J. Inst. Math. Jussieu (2024), **23**(3), 1417–1460
doi:10.1017/S147474802300021X

p-ADIC L-FUNCTIONS AND RATIONAL POINTS ON CM ELLIPTIC CURVES AT INERT PRIMES

ASHAY A. BURUNGALE[1], SHINICHI KOBAYASHI[2] AND KAZUTO OTA[3]

[1] *California Institute of Technology, 1200 E California Blvd, Pasadena CA 91125, & Department of Mathematics, The university of Texas at Austin, 2515 Speedway, Austin TX 78712*
(ashayburungale@gmail.com)

[2] *Faculty of Mathematics, Kyushu University, 744, Motooka, Nishi-ku, Fukuoka, 819-0395, Japan*
(kobayashi@math.kyushu-u.ac.jp)

[3] *Department of Mathematics, Graduate School of Science, Osaka University Toyonaka, Osaka 560-0043, Japan*
(kazutoota@math.sci.osaka-u.ac.jp)

(Received 23 September 2021; revised 30 April 2023; accepted 5 May 2023; first published online 17 July 2023)

Abstract Let K be an imaginary quadratic field and $p \geq 5$ a rational prime inert in K. For a $\mathbb{Q}$-curve E with complex multiplication by $\mathcal{O}_K$ and good reduction at p, K. Rubin introduced a p-adic L-function $\mathscr{L}_E$ which interpolates special values of L-functions of E twisted by anticyclotomic characters of K. In this paper, we prove a formula which links certain values of $\mathscr{L}_E$ outside its defining range of interpolation with rational points on E. Arithmetic consequences include p-converse to the Gross–Zagier and Kolyvagin theorem for E.

A key tool of the proof is the recent resolution of Rubin's conjecture on the structure of local units in the anticyclotomic $\mathbb{Z}_p$-extension Ψ_∞ of the unramified quadratic extension of $\mathbb{Q}_p$. Along the way, we present a theory of local points over Ψ_∞ of the Lubin–Tate formal group of height 2 for the uniformizing parameter $-p$.

Contents

1. Introduction

Since the seminal work of Coates and Wiles, Iwasawa theory of CM elliptic curves influences general Iwasawa theory. It continues to have applications to classical Diophantine problems. The nature of prime p is inherent to Iwasawa theory. For primes split in the CM field, CM Iwasawa theory is well-developed. In contrast, for non-split primes, new phenomena abound and CM Iwasawa theory is still incipient.

Let K be an imaginary quadratic field and $p \geq 5$ a rational prime which is *inert* in K. Let K_n be the n-th layer of the anticyclotomic $\mathbb{Z}_p$-extension K_∞ of K. Let E be an elliptic curve defined over $\mathbb{Q}$ with complex multiplication by $\mathcal{O}_K$. In the early 1980s, R. Greenberg found the formula

$$W(\varphi\chi) = (-1)^{n+1} W(\varphi)$$

for root numbers, where φ denotes the Hecke character of E and χ an anticyclotomic finite character of K of order $p^n > 1$. It led him to the formula

$$\mathrm{rank}_{\mathbb{Z}} E(K_n) - \mathrm{rank}_{\mathbb{Z}} E(K_{n-1}) = \varepsilon_n p^{n-1}(p-1) \tag{1.1}$$

for all n sufficiently large (cf. [24], [26], see also Corollary 3.11). Here, ε_n is 0 or 2 and $\varepsilon_n = 2$ if and only if $W(\varphi) = (-1)^n$. So, new points of infinite order occur in the alternate anticyclotomic layers. This behavior of the Mordell–Weil rank is peculiar to the inert case. For example, for a split prime p, we have $\mathrm{rank}_{\mathbb{Z}} E(K_\infty) < +\infty$ if $W(\varphi) = +1$. In the late 1980s K. Rubin envisioned an Iwasawa theory echoing such phenomena and made a fundamental conjecture on the structure of anticyclotomic local units (cf. [47]). Recently, we proved the conjecture [12]. The resolution has unexpectedly led us to new developments in supersingular Iwasawa theory. This is the first of the series of papers of our study.

