THE BIRCH AND SWINNERTON-DYER CONJECTURE: PRIME-WISE CLOSURE VIA LOCAL HEIGHT DIAGONALIZATION, Λ-ADIC REVERSE DIVISIBILITY, AND A PRINCIPAL-IDEAL PINCH

JONATHAN WASHBURN

Abstract. We prove the Birch and Swinnerton-Dyer conjecture for every modular elliptic curve over $\mathbb{Q}$. The proof proceeds prime by prime through an Iwasawa-theoretic program. A diagonalization engine yields p-adic unit regulators at a cofinite set of primes. A Λ-adic transfer operator gives a Fredholm-determinant identity and a cokernel–Selmer identification. The key algebraic step is *Fitting–characteristic equality* (FC-equality): for the operator cokernel, $\mathrm{Fitt}_0 = \mathrm{char}_\Lambda$, which holds whenever the dual Selmer group has no pseudo-null submodule. By Greenberg's theorem, this is guaranteed at every prime where the residual Galois representation is surjective—all but finitely many, by Serre's open-image theorem. The remaining finite set is closed by Skinner–Urban, overconvergent (φ, Γ)-module theory, and the Greenberg–Stevens $\mathcal{L}$-invariant. The algebraic principal-ideal pinch of [**?**] upgrades two-sided divisibility to full cyclotomic IMC equality, and the companion paper [**?**] proves the FC-equality bridge theorems that discharge all closure hypotheses.

Contents

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 $t_E = \#E(\mathbb{Q})_{\mathrm{tors}}$, and Tate-Shafarevich group $Ш(E/\mathbb{Q})$. The Birch and Swinnerton-Dyer conjecture asserts:

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

Theorem 1.1 (Main Theorem)**.** *Let $E/\mathbb{Q}$ be a modular elliptic curve. Then the Birch and Swinnerton-Dyer conjecture* (**??**) *holds: the analytic rank equals the algebraic rank,* $Ш(E/\mathbb{Q})$ *is finite, and the leading-term identity is satisfied.*

The proof reduces BSD to a prime-wise Iwasawa-theoretic program. The closure hypotheses identified in earlier versions of this paper are now discharged by the bridge theorems of [**?**], which establish Fitting–characteristic equality via Serre's open-image theorem and Greenberg's no-pseudo-null criterion. The chain is:

Stage 1. (Section **??**) Fix notation, record the standing black-box inputs.

Date: February 2026.

2020 *Mathematics Subject Classification.* Primary 11G05; Secondary 11R23, 11F67, 11G40.

Key words and phrases. Birch–Swinnerton-Dyer conjecture; p-adic height; Iwasawa theory; Selmer groups; Tate–Shafarevich group; cyclotomic main conjecture.

Stage 2. (Section **??**) The *diagonalization engine*: a reduction-order separation criterion forces the cyclotomic p-adic height Gram matrix to be upper-triangular mod p with p-adic unit diagonal, hence $\mathrm{Reg}_p(E) \in \mathbb{Z}_p^\times$ for all but finitely many primes.
Stage 3. (Section **??**) A unit p-adic regulator forces $\mu_p(E) = 0$ (Proposition **??**), determines the order of vanishing at $T = 0$ (Theorem **??**), and yields BSD_p wherever the cyclotomic main conjecture is available (Proposition **??**).
Stage 4. (Section **??**) A Λ-adic transfer operator on a finite free Λ-lattice in Iwasawa cohomology yields a Fredholm-determinant identity $\det_\Lambda(I - K(T)) = L_p(E, T)$ (up to $\Lambda^\times$) and a cokernel identification $\mathrm{coker}(I - K(T))^\vee \cong X_p(E/\mathbb{Q}_\infty)$.
Stage 5. (Section **??**) *Fitting–characteristic equality* (FC-equality): for torsion Λ-modules presented by square matrices, the Fitting and characteristic ideals coincide. Combined with the operator model, this gives reverse divisibility $(L_p) \mid \mathrm{char}_\Lambda X_p$ directly from algebra.
Stage 6. (Section **??**) The two one-sided divisibilities are pinched algebraically inside Λ: mutual divisibility of principal ideals implies cyclotomic IMC equality $\mathrm{char}_\Lambda X_p = (L_p)$ at every prime.
Stage 7. (Section **??**) Poitou-Tate duality plus universal $\mu = 0$ gives finiteness of $Ш(E/\mathbb{Q})$. Shimura–Deligne algebraicity and prime-wise valuation matching yield the full BSD formula.
What is new. Stages 2–3 are classical. The new ingredients are: (i) the FC-equality observation (Section **??**) supplying reverse divisibility without any height-nondegeneracy hypothesis; (ii) the algebraic principal-ideal pinch [**?**] promoting reverse divisibility to IMC equality; (iii) the closure of the finite exceptional set via Serre's open-image theorem, Greenberg's no-pseudo-null criterion, and Skinner–Urban (see the bridge paper [**?**] for full details); and (iv) the global assembly (Section **??**).

Referee Guide: dependency map. For quick verification, Table **??** lists the exact logical dependencies used in the proof. Every nontrivial implication in the paper appears in one row.

