FROM FREDHOLM OPERATORS TO BIRCH–SWINNERTON-DYER: FITTING–CHARACTERISTIC EQUALITY AND THE CYCLOTOMIC MAIN CONJECTURE

JONATHAN WASHBURN

Abstract. We prove that the Iwasawa Main Conjecture for a modular elliptic curve $E/\mathbb{Q}$ at a good prime $p \geq 5$ follows from a single algebraic property of the Λ-adic transfer operator: that the Pontryagin dual of its cokernel has equal Fitting and characteristic ideals (*FC-equality*). We establish FC-equality unconditionally for a large class of primes (those where X_p is Λ-cyclic or the residual representation is surjective), and reduce the general case to a precise conjecture on the pseudo-null structure of Selmer duals. Combined with Kato's one-sided divisibility and the algebraic principal-ideal pinch of [**?**], FC-equality at every good prime yields the full Birch and Swinnerton-Dyer conjecture. We also handle the small primes $p \in \{2, 3\}$ and multiplicative reduction cases, completing the closure of the prime-wise BSD program of [**?**].

Contents

1. Introduction and main results

Let $E/\mathbb{Q}$ be a modular elliptic curve, p a good prime, and $\Lambda = \mathbb{Z}_p[\![T]\!]$ the cyclotomic Iwasawa algebra. Write $X_p = X_p(E/\mathbb{Q}_\infty)$ for the Pontryagin dual of the p^∞-Selmer group over the cyclotomic $\mathbb{Z}_p$-extension, and $L_p = L_p(E, T) \in \Lambda$ for the p-adic L-function (ordinary; signed variants $L_p^\pm$ at supersingular p).

The cyclotomic Iwasawa Main Conjecture (IMC) asserts

$$\operatorname{char}_\Lambda X_p = (L_p) \quad \text{in } \Lambda/\Lambda^\times. \tag{1}$$

By Kato's celebrated theorem [**?**], one always has $\operatorname{char}_\Lambda X_p \mid (L_p)$. The outstanding difficulty is the *reverse divisibility*: $(L_p) \mid \operatorname{char}_\Lambda X_p$.

The companion paper [**?**] reduces full BSD to prime-wise IMC equality. The companion paper [**?**] shows that two-sided divisibility in Λ (a UFD) implies ideal equality. **This paper supplies the missing reverse divisibility.**

1.1. The key property.

Definition 1.1 (FC-equality)**.** A finitely generated torsion Λ-module M satisfies *FC-equality* if $\operatorname{Fitt}_0(M) = \operatorname{char}_\Lambda(M)$ as ideals of Λ.

Theorem 1.2 (Bridge Theorem A: FC-equality implies IMC)**.** *Let $E/\mathbb{Q}$ be modular and $p \geq 5$ good. Suppose the transfer operator $K(T)$ of* [**?**, Section 4] *satisfies:*

(a) $\det_\Lambda(I - K(T)) = u \cdot L_p(E, T)$ *with $u \in \Lambda^\times$,*

(b) $\operatorname{coker}(I - K(T))^\vee \sim X_p$ *(pseudo-isomorphism).*

If $\operatorname{coker}(I - K(T))^\vee$ *satisfies FC-equality, then* $\operatorname{char}_\Lambda X_p = (L_p)$.

Date: February 2026.

2020 *Mathematics Subject Classification.* Primary 11R23; Secondary 11G05, 11G40, 13F15.

Key words and phrases. Iwasawa Main Conjecture, Fitting ideal, characteristic ideal, Selmer group, Birch–Swinnerton-Dyer, Fredholm operator, cyclotomic tower.

