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

CHRISTINE ALAR AND FRANCESC CASTELLA

Abstract. Let $E/\mathbb{Q}$ be an elliptic curve with supersingular reduction at a prime $p > 2$. In [Spr15], Sprung formulated a p-adic variant of the Birch–Swinnerton-Dyer conjecture for a pair of "signed" p-adic L-functions attached to E decomposing the pair of unbounded p-adic L-functions constructed by Amice–Vélu and Višik. In this note, we show that the characteristic power series of the "signed" Selmer groups of E over the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ satisfy an analogue of Sprung's p-adic Birch–Swinnerton-Dyer conjecture. This extends a result obtained in [Cas25a] in the case $a_p = 0$.

Contents

The talk by the second-named author at the RIMS conference "Arithmetic aspects of automorphic forms and automorphic representations" (Kyoto, January 20–24, 2025) was based on recent [CGLS22, CGS25] and ongoing [ACD25] joint work on the Iwasawa theory of rational elliptic curves at Eisenstein primes. Since an outline of the main ideas in these works can already be found in the survey article [Cas25b], this contribution focuses on the Iwasawa theory of rational elliptic curves at *supersingular* (in particular, non-Eisenstein) primes, providing new evidence towards the Iwasawa Main Conjecture in this setting [PR93a].

Date: June 27, 2025.

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 $\mathbb{Q}_\infty/\mathbb{Q}$. 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 $\gamma \in \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$.

When p is ordinary for E, the Selmer group $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_\infty)$ was shown to be Λ-cotorsion by Kato [Kat04]; letting $\xi_p \in \Lambda \simeq \mathbb{Z}_p[[X]]$ denote a characteristic power series for $\mathcal{X}(E/\mathbb{Q}_\infty)$, the works of Schneider [Sch85] and Perrin-Riou [PR93b] (see also [PR84] for E with complex multiplication) prove 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. Under the additional hypothesis that $a_p = 0$ (a condition that holds automatically for $p > 3$ by the Hasse bound), such a result was obtained in [Cas25a] using Kobayashi's signed Selmer groups. Here we shall treat the general supersingular case $p \mid a_p$ (for $p > 2$).

Our main result is in terms of a characteristic power series of Sprung's $\sharp/\flat$-Selmer groups; in the rank zero case, a result along these lines was obtained in [Spr24, §5.2] by an adaptation of Greenberg's methods [Gre99], so we focus on the case of Mordell–Weil rank $r \geq 1$. The result we obtain may be seen as an algebraic analogue of the "Tandem p-adic Birch–Swinnerton-Dyer conjectures" formulated in [Spr15].

1.1. **Main result.**

Let $p > 2$ be a prime of good supersingular reduction for E. In [Spr12], Sprung introduced signed Selmer groups $\mathrm{Sel}_{p^\infty}^{\sharp/\flat}(E/\mathbb{Q}_\infty)$ whose Pontryagin dual

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

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 $\mathrm{Reg}_\nu \in \mathbb{Q}_p$ denote 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 $E(\mathbb{Q}) \otimes \mathbb{Z}_p$.

We consider also the *strict* 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 $N_{\sharp/\flat} \in D_p(E)$, and show that they are in the complement to the Hodge filtration $\mathrm{Fil}^0 D_p(E) = \mathbb{Q}_p\omega_E$, for ω_E a Néron differential on E. Write $\mathrm{Reg}_p^{\sharp/\flat}$ (resp. $\mathrm{Reg}_p^{\mathrm{str}}$) for the above p-adic regulator on $E(\mathbb{Q})$ (resp. $(E(\mathbb{Q}) \otimes \mathbb{Z}_p)_0$) associated to

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

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. Put*

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

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

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

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

$$(\xi_p^{\sharp,*}, \xi_p^{\flat,*}) \ \sim_p \ (\log_p \kappa(\gamma))^{-r} \cdot \left((-a_p^2 + 2a_p + p - 1)\mathrm{Reg}_p^\sharp, (-a_p + 2)\mathrm{Reg}_p^\flat\right) \cdot \frac{\#\text{Ш}(E/\mathbb{Q})[p^\infty] \cdot \mathrm{Tam}(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{\mathrm{tors}})^2},$$