In [47], Rubin constructed an anticyclotomic p-adic L-function $\mathscr{L}_E$ interpolating special values $L(\varphi\chi, 1)$ for finite anticyclotomic characters χ of K with $W(\varphi\chi) = +1$. If one expects a p-adic Birch and Swinnerton-Dyer conjecture for $\mathscr{L}_E$, the function should encode the rank behavior (1.1). The main result of this paper is a formula relating the value of $\mathscr{L}_E$ at a finite anticyclotomic character χ of K with $W(\varphi\chi) = -1$ to the formal group logarithm of a rational point on $E(K_n)^\chi$ behind the phenomenon (1.1) (see Theorems 1.1 and 1.2). It has an application for the Birch and Swinnerton-Dyer (BSD) conjecture, namely a p-converse to the Gross–Zagier and Kolyvagin theorem (see Theorem 1.5).

1.2. Main results. Let $p \geq 5$ be a prime. Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$. Fix embeddings $\iota_\infty : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and $\iota_p : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$.

Let K be an imaginary quadratic field with p *inert* and $\mathcal{O}_K$ the integer ring. Let $\mathcal{O}$ (resp. Φ) be the completion of $\mathcal{O}_K$ (resp. K) at p. In this introduction, we assume the class number h_K of K equals 1; however, the main text only assumes $p \nmid h_K$. Let K_∞ be the anticyclotomic $\mathbb{Z}_p$-extension of K and $\Gamma = \mathrm{Gal}(K_\infty/K)$. Let Ξ be the set of finite characters of Γ. Let

$$\Xi^+ = \{\chi \in \Xi \mid \mathrm{cond}^{\mathrm{r}}\chi \text{ is an even power of } p\},$$
$$\Xi^- = \{\chi \in \Xi \mid \mathrm{cond}^{\mathrm{r}}\chi \text{ is an odd power of } p\}.$$

In particular, $\mathbb{1} \in \Xi^+$ for $\mathbb{1}$ the trivial Hecke character of K. Let Λ be the anticyclotomic Iwasawa algebra $\mathcal{O}[[\Gamma]]$.

Let E be an elliptic curve defined over $\mathbb{Q}$ with complex multiplication by $\mathcal{O}_K$ with good reduction at p (note that E has supersingular reduction at p since p is inert). Let T be the p-adic Tate module of E, which is an $\mathcal{O}$-module of rank 1, and put $T^{\otimes -1} = \mathrm{Hom}_{\mathcal{O}}(T,\mathcal{O})$. Fix a minimal Weierstrass model of E over $\mathbb{Z}_{(p)}$ and let ω be the associated Néron differential form. Let $\Omega \in \mathbb{C}^\times$ be a CM period so that $\Omega\mathcal{O}_K$ is the period lattice. Let φ be the associated Hecke character of K. In particular,

$$L(E_{/\mathbb{Q}},s) = L(\varphi,s).$$

Let $W(\varphi)$ be the root number of the Hecke L-function $L(\varphi,s)$.

1.2.1. Rubin p-adic L-function. Here, we introduce Rubin's theory in terms of Galois cohomology. The relation to Rubin's original formulation is explained in Section 2.

Let Ψ_∞ be the anticyclotomic $\mathbb{Z}_p$-extension of Φ and Ψ_n the n-th layer. We denote the Iwasawa cohomology $\varprojlim_n H^1(\Psi_n, T^{\otimes -1}(1))$ by $\mathcal{H}^1$. For $\chi \in \Xi$, which factors through $\mathrm{Gal}(\Psi_m/\Phi)$, the dual exponential map for $\chi \otimes T^{\otimes -1}(1)$ normalized by ω defines a map $\delta_\chi : \mathcal{H}^1 \longrightarrow \Psi_m(\mathrm{Im}\,\chi)$ (cf. (2.9)). Then, we put

$$\mathcal{H}^1_\pm := \{v \in \mathcal{H}^1 \mid \delta_\chi(v) = 0 \quad \text{for every } \chi \in \Xi^\mp\}. \tag{1.2}$$

Rubin showed $\mathcal{H}^1_\pm$ is a free Λ-module of rank one (cf. [47, Prop. 8.1] and (2.7)). Rubin's conjecture, which is proved in [12], posits

$$\mathcal{H}^1 = \mathcal{H}^1_+ \oplus \mathcal{H}^1_-. \tag{1.3}$$

We fix a generator $v_\pm = (v_{\pm,n})_n$ of the local Λ-module $\mathcal{H}^1_\pm$. Let $\varepsilon \in \{+,-\}$ be the sign of the root number $W(\varphi)$ and let

$$\mathscr{L}_E := \mathscr{L}_p(\varphi,\Omega,v_\varepsilon) \in \Lambda \tag{1.4}$$

be the associated Rubin p-adic L-function [47, §10] (cf. §3.3.1). Let $\mathscr{L}_E(\chi)$ denote its evaluation at an anticyclotomic character χ.