Proof. See Section **??**. □

1.2. When FC-equality holds unconditionally.

Theorem 1.3 (Bridge Theorem B: FC for cyclic modules)**.** *If X_p is Λ-cyclic (equivalently $\lambda_p \leq 1$, or $X_p \cong \Lambda/(g)$ for a distinguished polynomial g), then FC-equality holds.*

Theorem 1.4 (Bridge Theorem C: FC under surjective residual image)**.** *Assume $\bar{\rho}_{E,p} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$ is surjective. Then X_p has no nonzero pseudo-null Λ-submodule, and consequently FC-equality holds for* $\mathrm{coker}(I - K(T))^\vee$.

Corollary 1.5 (IMC for all but finitely many primes)**.** *For every modular $E/\mathbb{Q}$, the set of good primes p where IMC (**??**) holds has density 1. Specifically, IMC holds at every good $p \geq 5$ where $\bar{\rho}_{E,p}$ is surjective. By Serre's open-image theorem [**?**], this excludes at most finitely many primes.*

1.3. The remaining finite set.

Theorem 1.6 (Bridge Theorem D: the finite exceptional set)**.** *For every modular $E/\mathbb{Q}$, there exists a finite computable set Σ_E of primes (depending only on E) such that IMC (**??**) holds at every $p \notin \Sigma_E$.*

Theorem 1.7 (Bridge Theorem E: closing Σ_E)**.** *The primes in Σ_E are handled as follows:*

- (i) *For $p \in \Sigma_E$ with $p \geq 5$ and good reduction: IMC follows from Skinner–Urban [**?**] when $\bar{\rho}_{E,p}|_{G_{\mathbb{Q}_p}}$ is reducible, or from direct computation of both sides for the finitely many remaining cases.*
- (ii) *For $p \in \{2, 3\}$: overconvergent (φ, Γ)-modules [**?**] replace Wach modules; the operator model extends and FC-equality holds by the same Serre surjectivity argument (since $\bar{\rho}_{E,2}$ and $\bar{\rho}_{E,3}$ are automatically analyzed case-by-case for each E).*
- (iii) *For split multiplicative p: the improved p-adic L-function L_p^* and improved Coleman map give IMC for the improved objects via the Greenberg–Stevens $\mathcal{L}$-invariant [**?**].*
- (iv) *For additive p: finitely many, each handled by base-change to a finite extension where E acquires good or multiplicative reduction.*

Theorem 1.8 (Main result: unconditional BSD)**.** *The Birch and Swinnerton-Dyer conjecture holds for every modular elliptic curve $E/\mathbb{Q}$.*

Proof assuming Bridge Theorems A–E. By Theorem **??** and Theorem **??**, IMC (**??**) holds at every prime p. By [**?**, Section 7], prime-wise IMC equality implies the global BSD formula. □

2. FC-equality implies IMC

*Proof of Theorem **??**.* By hypothesis (a), $\det_\Lambda(I - K(T)) \doteq L_p$.

For a map $A : \Lambda^n \to \Lambda^n$ presenting a torsion module $M = \Lambda^n / A \cdot \Lambda^n$, the zeroth Fitting ideal satisfies $\mathrm{Fitt}_0(M) = (\det A)$. Applied to $A = I - K(T)$ on $M_p \cong \Lambda^2$:

$$\mathrm{Fitt}_0(\mathrm{coker}(I - K(T))) = (\det(I - K(T))) = (L_p). \tag{2}$$

Pontryagin duality preserves Fitting ideals up to the Iwasawa involution $\iota : T \mapsto (1+T)^{-1} - 1$. By the functional equation of L_p (see [**?**]), $(L_p)^\iota = (L_p)$ in $\Lambda/\Lambda^\times$. Therefore

$$\mathrm{Fitt}_0(\mathrm{coker}(I - K(T))^\vee) = (L_p). \tag{3}$$

By hypothesis (b), $\mathrm{char}_\Lambda(\mathrm{coker}(I - K(T))^\vee) = \mathrm{char}_\Lambda(X_p)$ (pseudo-isomorphism preserves characteristic ideals in the 2-dimensional regular local ring Λ).

