A FORMULA OF PERRIN-RIOU AND CHARACTERISTIC POWER SERIES OF SIGNED SELMER GROUPS

FRANCESC CASTELLA

In memory of Professor John Coates

Abstract. We prove a conjecture of Kundu–Ray, following from the p-adic Birch–Swinnerton-Dyer conjecture for supersingular primes by Bernardi–Perrin-Riou and Kato's Main Conjecture, predicting an expression for the leading term (up to a p-adic unit) of a characteristic power series of Kobayashi's signed Selmer groups attached to elliptic curves $E/\mathbb{Q}$ with supersingular reduction at a prime $p > 2$ with $a_p = 0$. The proof is deduced from a similar formula due to Perrin-Riou for a generator of her module of arithmetic p-adic L-functions with values in the Dieudonné module of E.

Contents

1. Introduction

Let $E/\mathbb{Q}$ be an elliptic curve and p an odd prime of good reduction for E. Let $\mathcal{X}(E/\mathbb{Q}_\infty)$ denote the Pontryagin dual of the Selmer group $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_\infty)$ over the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}_\infty/\mathbb{Q}$. Let $\Lambda = \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]]$ be the cyclotomic Iwasawa algebra, which we identify with the one-variable power series ring $\mathbb{Z}_p[[X]]$ upon the choice of a topological generator $\gamma \in \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$.

Date: March 1, 2025.
This research was partially supported by the NSF grants DMS-2101458 and DMS-2401321.

When p is ordinary for E, the Selmer group $\mathcal{X}(E/\mathbb{Q}_\infty)$ is known to be Λ-torsion by work of Kato [Kat04], and letting $\xi_p \in \Lambda = \mathbb{Z}_p[[X]]$ denote a characteristic power series for $\mathcal{X}(E/\mathbb{Q}_\infty)$, the work of Schneider [Sch85] and Perrin-Riou [PR93b] (see also [PR84] for the case where E has complex multiplication) yields an analogue of the Birch–Swinnerton-Dyer conjecture for ξ_p, relating its order of vanishing at $X = 0$ to the Mordell–Weil rank of E, and expressing its leading coefficient in terms of arithmetic invariants of E.

The goal of this note is to prove an analogous result in the case where p is a prime of supersingular reduction for E with $a_p = 0$. Our main result is in terms of a characteristic power series of Kobayashi's signed Selmer groups; in the rank zero case, a result along these lines was first proved by B.-D. Kim [Kim13] by an adaptation of Greenberg's methods [Gre99], so we focus on the case of Mordell–Weil rank $r \geq 1$, where the result we obtain was conjectured by Kundu–Ray (*cf.* [KR21, Conjecture 3.15]), following Sprung's reformulation [Spr15] of the p-adic Birch–Swinnerton-Dyer conjecture of Bernardi and Perrin-Riou [BPR93] (see also Remark 1.1.1 below).

1.1. **Main result.** From now on, assume that $p > 2$ is a supersingular prime for E satisfying $a_p = 0$ (a condition that holds automatically unless $p = 3$). In [Kob03], Kobayashi introduced signed Selmer groups $\mathrm{Sel}_{p^\infty}^{\pm}(E/\mathbb{Q}_\infty)$ whose Pontryagin dual

$$\mathcal{X}^{\pm}(E/\mathbb{Q}_\infty) = \mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Sel}_{p^\infty}^{\pm}(E/\mathbb{Q}_\infty), \mathbb{Q}_p/\mathbb{Z}_p)$$

he showed to be Λ-torsion as a consequence of Kato's work.

As explained in the work of Bernardi–Perrin-Riou [BPR93], one can naturally attach a quadratic form h_ν on $E(\mathbb{Q})$ to every vector ν in the Dieudonné module $D_p(E) = \mathbb{Q}_p \otimes_{\mathbb{Q}} \mathrm{H}^1_{\mathrm{dR}}(E/\mathbb{Q})$, and we let $\mathrm{Reg}_\nu \in \mathbb{Q}_p$ be the discriminant of the associated bilinear (p-adic height) pairing

$$\langle \cdot, \cdot \rangle_\nu : E(\mathbb{Q}) \times E(\mathbb{Q}) \to \mathbb{Q}_p.$$

By linearity, these can be extended to $E(\mathbb{Q}) \otimes \mathbb{Z}_p$. Consider the *strict* (or *fine*, in the terminology of e.g. [Wut07]) Mordell–Weil group

$$(E(\mathbb{Q}) \otimes \mathbb{Z}_p)_0 := \ker\big\{E(\mathbb{Q}) \otimes \mathbb{Z}_p \to E(\mathbb{Q}_p)\hat{\otimes}\mathbb{Z}_p\big\},$$

where $E(\mathbb{Q}_p)\hat{\otimes}\mathbb{Z}_p$ is the p-adic completion of $E(\mathbb{Q}_p)$.

In Section 4, similarly as in the work of Sprung [Spr15] we shall introduce certain vectors $N^{\pm} \in D_p(E)$ in the complement to the Hodge filtration $\mathrm{Fil}^0 D_p(E) = \mathbb{Q}_p\omega_E$, where ω_E is a Néron differential on E. Write $\mathrm{Reg}_p^{\pm}$ (resp. $\mathrm{Reg}_p^{\mathrm{str}}$) for the above regulator on $E(\mathbb{Q})$ (resp. $E(\mathbb{Q}) \otimes \mathbb{Z}_p)_0$) associated to

$$h_{N^{\pm}/[\omega_E, N^{\pm}]_{\mathrm{dR}}} = h_{N^{\pm}}/[\omega_E, N^{\pm}]_{\mathrm{dR}},$$

where $[\cdot,\cdot]_{\mathrm{dR}}$ denotes the de Rham pairing on $D_p(E)$.

Let $\kappa : \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \simeq 1 + p\mathbb{Z}_p$ be the isomorphism defined by the p-adic cyclotomic character. The main result of this note is the following p-adic analogue of the Birch–Swinnerton-Dyer conjecture for supersingular primes.

Theorem A. *Let $E/\mathbb{Q}$ be an elliptic curve with good supersingular reduction at an odd prime p with $a_p = 0$. Put*

$$r = \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q})$$

and suppose $r \geq 1$. Let $\xi_p^{\pm} \in \Lambda \simeq \mathbb{Z}_p[[X]]$ be a characteristic power series for $\mathcal{X}^{\pm}(E/\mathbb{Q}_\infty)$. Then:

(i) $\varrho := \min\{\mathrm{ord}_X(\xi_p^+), \mathrm{ord}_X(\xi_p^-)\} \geq r$.

(ii) *If $Ш(E/\mathbb{Q})[p^\infty]$ is finite and $\mathrm{Reg}_p^{\mathrm{str}} \neq 0$, then equality holds in* (i)*, and the leading coefficient $(\xi_p^{+,*}, \xi_p^{-,*})$ of the vector $(\xi_p^+, \xi_p^-) \in \mathbb{Z}_p[[X]]^{\oplus 2}$ is given up to a p-adic unit by*

$$(\xi_p^{+,*}, \xi_p^{-,*}) \ \sim_p \ (\log_p \kappa(\gamma))^{-r} \cdot (\mathrm{Reg}_p^+, \mathrm{Reg}_p^-) \cdot \frac{\#Ш(E/\mathbb{Q})[p^\infty] \cdot \mathrm{Tam}(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{\mathrm{tors}})^2},$$

where $\log_p$ *is Iwasawa's branch of the p-adic logarithm and* $\mathrm{Tam}(E/\mathbb{Q}) = \prod_\ell c_\ell$ *is the product of the local Tamagawa numbers of* E.