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 the p-adic L-functions $L_p^{\sharp/\flat} \in \Lambda$ constructed in *op. cit.* (and recovering Pollack's p-adic L-functions $L_p^\pm$ [Pol03] as $(L_p^-, L_p^+) = (L_p^\sharp, L_p^\flat)$ in the case $a_p = 0$).
- Kato's Main Conjecture (see [PR93a, §3.4]), which is known to be equivalent to the assertion of [Spr12, Main Conjecture 7.21] expressing the characteristic ideals $(\xi_p^{\sharp/\flat})$ in terms of $L_p^{\sharp/\flat}$.

We note however, that the proof of Theorem A *does not assume* the Main Conjecture, and therefore it provides some evidence towards it.

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 main term in her leading coefficient formula is a p-adic regulator

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

attached to a $D_p(E)$-valued height pairing on $E(\mathbb{Q})$, where φ is the Frobenius operator. Building on a result of Büyükboduk–Lei [BL17] expressing Sprung's $\sharp/\flat$-Coleman maps in terms of Perrin-Riou's work [PR94] (generalizing a result of Lei [Lei11] in the case $a_p = 0$), we extract from $\mathcal{F}_p^{\mathrm{PR}}$ two power series $\mathcal{F}_p^{\sharp/\flat} \in \mathbb{Z}_p[[X]]$. By computing the coordinates of (1.1) relative to a certain basis $(\nu_\sharp, \nu_\flat)$ of $D_p(E)$ on the one hand, and 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 $\mathcal{F}_p^{\sharp/\flat}$ closely related to those in Theorem A for the characteristic power series $\xi_p^{\sharp/\flat}$. We note here that similar computations were performed by Sprung [Spr15] in his study of the aforementioned p-adic analogues of the Birch–Swinnerton-Dyer conjecture for $L_p^{\sharp/\flat}$. Finally, from an application of global duality we relate $\mathcal{F}_p^{\sharp/\flat}$ to the characteristic ideal of $\mathcal{X}^{\sharp/\flat}(E/\mathbb{Q}_\infty)$.

1.3. **Acknowledgements.** We would like thank Kenichi Namikawa and Keiichi Gunji for their invitation to speak at the RIMS conference "Arithmetic aspects of automorphic forms and automorphic representations" (Kyoto, January 20–24, 2025) and the opportunity to contribute to these proceedings. A substantial part of this note, stemming from the first-named author PhD thesis, was written during a visit of the second-named author to NCTS in Taipei during February 2025, and we would also like to thank Ming-Lun Hsieh for the hospitality, and NCTS for the excellent working conditions.

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. As in the Introduction, let $D_p(E)$ 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 $V = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T$. The Galoic group $G_\infty := \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ decomposes as

$$G_\infty = \Gamma \times \Delta,$$

where Γ is the Galois group of the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty/\mathbb{Q}$, and $\Delta = \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ is cyclic of order $p-1$. We shall often identify Γ with $\mathrm{Gal}(\mathbb{Q}_{p,\infty}/\mathbb{Q}_p)$, the Galois group of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}_p$, and let $\Lambda = \mathbb{Z}_p[[\Gamma]]$ be the cyclotomic Iwasawa algebra, often identified with the formal 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 $\mathcal{H}(\Gamma) = \{f(\gamma-1) \mid f \in \mathcal{H}\} \subset \mathbb{Q}_p[\![\Gamma]\!]$. 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

$$V \simeq V^*(1) := \mathrm{Hom}_{\mathbb{Q}_p}(V, \mathbb{Q}_p(1))$$

(and therefore, $\mathbf{D}_{\mathrm{dR}}(V^*(1)) := (V^*(1) \otimes_{\mathbb{Q}_p} \mathbf{B}_{\mathrm{dR}})^{G_{\mathbb{Q}_p}} \simeq D_p(E)$ 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 the Bloch–Kato exponential maps $\exp_{\mathbb{Q}_{p,n},V^*(1)} : \mathbb{Q}_{p,n} \otimes_{\mathbb{Q}_p} \mathbf{D}_{\mathrm{dR}}(V^*(1)) \to \mathrm{H}^1(\mathbb{Q}_{p,n}, V^*(1))$ *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]. □