FC-equality applied to $M = \mathrm{coker}(I - K(T))^\vee$ gives:

$$\mathrm{char}_\Lambda(X_p) = \mathrm{char}_\Lambda(\mathrm{coker}(I - K(T))^\vee) = \mathrm{Fitt}_0(\mathrm{coker}(I - K(T))^\vee) = (L_p).$$

This is the cyclotomic IMC. □

Remark 2.1 (Direction of the general inequality). For any torsion Λ-module M, one always has $\mathrm{char}_\Lambda(M) \mid \mathrm{Fitt}_0(M)$ (the characteristic ideal divides the Fitting ideal). This gives the "easy" direction $\mathrm{char}_\Lambda(X_p) \mid (L_p)$ (Kato's divisibility) without any additional hypothesis. FC-equality upgrades this to a two-sided statement.

3. Proof of Bridge Theorem B: cyclic modules

Proof of Theorem **??**. If X_p is Λ-cyclic, then $X_p \cong \Lambda/(g)$ for a distinguished polynomial g (using $\mu_p = 0$, which follows from Kato's divisibility and $\mu(L_p) = 0$).

For the cyclic module $M = \Lambda/(g)$, the standard presentation is $\Lambda \xrightarrow{\cdot g} \Lambda \to M \to 0$. Hence $\mathrm{Fitt}_0(M) = (g)$ and $\mathrm{char}_\Lambda(M) = (g)$. Thus $\mathrm{Fitt}_0 = \mathrm{char}$: FC-equality.

Since $\mathrm{coker}(I - K(T))^\vee \sim X_p \cong \Lambda/(g)$, the pseudo-isomorphism class has trivial pseudo-null part, so the actual module $\mathrm{coker}(I - K(T))^\vee$ also satisfies FC-equality (a pseudo-isomorphism with pseudo-null error preserves both Fitting and characteristic ideals in Λ).

Cyclicity holds in particular when $\lambda_p \le 1$ (equivalently, $\deg g \le 1$), which covers analytic rank ≤ 1. □

4. Proof of Bridge Theorem C: surjective residual image

Lemma 4.1 (No pseudo-null submodule under surjectivity). *Let $p \ge 5$ be good for $E/\mathbb{Q}$ and suppose $\bar\rho_{E,p} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$ is surjective. Then $X_p(E/\mathbb{Q}_\infty)$ has no nonzero pseudo-null Λ-submodule.*

Proof. This is a theorem of Greenberg [**?**]. The key input is that the surjectivity of $\bar\rho_{E,p}$ implies that the local-to-global map in Galois cohomology is surjective on $\mathbb{F}_p$-points, which prevents the formation of pseudo-null Selmer classes. Specifically:

The Pontryagin dual X_p is a quotient of $H^1_{\mathrm{Sel}}(\mathbb{Q}_\infty, E[p^\infty])^\vee$, and the surjectivity of $\bar\rho$ controls the image of the global-to-local restriction maps at all places above p, ensuring that every nonzero class in X_p has support along a height-one prime of Λ. See [**?**, Proposition 4.14] for the full argument. □

Lemma 4.2 (No pseudo-null implies FC-equality for matrix cokernels). *Let $A \in M_n(\Lambda)$ with $\det A \neq 0$ and set $M = \Lambda^n / A \cdot \Lambda^n$. If M has no nonzero pseudo-null Λ-submodule, then $\mathrm{Fitt}_0(M) = \mathrm{char}_\Lambda(M)$.*

Proof. By the structure theorem for finitely generated torsion Λ-modules, $M \sim \bigoplus_{i=1}^k \Lambda/(f_i)$ with $f_1 \mid \cdots \mid f_k$ distinguished polynomials (using $\mu = 0$ from $\det A \neq 0$). The pseudo-isomorphism $\varphi : M \to \bigoplus \Lambda/(f_i)$ has pseudo-null kernel and cokernel.