Remark 1.1.1. The conclusion of Theorem A is predicted by the combination of:

- The p-adic Birch–Swinnerton-Dyer conjecture for supersingular primes p formulated by Bernardi–Perrin-Riou [BPR93] (see also [PR03, Conj. 2.5]), as reformulated by Sprung [Spr15] in terms of signed p-adic L-functions $L_p^\pm$;
- Kato's Main Conjecture (see [PR93a, §3.4]), which is known to be equivalent to Kobayashi's Main Conjecture predicting the equality

$$(\xi_p^\pm) \stackrel{?}{=} (L_p^\pm)$$

as principal ideals in Λ (see [Kob03, Thm. 7.4]).

This prediction is recorded in [KR21, Conjecture 3.15] (which the added prediction that $\mathrm{ord}_X(\xi_p^\pm)$ is independent of the choice of sign $\pm$).

Remark 1.1.2. In [RS23], for any two elliptic curves E_1, E_2 over $\mathbb{Q}$ with good supersingular reduction at a prime $p > 2$ with $a_p = 0$ and $E_1[p] \simeq E_2[p]$ as $G_\mathbb{Q}$-modules, Ray and Sujatha establish relations mod p between the (Σ-imprimitive) *truncated* Γ*-Euler characteristics* of their respective signed Selmer groups $\mathrm{Sel}_{p^\infty}^\pm(E_i/\mathbb{Q}_\infty)$, defined as

$$\chi_t^\pm(\Gamma, E_i) := \frac{\#\ker(\phi_{E_i})}{\#\mathrm{coker}(\phi_{E_i})},$$

where $\phi_{E_i} : \mathrm{Sel}_{p^\infty}^\pm(E_i/\mathbb{Q}_\infty)^\Gamma \to \mathrm{Sel}_{p^\infty}^\pm(E_i/\mathbb{Q}_\infty)_\Gamma$, sending $s \mapsto s \bmod (\gamma - 1)$, is the natural map from the Γ-invariants to the Γ-coinvariants. Using the structure theorem for finitely generated Λ-modules, one easily checks that $\chi_t^\pm(\Gamma, E_i)$ is defined, in the sense that both $\ker(\phi_{E_i})$ and $\mathrm{coker}(\phi_{E_i})$ are finite, whenever γ acts semi-simply on $\mathrm{Sel}_{p^\infty}^\pm(E_i/\mathbb{Q}_\infty)$ (a condition expected to always hold in the cyclotomic setting; see [CHK+23, Lem. 6.1] for a more general result), in which case one has

$$\chi_t^\pm(\Gamma, E_i) = |\xi_p^{\pm,*}(E_i)|_p^{-1}$$

(see e.g. [Zer09, Lem. 2.11]), where $\xi_p^{\pm,*}(E_i)$ is the leading coefficient of a characteristic power series for $\mathcal{X}^\pm(E_i/\mathbb{Q}_\infty)$, and $|\cdot|_p$ denotes the p-adic absolute value on $\mathbb{Q}_p$ with $|p|_p = 1/p$. Thus in particular [RS23, Thm. 5.5] (for at least one of the signs $\pm$) becomes a congruence relation mod p between the arithmetic invariants appearing in Theorem A.

In a similar vein, as a consequence of Theorem A, [KR21, Thm. 3.16] (for at least one of the signs $\pm$) now holds unconditionally.

1.2. **Outline of the proof.** In [PR93a], Perrin-Riou proved a p-adic Birch–Swinnerton-Dyer formula for a certain arithmetic p-adic L-function

$$\mathcal{F}_p^{\mathrm{PR}} \in D_p(E) \otimes_{\mathbb{Q}_p} \mathcal{H},$$

where $\mathcal{H} \subset \mathbb{Q}_p[[X]]$ is the ring of power series convergent in the p-adic open unit disk. A term in her leading coefficient formula is a p-adic regulator

$$(1-\varphi)^2 \mathrm{Reg}_p^{\mathrm{PR}} \in D_p(E) \tag{1.1}$$

where φ is the Frobenius operator. Building on a result of Lei [Lei11] expressing Kobayashi's signed Coleman maps in terms of Perrin-Riou's work [PR94], we extract from $\mathcal{F}_p^{\mathrm{PR}}$ two signed power series $\mathcal{F}_p^\pm \in \mathbb{Z}_p[[X]]$. By direct computation of the coordinates of (1.1) relative to a certain basis (ν_-, ν_+) of $D_p(E)$ on the one hand, and of the same coordinates of the leading coefficient $\mathcal{F}_p^{\mathrm{PR},*} \in D_p(E)$ of $\mathcal{F}_p^{\mathrm{PR}}$ on the other hand, from Perrin-Riou's formula we arrive at expressions for the order of vanishing and the leading coefficient of $\mathcal{F}_p^\pm$ agreeing with those in Theorem A for the characteristic power series $\xi_p^\pm$. We note here that similar computations (that in fact served as the original motivation for this note)

were performed by Sprung [Spr15] in his study of p-adic analogues of the Birch–Swinnerton-Dyer conjecture for the signed (or rather, $\sharp/\flat$-) p-adic L-functions constructed in [Spr12]. Finally, from an application of global duality we show that $\mathcal{F}_p^{\pm}$ generates the characteristic ideal of $\mathcal{X}^{\pm}(E/\mathbb{Q}_\infty)$.

1.3. **Acknowledgements.** We would like to dedicate this note to the memory of Prof. John Coates. It is a pleasure to thank Professors Ye Tian, Yichao Tian, and Xin Wan for the opportunity to make this small contribution to a special issue honoring such a great mathematician. We also thank Anwesh Ray and Debanjana Kundu for their comments on the topic of this note, and Antonio Lei for bringing [RS23] to our attention.

2. A formula of Perrin-Riou

In this section we recall a p-adic Birch–Swinnerton-Dyer formula for arithmetic p-adic L-functions established in [PR93a].

2.1. **Dieudonné modules.** Let $E/\mathbb{Q}$ be an elliptic curve, and p an odd prime of good reduction for E. Let

$$D_p(E) := \mathbb{Q}_p \otimes_{\mathbb{Q}} \mathrm{H}^1_{\mathrm{dR}}(E/\mathbb{Q})$$

denote the Dieudonné module of E. This is a 2-dimensional $\mathbb{Q}_p$-vector space equipped with a Frobenius operator φ, a Hodge filtration $D_p(E) \supset \mathrm{Fil}^0 D_p(E) \supset 0$, with $\mathrm{Fil}^0 D_p(E)$ spanned by the class of a Néron differential $\omega_E \in \Omega_{E/\mathbb{Z}}$, and a non-degenerate alternating pairing

$$[\cdot,\cdot]_{\mathrm{dR}} : D_p(E) \times D_p(E) \to \mathbb{Q}_p.$$

The operator φ has characteristic polynomial $x^2 - \frac{a_p}{p}x + \frac{1}{p}$, where $a_p := p + 1 - \#E(\mathbb{F}_p)$.