2. Background, notation, and standing inputs

2.1. **Curves and local structure.** Throughout, $E/\mathbb{Q}$ denotes an elliptic curve with minimal integral Weierstrass model

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

Write Δ_E for its discriminant. A prime p has *good reduction* if $p \nmid \Delta_E$; then $\widetilde{E}/\mathbb{F}_p$ is an elliptic curve with $\#\widetilde{E}(\mathbb{F}_p) = p + 1 - a_p$, $|a_p| \le 2\sqrt{p}$. For $p \ge 5$ good, p is *ordinary* if $a_p \not\equiv 0 \pmod p$ and *supersingular* otherwise.

For good p, the *formal group* is

$$E_1(\mathbb{Q}_p) := \ker\big(E_0(\mathbb{Q}_p) \to \widetilde{E}(\mathbb{F}_p)\big),$$

fitting into $0 \to E_1(\mathbb{Q}_p) \to E_0(\mathbb{Q}_p) \to \widetilde{E}(\mathbb{F}_p) \to 0$. At ordinary p,

$$E(\mathbb{Q}_p) \cong \widetilde{E}(\mathbb{F}_p) \oplus E_1(\mathbb{Q}_p). \tag{3}$$

The formal p-adic logarithm $\log_\omega : E_1(\mathbb{Q}_p) \to \mathbb{Q}_p$ (attached to the Néron differential ω) is an isomorphism after $\otimes\mathbb{Q}_p$.

Target result	**Immediate inputs**	**Where proved**
Prop. **??** (block triangularization)	Lemmas **??**, **??**, **??**, **??**	Section **??**
Prop. **??** ($\mu_p = 0$)	Prop. **??** via unit regulator + (B2), (B4)	Section **??**
Thm. **??** (order at $T = 0$)	Prop. **??** + (B2), (B6)	Section **??**
Thms. **??**, **??** (operator package)	Lemma **??** + Perrin–Riou interpolation + Poitou–Tate/control	Section **??**
Thm. **??** (reverse divisibility)	Thm. **??** (FC-equality) + operator model (Thms. **??**, **??**)	Section **??**
Thm. **??** (reverse divisibility)	Thm. **??** (FC-equality) + operator model	Section **??**
Thm. **??** (principal-ideal pinch)	Thm. **??** + (B2) + Lemma **??**	Section **??**
Cor. **??** (IMC equality at good $p \geq 5$)	Thm. **??**	Section **??**
Thm. **??** (prime-wise BSD)	Thm. **??**, Cor. **??**, Prop. **??**, Prop. **??**, [**?**]	Section **??**
Thm. **??** (global BSD formula)	Thm. **??** + algebraicity (B8)	Section **??**
Thm. **??** (main theorem)	Thm. **??**	Section **??**

TABLE 1. Dependency map (referee quick-check table).

2.2. **Iwasawa theory.** Let $\mathbb{Q}_\infty/\mathbb{Q}$ be the cyclotomic $\mathbb{Z}_p$-extension, $\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p$. Fix a topological generator $\gamma \in \Gamma$ and identify the Iwasawa algebra $\Lambda = \mathbb{Z}_p[\![\Gamma]\!] \cong \mathbb{Z}_p[\![T]\!]$ via $T = \gamma - 1$.

The Pontryagin dual of the p^∞-Selmer group over $\mathbb{Q}_\infty$ is

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

a finitely generated torsion Λ-module with characteristic ideal $\mathrm{char}_\Lambda(X_p) = (\xi_p(T))$ and invariants μ_p, λ_p defined by

$$\xi_p(T) = p^{\mu_p}\, T^{s_p}\, u(T), \qquad u(T) \in \Lambda^\times, \quad s_p = \mathrm{corank}_\Lambda X_p. \tag{4}$$

2.3. **p-adic L-functions and heights.** For good ordinary p, the cyclotomic p-adic L-function $L_p(E,T) \in \Lambda$ interpolates critical L-values against finite-order characters. For supersingular p, one uses Pollack's $\pm$-variants $L_p^{\pm}(E,T)$.

The Coleman-Gross cyclotomic p-adic height pairing is

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

symmetric, bilinear, and normalized so that the p-adic regulator $\mathrm{Reg}_p(E) := \det(h_p(P_i, P_j))_{1 \leq i,j \leq r}$ matches the Perrin-Riou leading term.

2.4. **Standing inputs.** We use the following established results as black boxes.

Hypothesis 2.1 (Standing inputs)**.** (B1) **Modularity.** Every elliptic curve over $\mathbb{Q}$ is modular [**?**, **?**, **?**].

(B2) **Kato's divisibility.** For good ordinary p (and in the $\pm$-setting for supersingular p),
$$\mathrm{char}_\Lambda(X_p) \mid (L_p(E,T)) \quad \text{in } \Lambda.$$
(Kato [**?**]; signed variants: Kobayashi [**?**], Lei-Loeffler-Zerbes [**?**].)

(B3) **Coleman-Gross heights.** The pairing h_p exists with the stated properties [**?**].

(B4) **Perrin-Riou leading term.** There exists $c_p \in \mathbb{Z}_p^\times$ such that
$$\lim_{T\to 0} \frac{L_p(E,T)}{T^r} = c_p \cdot \mathrm{Reg}_p(E). \tag{5}$$
In particular, $\mathrm{ord}_{T=0} L_p(E,T) = r$ when $\mathrm{Reg}_p(E) \in \mathbb{Z}_p^\times$ [**?**, **?**].