For $\chi \in \Xi^\varepsilon$ (resp. $\chi \in \Xi^{-\varepsilon}$), the Hecke L-function $L(\varphi\chi,s)$ is self-dual and $W(\varphi\chi) = +1$ (resp. $W(\varphi\chi) = -1$). The interpolation property of the Rubin p-adic L-function is given by

$$\mathscr{L}_E(\chi) = \frac{1}{\delta_{\chi^{-1}}(v_\varepsilon)} \cdot \frac{L_{p\mathfrak{f}}(\overline{\varphi\chi},1)}{\Omega} \quad (\chi \in \Xi^\varepsilon), \tag{1.5}$$

https://doi.org/10.1017/S147474802300021X Published online by Cambridge University Press

where the non-vanishing of $\delta_{\chi^{-1}}(v_\varepsilon)$ is a consequence of Rubin's conjecture, and $L_{p\mathfrak{f}}(\overline{\varphi\chi},s)$ denotes the associated L-function whose Euler factors at the primes dividing $p\mathfrak{f}$ are removed.

For $\chi\in\Xi^{-\varepsilon}$, note that $L(\overline{\varphi\chi},1)=0$ by the functional equation and $\mathscr{L}_E(\chi)$ is not related to $L(\overline{\varphi\chi},1)$ directly. In light of the BSD conjecture, it is natural to seek:

$$\text{links between } \mathscr{L}_E(\chi) \text{ for } \chi\in\Xi^{-\varepsilon} \text{ and rational points in } E(K_\infty)^\chi. \tag{Q}$$

This question is due to Rubin [47, p. 421].

Theorem 1.1. *Let $E_{/\mathbb{Q}}$ be a CM elliptic curve with root number -1 and K the CM field. Let $p\geq 5$ be a prime of good supersingular reduction for $E_{/\mathbb{Q}}$ and $\mathscr{L}_E$ the Rubin p-adic L-function as in (1.4). Then, there exists a rational point $P\in E(\mathbb{Q})$ with the following properties.*

(a) *We have*

$$\mathscr{L}_E(\mathbb{1})=\left(1+\frac{1}{p}\right)\frac{\log_\omega(P)^2}{\log_\omega(v_{-,0})}\cdot c_P$$

for[1] *some $c_P\in\mathbb{Q}^\times\mathcal{O}_K^\times$.*

(b) *P is non-torsion if and only if* $\mathrm{ord}_{s=1}L(E_{/\mathbb{Q}},s)=1$.

(c) *If* $\mathrm{ord}_{s=1}L(E_{/\mathbb{Q}},s)=1$, *then*

$$c_P=\frac{L'(E_{/\mathbb{Q}},1)}{\Omega\langle P,P\rangle_\infty}$$

for $\langle\ ,\ \rangle_\infty$ the Néron–Tate height pairing.

See also Theorem 4.8 in a more general setting.

The formula is the principal result of this paper. It gives a p-adic criterion for E to have analytic rank one. For such curves, the p-adic L-value in turn leads to a p-adic construction of a rational point of infinite order which is independent of the choice of v_- (cf. Corollary 4.9).

Our second result is an interpolation of the Rubin p-adic L-function at higher order characters in $\Xi^{-\varepsilon}$.

Theorem 1.2. *Let $E_{/\mathbb{Q}}$ be a CM elliptic curve and K the CM field. Let φ be the associated Hecke character and ε the sign of the root number of φ. Let $p\geq 5$ be a prime of good supersingular reduction for $E_{/\mathbb{Q}}$ and $\mathscr{L}_E$ the Rubin p-adic L-function as in (1.4). Let $\chi\in\Xi^{-\varepsilon}$ be a Hecke character with conductor p^{n+1}. Let $z_\chi\in H^1(K_n,T_pE)^\chi$ be the image of a system of elliptic units of E (cf. §3.1.2). Then,*

$$z_\chi\in H^1_{\mathrm{f}}(K_n,T_pE)^\chi,$$

and it has the following properties.

[1] Note that $v_{-,0}\in E(\Phi)$ since $\mathbb{1}\in\Xi^+$ and $\exp^*_E(v_{-,0})=0$, by definition; hence, $\log_\omega(v_{-,0})$ is well-defined.

https://doi.org/10.1017/S147474802300021X Published online by Cambridge University Press

(a) *We have*

$$\mathscr{L}_E(\chi^{-1}) = \delta_\chi(v_{-\varepsilon}) \cdot \log_\omega(z_\chi).$$

(b) *If* $\mathrm{ord}_{s=1} L(\varphi\chi^{-1}, s) = 1$*, then* $z_\chi \in H^1_{\mathrm{f}}(K_n, V_p E)^\chi$ *is a generator of the* $\mathbb{Q}_p(\chi)$*-vector space* $(E(K_n) \otimes \mathbb{Q}_p(\chi))^\chi$.