2.2. **Arithmetic p-adic L-function.** Let T be the p-adic Tate module of E, and put $V = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T$. As in the Introduction, let Γ be the Galois group of the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty/\mathbb{Q}$, which we shall often identify with the Galois group of the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_{p,\infty}/\mathbb{Q}_p$, and let $\Lambda = \mathbb{Z}_p[[\Gamma]]$ be the cyclotomic Iwasawa algebra, often identified with the 1-variable power series ring $\mathbb{Z}_p[[X]]$ via $\gamma = 1 + X$ upon the choice of a fixed topological generator $\gamma \in \Gamma$. For each $n \geq 0$, let $\mathbb{Q}_n$ (resp. $\mathbb{Q}_{p,n}$) be the unique subextension of $\mathbb{Q}_\infty$ (resp. $\mathbb{Q}_{p,\infty}$) of degree p^n over $\mathbb{Q}$ (resp. $\mathbb{Q}_p$).

For $h \geq 0$, let

$$\mathcal{H}_h = \left\{ \sum_{n\geq 0} c_n X^n \in \mathbb{Q}_p[[X]] \,\Big|\, \lim_{n\to\infty} \frac{|c_n|_p}{n^h} = 0 \right\},$$

where $|\cdot|_p$ denotes the p-adic absolute value on $\mathbb{Q}_p$ with the standard normalization $|p|_p = 1/p$, and put $\mathcal{H} = \bigcup_{h\geq 0} \mathcal{H}_h$ and $\mathcal{H}(\Gamma) = \{f(\gamma - 1) \,|\, f \in \mathcal{H}\}$. Write

$$\mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_{p,\infty}, T) := \varprojlim_n \mathrm{H}^1(\mathbb{Q}_{p,n}, T)$$

for the Iwasawa cohomology of T, and put $\mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_{p,\infty}, V) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_{p,\infty}, T)$.

We begin by recalling Perrin-Riou's big exponential map, which we state below in a rather rough form (see e.g. [PR93a, §1] for a more precise statement). The Weil pairing gives a natural identification $V \simeq V^*(1) := \mathrm{Hom}_{\mathbb{Q}_p}(V, \mathbb{Q}_p(1))$ (so in particular, $\mathbf{D}_{\mathrm{dR}}(V^*(1)) := (V^*(1) \otimes_{\mathbb{Q}_p} \mathbf{B}_{\mathrm{dR}})^{G_{\mathbb{Q}_p}} \simeq D_p(E)$ by the comparison isomorphism), but in the following we shall nonetheless keep the distinction between the two.

Theorem 2.2.1. *There exists an injective Λ-module homomorphism*

$$\Omega_{V^*(1)} : \Lambda \otimes_{\mathbb{Z}_p} \mathbf{D}_{\mathrm{dR}}(V^*(1)) \to \mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_{p,\infty}, V^*(1)) \otimes_{\mathbb{Q}_p} \mathcal{H}(\Gamma)$$

interpolating $\exp_{\mathbb{Q}_{p,n}, V^*(1)}$ *for all $n \geq 0$.*

Proof. This follows by taking $h = 1$ and $j = 0$ in [PR94, §3.2.3] (see also [PR93a, Thm. 1.3]. □

For any $\eta \in \mathbf{D}_{\mathrm{dR}}(V^*(1))$, the map $\Omega_{V^*(1)}$ may be evaluated at $\eta\otimes(1+X)$. Given $\mathbf{z} \in \mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_{p,\infty}, V)$, we thus define

$$\mathscr{L}_{\mathbf{z}} : \mathbf{D}_{\mathrm{dR}}(V^*(1)) \to \mathcal{H}(\Gamma), \quad \eta \mapsto \left\langle \Omega_{V^*(1)}(\eta \otimes (1+X)), \mathbf{z} \right\rangle_{\mathbb{Q}_{p,\infty}},$$

where $\langle \cdot, \cdot \rangle_{\mathbb{Q}_{p,\infty}} : \mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_{p,\infty}, V^*(1)) \times \mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_{p,\infty}, V) \to \Lambda$ is Perrin-Riou's Λ-adic Tate pairing (see e.g. [PR93a, §2.1.2]), given by

$$\langle \mathbf{x}, \mathbf{y} \rangle_{\mathbb{Q}_{p,\infty}} := \left(\sum_{\sigma \in \Gamma_n} \langle x_n^{\sigma^{-1}}, y_n \rangle_{\mathbb{Q}_{p,n}} \cdot \sigma \right)_n$$

for $\mathbf{x} = (x_n)_n$, $\mathbf{y} = (y_n)_n$ and $\Gamma_n = \mathrm{Gal}(\mathbb{Q}_{p,n}/\mathbb{Q}_p)$.

In the following, we shall view $\mathscr{L}_{\mathbf{z}}$ as an element

$$\mathscr{L}_{\mathbf{z}} \in D_p(E) \otimes_{\mathbb{Q}_p} \mathcal{H}(\Gamma)$$

using the canonical isomorphism $\mathrm{Hom}_{\mathbb{Q}_p}(\mathbf{D}_{\mathrm{dR}}(V^*(1)), \mathcal{H}(\Gamma)) \simeq \mathbf{D}_{\mathrm{dR}}(V) \otimes_{\mathbb{Q}_p} \mathcal{H}(\Gamma)$ induced by $[\cdot,\cdot]_{\mathrm{dR}}$ and the identification $\mathbf{D}_{\mathrm{dR}}(V) \simeq D_p(E)$ arising from the comparison isomorphsm.

Let $\mathrm{Sel}^{\mathrm{str}}_{p^\infty}(E/\mathbb{Q}_n)$ be the *strict Selmer group* defined by

$$\mathrm{Sel}^{\mathrm{str}}_{p^\infty}(E/\mathbb{Q}_n) := \ker \left\{ \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_n) \xrightarrow{\mathrm{res}_p} E(\mathbb{Q}_{p,n}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \right\},$$

and put $\mathrm{Sel}^{\mathrm{str}}_{p^\infty}(E/\mathbb{Q}_\infty) = \varinjlim_n \mathrm{Sel}^{\mathrm{str}}_{p^\infty}(E/\mathbb{Q}_n)$. For any finite set of primes S containing p and ∞, let $\mathbb{Q}^S$ denote the maximal extension of $\mathbb{Q}$ unramified outside S, and put

$$\mathbb{H}^1(T) := \varprojlim_n \mathrm{H}^1(\mathrm{Gal}(\mathbb{Q}^S/\mathbb{Q}_n), T).$$

(This is easily checked to be independent of S; see e.g [PR93a, p. 983].)

By Kato's work [Kat04], $\mathrm{Sel}^{\mathrm{str}}_{p^\infty}(E/\mathbb{Q}_\infty)$ is Λ-cotorsion and $\mathbb{H}^1(T)$ is torsion-free of Λ-rank 1.