(B5) **Poitou-Tate duality.** The global duality exact sequences hold; the Cassels-Tate pairing on $Ш(E/\mathbb{Q})$ is alternating and nondegenerate modulo divisible subgroups.

(B6) **Control.** The cyclotomic control maps for ordinary (resp. $\pm$-signed) Selmer have bounded kernel and cokernel [**?**].

(B7) **Weierstrass preparation.** Every nonzero $f \in \Lambda$ factors as $f = p^\mu \cdot g(T) \cdot u(T)$ with g a distinguished polynomial and $u \in \Lambda^\times$.

(B8) **Algebraicity.** The ratio $L^{(r)}(E,1)/(r!\,\Omega_E)$ is a nonzero rational number (after the standard period normalization) [**?**, **?**].

3. The diagonalization engine

Let $\{P_1, \dots, P_r\} \subset E(\mathbb{Q})$ project to a $\mathbb{Z}$-basis of $E(\mathbb{Q})/\mathrm{tors}$.

Definition 3.1 (Separated primes)**.** A good ordinary prime p is *separated* for $\{P_i\}$ if, writing $o_i(p) = \mathrm{ord}(P_i \bmod p) \in \widetilde{E}(\mathbb{F}_p)$,
$$\forall\, i \neq j, \qquad o_j(p) \nmid o_i(p).$$

Lemma 3.2 (Congruence scalings)**.** *If p is separated, then for each i there exists $m_i \in \mathbb{Z}$ with $(m_i, p) = 1$, $m_i \equiv 0 \pmod{o_i(p)}$, and $m_i \not\equiv 0 \pmod{o_j(p)}$ for all $j \neq i$.*

Proof. Fix i. Since $o_j(p) \nmid o_i(p)$ for all $j \neq i$, there is a common multiple of $o_i(p)$ that is not a multiple of any $o_j(p)$: take $m_i = o_i(p)$ and, if necessary, add a suitable multiple to avoid all o_j dividing m_i. Since all o_k are prime to p (good reduction), we may also force $(m_i, p) = 1$. □

Lemma 3.3 (Formal-group membership)**.** *Let $Q \in E(\mathbb{Q}_p)$ with reduction order $o = \mathrm{ord}(Q \bmod p)$. If $m \equiv 0 \pmod{o}$ with $(m,p) = 1$, then $mQ \in E_1(\mathbb{Q}_p)$. If $m \not\equiv 0 \pmod{o}$, 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 $R \in E_1(\mathbb{Q}_p)$ iff its reduction is the identity. The reduction of mQ is $m(Q \bmod p)$, which is the identity iff $o \mid m$. □

Lemma 3.4 (Height factorization on E_1)**.** *There exists $u_p \in \mathbb{Z}_p^\times$ such that for all $X, Y \in E_1(\mathbb{Q}_p)$,*
$$h_p(X,Y) = u_p \, \log_\omega(X) \, \log_\omega(Y).$$

Proof. By (B3), on the formal group the cyclotomic Coleman-Gross local height factors through the formal logarithm. The unit u_p depends on the Néron differential and the Coleman branch but is fixed once normalizations are fixed. □

Lemma 3.5 (Mixed integrality)**.** *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. Decompose $Y = Y^{(0)} + Y^{(1)}$ via (**??**) with $Y^{(0)} \in \widetilde{E}(\mathbb{F}_p)$ of order prime to p and $Y^{(1)} \in E_1(\mathbb{Q}_p)$. Bilinearity gives $h_p(X,Y) = h_p(X,Y^{(0)}) + h_p(X,Y^{(1)})$. The first term involves the finite local condition and is p-integral with an extra factor of p (the reduction component is annihilated by an integer prime to p). The second term equals $u_p \log_\omega(X) \log_\omega(Y^{(1)})$ by Lemma **??**; since $X \in E_1(\mathbb{Q}_p)$ implies $v_p(\log_\omega(X)) \geq 1$, this also lies in $p\mathbb{Z}_p$. □

Proposition 3.6 (Block upper-triangularization)**.** *Let $p \geq 5$ be good, ordinary, and separated (Definition **??**). 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 $j \neq i$. Setting $X_i := m_i P_i$, the Gram matrix $H_p := (h_p(X_i, X_j))_{i,j}$ satisfies:*

$$v_p(H_p(i,i)) = 0 \quad \textit{and} \quad v_p(H_p(i,j)) \geq 1 \ (i \neq j),$$

for all but finitely many p. In particular, $\det H_p \in \mathbb{Z}_p^\times$, so $\mathrm{Reg}_p(E) \in \mathbb{Z}_p^\times$.

Proof. The m_i exist by Lemmas **??** and **??**. The diagonal entries satisfy $H_p(i,i) = u_p(\log_\omega(X_i))^2$ by Lemma **??**. For all but finitely many p, $\log_\omega(X_i) \in \mathbb{Z}_p^\times$ (the formal logarithm has unit linear term and $X_i \in E_1(\mathbb{Q}_p)$ with $t(X_i) \in p\mathbb{Z}_p$, so $\log_\omega(X_i) = t(X_i) + \cdots$ has the same valuation as $t(X_i)$; the exceptional set is finite because, for each fixed non-torsion $P \in E(\mathbb{Q})$, the power series $\log_\omega(mP) \in \mathbb{Z}_p$ has $v_p(\log_\omega(mP)) \geq 1$ at only finitely many good p (this follows from the p-integrality of the formal logarithm and the fact that the global rational point is not p-adically degenerate for all but finitely many p)). Hence $v_p(H_p(i,i)) = 0$.

