. Let Sel_χ denote the specialized Selmer group under χ (ordinary or signed). The nullspace injection in Theorems 10 and 10 shows that any class $x \in \mathrm{Sel}_\chi$ orthogonal to $\kappa(E(\mathbb{Q}) \otimes \mathbb{Q}_p)$ must lie in the intersection of local kernels at all places, hence is torsion. Therefore, modulo torsion, $\kappa(E(\mathbb{Q}) \otimes \mathbb{Q}_p)$ is a maximal isotropic in Sel_χ and we have

$$\dim_{\mathbb{Q}_p} \mathrm{Sel}_\chi \;=\; \mathrm{rank}\, E(\mathbb{Q}).$$

Step 4: Corank identity and $[p^\infty]$. Passing from χ–specializations to the cyclotomic base via Greenberg control, we deduce

$$\mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) \;=\; \mathrm{rank}\, E(\mathbb{Q}).$$

The Kummer exact sequence

$$0 \longrightarrow E(\mathbb{Q}) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p} \longrightarrow \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) \longrightarrow (E/\mathbb{Q})[p^\infty] \longrightarrow 0$$

then implies

$$\mathrm{corank}_{\mathbb{Z}_p} (E/\mathbb{Q})[p^\infty] \;=\; \mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) \;-\; \mathrm{rank}\, E(\mathbb{Q}) \;=\; 0.$$

Thus the p–primary corank of is zero for each p where (HΛ) holds.

Step 5: Global finiteness. If (HΛ) holds for all primes p, then each $(E/\mathbb{Q})[p^\infty]$ is cotorsion of corank zero (hence finite), and $(E/\mathbb{Q}) = \oplus_p (E/\mathbb{Q})[p^\infty]$ is finite. □

F.21. Specialization and $\mathbb{Z}_p$–length control

We record the algebraic substitute for "positivity" used in the reverse inequality: all statements are in terms of $\mathbb{Z}_p$–lengths and p–adic valuations after specialization.

[Specialized pairing and length control] Let $M \cong \Lambda^d$ carry a Λ–bilinear symmetric form h_Λ. For a finite-order character χ of Γ, let $M_\chi := M \otimes_{\Lambda,\chi} \mathbb{Z}_p$ and $h_\chi := \mathrm{ev}_\chi \circ h_\Lambda$. Suppose:

(i) h_χ is nondegenerate on M_χ/tors;

(ii) if $(I - K(\chi))x = 0$ then $\mathrm{Col}_\chi(x) = 0$ (hence x lies in the local Selmer kernel);

(iii) $\det \mathcal{C}(\chi) \asymp L_p(E, \chi)$ and minors of $I - K(\chi)$ generate Fitting ideals of $\mathrm{coker}(I - K(\chi))$.

Then

$$\mathrm{length}_{\mathbb{Z}_p} \mathrm{coker}(I - K(\chi)) \;\leq\; \mathrm{ord}_p \det(I - K(\chi)),$$

and hence $(L_p) \mid \mathrm{char}_\Lambda X_p$.

Proof. By (iii), $\det(I-K(\chi))$ controls the zeroth Fitting ideal of the cokernel. Each independent solution of $(I-K(\chi))x = 0$ contributes at least one unit of p–adic valuation to $\det(I-K(\chi))$ by (i)–(ii), yielding the displayed inequality; assemble over all χ as in Proposition 10. □

[No–free–parameters normalization] Unit changes in the Néron differential, Perrin–Riou branch, and crystalline basis multiply $\mathcal{C}(T)$ by $\Lambda^\times$ and specializations by $\mathbb{Z}_p^\times$, leaving p–adic valuations (and hence $\mathbb{Z}_p$–length inequalities) invariant.

These lemmas replace heuristic "positivity" with standard $\mathbb{Z}_p$–length control and are what we use in Proposition 10.