See also Theorem 3.16 in a more general setting.

Note that $\mathrm{ord}_{s=1} L(\varphi\chi, s) = 1$ for all but finitely many $\chi \in \Xi^{-\varepsilon}$ (cf. [45]). So, in view of Theorem 1.2 (b), the Rubin p-adic L-function leads to a construction of new points of infinite order in the alternate anticyclotomic layers (cf. (1.1)).

Remark 1.3. For $\chi \in \Xi^{-\varepsilon}$, one expects that if $z_{\chi^{-1}}$ is non-zero, then $\mathrm{ord}_{s=1} L(\varphi\chi, s) = 1$ and

$$\mathrm{ord}_{s=1} L(\varphi\chi, s) = 1 + \mathrm{ord}_\chi \mathscr{L}_E.$$

An evidence appears in [12, Thm. 2.4]. It seems interesting to compare Theorems 1.1 and 1.2 with the exceptional zero conjecture of Mazur, Tate and Teitelbaum [39].

As a corollary of the above theorems, we obtain a refined (non-asymptotic) version of (1.1).

Corollary 1.4. *Let* $E_{/\mathbb{Q}}$ *be a CM elliptic curve and* K *the CM field.*

(i) *If* $L(E_{/\mathbb{Q}}, 1)/\Omega$ *is a p-adic unit, then for all* $n \geq 1$*, we have*

$$\mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(E_{/K_n}) - \mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(E_{/K_{n-1}}) = \varepsilon_n p^{n-1}(p-1),$$

where $\varepsilon_n = 0$ *(resp. 2) for n odd (resp. even).*

(ii) *Suppose that* $\mathrm{ord}_{s=1} L(E_{/\mathbb{Q}}, s) = 1$ *and there exists a rational point* $P \in E(\mathbb{Q})$ *whose image generates the free* $\mathbb{Z}_p$*-module* $E(\mathbb{Q}_p)/E(\mathbb{Q}_p)_{\mathrm{tor}}$ *of rank 1. If*

$$L'(E_{/\mathbb{Q}}, 1)/\Omega\langle P, P\rangle_\infty$$

is a p-adic unit, then for all $n \geq 1$*, we have*

$$\mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(E_{/K_n}) - \mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(E_{/K_{n-1}}) = \varepsilon_n p^{n-1}(p-1),$$

where $\varepsilon_n = 0$ *(resp. 2) for n even (resp. odd).*

In particular, if $\text{Ш}(E_{/K_n})$ *is finite, then*

$$\mathrm{rank}_{\mathbb{Z}} E(K_n) - \mathrm{rank}_{\mathbb{Z}} E(K_{n-1}) = \varepsilon_n p^{n-1}(p-1).$$

A key to the proof of main results is a theory of local points, similarly as [31, §8] underlies the cyclotomic signed Iwasawa theory [31] (cf. Section 2.3.) In the case of cyclotomic deformation, such a theory is the core of Perrin-Riou theory. However, Perrin-Riou theory for the anticyclotomic $\mathbb{Z}_p$-extension is not yet developed sufficiently to be applicable to our case. Instead, we use Rubin's conjecture to construct local points. It may give some insight towards a Perrin-Riou theory for the anticyclotomic $\mathbb{Z}_p$-extension.

1.2.3. *p*-converse to a theorem of Gross–Zagier and Kolyvagin.

Theorem 1.5. *Let* $E_{/\mathbb{Q}}$ *be a CM elliptic curve with good supersingular reduction at* $p \geq 5$. *If* $\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_{p^\infty}(E) = 1$ *and* $Ш(E)[p^\infty]$ *is finite, then* $\mathrm{ord}_{s=1}L(E_{/\mathbb{Q}}, s) = 1$.

See also Theorem 4.18 in a more general setting. Just as the Bertolini–Darmon–Prasanna formula is employed in the proof of Skinner's p-converse [52], our approach is based on Theorem 1.1.

Remark 1.6.

(i) The first results towards the p-converse were due to Rubin [51], which treated CM elliptic curves and ordinary primes p. The first general results for non-CM curves were independently due to Skinner [52] and Zhang [56] a few years back.