Definition 2.2.2. Let $\mathbf{z} \in \mathbb{H}^1(T)$ be a nonzero element, and put

$$\mathcal{F}_p^{\mathrm{PR}} := \mathscr{L}_{\mathbf{z}_p} \cdot \frac{g_{\mathrm{str}}}{h_{\mathbf{z}}} \in D_p(E)[[X]],$$

where $\mathbf{z}_p = \mathrm{res}_p(\mathbf{z})$ denotes the image of $\mathbf{z}$ under the restriction map $\mathbb{H}^1(T) \to \mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_{p,\infty}, T)$ and g_{str} (resp. $h_{\mathbf{z}}$) is a characteristic power series for $\mathrm{Sel}^{\mathrm{str}}_{p^\infty}(E/\mathbb{Q}_\infty)^\vee$ (resp. $\mathbb{H}^1(T)/(\mathbf{z})$).

We note that $\mathcal{F}_p^{\mathrm{PR}}$ gives a generator of the Λ-module of *arithmetic p-adic L-functions* as introduced in Perrin-Riou's work (see e.g. [PR93a, §3.4.3] and [PR03, §3.1]).

2.3. **p-adic regulators.** Let

$$y^2 - a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

be a minimal Weierstrass model for E. Take $\omega_E = \frac{dx}{2y+a_1x+a_3}$ and put $\eta = x\omega_E$; then the pair (ω_E, η) forms a basis for $D_p(E)$.

For each $\nu \in D_p(E)$, we let h_ν be the quadratic form on $E(\mathbb{Q})$ defined as in [BPR93]. In particular, $h_\nu(P) = -\log_{\omega_E}(P)^2$, where $\log_{\omega_E}$ is the logarithm on $E(\mathbb{Q})$ associated to ω_E, h_η is Bernardi's p-adic height using p-adic σ-functions [Ber81], and h_ν for an arbitrary $\nu = a\omega_E + b\eta \in D_p(E)$ is defined by linearity as $ah_{\omega_E} + bh_\eta$.

Definition 2.3.1. Let $r = \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q})$, and let Reg_ν denote the discriminant of the quadratic form $\langle P, Q \rangle_\nu := h_\nu(P+Q) - h_\nu(P) - h_\nu(Q)$ on $E(\mathbb{Q})$, i.e.

$$\mathrm{Reg}_\nu = \frac{\det(\langle P_i, P_j \rangle_\nu)}{[E(\mathbb{Q}) : \sum_{i=1}^r \mathbb{Z}P_i]^2}, \tag{2.1}$$

where $P_1, \ldots, P_r$ is any system of r points in $E(\mathbb{Q})$ giving a basis of $E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Lemma 2.3.2. *Suppose $r = \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) \geq 1$. Then there exists a unique $\mathrm{Reg}_p^{\mathrm{PR}} \in D_p(E)$ such that*

$$\big[\mathrm{Reg}_p^{\mathrm{PR}}, \nu\big]_{\mathrm{dR}} = \widetilde{\mathrm{Reg}}_\nu, \quad \textit{where} \quad \widetilde{\mathrm{Reg}}_\nu := \frac{\mathrm{Reg}_\nu}{[\omega_E, \nu]_{\mathrm{dR}}^{r-1}}$$

for all $\nu \notin \mathrm{Fil}^0 D_p(E)$.

Proof. This is shown in [PR03, Lem. 2.6] (whose statement is missing the factor $[\omega_E, \nu]^{r-1}$ as noted in [SW13, Lem. 4.2]). □

As in the Introduction, let $(E(\mathbb{Q}) \otimes \mathbb{Z}_p)_0 \subset E(\mathbb{Q}) \otimes \mathbb{Z}_p$ be the strict Mordell–Weil group.

Definition 2.3.3. Write $\mathrm{Reg}_p^{\mathrm{str}}$ for the discriminant of the bilinear (p-adic height) pairing associated to the restriction to $(E(\mathbb{Q}) \otimes \mathbb{Z}_p)_0$ of the normalized quadratic form

$$h_{\nu/[\omega_E,\nu]_{\mathrm{dR}}} = h_\nu / [\omega_E, \nu]_{\mathrm{dR}}$$

for any $\nu \notin \mathrm{Fil}^0 D_p(E)$ (this is independent of ν).

2.4. **Perrin-Riou's formula.** The following key result is a p-adic analogue of the Birch–Swinnerton-Dyer conjecture for the arithmetic p-adic L-function $\mathcal{F}_p^{\mathrm{PR}}$.

Theorem 2.4.1. *Let $E/\mathbb{Q}$ be an elliptic curve with good supersingular reduction at an odd prime p, and put $r = \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q})$. Then:*

(i) *$\mathcal{F}_p^{\mathrm{PR}}$ vanishes to order at least r at $X = 0$.*
(ii) *If $Ш(E/\mathbb{Q})[p^\infty]$ is finite and $\mathrm{Reg}_p^{\mathrm{str}} \neq 0$ then equality holds in* (i)*, and writing*

$$\mathcal{F}_p^{\mathrm{PR},(r)} := X^{-r} \mathcal{F}_p^{\mathrm{PR}} \in D_p(E)[[X]]$$

we have that $\mathcal{F}_p^{\mathrm{PR},*} := \mathcal{F}_p^{\mathrm{PR},(r)}(0) \in D_p(E)$ satisfies the equality up to a p-adic unit

$$\mathcal{F}_p^{\mathrm{PR},*} \ \sim_p \ (\log_p \kappa(\gamma))^{-r} \cdot (1-\varphi)^2 \mathrm{Reg}_p^{\mathrm{PR}} \cdot \frac{\#Ш(E/\mathbb{Q})[p^\infty] \cdot \mathrm{Tam}(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{\mathrm{tors}})^2}.$$

Proof. This is shown in Propositions 3.4.5 and 3.4.6 in [PR93a] (see also [PR03, Thm. 3.1]). □

Remark 2.4.2. A result similar to Theorem 2.4.1 is obtained in [PR00] for much more general p-adic representations V.

3. Perrin-Riou's big exponential and signed Coleman maps

By Kobayashi's definition in [Kob03], the local conditions at p defining the signed Selmer groups $\mathrm{Sel}_{p^\infty}^{\pm}(E/\mathbb{Q}_n)$ are given by $E^{\pm}(\mathbb{Q}_{p,n}) \otimes \mathbb{Q}_p/\mathbb{Z}_p = \ker(\mathrm{Col}_n^{\pm})^{\perp}$, where the superscript $\perp$ denotes the orthogonal complement under the local Tate duality

$$\mathrm{H}^1(\mathbb{Q}_{p,n}, E[p^\infty]) \times \mathrm{H}^1(\mathbb{Q}_{p,n}, T) \to \mathbb{Q}_p/\mathbb{Z}_p$$

and $\mathrm{Col}_n^{\pm} : \mathrm{H}^1(\mathbb{Q}_{p,n}, T) \to \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}_{p,n}/\mathbb{Q}_p)]$ are *signed Coleman maps* constructed in [Kob03] using Honda's theory of formal groups. In this section, we recall a result of Lei [Lei11] giving an independent construction of Kobayashi's

$$\mathrm{Col}^{\pm} := \varprojlim_n \mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_{p,\infty}, T) \to \Lambda$$

in terms of the map $\Omega_{V^*(1)}$ of Theorem 2.2.1.