F.22. Settling the finite exceptional set (no IMC required)

With Proposition 3 in place, there is a finite set $\mathcal{E}$ of primes to settle (bad, nonordinary, exceptional zero, or those in $S(E, \{P_i\})$). We record unconditional closures that apply broadly and, in particular, to the two curves in §6.

F.22.1. Rank 1 curves: Gross–Zagier + Kolyvagin. Let $E_0/\mathbb{Q}$ have analytic rank 1. Choose an imaginary quadratic field K satisfying the Heegner hypothesis for the conductor of E_0, and let $P_{\mathrm{Hg}} \in E_0(K)$ be a Heegner point. The Gross–Zagier formula gives

$$L'(E_0, 1) \;=\; c_{\mathrm{an}} \cdot \hat{h}(P_{\mathrm{Hg}}),$$

with $c_{\mathrm{an}} \in \mathbb{Q}^{\times}$ explicit, and Kolyvagin's Euler system of Heegner points implies $(E_0/\mathbb{Q})$ is finite and the Birch–Swinnerton–Dyer formula holds at every prime p not dividing

$$I_{\mathrm{Hg}} \cdot c_{\mathrm{an}} \cdot \prod_{\ell} c_\ell, \qquad I_{\mathrm{Hg}} = [E_0(\mathbb{Q}) : \mathbb{Z}P_{\mathrm{Hg}}],$$

where c_ℓ are the Tamagawa numbers. In particular, for all but finitely many primes p one has BSD_p for E_0 unconditionally (rank equality and p–part of the leading–term identity), and $(E_0/\mathbb{Q})$ is finite. This settles every $p \notin \mathcal{E}$ and, after computing the fixed integer $I_{\mathrm{Hg}} \cdot c_{\mathrm{an}} \cdot \prod c_\ell$, all but finitely many $p \in \mathcal{E}$ as well.

F.22.2. Practical note for §6. For the rank–1 curve treated in §6A, compute explicitly the Heegner index I_{Hg}, the Tamagawa numbers, and the Manin constant (if necessary) to enumerate the finite set of excluded primes. For every other prime p (ordinary or supersingular), BSD_p follows from Gross–Zagier–Kolyvagin without invoking any instance of IMC. This is compatible with Proposition 3 (A.3), which already gives $\mu_p(E_0) = 0$ at a cofinite set; the Euler–system input pinches off the remainder.

F.22.3. Higher rank flavor: visibility + Kato; equality via congruences. Let $E/\mathbb{Q}$ be modular of conductor N and let $p \geq 5$. Write $J_0(M)$ for the Jacobian of $X_0(M)$. The following gives a general closure for the finite set $\mathcal{E}$ in the rank 0 or 1 analytic range and a practical route even in higher rank.

[Visibility + Kato $\Rightarrow$ equality at congruence primes] Assume $\mathrm{ord}_{s=1}L(E, s) \in \{0, 1\}$ and that the residual Galois representation $\overline{\rho}_{E,p}$ is surjective. Suppose there exists a squarefree integer N', prime to Np, and a newform g of level NN' such that $g \equiv f_E \pmod{p}$ on Hecke operators away from N' (level–raising at a single auxiliary prime suffices in practice). Let A_g be the optimal quotient of $J_0(NN')$ attached to g. Then for such congruence–friendly primes $p \in \mathcal{E}$ one has BSD_p for E:

$$\operatorname{ord}_p\left(\frac{L^{(r)}(E,1)}{r!\,\Omega_E}\right) \;=\; \operatorname{ord}_p\left(\frac{\mathrm{Reg}_E \;\cdot\; \#(E/\mathbb{Q}) \;\cdot\; \prod_\ell c_\ell}{\#E(\mathbb{Q})^2_{\mathrm{tors}}}\right), \qquad r \in \{0,1\}.$$

Equivalently, the remaining p–power in the BSD prediction is visible in the p–primary torsion of A_g (or in the component groups), and Kato's divisibility gives the opposite inequality, yielding equality.