The ring $\mathbb{Z}_p[[X]]$ is equipped with commuting $\mathbb{Z}_p$-linear actions of φ and Γ given by $X \mapsto (1+X)^p - 1$ and $X \mapsto (1+X)^{\kappa(\gamma)} - 1$, respectively, where $\kappa : \mathrm{Gal}(\mathbb{Q}_{p,\infty}/\mathbb{Q}_p) \to 1 + p\mathbb{Z}_p$ is the cyclotomic character. We also consider the left inverse ψ of φ defined by

$$(\varphi \circ \psi)(f)(X) = \frac{1}{p} \sum_{\zeta^p = 1} f(\zeta(1+X) - 1).$$

The action of Γ on $(1+X) \in \mathbb{Z}_p[[X]]^{\psi=0}$ extends to a Λ-module isomorphism $\Lambda \xrightarrow{\simeq} \mathbb{Z}_p[[X]]^{\psi=0}$ sending $1 \mapsto (1+X)$; this is often referred to as the *Mellin transform* (see e.g [PR94, §1.1.6]), and thus for any

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

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

where $\langle \cdot, \cdot \rangle_{\mathbb{Q}_{p,\infty}}$ is the $\mathcal{H}(\Gamma)$-linear extension of Perrin-Riou's Λ-adic Tate pairing (still denoted in the same way by a slight abuse of notation)

$$\langle \cdot, \cdot \rangle_{\mathbb{Q}_{p,\infty}} : \mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_{p,\infty}, T^*(1)) \times \mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_{p,\infty}, T) \to \Lambda$$

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 $\mathscr{L}_{\mathbf{z}_p}$ as an element

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

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 place S of $\mathbb{Q}$ 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

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

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 $\mathcal{F}^{\mathrm{PR}}_p$ 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, $h_{\omega_E}(P) = -\log_{\omega_E}(P)^2$, 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 $P_1, \dots, P_r$ 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*

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

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 $\text{Ш}(E/\mathbb{Q})[p^\infty]$ 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

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

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 $\sharp/\flat$-Coleman maps

By Sprung's definition in [Spr12], the local conditions at p defining the $\sharp/\flat$-Selmer groups $\mathrm{Sel}_{p^\infty}^{\sharp/\flat}(E/\mathbb{Q}_n)$ are given by

$$\mathrm{H}^1_{\sharp/\flat}(\mathbb{Q}_{p,n}, E[p^\infty]) := \ker(\mathrm{Col}_n^{\sharp/\flat})^\perp \subset \mathrm{H}^1(\mathbb{Q}_{p,n}, E[p^\infty]),$$

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 $\mathrm{Col}_n^{\sharp/\flat} : \mathrm{H}^1(\mathbb{Q}_{p,n}, T) \to \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}_{p,n}/\mathbb{Q}_p)]$ are certain $\sharp/\flat$-*Coleman maps* constructed in *op. cit.* using Honda's theory of formal groups (in a similar vein as done by Kobayashi [Kob03] to construct signed Coleman maps in the case $a_p = 0$). In this section, we recall a result of Büyükboduk–Lei [BL17] giving an independent construction of Sprung's

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

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

3.1. Logarithm matrix.

For every $n \geq 1$, let

$$\Phi_n(X) = \sum_{i=1}^{p-1} X^{p^{n-1}i}$$

denote the p^n-th cyclotomic polynomial.

Definition 3.1.1. The *logarithm matrix* $M_{\log} \in M_{2\times 2}(\mathcal{H})$ is defined by

$$M_{\log} := \lim_{n\to\infty} \begin{pmatrix} a_p & 1 \\ -\Phi_1(1+X) & 0 \end{pmatrix} \cdots \begin{pmatrix} a_p & 1 \\ -\Phi_n(1+X) & 0 \end{pmatrix} \begin{pmatrix} a_p & 1 \\ -p & 0 \end{pmatrix}^{-(n+2)} \begin{pmatrix} -1 & -1 \\ \beta & \alpha \end{pmatrix},$$

where α, β are the roots of $x^2 - a_p x + p$.