3.1. **Logarithm matrix.** Put

$$\log_p^+ = \frac{1}{p}\prod_{m=1}^{\infty}\frac{\Phi_{2m}(1+X)}{p}, \qquad \log_p^- = \frac{1}{p}\prod_{m=1}^{\infty}\frac{\Phi_{2m-1}(1+X)}{p},$$

where $\Phi_n(X) = \sum_{i=1}^{p-1} X^{p^{n-1}i}$ is the p^n-th cyclotomic polynomial.

Definition 3.1.1. Let $\alpha, \beta \in \{\pm\sqrt{-p}\}$ be the roots of $x^2 - a_p x + p$ (recall that we assume $a_p = 0$), and define the *logarithm matrix* $M_{\log} \in M_{2\times 2}(\mathcal{H})$ by

$$M_{\log} := \begin{pmatrix} \log_p^+ & \log_p^+ \\ \alpha\log_p^- & \beta\log_p^- \end{pmatrix}.$$

3.2. **A result of Lei.** Given $\eta \in \mathbf{D}_{\mathrm{dR}}(V^*(1))$, we define the *Coleman map*

$$\mathrm{Col}_\eta : \mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_{p,\infty}, V) \to \mathcal{H}(\Gamma) \tag{3.1}$$

by $\mathbf{z} \mapsto \left\langle \Omega_{V^*(1)}(\eta \otimes (1+X)), \mathbf{z}\right\rangle_{\mathbb{Q}_{p,\infty}}$. Thus, note that $\mathrm{Col}_\eta(\mathbf{z}) = \mathscr{L}_{\mathbf{z}}(\eta)$ by definition.

Theorem 3.2.1. *Let $\eta_\alpha, \eta_\beta \in \mathbf{D}_{\mathrm{dR}}(V^*(1)) \simeq D_p(E)$ be the unique vectors satisfying*

$$\varphi(\eta_\alpha) = \alpha^{-1}\eta_\alpha, \qquad \varphi(\eta_\beta) = \beta^{-1}\eta_\beta, \qquad [\eta_\alpha, \omega_E]_{\mathrm{dR}} = [\eta_\beta, \omega_E]_{\mathrm{dR}} = 1.$$

Then for any $\mathbf{z} \in \mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_{p,\infty}, T)$ we have the decomposition

$$(\mathrm{Col}_{\eta_\beta}(\mathbf{z}), \mathrm{Col}_{\eta_\alpha}(\mathbf{z})) = (\mathrm{Col}^-(\mathbf{z}), \mathrm{Col}^+(\mathbf{z}))\, M_{\log}, \tag{3.2}$$

where $M_{\log} \in M_{2\times 2}(\mathcal{H}(\Gamma))$ is the logarithm matrix of Definition 3.1.1 with $X = \gamma - 1$.

Proof. The existence of unique η_α, η_β satisfying the conditions in the statement is shown in [Kat04, Thm. 16.6], while the proof of the decomposition (3.2) is given in [Lei11, §3.4.2]. More precisely, the Coleman maps $\mathrm{Col}_{\eta^\pm}$ of (3.1) associated to the vectors $\eta^- := \frac{\beta\eta_\alpha - \alpha\eta_\beta}{\beta-\alpha}$, $\eta^+ := \frac{\eta_\beta - \eta_\alpha}{\beta-\alpha}$ are shown to be divisible by $\log_p^\pm$, respectively[1], upon evaluation at any $\mathbf{z} \in \mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_{p,\infty}, T)$. That the maps

$$\mathrm{Col}^\pm : \mathbf{z} \mapsto \mathrm{Col}_{\eta^\pm}(\mathbf{z})/\log_p^\pm$$

satisfy the relation in the statement is then clear; and that they agree with the signed Coleman maps $\mathrm{Col}^\pm$ in [Kob03] follows from a relation between both constructions and the pairings P_n introduced by Kurihara [Kur02] (see also [Lei11, Rem. 3.16]). □

Remark 3.2.2. Letting $f \in S_2(\Gamma_0(N))$ be the newform associated to E by modularity, note that our vector $\eta_\alpha \in \mathbf{D}_{\mathrm{dR}}(V^*(1))$ corresponds to $\eta_\beta \in \mathbf{D}_{\mathrm{dR}}(V_f) \simeq \mathbf{D}_{\mathrm{dR}}(V^*)$ (with Frobenius eigenvalue β) in Lei's notation; and likewise our η_β corresponds to η_α in [Lei11]. In particular, by Kato's reciprocity law (as recalled in [*op. cit.*, Thm. 3.10]), Kato's zeta element $\mathbf{z}^{\mathrm{Kato}}$ satisfies

$$\mathrm{Col}_{\eta_\beta}(\mathbf{z}^{\mathrm{Kato}}) = L_{p,\alpha},$$

where $L_{p,\alpha}$ denotes the p-adic L-function of [MTT86] associated to f and the allowable root α; and likewise $\mathrm{Col}_{\eta_\alpha}(\mathbf{z}^{\mathrm{Kato}}) = L_{p,\beta}$.

4. Coordinate computations

The main result of this section is the computation of the coordinates of the modified Perrin-Riou's p-adic regulator appearing in Theorem 2.4.1 relative to an ordered basis (ν_-, ν_+) of $D_p(E)$ motivated by the decomposition in Theorem 3.2.1.

[1] Note that for consistency with [Kob03] our signs are opposite to [Lei11].

4.1. **Dual bases.** Recall that $\omega_E \in D_p(E)$ denotes the class of a fixed Néron differential.

Lemma 4.1.1. *Put*

$$\nu_\alpha := \frac{1}{2}\left(\omega_E - \beta\varphi(\omega_E)\right), \qquad \nu_\beta := \frac{1}{2}\left(\omega_E - \alpha\varphi(\omega_E)\right).$$

Let $\eta_\alpha, \eta_\beta \in \mathbf{D}_{\mathrm{dR}}(V^*(1)) \simeq D_p(E)$ be as in Theorem 3.2.1. Then (ν_α, ν_β) and $(\eta_\beta, \eta_\alpha)$ are dual bases of $D_p(E)$ under $[\cdot,\cdot]_{\mathrm{dR}}$, in the sense that

$$[\eta_\alpha, \nu_\alpha]_{\mathrm{dR}} = [\eta_\beta, \nu_\beta]_{\mathrm{dR}} = 0, \qquad [\eta_\alpha, \nu_\beta]_{\mathrm{dR}} = [\eta_\beta, \nu_\alpha]_{\mathrm{dR}} = 1.$$

Proof. From the relations $\varphi^2 = 1/p$, $\alpha + \beta = 0$, and $\alpha\beta = p$ we readily see that $\varphi(\nu_\alpha) = \alpha^{-1}\nu_\alpha$ and $\varphi(\nu_\beta) = \beta^{-1}\nu_\beta$, which implies the first two equalities in the statement by the alternating property of $[\cdot,\cdot]_{\mathrm{dR}}$. On the other hand, noting that the classes η_α and η_β are necessarily multiples of ν_α and ν_β, respectively, from the defining relations $[\eta_\alpha, \omega_E]_{\mathrm{dR}} = [\eta_\beta, \omega_E]_{\mathrm{dR}} = 1$ in Theorem 3.2.1 we find

$$\eta_\alpha = \frac{-1}{[\beta\varphi(\omega_E), \omega_E]_{\mathrm{dR}}}(\omega_E - \beta\varphi(\omega_E)), \qquad \eta_\beta = \frac{-1}{[\alpha\varphi(\omega_E), \omega_E]_{\mathrm{dR}}}(\omega_E - \alpha\varphi(\omega_E)),$$

and this yields the equalities $[\eta_\alpha, \nu_\beta]_{\mathrm{dR}} = [\eta_\beta, \nu_\alpha]_{\mathrm{dR}} = 1$. □