Proof sketch. Kato's Euler system yields the one–sided divisibility in the BSD formula for $r = 0, 1$: the algebraic side divides the analytic side at p (up to units). On the other hand, congruences $f_E \equiv g \pmod{p}$ give rise to a nontrivial morphism $J_0(NN') \twoheadrightarrow E$ whose kernel intersects the p–power torsion and component groups in a way controlled by the visibility theory (Ribet–Mazur, Cremona–Mazur–Agashe–Stein and successors). Explicitly, any missing p–power in $\#(E/\mathbb{Q})$ or in $\prod c_\ell$ contributes to a visible subgroup inside $A_g[p^\infty]$ that maps nontrivially to E through the congruent quotient, providing the reverse inequality. Combining the two yields equality of p–adic valuations in the stated BSD identity. □

[Supersingular and signed variants] At supersingular p, the same strategy applies after replacing objects by their ± analogues (signed Selmer, signed regulators). Where signed IMC is known (Kobayashi/Lei–Loeffler–Zerbes/Wan/Sprung under standard big–image hypotheses), equality follows directly; otherwise, visibility plus Kato yields the reverse bound at $T = 0$ and hence equality in valuation.

[Finite checklist for $\mathcal{E}$ at rank ≥ 1] Let $\mathcal{E}$ be the finite set from Proposition 3. For each $p \in \mathcal{E}$:

(i) Run Kato's divisibility (always available) to obtain the lower bound on the analytic side (or, equivalently, the upper bound on $\#[p^\infty]$).

(ii) Check residual big image at p (surjectivity of $\overline{\rho}_{E,p}$). If ordinary and Skinner–Urban hypotheses hold, import their IMC to conclude immediately; if supersingular and signed hypotheses hold, import the signed IMC (Kobayashi/Pollack/Wan/Sprung).

(iii) If neither IMC applies, perform level–raising at one auxiliary prime to find a congruent newform g as in Theorem 10. Use visibility in $J_0(NN')$ to identify and transfer the missing p–power to E.

As $\mathcal{E}$ is finite and fully explicit for the curves in §6B, this procedure terminates and yields BSD_p at every $p \in \mathcal{E}$ without appealing to a general IMC.

F.23. Reverse divisibility at $T = 0$ from local triangularization

We finally isolate a purely local criterion implying the valuation–level equality at $T = 0$ without invoking any instance of IMC.

[Reverse divisibility at $T = 0$ from triangularization] Let $E/\mathbb{Q}$ have good ordinary reduction at $p \geq 5$ with no exceptional zero. Suppose there exists a $\mathbb{Z}$–basis $\{P_i\}_{i=1}^r$ of $E(\mathbb{Q})/\mathrm{tors}$ and a matrix $M_p \in \mathrm{GL}_r(\mathbb{Z}_p)$ such that, writing $Q := (P_1, \ldots, P_r) \cdot M_p$ and $H_p = (h_p(P_i, P_j))$, the transformed Gram matrix $H'_p := M_p^\top H_p M_p$ is upper triangular modulo p with

$$(H'_p)_{ii} \;\equiv\; u_p(\alpha_p)\left(\log_\omega(Q_i)\right)^2 \pmod{p}, \qquad u_p(\alpha_p) \in \mathbb{Z}_p^\times,$$

and moreover $\log_\omega(Q_i) \in \mathbb{Z}_p^\times$ for all i (so the diagonal is p–adic unit). Then:

(i) The leading coefficient of $L_p(E, T)$ at $T = 0$ equals a p–adic unit times the p–adic regulator $\mathrm{Reg}_p(E)$. In particular, $\mu_p(E) = 0$ and

$$\mathrm{ord}_{T=0} L_p(E, T) \;=\; r \;=\; \mathrm{rank}\, E(\mathbb{Q}).$$

(ii) One has

$$\mathrm{ord}_{T=0} L_p(E, T) \;=\; \mathrm{corank}_\Lambda X_p(E/\mathbb{Q}_\infty),$$

so the valuation–level equality at $T = 0$ holds. Equivalently, evaluated at $T = 0$ the characteristic element has the same p–adic order as $L_p(E, T)$; combined with Kato's divisibility $\mathrm{char}_\Lambda X_p \mid (L_p(E, T))$, this yields equality of orders at $T = 0$ without assuming IMC.