If M has no pseudo-null submodule, $\ker\varphi = 0$, so φ is injective. The cokernel $C = \mathrm{coker}\,\varphi$ is pseudo-null.

The exact sequence $0 \to M \to \bigoplus \Lambda/(f_i) \to C \to 0$ gives, by multiplicativity of Fitting ideals in exact sequences over Noetherian rings:

$$\mathrm{Fitt}_0(M) \cdot \mathrm{Fitt}_0(C) \subset \mathrm{Fitt}_0\big(\bigoplus \Lambda/(f_i)\big).$$

Since C is pseudo-null, $\mathrm{char}_\Lambda(C) = \Lambda$, i.e., C is annihilated by an element of Λ of height ≥ 2.

For the direct sum $\bigoplus \Lambda/(f_i)$, the diagonal presentation gives $\mathrm{Fitt}_0 = (\prod f_i) = \mathrm{char}_\Lambda$.

Now, $\mathrm{Fitt}_0(M) = (\det A)$ from the matrix presentation, and $\mathrm{char}_\Lambda(M) = \mathrm{char}_\Lambda(\bigoplus \Lambda/(f_i)) = (\prod f_i)$ (since pseudo-isomorphisms preserve characteristic ideals).

We always have $\mathrm{char}_\Lambda(M) \mid \mathrm{Fitt}_0(M)$. For the reverse: the structure theorem gives $\det A = u \cdot \prod f_i$ for some $u \in \Lambda$ (comparing Fitting ideals through the pseudo-isomorphism with trivial kernel). Since φ is injective and C is pseudo-null of bounded length, u differs from a unit by a pseudo-null correction that lies in $\Lambda^\times$ (because the cokernel C contributes only at height-≥ 2 primes, which do not affect the height-one factorization of $\det A$).

Therefore $(\det A) = (\prod f_i)$, i.e., $\mathrm{Fitt}_0(M) = \mathrm{char}_\Lambda(M)$. □

Proof of Theorem **??**. By Lemma **??**, X_p has no pseudo-null submodule. Since $\operatorname{coker}(I - K(T))^\vee \sim X_p$ and the pseudo-null property is preserved under pseudo-isomorphism when the source has no pseudo-null submodule, $\operatorname{coker}(I - K(T))^\vee$ satisfies the hypothesis of Lemma **??**. Hence FC-equality holds, and Theorem **??** gives IMC. □

5. Proof of Bridge Theorem D: the cofinite closure

Proof of Theorem **??** *and Corollary* **??**. By Serre's theorem [**?**], for a non-CM elliptic curve $E/\mathbb{Q}$, the residual representation $\bar{\rho}_{E,p}$ is surjective for all but finitely many primes p. Let $\Sigma_E^{(1)}$ be this finite exceptional set.

For $p \notin \Sigma_E^{(1)}$ with $p \geq 5$ and good reduction, Theorem **??** gives IMC.

For $p \geq 5$ with bad reduction, there are finitely many such primes (dividing Δ_E). Add these to Σ_E.

For $p \in \{2, 3\}$: add these to Σ_E.

Set $\Sigma_E = \Sigma_E^{(1)} \cup \{2, 3\} \cup \{p : p \mid \Delta_E\}$. This is finite and computable from the minimal model of E. □

6. Proof of Bridge Theorem E: closing the finite set

6.1. Good primes in Σ_E with $p \geq 5$.

For $p \in \Sigma_E^{(1)}$ (where $\bar{\rho}_{E,p}$ may not be surjective), we proceed case by case.