That the above limit converges to an element in $M_{2\times 2}(\mathcal{H})$ is shown in [Spr12, Lem. 4.4] (see also [BL17, Prop. 2.5]).

Remark 3.1.2. When $a_p = 0$ one can readily check that

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

where

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

are Pollack's "half logarithms" [Pol03].

3.2. A result of Büyükboduk–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 $\mathbf{z}_p \mapsto \langle \Omega_{V^*(1)}(\eta \otimes (1+X)), \mathbf{z}_p \rangle_{\mathbb{Q}_{p,\infty}}$. Thus, note that $\mathrm{Col}_\eta(\mathbf{z}_p) = \mathscr{L}_{\mathbf{z}_p}(\eta)$ 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 $\mathbf{z}_p \in \mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_{p,\infty}, T)$ we have the decomposition

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

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]. On the other hand, by the results of [BL17, §2.3] (see esp. Theorem 2.13 in *loc. cit.* and also [BBL24, Eq. (5.3)] for the case of elliptic curves), associated to the basis $(\omega_E, \varphi(\omega_E))$ of $D_p(E)$ (which yields a basis of $\mathbf{D}_{\mathrm{cris}}(T)$ in the notations of [BL17]), there exist unique Λ-linear maps

$$\mathrm{Col}_{\mathrm{BL}}^{\sharp/\flat} : \mathrm{H}^1(\mathbb{Q}_{p,\infty}, T) \to \Lambda$$

for which one has a decomposition

$$(\mathrm{Col}_{\eta_\beta}(\mathbf{z}_p), \mathrm{Col}_{\eta_\alpha}(\mathbf{z}_p)) = (\mathrm{Col}_{\mathrm{BL}}^\sharp(\mathbf{z}_p), \mathrm{Col}_{\mathrm{BL}}^\flat(\mathbf{z}_p))\, M_{\log},$$

for all $\mathbf{z}_p \in \mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_{p,\infty}, T)$; that the maps $\mathrm{Col}_{\mathrm{BL}}^{\sharp/\flat}$ agree with Sprung's $\mathrm{Col}^{\sharp/\flat}$ follows from the relation between both constructions and the pairings P_n introduced by Kurihara [Kur02]. □

Remark 3.2.2. Letting $f \in S_2(\Gamma_0(N))$ be the newform associated to E by modularity, by Kato's reciprocity law [Kat04, Thm. 16.6], Kato's zeta element $\mathbf{z}^{\mathrm{Kato}} \in \mathbb{H}^1(V)$ satisfies

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

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

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.

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*

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

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 $\varphi^2 - \frac{a_p}{p}\varphi + \frac{1}{p} = 0$ and $\alpha + \beta = a_p$, 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 $\mathrm{Reg}_p^{\mathrm{PR}} = a\nu_\alpha + b\nu_\beta$, and 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 $Z_{\log} := M_{\log}|_{X=0} = \left(\begin{smallmatrix} a_p & 1 \\ -p & 0 \end{smallmatrix}\right)^{-2}\left(\begin{smallmatrix} -1 & -1 \\ \beta & \alpha \end{smallmatrix}\right)$, and define $N_{\sharp/\flat}, \nu_{\sharp/\flat} \in D_p(E)$ by

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

Remark 4.2.2. Since $\det(Z_{\log}) = \frac{\beta-\alpha}{p^2} \neq 0$, the pair $(\nu_\sharp, \nu_\flat)$ is a basis of $D_p(E)$. To orient the reader, we also note that the introduction of $N_{\sharp/\flat}$ (resp. $\nu_{\sharp/\flat}$) is motivated by the result of the computation in Proposition 4.2.4 (resp. the computation leading to (5.5)) below. Here we are adopting the notations in [Spr15, §4.3], but note that the definition of $N_{\sharp/\flat}$ in *loc. cit.* is slightly different).