Lemma 4.1.2. *In terms of the basis (ν_α, ν_β) of $D_p(E)$ in Lemma 4.1.1, we have*

$$\mathrm{Reg}_p^{\mathrm{PR}} = \frac{\mathrm{Reg}_{\nu_\beta}}{[\omega_E, \nu_\beta]_{\mathrm{dR}}^r}\,\nu_\alpha + \frac{\mathrm{Reg}_{\nu_\alpha}}{[\omega_E, \nu_\alpha]_{\mathrm{dR}}^r}\,\nu_\beta.$$

Proof. Writing $\mathrm{Reg}_p^{\mathrm{PR}} = a\nu_\alpha + b\nu_\beta$, using the defining property of $\mathrm{Reg}_p^{\mathrm{PR}}$, the relation $\nu_\alpha + \nu_\beta = \omega_E$, and the fact that $[\cdot,\cdot]_{\mathrm{dR}}$ is alternating, we find

$$\widetilde{\mathrm{Reg}}_{\nu_\alpha} = \left[\mathrm{Reg}_p^{\mathrm{PR}}, \nu_\alpha\right]_{\mathrm{dR}} = [b\nu_\beta, \nu_\alpha]_{\mathrm{dR}} = b[\omega_E, \nu_\alpha]_{\mathrm{dR}},$$

and so $b = \widetilde{\mathrm{Reg}}_{\nu_\alpha}/[\omega_E, \nu_\alpha]_{\mathrm{dR}}$ as claimed. Similarly, we find $a = \widetilde{\mathrm{Reg}}_{\nu_\beta}/[\omega_E, \nu_\beta]_{\mathrm{dR}} = \mathrm{Reg}_{\nu_\beta}/[\omega_E, \nu_\beta]_{\mathrm{dR}}^r$, whence the result. □

4.2. **The modified regulator $(1-\varphi)^2\mathrm{Reg}_p^{\mathrm{PR}}$ in coordinates.** The main result of this section is Proposition 4.2.4. In the context of the analytic p-adic L-functions of [Spr12], similar computations were performed by Sprung [Spr15], whose notations we largely follow.

Definition 4.2.1. Put $Z_{\log} := M_{\log}|_{X=0} = \frac{1}{p}\left(\begin{smallmatrix} 1 & 1 \\ \alpha & \beta \end{smallmatrix}\right)$, and let $N_\pm, \nu_\pm \in D_p(E)$ be the vectors given by

$$(N_-, N_+) = (\nu_\beta, -\nu_\alpha)\begin{pmatrix} (1-\alpha^{-1})^2 & \\ & (1-\beta^{-1})^2 \end{pmatrix} Z_{\log}^{-1} \cdot \det(Z_{\log}), \qquad \begin{pmatrix} \nu_- \\ \nu_+ \end{pmatrix} = Z_{\log}\begin{pmatrix} \nu_\alpha \\ \nu_\beta \end{pmatrix}.$$

Note that the pair (ν_-, ν_+) is a basis of $D_p(E)$. We also note that the introduction of $N_\pm$ (resp. $\nu_\pm$) is motivated by the result of the computation in Proposition 4.2.4 (resp. the computation leading to (5.5)) below.

Lemma 4.2.2. *We have $N_\pm \notin \mathrm{Fil}^0 D_p(E)$.*

Proof. It suffices to show $[\omega_E, N_\pm]_{\mathrm{dR}} \neq 0$. Directly from the definition we have

$$(N_-, N_+) = \left((1-\alpha^{-1})^2\beta\nu_\beta + (1-\beta^{-1})^2\alpha\nu_\alpha, -(1-\alpha^{-1})^2\nu_\beta - (1-\beta^{-1})^2\nu_\alpha\right).$$

Thus from the relation $\omega_E = \nu_\alpha + \nu_\beta$ we obtain

$$[\omega_E, N_-]_{\mathrm{dR}} = \left((1-\alpha^{-1})^2\beta - (1-\beta^{-1})^2\alpha\right)[\omega_E, \nu_\beta]_{\mathrm{dR}} = \frac{2\alpha(p-1)}{-p} \cdot [\omega_E, \nu_\beta]_{\mathrm{dR}}; \tag{4.1}$$

and similarly,

$$[\omega_E, N_+]_{\mathrm{dR}} = \left((1-\beta^{-1})^2 - (1-\alpha^{-1})^2\right)[\omega_E, \nu_\beta]_{\mathrm{dR}} = \frac{4}{\alpha} \cdot [\omega_E, \nu_\beta]_{\mathrm{dR}}. \tag{4.2}$$

Since $[\omega_E, \nu_\beta]_{\mathrm{dR}} \neq 0$ by weak-admissibility of $D_p(E)$ (see e.g. [GM09, §3.2]) and the non-degeneracy of $[\cdot,\cdot]_{\mathrm{dR}}$, the result follows. □

Remark 4.2.3. From the definitions, we directly find $(N_+, N_-) = (\frac{1}{p}-1)\omega_E - 2\varphi(\omega_E), 2\omega_E + (1-p)\varphi(\omega_E))$ consistently with Lemma 4.2.2, but the above computations will be useful later.

Proposition 4.2.4. *Suppose $r = \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) \geq 1$. Then the coordinates (c_+, c_-) of $(1-\varphi)^2 \mathrm{Reg}_p^{\mathrm{PR}} \in D_p(E)$ with respect to the ordered basis (ν_+, ν_-) are given by*

$$(c_+, c_-) = \Big(2\,\frac{\mathrm{Reg}_{N_+}}{[\omega_E, N_+]_{\mathrm{dR}}^r}, (p-1)\,\frac{\mathrm{Reg}_{N_-}}{[\omega_E, N_-]_{\mathrm{dR}}^r}\Big).$$