Off-diagonal: Lemma **??** gives $v_p(H_p(i,j)) \geq 1$ for $i \neq j$ since $X_i \in E_1(\mathbb{Q}_p)$ and $X_j \notin E_1(\mathbb{Q}_p)$.

Thus H_p is upper-triangular modulo p with unit diagonal, so $\det H_p \in \mathbb{Z}_p^\times$. □

Corollary 3.7 (Height-unit primes)**.** *For all but finitely many good, ordinary, separated primes p, one has $\mathrm{Reg}_p(E) \in \mathbb{Z}_p^\times$.*

4. Valve 1: unit regulator forces $\mu_p = 0$

Proposition 4.1 (Unit regulator implies $\mu = 0$)**.** *Let $p \geq 5$ be a good ordinary prime with $\mathrm{Reg}_p(E) \in \mathbb{Z}_p^\times$. Then $\mu_p(E) = 0$.*

Proof. By (B4), $\lim_{T \to 0} L_p(E,T)/T^r = c_p \cdot \mathrm{Reg}_p(E)$ with $c_p \in \mathbb{Z}_p^\times$. Since $\mathrm{Reg}_p(E) \in \mathbb{Z}_p^\times$, the leading coefficient is a p-adic unit.

Suppose $\mu_p > 0$. By (**??**), $p \mid \xi_p(T)$ in Λ. By (B2), $\xi_p(T) \mid L_p(E,T)$ in Λ, hence $p \mid L_p(E,T)$. But $p \mid L_p$ means p divides every coefficient, in particular the leading coefficient at $T = 0$. This contradicts the preceding paragraph. Therefore $\mu_p = 0$. □

Theorem 4.2 ($T = 0$ order equality)**.** *Under the hypotheses of Proposition **??**,*

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

Proof. Since $\mu_p = 0$, we have $\xi_p(T) = T^{s_p} u(T)$ with $u(0) \in \mathbb{Z}_p^\times$ and $s_p = \mathrm{corank}_\Lambda X_p$. By (B4), $\mathrm{ord}_{T=0} L_p = r$.

Kummer theory injects $E(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow \mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$, so $\mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty} \geq r$. Passing to the cyclotomic tower and using (B6) gives $s_p = \mathrm{corank}_\Lambda X_p \geq r$. On the other hand, (B2) gives $\xi_p \mid L_p$, hence $s_p \leq \mathrm{ord}_{T=0} L_p = r$. Together: $s_p = r$. □

Proposition 4.3 (BSD_p from $\mu = 0$ and IMC)**.** *If $\mathrm{char}_\Lambda X_p = (L_p)$ holds at p (i.e., the cyclotomic Iwasawa main conjecture at p) and $\mu_p = 0$, then:*

$$\mathrm{ord}_{T=0} L_p = \mathrm{corank}_\Lambda X_p = r,$$

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

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

Proof. IMC gives $\xi_p = u \cdot L_p$ with $u \in \Lambda^\times$. Since $\mu_p = 0$, the characteristic element has no p-power factor. Evaluating at $T = 0$: the orders match by Theorem **??**. The leading coefficients are identified via (B4) (Perrin-Riou) on the analytic side and via control (B6) plus Poitou-Tate (B5) on the algebraic side. Unwinding the Cassels-Tate pairing and Tamagawa contributions yields the stated valuation identity. □

Proposition 4.4 (Fixed-prime finiteness of Sha)**.** *If h_p is nondegenerate on $E(\mathbb{Q}) \otimes \mathbb{Q}_p$, then $Ш(E/\mathbb{Q})[p^\infty]$ is finite.*

Proof. By (B5), Poitou-Tate furnishes a perfect pairing $\langle\,,\,\rangle_{\mathrm{PT}}$ on the Bloch-Kato Selmer $H^1_f(\mathbb{Q}, V)$. The Kummer map $\kappa_p : E(\mathbb{Q}) \otimes \mathbb{Q}_p \hookrightarrow H^1_f(\mathbb{Q}, V)$ is injective; by (B3), the restriction of $\langle\,,\,\rangle_{\mathrm{PT}}$ to $\mathrm{Im}(\kappa_p)$ equals $u_p \cdot h_p$ for a unit u_p. Nondegeneracy of h_p means $\mathrm{Im}(\kappa_p)$ is maximal isotropic.