Lemma 4.2.3. *We have $N_\sharp, N_\flat \notin \mathrm{Fil}^0 D_p(E)$.*

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

$$(N_\sharp, N_\flat) = \big((1-\alpha^{-1})^2\nu_\beta, -(1-\beta^{-1})^2\nu_\alpha\big) \begin{pmatrix} -pa_p - p\alpha + a_p^2\alpha & -p + a_p\alpha \\ pa_p + p\beta - a_p^2\beta & p - a_p\beta \end{pmatrix} \frac{1}{\beta-\alpha} \tag{4.1}$$

Using the relation $\nu_\alpha + \nu_\beta = \omega_E$, this yields

$$[\omega_E, N_\sharp]_{\mathrm{dR}} = \frac{1}{\beta-\alpha}\big((1-\alpha^{-1})^2(-pa_p - p\alpha + a_p^2\alpha) + (1-\beta^{-1})^2(pa_p + p\beta - a_p^2\beta)\big)[\omega_E, \nu_\beta]_{\mathrm{dR}},$$

which after a tedious but straightforward computation reduces to

$$[\omega_E, N_\sharp] = (-a_p^2 + 2a_p + (p-1))[\omega_E, \nu_\beta]. \tag{4.2}$$

Hence to show that $N_\sharp \notin \mathrm{Fil}^0 D_p(E)$ it remains to see that

$$-a_p^2 + 2a_p + (p-1) \neq 0, \tag{4.3}$$

which is clear under $a_p \neq 0$. Since $p > 2$, the case $a_p \neq 0$ only occurs when $p = 3$, in which case the Hasse bound forces $3^2 \nmid a_3$, and comparing 3-adic valuations we see that (4.3) also holds in this case, concluding the proof that $N_\sharp \notin \mathrm{Fil}^0 D_p(E)$.

Similarly, from (4.1) we obtain

$$[\omega_E, N_\flat]_{\mathrm{dR}} = \frac{1}{\beta-\alpha}\big((1-\alpha^{-1})^2(-p + a_p\alpha) + (1-\beta^{-1})^2(p - a_p\beta)\big)[\omega_E, \nu_\beta]_{\mathrm{dR}},$$

which after a straightforward computation reduces to

$$[\omega_E, N_\flat]_{\mathrm{dR}} = (-a_p + 2)[\omega_E, \nu_\beta]_{\mathrm{dR}}. \tag{4.4}$$

Since the divisibility $p \mid a_p$ (and $p > 2$) implies $a_p \neq 2$, this concludes the proof. □

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

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

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 4.2.3 and its proof the quantities $\widetilde{\mathrm{Reg}}_{\nu_\alpha}$, $\widetilde{\mathrm{Reg}}_{\nu_\beta}$, $\widetilde{\mathrm{Reg}}_{N_\sharp}$, $\widetilde{\mathrm{Reg}}_{N_\flat}$ are all defined. Thus from the expression for $\mathrm{Reg}_p^{\mathrm{PR}}$ in Lemma 4.1.2 we obtain

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

using the relation $[\omega_E, \nu_\alpha]_{\rm dR} = -[\omega_E, \nu_\beta]_{\rm dR}$ and the aforementioned linearity for the third equality. In light of (4.2) and (4.4), this yields the result. □

5. Proof of the main result

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

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

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

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

where $\mathbf{z}_p = \mathrm{res}_p(\mathbf{z}) \in \mathrm{H}^1_{\rm Iw}(\mathbb{Q}_{p,\infty}, T)$ and $g_{\rm str}$ 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. Put*

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

and suppose $r \geq 1$. Then:

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

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

$$(\mathcal{F}_p^{\sharp,\ast}, \mathcal{F}_p^{\flat,\ast}) \sim_p (\log_p \kappa(\gamma))^{-r} \cdot \big((-a_p^2 + 2a_p + p - 1)\mathrm{Reg}_p^\sharp, (-a_p + 2)\mathrm{Reg}_p^\flat\big) \cdot \frac{\#Ш(E/\mathbb{Q})[p^\infty] \cdot \mathrm{Tam}(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{\rm tors})^2}.$$

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 $\mathcal{F}_p^{\rm PR} \in D_p(E)[[X]]$ of Definition 2.2.2 in matrix form as

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

In particular, from (5.2) and the product rule we readily find

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

for all $t \geq 0$, where we recall that $Z_{\log} = M_{\log}|_{X=0}$. Since the matrix $Z_{\log}$ is invertible, this shows that