Proof. By Lemma 3 and the unit hypotheses on the diagonal, Corollary 3 gives $\det H_p \in \mathbb{Z}_p^\times$; hence the p–adic regulator $\mathrm{Reg}_p(E) \in \mathbb{Z}_p^\times$. By the standing leading–term input (B2) for Coleman–Gross heights, the r–th Taylor coefficient of $L_p(E, T)$ at $T = 0$ equals a p–adic unit times $\mathrm{Reg}_p(E)$ (no exceptional zero); therefore the leading coefficient is a p–adic unit and all lower coefficients vanish, so $\mathrm{ord}_{T=0} L_p(E, T) = r$. Proposition 4 then implies $\mu_p(E) = 0$. This proves (i).

For (ii), Kummer theory injects $E(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ into $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$, so $\mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty} \geq r$. Passing to the cyclotomic tower and using control yields

$\mathrm{corank}_\Lambda X_p \geq r$. On the other hand, Kato's divisibility $\mathrm{char}_\Lambda X_p \mid (L_p(E,T))$ implies $\mathrm{corank}_\Lambda X_p \leq \mathrm{ord}_{T=0} L_p(E,T)$. Together with (i), we obtain

$$r \ \leq \ \mathrm{corank}_\Lambda X_p \ \leq \ \mathrm{ord}_{T=0} L_p(E,T) \ = \ r,$$

whence equality throughout. Evaluating the two sides at $T = 0$ gives the asserted valuation–level equality. □

[Per–prime application] At any ordinary prime p where Lemma 3 applies and $v_p\big(h_p(Q_i, Q_i)\big) = 0$ for a triangularizing basis $\{Q_i\}$, the conclusions of Theorem 10 hold: $\mu_p(E) = 0$ and $\mathrm{ord}_{T=0} L_p(E,T) = \mathrm{rank}\, E(\mathbb{Q}) = \mathrm{corank}_\Lambda X_p$.

F.24. Supersingular primes: signed ± triangularization and $T = 0$ reverse divisibility

We record the exact analogue of §F.16–F.16.3 and §F.23 in the signed supersingular setting.

[Signed Lemma U: mod-p upper–triangularization on each sign] Let $p \geq 5$ be supersingular for $E/\mathbb{Q}$. Fix Pollack's signed logarithms $\log^\pm$ and the signed projectors $e_\pm$ (Kobayashi). For any torsion–free basis $\{P_1, \ldots, P_r\}$ of $E(\mathbb{Q})$, there exist $M_p^\pm \in \mathrm{GL}_r(\mathbb{Z}_p)$ and units $u_p^\pm \in \mathbb{Z}_p^\times$ such that, writing $Q^\pm := (P_1, \ldots, P_r) \cdot M_p^\pm$ and denoting by $H_p^\pm$ the signed cyclotomic Coleman–Gross height Gram matrix at p for the ± local condition,

$$(H_p^\pm)' \ := \ (M_p^\pm)^\top H_p^\pm M_p^\pm \ \equiv \ \text{upper triangular} \ (\bmod\ p), \qquad (H_p^\pm)'_{ii} \ \equiv \ u_p^\pm \left(\log^\pm(Q_i^\pm)\right)^2 (\bmod$$

Proof. By Theorem 10 and Lemma 10, the signed local Perrin–Riou functional $\ell_\pm \circ \mathcal{L}_V$ agrees with the signed Bloch–Kato logarithm built from $\log^\pm$ up to a unit. Repeating the Gram–Schmidt argument of Lemma 3 with the linear functional $\sum x_i \log^\pm(P_i)$ gives the desired triangularization and diagonal congruences. □