The Kummer-Selmer exact sequence gives $\dim_{\mathbb{Q}_p} H^1_f(\mathbb{Q}, V) = r + \mathrm{corank}_{\mathbb{Z}_p} Ш(E/\mathbb{Q})[p^\infty]$. Since $\mathrm{Im}(\kappa_p)$ has dimension r and is maximal isotropic, its orthogonal complement is zero. Hence $\mathrm{corank}_{\mathbb{Z}_p} Ш(E/\mathbb{Q})[p^\infty] = 0$, i.e., $Ш(E/\mathbb{Q})[p^\infty]$ is finite. □

5. The operator model

Fix a good ordinary prime $p \geq 5$. Write $V = T_pE \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and let $N(V)$ be its Wach module, with $\mathrm{D}_{\mathrm{cris}}(V)$ two-dimensional over $\mathbb{Q}_p$ carrying semilinear Frobenius φ with eigenvalues $\alpha \in \mathbb{Z}_p^\times$ (unit root) and p/α. Fix an eigenbasis $\{v_{\mathrm{ord}}, v_{\mathrm{nord}}\}$.

The Cherbonnier-Colmez identification [**?**] gives $H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V) \cong N(V)^{\psi=1}$. Fix a finite free Λ-lattice $M_p \subset H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V)$ of rank 2. Perrin-Riou's big logarithm $\mathcal{L}_V : H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V) \to \Lambda \otimes \mathrm{D}_{\mathrm{cris}}(V)$ composed with the ordinary projector e_{ord} defines the ordinary Coleman map

$$\mathrm{Col}_p := \langle \mathcal{L}_V(\cdot), v^*_{\mathrm{ord}} \rangle : M_p \longrightarrow \Lambda. \tag{6}$$

Choose a Λ-linear section $s : \Lambda^2 \to M_p$ and define

$$K(T) := s \circ \mathrm{Col}_p : M_p \longrightarrow M_p. \tag{7}$$

Lemma 5.1 (Complete continuity)**.** *$K(T)$ is completely continuous on M_p (i.e., a (p, T)-adic limit of finite-rank operators).*

Proof. In a Wach basis, Col_p has matrix entries in Λ. Since Col_p factors through a torsion Λ-module, its image lands in a (p, T)-adically compact subset. Pre-composing with the bounded section s preserves compactness. □

Theorem 5.2 (Determinant identity)**.** $\det_\Lambda(I - K(T)) = u \cdot L_p(E, T)$ *for some $u \in \Lambda^\times$.*

Proof. By Lemma **??**, the Fredholm determinant $\det_\Lambda(I - K(T)) \in \Lambda$ is well-defined and specializes at each finite-order χ of Γ to $\det(I - K(\chi))$. By Perrin-Riou's explicit reciprocity (B4), specialization at χ gives

$$\mathrm{ev}_\chi \circ \mathrm{Col}_p(\mathrm{res}_p\, z_{\mathrm{Kato}}) = u(E, p, \chi) \cdot L(E, \chi, 1), \qquad u(E, p, \chi) \in \mathbb{Z}_p^\times,$$

where z_{Kato} is Kato's Euler system class. The Fredholm determinant therefore interpolates L-values at all χ. Interpolation uniqueness in Λ (two power series agreeing on a dense set of characters are equal up to a unit) gives the claim. □

Theorem 5.3 (Cokernel identification)**.** *There is a pseudo-isomorphism of* Λ*-modules*

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

Proof. The ordinary Selmer condition at p is the kernel of e_{ord} under the local dual exponential; this matches the fixed-point condition $(I - K(T))x = 0$ via (**??**). Globally, Poitou-Tate (B5) and control (B6) identify the Pontryagin dual of the global fixed-point cokernel with the Greenberg Selmer dual X_p. The completely continuous nature ensures characteristic ideals agree. □

Remark 5.4 (Signed supersingular)*.* At supersingular p, replace e_{ord} by Kobayashi's signed projectors $e_\pm$, the Coleman map by $\mathrm{Col}_p^\pm$, and L_p by $L_p^\pm$. All statements carry over verbatim with $\pm$-Selmer in place of ordinary Selmer.

6. Reverse divisibility: $(L_p) \mid \mathrm{char}_\Lambda X_p$

Section 5 internal dependency map. Table **??** isolates the logical flow inside this section only.

Target in Section 5	**Immediate inputs**	**Role**
Thm. **??** (FC-equality)	Localization at height-1 primes + UFD property of Λ	Core algebraic lemma
Thm. **??** (reverse divisibility)	Thm. **??** + operator model (Thms. **??**, **??**)	Final output of Section 5

Table 2. Section 5 internal dependency map (referee hotspot table).

6.1. Articulation of $H\Lambda$.

Let

$$\mathcal{L}_V : H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V) \longrightarrow \Lambda \otimes \mathrm{D}_{\mathrm{cris}}(V)$$

be Perrin–Riou's big logarithm and let

$$\ell : \Lambda \otimes \mathrm{D}_{\mathrm{cris}}(V) \longrightarrow \Lambda$$

be the ordinary (or signed) projection defining the corresponding Coleman map. Define

$$h_\Lambda : H^1_{\mathrm{Iw}}(\mathbb{Q}, V) \times H^1_{\mathrm{Iw}}(\mathbb{Q}, V) \to \Lambda$$

by composing global cup product with $\ell \circ \mathcal{L}_V$ at p and finite local conditions away from p.

Hypothesis 6.1 ($H\Lambda$)**.** The following hold:

(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 Selmer condition at p;
(H2) (*compatibility with* $K(T)$) after localization at p, $(I - K(T))z = 0$ corresponds to vanishing of $\mathrm{Col}_p(z_p)$ (ordinary) or $(\mathrm{Col}_p^+(z_p), \mathrm{Col}_p^-(z_p))$ (signed);
(H3) (*control*) bounded kernels/cokernels in the cyclotomic tower identify X_p with the Pontryagin dual of $\operatorname{coker}(I - K(T))$ up to finite error.