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

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 $\mathrm{Reg}_p^{\rm str} \neq 0$; then $\varrho = r$ by (5.4) and Theorem 2.4.1(ii). Now put

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

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

$$\mathcal{F}_p^{{\rm PR},\ast} = \mathcal{F}_p^{{\rm PR},(r)}(0) = \big(\mathcal{F}_p^{\sharp,(r)}(0), \mathcal{F}_p^{\flat,(r)}(0)\big) \begin{pmatrix} \nu_\sharp \\ \nu_\flat \end{pmatrix} = \big(\mathcal{F}_p^{\sharp,\ast}, \mathcal{F}_p^{\flat,\ast}\big) \begin{pmatrix} \nu_\sharp \\ \nu_\flat \end{pmatrix}. \tag{5.5}$$

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

$$(d_\sharp, d_\flat) \ \sim_p \ (\log_p \kappa(\gamma))^{-r} \cdot \big((-a_p^2 + 2a_p + p - 1)\mathrm{Reg}_p^\sharp, (-a_p + 2)\mathrm{Reg}_p^\flat\big) \cdot \frac{\#\text{Ш}(E/\mathbb{Q})[p^\infty] \cdot \mathrm{Tam}(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{\mathrm{tors}})^2},$$

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 $\mathcal{F}_p^{\sharp/\flat} \in \mathbb{Z}_p[[X]]$ introduced in (5.1) generates the characteristic ideal of $\mathcal{X}^{\sharp/\flat}(E/\mathbb{Q}_\infty)$.

As explained in [Spr12, §7.2], Poitou–Tate duality gives rise to the four-term exact sequence

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

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

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

where $\mathbf{z}_p$ denotes the image of $\mathbf{z}$ in $\mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_{p,\infty}, T)$.

Since the Λ-linear maps $\mathrm{Col}^{\sharp/\flat}$ have pseudo-null cokernel by Proposition 7.3 and Proposition 7.6 in [Spr12], we see that the second term in (5.6) has characteristic ideal generated by $\mathrm{Col}^{\sharp/\flat}(\mathbf{z}_p)$, and so the fact that $\mathcal{F}_p^{\sharp/\flat}$ has the desired property follows by multiplicativity. □

References

[ACD25] Raúl Alonso, Francesc Castella, and Kim Tuan Do. 2025. in preparation.

[BBL24] Ashay Burungale, Kâzım Büyükboduk, and Antonio Lei. Anticyclotomic Iwasawa theory of abelian varieties of GL_2-type at non-ordinary primes. *Adv. Math.*, 439:Paper No. 109465, 63, 2024.

[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.

[BL17] Kâzım Büyükboduk and Antonio Lei. Integral Iwasawa theory of Galois representations for non-ordinary primes. *Math. Z.*, 286(1-2):361–398, 2017.

[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.

[Cas25a] Francesc Castella. A formula of Perrin-Riou and characteristic power series of signed Selmer groups. 2025. *Pure Appl. Math. Q.*, Special Issue in Honor of John Coates, to appear.

[Cas25b] Francesc Castella. On the Iwasawa theory of elliptic curves at Eisenstein primes. 2025. Proceedings of the 2022 ICTS workshop *Elliptic curves and the special values of L-functions*, to appear.

[CGLS22] Francesc Castella, Giada Grossi, Jaehoon Lee, and Christopher Skinner. On the anticyclotomic Iwasawa theory of rational elliptic curves at Eisenstein primes. *Invent. Math.*, 227:517–580, 2022.

[CGS25] Francesc Castella, Giada Grossi, and Christopher Skinner. Mazur's main conjecture at Eisenstein primes. *Math. Ann.*, 2025. to appear.

[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.

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

[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.

[Pol03] Robert Pollack. On the p-adic L-function of a modular form at a supersingular prime. *Duke Math. J.*, 118(3):523–558, 2003.

[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.

[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.

[Spr24] Florian Sprung. On Iwasawa main conjectures for elliptic curves at supersingular primes: beyond the case $a_p = 0$. *Adv. Math.*, 449:Paper No. 109741, 47, 2024.

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

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

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