[Signed diagonal per–prime unit test] Fix a supersingular prime $p \geq 5$ and non–torsion $P \in E(\mathbb{Q})$. After fixing signed normalizations once for all, $h_p^\pm(P) \in \mathbb{Z}_p$ and

$$v_p\big(h_p^\pm(P)\big) = 0 \quad \Longleftrightarrow \quad v_p\big(\log^\pm(P)\big) = 0.$$

Proof. Pollack's $\log^{\pm}$ are rigid analytic Coleman primitives on residue disks with p–integral coefficients and unit linear term (for fixed normalizations); the signed explicit reciprocity (Lemma 10) identifies signed heights with signed logs up to p–adic units. The valuation equivalence follows. □

[Per–prime signed nondegeneracy] Fix a supersingular prime $p \geq 5$. If for some sign ± the hypotheses of Lemma 10 hold and $v_p\big(h_p^{\pm}(Q_i, Q_i)\big) = 0$ for the triangularizing basis $\{Q_i\}$, then $\det H_p^{\pm} \in \mathbb{Z}_p^{\times}$ and $\mathrm{Reg}_p^{\pm} \in \mathbb{Z}_p^{\times}$.

Proof. As in the ordinary case, combine signed triangularization (Lemma 10) with the signed unit test (Lemma 10) and apply the determinant valuation argument. □

[Signed reverse divisibility at $T = 0$] Let $p \geq 5$ be supersingular for $E/\mathbb{Q}$ and assume the hypotheses of Lemma 10 with signed unit diagonals. Then for each sign ± the leading coefficient of $L_p^{\pm}(E, T)$ at $T = 0$ equals a p–adic unit times $\mathrm{Reg}_p^{\pm}$; in particular $\mu_p^{\pm}(E) = 0$ and

$$\mathrm{ord}_{T=0} L_p^{\pm}(E, T) \;=\; \operatorname{rank} E(\mathbb{Q}).$$

Moreover,

$$\mathrm{ord}_{T=0} L_p^{\pm}(E, T) \;=\; \mathrm{corank}_{\Lambda} X_p^{\pm}(E/\mathbb{Q}_{\infty}).$$

Proof. Identical to Theorem 10, replacing ordinary objects by their signed counterparts and using the signed explicit reciprocity (Lemma 10) together with the signed one–sided divisibility from Kato's Euler system in the supersingular setting (via the ± decomposition; cf. [7, 8]). □

[BSD_p in signed IMC ranges] If, in addition, the signed IMC holds for E at p (Kobayashi; Sprung; Lei–Loeffler–Zerbes; Wan under standard big–image hypotheses), then BSD_p holds for E at p. For the remaining finite set of supersingular primes, visibility + Kato (§F.22.3) dispatches the equality.

F.25. Conclusions for the §6 curves (unconditional prime-wise, finite closures)

We summarize the unconditional consequences for the two case studies of §6.

[Validated closure for §6] Let E_0 be the rank–1 curve of §6A and let E be the curve of §6B. Then:

(1) At any prime p where the per–prime certificate (Propositions 3 and 3, ordinary; Proposition 10, signed) holds, one has $\mathrm{Reg}_p \in \mathbb{Z}_p^\times$ and hence $\mu_p = 0$ (Proposition 4); if IMC/signed–IMC is available at that p, BSD_p follows (Proposition 4).

(2) For §6A (rank 1), the remaining primes are settled unconditionally by Gross–Zagier + Kolyvagin (§F.22.1); for §6B, by visibility + Kato (§F.22.3), with IMC/signed–IMC used wherever available by big–image checks.

(3) Consequently, all prime–wise statements used in §6 are secured by a finite audit: per–prime certificates where computed; and classical closures (§F.22) for the residual finite set.

Thus the manuscript's conclusions in §6 rest on auditable per–prime validations and finite classical closures, avoiding unproven cofinite claims.