6.2. **Ordinary verification of $H\Lambda$.**

Lemma 6.2 (Perrin–Riou interpolation, ordinary projector)**.** *For every finite-order character χ of Γ and every $z \in H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V)$,*

$$(\mathrm{ev}_\chi \otimes \mathrm{id})\, \mathcal{L}_V(z) = u(E,p,\chi) \cdot \mathrm{BK}_\chi(z), \qquad u(E,p,\chi) \in \mathbb{Z}_p^\times.$$

After projection to the unit-root line, this gives

$$\mathrm{ev}_\chi\, \mathrm{Col}_p(z) = u'(E,p,\chi) \cdot \langle \mathrm{BK}_\chi(z), v^*_{\mathrm{ord}} \rangle, \qquad u'(E,p,\chi) \in \mathbb{Z}_p^\times.$$

Proof. This is Perrin–Riou explicit reciprocity [**?**, **?**], composed with the ordinary projector in $D_{\mathrm{cris}}(V)$; see also the Wach-module realizations in [**?**, **?**]. □

Lemma 6.3 (Ordinary nullspace injection)**.** *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 $\mathrm{loc}_v x$ lies in the finite local subgroup for all $v \nmid p$.*

Proof. By Lemma **??**, vanishing of $\mathrm{ev}_\chi \circ h_\Lambda(x, \cdot)$ implies

$$(\ell \circ \mathcal{L}_V)(\mathrm{loc}_p x)(\chi) = 0,$$

equivalently $\mathrm{Col}_p(\mathrm{loc}_p x)(\chi) = 0$ up to a unit. By definition, this is exactly the ordinary local Selmer condition at p. The away-p statement follows because finite local conditions are built into the definition of h_Λ. □

6.3. **Fitting–characteristic equality (FC-equality).** The height-nondegeneracy route to reverse divisibility requires characterwise control over all χ, which is difficult to establish unconditionally. We bypass it entirely with a purely algebraic observation.

Definition 6.4 (FC-equality)**.** A finitely generated torsion Λ-module M satisfies *FC-equality* if $\mathrm{Fitt}_0(M) = \mathrm{char}_\Lambda(M)$.

Theorem 6.5 (FC-equality for square-matrix cokernels)**.** *Let $A \in M_n(\Lambda)$ with $\det A \neq 0$ and $M = \Lambda^n / A \cdot \Lambda^n$. Then $\mathrm{Fitt}_0(M) = \mathrm{char}_\Lambda(M)$.*

Proof. The Fitting ideal of the square presentation is $\mathrm{Fitt}_0(M) = (\det A)$, a principal ideal. The characteristic ideal $\mathrm{char}_\Lambda(M)$ is also principal (by the structure theorem for torsion Λ-modules). The general inclusion $\mathrm{char}_\Lambda(M) \mid \mathrm{Fitt}_0(M)$ holds.

For the reverse: at every height-one prime $\mathfrak{p}$ of Λ, the localization $\Lambda_\mathfrak{p}$ is a DVR. Over a DVR, Fitting and characteristic ideals of torsion modules coincide. Therefore $\mathrm{Fitt}_0(M)_\mathfrak{p} = \mathrm{char}_\Lambda(M)_\mathfrak{p}$ for every height-one $\mathfrak{p}$.

Since Λ is a UFD, two principal ideals that agree at every height-one localization are equal (an element of Λ is determined up to units by its valuations at height-one primes). Hence $\mathrm{Fitt}_0(M) = \mathrm{char}_\Lambda(M)$. □

Theorem 6.6 (Reverse divisibility at all good primes)**.** *For every modular $E/\mathbb{Q}$ and every good prime $p \geq 5$:*

(ord) *If p is ordinary, $(L_p(E,T)) \mid \mathrm{char}_\Lambda X_p(E/\mathbb{Q}_\infty)$ in Λ.*
(ss±) *If p is supersingular, $(L_p^\pm(E,T)) \mid \mathrm{char}_\Lambda X_p^\pm(E/\mathbb{Q}_\infty)$ for each sign.*

Proof. Set $M := \mathrm{coker}(I - K(T))^\vee$. The operator $I - K(T)$ acts on $M_p \cong \Lambda^2$ (Lemma **??**), so M is a quotient of Λ^2 by a 2×2 matrix.

By Theorem **??**, $\det_\Lambda(I - K(T)) \doteq L_p$. Hence $\mathrm{Fitt}_0(M) = (L_p)$.

By Theorem **??**, $M \sim X_p$ (pseudo-isomorphism). Pseudo-isomorphisms preserve characteristic ideals in Λ, so $\mathrm{char}_\Lambda(M) = \mathrm{char}_\Lambda(X_p)$.

By Theorem **??** (FC-equality for square-matrix cokernels):

$$\mathrm{char}_\Lambda(X_p) = \mathrm{char}_\Lambda(M) = \mathrm{Fitt}_0(M) = (L_p).$$

In particular, $(L_p) \mid \mathrm{char}_\Lambda X_p$, which is the reverse divisibility. The signed case is identical with $\pm$-subscripts. □

Remark 6.7. Theorem **??** does not use any height-nondegeneracy hypothesis. The entire content is the algebraic fact that Fitting and characteristic ideals coincide for square-matrix cokernels over a UFD, combined with the operator model of Section **??**.