Proof. We begin by noting that the association $\nu \mapsto \widetilde{\mathrm{Reg}}_\nu = \mathrm{Reg}_\nu / [\omega_E, \nu]_{\mathrm{dR}}^{r-1}$ is linear in $\nu \in D_p(E) \smallsetminus \mathrm{Fil}^0 D_p(E)$ (whenever defined), and by Lemma 4.2.2 and its proof the quantities $\widetilde{\mathrm{Reg}}_{\nu_\alpha}$, $\widetilde{\mathrm{Reg}}_{\nu_\beta}$, $\widetilde{\mathrm{Reg}}_{N_+}$, $\widetilde{\mathrm{Reg}}_{N_-}$ are all defined. Thus from the expression for $\mathrm{Reg}_p^{\mathrm{PR}}$ in Lemma 4.1.2 we obtain

$$\begin{aligned}
(1-\varphi)^2 \mathrm{Reg}_p^{\mathrm{PR}} &= \Big(\frac{\mathrm{Reg}_{\nu_\beta}}{[\omega_E, \nu_\beta]_{\mathrm{dR}}^r}, \frac{\mathrm{Reg}_{\nu_\alpha}}{[\omega_E, \nu_\alpha]_{\mathrm{dR}}^r}\Big) \begin{pmatrix} (1-\alpha^{-1})^2 & \\ & (1-\beta^{-1})^2 \end{pmatrix} \begin{pmatrix} \nu_\alpha \\ \nu_\beta \end{pmatrix} \\
&= \Big(\frac{\widetilde{\mathrm{Reg}}_{\nu_\beta}}{[\omega_E, \nu_\beta]_{\mathrm{dR}}}, \frac{\widetilde{\mathrm{Reg}}_{\nu_\alpha}}{[\omega_E, \nu_\alpha]_{\mathrm{dR}}}\Big) \begin{pmatrix} (1-\alpha^{-1})^2 & \\ & (1-\beta^{-1})^2 \end{pmatrix} Z_{\log}^{-1} \begin{pmatrix} \nu_- \\ \nu_+ \end{pmatrix} \\
&= \Big(\frac{\widetilde{\mathrm{Reg}}_{N_-}}{[\omega_E, \nu_\beta]_{\mathrm{dR}}}, \frac{\widetilde{\mathrm{Reg}}_{N_+}}{[\omega_E, \nu_\beta]_{\mathrm{dR}}}\Big) \begin{pmatrix} \nu_- \\ \nu_+ \end{pmatrix} \frac{p}{\beta - \alpha},
\end{aligned}$$

using the relations $\widetilde{\mathrm{Reg}}_{-\nu_\alpha} = -\widetilde{\mathrm{Reg}}_{\nu_\alpha}$ and $[\omega_E, \nu_\beta]_{\mathrm{dR}} = -[\omega_E, \nu_\alpha]_{\mathrm{dR}}$ for the last equality. In light of (4.1) and (4.2), this yields the result. □

5. Proof of the main result

As in the Introduction, we denote by $\mathrm{Reg}_p^\pm \in \mathbb{Q}_p$ the p-adic regulator of Definition 2.3.1 associated to $h_{N_\pm/[\omega_E, N_\pm]_{\mathrm{dR}}}$, so

$$\mathrm{Reg}_p^\pm := \mathrm{Reg}_{N_\pm/[\omega_E, N_\pm]_{\mathrm{dR}}} = \frac{\mathrm{Reg}_{N_\pm}}{[\omega_E, N_\pm]_{\mathrm{dR}}^r},$$

where $r = \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q})$.

5.1. Signed arithmetic p-adic L-functions.

For $\mathbf{z} \in \mathbb{H}^1(T)$ any non-torsion element, we put

$$\mathcal{F}_p^\pm := \mathrm{Col}^\pm(\mathbf{z}_p) \cdot \frac{g_{\mathrm{str}}}{h_{\mathbf{z}}} \in \mathbb{Z}_p[[X]], \tag{5.1}$$

where g_{str} and $h_{\mathbf{z}}$ are as in Definition 2.2.2. The following is the main result of this note.

Theorem 5.1.1. *Let $E/\mathbb{Q}$ be an elliptic curve with good supersingular reduction at an odd prime p with $a_p = 0$. Put*

$$r := \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}),$$

and suppose $r \geq 1$. Then:

(i) $\varrho := \min\{\mathrm{ord}_X(\mathcal{F}_p^+), \mathrm{ord}_X(\mathcal{F}_p^-)\} \geq r$.

(ii) *If $Ш(E/\mathbb{Q})[p^\infty]$ is finite and $\mathrm{Reg}_p^{\mathrm{str}} \neq 0$, then equality holds in* (i) *and the leading coefficient $(\mathcal{F}_p^{+,*}, \mathcal{F}_p^{-,*})$ of the vector $(\mathcal{F}_p^+, \mathcal{F}_p^-) \in \mathbb{Z}_p[[X]]^{\oplus 2}$ is given up to a p-adic unit by*

$$(\mathcal{F}_p^{+,*}, \mathcal{F}_p^{-,*}) \;\sim_p\; (\log_p \kappa(\gamma))^{-r} \cdot (\mathrm{Reg}_p^+, \mathrm{Reg}_p^-) \cdot \frac{\#Ш(E/\mathbb{Q})[p^\infty] \cdot \mathrm{Tam}(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{\mathrm{tors}})^2}.$$

Proof. We begin by noting that by Theorem 3.2.1 and Lemma 4.1.1, we can rewrite the arithmetic p-adic L-function $\mathcal{F}_p^{\mathrm{PR}} \in D_p(E)[[X]]$ of Definition 2.2.2 in matrix form as

$$\mathcal{F}_p^{\mathrm{PR}} = (\mathcal{F}_p^-, \mathcal{F}_p^+) M_{\log} \begin{pmatrix} \nu_\alpha \\ \nu_\beta \end{pmatrix}. \tag{5.2}$$

In particular, since $\log_p^{\pm}|_{X=0} \neq 0$, from (5.2) and the product rule we readily find

$$\frac{d^t}{dX^t}\mathcal{F}_p^{\mathrm{PR}}\Big|_{X=0} = \Big(\frac{d^t}{dX^t}\mathcal{F}_p^-\Big|_{X=0}, \frac{d^t}{dX^t}\mathcal{F}_p^+\Big|_{X=0}\Big) Z_{\log} \begin{pmatrix} \nu_\alpha \\ \nu_\beta \end{pmatrix} \tag{5.3}$$

for all $t \geq 0$. Since the matrix $Z_{\log}$ is invertible, this shows that

$$\mathrm{ord}_X(\mathcal{F}_p^{\mathrm{PR}}) = \varrho, \tag{5.4}$$

and therefore the proof of part (i) follows from Theorem 2.4.1(i). For the proof of part (ii), suppose $Ш(E/\mathbb{Q})[p^\infty]$ is finite and $\mathrm{Reg}_p^{\mathrm{str}} \neq 0$; then $\varrho = r$ by (5.4) and Theorem 2.4.1(ii). Now put

$$\mathcal{F}_p^{\mathrm{PR},(r)} := X^{-r}\mathcal{F}_p^{\mathrm{PR}} \in D_p(E)[[X]], \qquad \mathcal{F}_p^{\pm,(r)} := X^{-r}\mathcal{F}_p^{\pm} \in \mathbb{Z}_p[[X]],$$

and note that (5.3) yields the middle equality in the chain

$$\mathcal{F}_p^{\mathrm{PR},*} = \mathcal{F}_p^{\mathrm{PR},(r)}(0) = \big(\mathcal{F}_p^{-,(r)}(0), \mathcal{F}_p^{+,(r)}(0)\big) \begin{pmatrix} \nu_- \\ \nu_+ \end{pmatrix} = \big(\mathcal{F}_p^{-,*}, \mathcal{F}_p^{+,*}\big) \begin{pmatrix} \nu_- \\ \nu_+ \end{pmatrix}. \tag{5.5}$$

On the other hand, by Theorem 2.4.1(ii) and Proposition 4.2.4 we have that the coordinates (d_+, d_-) of $\mathcal{F}_p^{\mathrm{PR},*}$ with respect to (ν_+, ν_-) are given up to a p-adic unit by

$$(d_+, d_-) \ \sim_p \ (\log_p \kappa(\gamma))^{-r} \cdot (\mathrm{Reg}_p^+, \mathrm{Reg}_p^-) \cdot \frac{\#Ш(E/\mathbb{Q})[p^\infty] \cdot \mathrm{Tam}(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{\mathrm{tors}})^2},$$

which together with (5.5) concludes the proof of part (ii). □

5.2. **Proof of Theorem A.**

Proof of Theorem A. In view of Theorem 5.1.1, it suffices to show that the power series $\mathcal{F}_p^{\pm} \in \mathbb{Z}_p[[X]]$ introduced in (5.1) generates the characteristic ideal of $\mathcal{X}^{\pm}(E/\mathbb{Q}_\infty)$.