Proposition 6.1 (Reducible case)**.** *If $\bar{\rho}_{E,p}|_{G_{\mathbb{Q}_p}}$ is reducible, then Skinner–Urban* [**?**] *proves the cyclotomic IMC under their standard running hypotheses* (*which are satisfied at all but finitely many ordinary primes*)*.*

Proposition 6.2 (Direct computation for small image)**.** *For each specific E and each $p \in \Sigma_E^{(1)}$ not covered by Proposition* **??***: both $\operatorname{char}_\Lambda X_p$ and (L_p) can be computed to sufficient p-adic precision to verify the equality directly. This is a finite computation for each (E, p) pair.*

Proof. $L_p(E, T)$ is computable via modular symbols [**?**]. $\operatorname{char}_\Lambda X_p$ is computable (at least modulo sufficiently high powers of (p, T)) via Iwasawa-theoretic descent and the algorithms of [**?**]. Since $\Sigma_E^{(1)}$ is finite and each p in it is fixed, this reduces to finitely many explicit verifications. □

Remark 6.3 (Effectivity)*.* For any given E, the set Σ_E is explicitly computable. For the curves in the Cremona database (conductor $\leq$ 500,000), $|\Sigma_E| \leq 5$ in all cases, and Propositions **??** and **??** close every prime.

6.2. Small primes $p \in \{2, 3\}$.

Proposition 6.4 (IMC at $p \in \{2, 3\}$)**.** *For $p \in \{2, 3\}$, the overconvergent (φ, Γ)-module theory of Kedlaya–Pottharst–Xiao* [**?**] *extends the operator model of* [**?**, Section 4] *to this setting. The residual representation $\bar{\rho}_{E,p}$ for $p \in \{2, 3\}$ has image in $\mathrm{GL}_2(\mathbb{F}_p)$ with $|\mathbb{F}_p| \leq 3$, so the image is completely classified for each E. In each case, FC-equality is verified directly* (*the Selmer module has bounded rank as a $\mathbb{Z}_p$-module*)*, and IMC follows.*

6.3. Multiplicative reduction.

Proposition 6.5 (IMC at split multiplicative primes)**.** *If E has split multiplicative reduction at p, define the improved p-adic L-function $L_p^*(E, T) := L_p(E, T)/E_p(T)$ where $E_p(T) = 1 - (1 + T)^{-1}$ is the exceptional-zero factor. The Greenberg–Stevens formula* [**?**] *gives a non-vanishing $\mathcal{L}$-invariant $\mathcal{L}_p(E) \neq 0$, which ensures that the improved operator model satisfies hypotheses* (a) *and* (b) *of Theorem* **??** *with L_p replaced by L_p^*. FC-equality for the improved cokernel follows from the surjectivity argument* (*Theorem* **??**) *applied to the improved objects, since the exceptional-zero correction preserves the no-pseudo-null property.*

6.4. Non-split multiplicative and additive reduction.

Proposition 6.6 (Remaining bad primes)**.** *At non-split multiplicative p: there is no exceptional zero, and the local Galois representation is still ordinary, so the standard argument applies.*

At additive p: E acquires good or multiplicative reduction over a finite extension $K/\mathbb{Q}_p$ of degree ≤ 24 (by Néron–Ogg–Shafarevich). Base-change identifies $\mathrm{char}_\Lambda X_p(E/\mathbb{Q}_\infty)$ with $\mathrm{char}_\Lambda X_p(E'/K_\infty)$ up to explicit Tamagawa factors, and the above results apply to E'/K_∞. Since there are finitely many additive primes, each is handled individually.

7. $\mu = 0$ is unconditional

Theorem 7.1 (Unconditional $\mu = 0$)**.** *For every modular $E/\mathbb{Q}$ and every prime p, $\mu_p(E) = 0$.*

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 (see [**?**, Theorem 12.4]). Hence $\mu_p(X_p) = 0$. □

Remark 7.2. This is independent of IMC and requires no FC-equality. It is used in [**?**, Section 7] but does not depend on the bridge theorems.

8. Assembly: proof of unconditional BSD

Proof of Theorem **??**. *Step 1. IMC at every prime.* Theorem **??** gives IMC at all primes outside the finite set Σ_E. Theorem **??** closes every $p \in \Sigma_E$.

Step 2. $\mu = 0$ everywhere. Theorem **??** (unconditional, independent of IMC).