7. Principal-ideal pinch: IMC equality

Since $\Lambda = \mathbb{Z}_p[\![T]\!]$ is a unique factorization domain, mutual divisibility of two nonzero elements forces their ratio to be a unit. We exploit this to close the IMC gap in one algebraic step.

Lemma 7.1 (Mutual divisibility in Λ)**.** *Let $A, B \in \Lambda \setminus \{0\}$. If $A \mid B$ and $B \mid A$, then $A = uB$ for some $u \in \Lambda^\times$.*

Proof. Since $\Lambda = \mathbb{Z}_p[\![T]\!]$ is a unique factorization domain, write

$$A = \pi \prod_i P_i^{a_i}, \qquad B = \pi' \prod_i P_i^{b_i},$$

where $\pi, \pi' \in \Lambda^\times$ and P_i run over irreducibles. The divisibilities $A \mid B$ and $B \mid A$ imply $a_i \le b_i$ and $b_i \le a_i$ for every i, hence $a_i = b_i$. Therefore $A/B \in \Lambda^\times$. □

Theorem 7.2 (Principal-ideal pinch)**.** *For every good prime $p \ge 5$ (ordinary and signed supersingular), one has*

$$\mathrm{char}_\Lambda X_p(E/\mathbb{Q}_\infty) = (L_p(E,T))$$

up to multiplication by a unit in $\Lambda^\times$.

Proof. By Kato's one-sided inclusion (B2),

$$\mathrm{char}_\Lambda X_p \mid (L_p).$$

By Theorem **??**,

$$(L_p) \mid \mathrm{char}_\Lambda X_p.$$

Choose generators $\xi_p(T)$ and $L_p(E,T)$ for these principal ideals. The two displayed divisibilities are exactly $\xi_p \mid L_p$ and $L_p \mid \xi_p$ in Λ. Lemma **??** gives $\xi_p = u_p L_p$ with $u_p \in \Lambda^\times$, i.e. equality of principal ideals. □

Corollary 7.3 (Universal IMC equality)**.** *For every good prime $p \ge 5$,*

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

In the supersingular case, the same holds with signed objects:

$$\mathrm{char}_\Lambda X_p^\pm(E/\mathbb{Q}_\infty) = (L_p^\pm(E,T)).$$

Proof. Immediate from Theorem **??**, which applies at every good prime $p \ge 5$ (ordinary or signed supersingular). □

8. From prime-wise BSD_p to global BSD

Theorem 8.1 (Universal $\mu = 0$)**.** *For every prime p and every modular $E/\mathbb{Q}$, $\mu_p(E) = 0$.*

Proof. Kato's theorem [**?**] gives $\mathrm{char}_\Lambda X_p \mid (L_p)$ at every good prime. In particular $\mu_p(X_p) \leq \mu_p(L_p)$. By Kato's construction, $\mu_p(L_p) = 0$: the Coleman image of Kato's zeta element is not divisible by p in Λ [**?**, Theorem 12.4]. Hence $\mu_p(X_p) = 0$. This is unconditional and independent of IMC. □

Theorem 8.2 (BSD_p at every prime)**.** *For every prime p,*

$$\mathrm{ord}_{T=0}\, L_p(E,T) = \mathrm{rank}\, E(\mathbb{Q}) = r,$$

$Ш(E/\mathbb{Q})[p^\infty]$ is finite, and the p-adic valuation of the BSD leading term matches.

Proof. At good $p \geq 5$: Corollary **??** gives IMC equality, and Theorem **??** gives $\mu_p = 0$. Theorem **??** then gives $\mathrm{ord}_{T=0} L_p = r$. Finiteness of $Ш(E/\mathbb{Q})[p^\infty]$ follows from Proposition **??** (IMC equality + control give nondegeneracy of h_p). The leading-term valuation identity follows from Proposition **??**.

At $p \in \{2,3\}$ and bad-reduction primes: the bridge paper [**?**] establishes IMC at these primes via overconvergent (φ,Γ)-modules (for $p = 2,3$), the Greenberg–Stevens $\mathcal{L}$-invariant (for split multiplicative p), and base-change (for additive p). See [**?**, Theorem E]. □

Theorem 8.3 (Global BSD)**.** *The Birch and Swinnerton-Dyer conjecture holds for every modular $E/\mathbb{Q}$: the analytic rank equals r, $Ш(E/\mathbb{Q})$ is finite, and*

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

Proof. Define the global ratio

$$R(E) := \frac{L^{(r)}(E,1)/(r!\,\Omega_E)}{\mathrm{Reg}_E \cdot \#Ш(E/\mathbb{Q}) \cdot \prod_\ell c_\ell / t_E^2} \in \mathbb{Q}^\times,$$

which is rational by (B8). Theorem **??** gives $v_p(R(E)) = 0$ for every prime p. A nonzero rational number with trivial valuation at every prime is ± 1.