As explained in [Lei11, §6.4], Poitou–Tate duality gives rise to the four-term exact sequence

$$0 \to \mathbb{H}^1(T) \to \mathrm{Im}(\mathrm{Col}^{\pm}) \to \mathcal{X}^{\pm}(E/\mathbb{Q}_\infty) \to \mathrm{Sel}_{p^\infty}^{\mathrm{str}}(E/\mathbb{Q}_\infty)^\vee \to 0.$$

This induces

$$0 \to \frac{\mathbb{H}^1(T)}{(\mathbf{z})} \to \frac{\mathrm{Im}(\mathrm{Col}^{\pm})}{(\mathrm{Col}^{\pm}(\mathbf{z}_p))} \to \mathcal{X}^{\pm}(E/\mathbb{Q}_\infty) \to \mathrm{Sel}_{p^\infty}^{\mathrm{str}}(E/\mathbb{Q}_\infty)^\vee \to 0. \tag{5.6}$$

Since the Λ-linear maps $\mathrm{Col}^{\pm}$ have pseudo-null cokernel by [Kob03, Thm. 6.2], we see that the second term in (5.6) has characteristic ideal generated by $\mathrm{Col}^{\pm}(\mathbf{z}_p)$, and so the fact that $\mathcal{F}_p^{\pm}$ has the desired property follows by multiplicativity. □

References

[Ber81] Dominique Bernardi. Hauteur p-adique sur les courbes elliptiques. In *Seminar on Number Theory, Paris 1979–80*, volume 12 of *Progr. Math.*, pages 1–14. Birkhäuser, Boston, MA, 1981.

[BPR93] Dominique Bernardi and Bernadette Perrin-Riou. Variante p-adique de la conjecture de Birch et Swinnerton-Dyer (le cas supersingulier). *C. R. Acad. Sci. Paris Sér. I Math.*, 317(3):227–232, 1993.

[CHK+23] Francesc Castella, Chi-Yun Hsu, Debanjana Kundu, Yu-Sheng Lee, and Zheng Liu. Derived p-adic heights and the leading coefficient of the Bertolini–Darmon–Prasanna p-adic L-functions. 2023. preprint, arXiv:2308.10474.

[GM09] Eknath Ghate and Ariane Mézard. Filtered modules with coefficients. *Trans. Amer. Math. Soc.*, 361(5):2243–2261, 2009.

[Gre99] Ralph Greenberg. Iwasawa theory for elliptic curves. In *Arithmetic theory of elliptic curves (Cetraro, 1997)*, volume 1716 of *Lecture Notes in Math.*, pages 51–144. Springer, Berlin, 1999.

[Kat04] Kazuya Kato. p-adic Hodge theory and values of zeta functions of modular forms. Number 295, pages ix, 117–290. 2004. Cohomologies p-adiques et applications arithmétiques. III.

[Kim13] Byoung Du Kim. The plus/minus Selmer groups for supersingular primes. *J. Aust. Math. Soc.*, 95(2):189–200, 2013.

[Kob03] Shin-ichi Kobayashi. Iwasawa theory for elliptic curves at supersingular primes. *Invent. Math.*, 152(1):1–36, 2003.

[KR21] Debanjana Kundu and Anwesh Ray. Statistics for Iwasawa invariants of elliptic curves. *Trans. Amer. Math. Soc.*, 374(11):7945–7965, 2021.

[Kur02] Masato Kurihara. On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction. I. *Invent. Math.*, 149(1):195–224, 2002.

[Lei11] Antonio Lei. Iwasawa theory for modular forms at supersingular primes. *Compos. Math.*, 147(3):803–838, 2011.

[MTT86] B. Mazur, J. Tate, and J. Teitelbaum. On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer. *Invent. Math.*, 84(1):1–48, 1986.

[PR84] Bernadette Perrin-Riou. Arithmétique des courbes elliptiques et théorie d'Iwasawa. *Mém. Soc. Math. France (N.S.)*, (17):130, 1984.

[PR93a] Bernadette Perrin-Riou. Fonctions L p-adiques d'une courbe elliptique et points rationnels. *Ann. Inst. Fourier (Grenoble)*, 43(4):945–995, 1993.

[PR93b] Bernadette Perrin-Riou. Théorie d'Iwasawa et hauteurs p-adiques (cas des variétés abéliennes). In *Séminaire de Théorie des Nombres, Paris, 1990–91*, volume 108 of *Progr. Math.*, pages 203–220. Birkhäuser Boston, Boston, MA, 1993.

[PR94] Bernadette Perrin-Riou. Théorie d'Iwasawa des représentations p-adiques sur un corps local. *Invent. Math.*, 115(1):81–161, 1994. With an appendix by Jean-Marc Fontaine.

[PR00] Bernadette Perrin-Riou. *p-adic L-functions and p-adic representations*, volume 3 of *SMF/AMS Texts and Monographs*. American Mathematical Society, Providence, RI; Société Mathématique de France, Paris, 2000. Translated from the 1995 French original by Leila Schneps and revised by the author.

[PR03] Bernadette Perrin-Riou. Arithmétique des courbes elliptiques à réduction supersingulière en p. *Experiment. Math.*, 12(2):155–186, 2003.

[RS23] Anwesh Ray and R. Sujatha. Euler characteristics and their congruences for multisigned Selmer groups. *Canad. J. Math.*, 75(1):298–321, 2023.

[Sch85] Peter Schneider. p-adic height pairings. II. *Invent. Math.*, 79(2):329–374, 1985.

[Spr12] Florian E. Ito Sprung. Iwasawa theory for elliptic curves at supersingular primes: a pair of main conjectures. *J. Number Theory*, 132(7):1483–1506, 2012.

[Spr15] Florian Sprung. A formulation of p-adic versions of the Birch and Swinnerton-Dyer conjectures in the supersingular case. *Res. Number Theory*, 1:Paper No. 17, 13, 2015.

[SW13] William Stein and Christian Wuthrich. Algorithms for the arithmetic of elliptic curves using Iwasawa theory. *Math. Comp.*, 82(283):1757–1792, 2013.

[Wut07] Christian Wuthrich. Iwasawa theory of the fine Selmer group. *J. Algebraic Geom.*, 16(1):83–108, 2007.

[Zer09] Sarah Livia Zerbes. Generalised Euler characteristics of Selmer groups. *Proc. Lond. Math. Soc. (3)*, 98(3):775–796, 2009.

University of California Santa Barbara, South Hall, Santa Barbara, CA 93106, USA
Email address: castella@ucsb.edu