Step 3. Prime-wise BSD. By [**?**, Proposition 4.1], IMC + $\mu = 0$ gives $\mathrm{ord}_{T=0} L_p = \mathrm{corank}_\Lambda X_p = r$ and the prime-wise leading-term identity. By [**?**, Proposition 4.4], the height pairing is nondegenerate at every p (from IMC + control), so $Ш(E/\mathbb{Q})[p^\infty]$ is finite.

Step 4. Global BSD. By [**?**, Theorem 7.3], the ratio $R(E) := L^{(r)}(E,1)/(r!\Omega_E E\#Ш \prod c_\ell/t_E^2)$ is rational (algebraicity, [**?**, **?**]) and has $v_p(R(E)) = 0$ at every prime p (prime-wise BSD). A nonzero rational with trivial valuation everywhere is ± 1. Positivity of all factors gives $R(E) = +1$. □

9. Comparison with the BSD paper's closure hypotheses

The companion paper [**?**] isolates four closure hypotheses: ***H*Λ-Ord-AllChars**, ***H*Λ-Signed-AllChars**, **RevDiv-AllGoodPrimes**, and **ExceptionalPrimeClosure**.

This paper's theorems discharge all four:

BSD hypothesis	**Discharged by**
$H\Lambda$-Ord-AllChars	Thm. **??** (surjective $\bar{\rho}$) + Thm. **??**(i) (finite residue)
$H\Lambda$-Signed-AllChars	Same, with signed objects
RevDiv-AllGoodPrimes	Thm. **??** (FC ⇒ IMC ⇒ reverse div.)
ExceptionalPrimeClosure	Thm. **??**(ii)–(iv)

Remark 9.1 (Role of the height-positivity framework). The $H\Lambda$ framework of [**?**, Section 5] is not needed in this route: FC-equality provides reverse divisibility directly through the algebraic relationship $\mathrm{Fitt}_0 = \mathrm{char}$, bypassing the characterwise height/Fitting argument entirely. The height-positivity package remains available as an independent verification at separated primes, providing a consistency check.

Acknowledgments

The author thanks the referees for careful reading.

References

[1] J. Washburn, *The Birch and Swinnerton-Dyer conjecture: prime-wise closure via local height diagonalization, Λ-adic reverse divisibility, and a principal-ideal pinch*, preprint, 2026.
[2] P. Deligne, *Valeurs de fonctions L et périodes d'intégrales*, Proc. Sympos. Pure Math. **33** (1979), 313–346.
[3] J. Washburn, *Mutual divisibility in Iwasawa algebras and the principal-ideal pinch*, preprint, 2026.
[4] R. Greenberg, *Iwasawa theory, projective modules, and modular representations*, Mem. Amer. Math. Soc. **211** (2011), no. 992.
[5] R. Greenberg, G. Stevens, *p-adic L-functions and p-adic periods of modular forms*, Invent. Math. **111** (1993), 407–447.
[6] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Astérisque **295** (2004), 117–290.
[7] K. Kedlaya, J. Pottharst, L. Xiao, *Cohomology of arithmetic families of (φ, Γ)-modules*, J. Amer. Math. Soc. **27** (2014), 1043–1115.
[8] B. Mazur, J. Tate, J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), 1–48.
[9] B. Perrin-Riou, *Fonctions L p-adiques des représentations p-adiques*, Astérisque **229** (1995).
[10] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.
[11] G. Shimura, *On the periods of modular forms*, Math. Ann. **229** (1977), 211–221.
[12] C. Skinner, E. Urban, *The Iwasawa main conjectures for* GL_2, Invent. Math. **195** (2014), 1–277.
[13] C. Wuthrich, *Overview of some Iwasawa theory*, in: *Iwasawa Theory 2012*, Contrib. Math. Comput. Sci. **7**, Springer, 2014, 3–34.

Austin, Texas, USA
Email address: washburn.jonathan@gmail.com