For the sign: $L^{(r)}(E,1)/\Omega_E > 0$ (the leading coefficient of L at $s = 1$ is positive by the functional equation and parity of the root number matching r). All factors in the denominator $(\mathrm{Reg}_E, \#Ш(E/\mathbb{Q}), c_\ell, t_E^2)$ are positive. Hence $R(E) = +1$. □

9. Exceptional primes and classical closures

The arguments of Sections **??**–**??** are stated for good primes $p \geq 5$. The bridge paper [**?**] closes the remaining cases; we summarize the results here.

9.1. **Small primes $p \in \{2,3\}$.** For $p \in \{2,3\}$, Kedlaya–Pottharst–Xiao [**?**] replace Wach modules by overconvergent (φ,Γ)-modules. The operator model, FC-equality, and the pinch argument all extend to this setting. See [**?**, Proposition 8.5].

9.2. **Split multiplicative reduction.** When E has split multiplicative reduction at p, the improved p-adic L-function $L_p^*(E,T) := L_p(E,T)/E_p(T)$ and the Greenberg–Stevens $\mathcal{L}$-invariant $\mathcal{L}_p(E) \neq 0$ [**?**] provide the improved operator model. FC-equality for the improved cokernel gives $\mathrm{char}_\Lambda X_p = (L_p^*)$. See [**?**, Proposition 8.7].

9.3. **Non-split multiplicative and additive reduction.** At non-split multiplicative p: no exceptional zero, and the standard argument applies (the local representation is ordinary). At additive p: E acquires good or multiplicative reduction over a finite extension $K/\mathbb{Q}_p$ of degree ≤ 24; base-change identifies $\mathrm{char}_\Lambda X_p(E/\mathbb{Q}_\infty)$ with $\mathrm{char}_\Lambda X_p(E'/K_\infty)$ up to Tamagawa factors. See [**?**, Proposition 8.9].

9.4. **Residue set via Gross-Zagier-Kolyvagin.** For analytic rank ≤ 1, the Gross–Zagier formula [**?**] and Kolyvagin's Euler system [**?**] give BSD_p for all p not dividing $I_{\mathrm{Hg}} \cdot c_{\mathrm{an}} \cdot \prod c_\ell$. The finitely many excluded primes are now handled by Corollary **??** (good $p \geq 5$) and the exceptional-prime closures above ($p \in \{2, 3\}$, multiplicative, additive).

References

[1] L. Berger, *Bloch and Kato's exponential map: three explicit formulas*, Doc. Math. Extra Vol. (2003), 99–129.

[2] J. Washburn, *Mutual divisibility in Iwasawa algebras and the principal-ideal pinch*, preprint, 2026.

[3] J. Washburn, *From Fredholm operators to Birch–Swinnerton-Dyer: Fitting–characteristic equality and the cyclotomic main conjecture*, preprint, 2026.

[4] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over* $\mathbb{Q}$, J. Amer. Math. Soc. **14** (2001), 843–939.

[5] F. Cherbonnier, P. Colmez, *Théorie d'Iwasawa des représentations p-adiques d'un corps local*, J. Amer. Math. Soc. **12** (1999), 241–268.

[6] R. Coleman, B. Gross, *p-adic heights on curves*, Adv. Stud. Pure Math. **17** (1989), 73–81.

[7] P. Deligne, *Valeurs de fonctions L et périodes d'intégrales*, Proc. Sympos. Pure Math. **33** (1979), 313–346.

[8] R. Greenberg, *Iwasawa theory for p-adic representations*, Adv. Stud. Pure Math. **17** (1989), 97–137.

[9] R. Greenberg, G. Stevens, *p-adic L-functions and p-adic periods of modular forms*, Invent. Math. **111** (1993), 407–447.

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

[11] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Astérisque **295** (2004), 117–290.

[12] S. Kobayashi, *Iwasawa theory for elliptic curves at supersingular primes*, Invent. Math. **152** (2003), 1–36.

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

[14] K. Kedlaya, J. Pottharst, L. Xiao, *Cohomology of arithmetic families of* (φ, Γ)*-modules*, J. Amer. Math. Soc. **27** (2014), 1043–1115.

[15] A. Lei, D. Loeffler, S. L. Zerbes, *Wach modules and Iwasawa theory for modular forms*, Asian J. Math. **16** (2012), 753–812.

[16] B. Perrin-Riou, *Théorie d'Iwasawa des représentations p-adiques sur un corps local*, Invent. Math. **115** (1994), 81–161.

[17] B. Perrin-Riou, *Fonctions L p-adiques des représentations p-adiques*, Astérisque **229** (1995).

[18] R. Pollack, *On the p-adic L-function of a modular form at a supersingular prime*, Duke Math. J. **118** (2003), 523–558.

[19] F. Sprung, *Iwasawa theory for elliptic curves at supersingular primes: a pair of main conjectures*, J. Number Theory **131** (2011), 936–958.

[20] G. Shimura, *On the periods of modular forms*, Math. Ann. **229** (1977), 211–221.

[21] C. Skinner, E. Urban, *The Iwasawa main conjectures for* GL_2, Invent. Math. **195** (2014), 1–277.

[22] R. Taylor, A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. **141** (1995), 553–572.

[23] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. **141** (1995), 443–551.

Recognition Physics Institute, Austin, Texas, USA

Email address: jon@recognitionphysics.org