(ii) One may seek a refined p-converse:

$$\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_{p^\infty}(E) = 1 \implies \mathrm{ord}_{s=1}L(E_{/\mathbb{Q}}, s) = 1 \tag{1.6}$$

(cf. [56], [18], [16],[10], [11]). While it may be possible to approach Theorem 1.5 via the p-adic Gross–Zagier formula [32], with a view to (1.6), our approach instead employs Theorem 1.1.

Background

An impetus to Theorems 1.1 and 1.2 is a formula of Rubin. For primes p *split* in an imaginary quadratic field K, Rubin proved an influential formula [50] which links certain values of the Katz p-adic L-function of K to the formal group logarithm of rational points on elliptic curves with CM by K (cf. [42], [44]). The last decade has led to a revival of Rubin's formula. For an arbitrary elliptic curve $E_{/\mathbb{Q}}$ and K an imaginary quadratic field satisfying Heegner hypothesis for E with p *split*, the Bertolini–Darmon–Prasanna (BDP) formula relates certain values of a Rankin–Selberg p-adic L-function $\mathscr{L}_E^{\mathrm{Gr}}$ of $E_{/K}$ with the formal group logarithm of Heegner points on E (cf. [6], [34]). Since its advent, the BDP formula has influenced the arithmetic of elliptic curves and inspired progress towards the BSD conjecture, with an instance being p-converse to the Gross–Zagier and Kolyvagin theorem due to Skinner (cf. [52]), which is a p-adic criterion for $E_{/\mathbb{Q}}$ to have both algebraic and analytic rank one. The p-converse is based on the BDP formula and an Iwasawa theory of $\mathscr{L}_E^{\mathrm{Gr}}$. Subsequently, Liu–Zhang–Zhang interpreted the BDP formula as a p-adic Waldspurger formula and generalised it to modular elliptic curves over totally real fields (cf. [37]).

An emerging search is the analogue of the BDP formula[2] over imaginary quadratic fields with p *non-split*, and a pertinent Iwasawa main conjecture (the conjectural backdrop of Iwasawa theory excludes such a non-split setting; cf. [25], [44], [31]). The ensuing CM case is perhaps the first instance, whose investigation we plan to continue (cf. [13], [14]).

[2]Based on recent developments in the p-adic geometry of modular curves, certain analogues appear in [4], [36]. A salient feature of these works is that the p-adic L-functions, whose growth behaviour is not yet well understood, are locally analytic. The formulation of a relevant Iwasawa main conjecture is a fundamental open problem.

https://doi.org/10.1017/S147474802300021X Published online by Cambridge University Press

1.3. Plan

Section 2 presents the local theory. In Section 3, certain global aspects appear, including (1.1) and Theorem 1.2. Then Section 4 treats Theorems 1.1 and 1.5.

The proof of Theorem 1.1 is based on the appendices to which the reader may refer prior to Section 4. Appendix A describes a variant of the p-adic Gross–Zagier formula [32] in which the p-adic logarithm of Heegner points appears (see Theorem A.6). Appendix B exhibits another consequence: the Perrin-Riou conjecture [42] for GL_2-type abelian varieties at primes of good non-ordinary reduction (see Theorem B.3).

2. Local points

2.1. The set-up

We introduce the module of anticyclotomic local units as well as its signed submodules following [47], [12].

2.1.1. Notation. Let $p \geq 5$ be a prime. Let Φ be the unramified quadratic extension of $\mathbb{Q}_p$ and $\mathcal{O}$ the integer ring. We fix a Lubin–Tate formal group $\mathscr{F}$ over $\mathcal{O}$ for the uniformizing parameter $\pi := -p$. Let λ denote the logarithm of $\mathscr{F}$.

For $n \geq 0$, write $\Phi_n = \Phi(\mathscr{F}[\pi^{n+1}])$, the extension of Φ in $\mathbb{C}_p$ generated by the π^{n+1}-torsion points of $\mathscr{F}$, and put $\Phi_\infty = \cup_{n\geq 0}\Phi_n$. Let

$$\kappa_{\mathscr{F}} : \mathrm{Gal}(\Phi_\infty/\Phi) \to \mathrm{Aut}(T_\pi\mathscr{F}) \cong \mathcal{O}^\times$$

be the natural isomorphism induced by the Galois action on the π-adic Tate module $T_\pi\mathscr{F} =: T$. Let Θ_n be the subfield of Φ_n with $[\Theta_n : \Phi] = p^{2n}$ and $\Theta_\infty = \cup_{n\geq 1}\Theta_n$ the $\mathbb{Z}_p^2$-extension of Φ. Let Ψ_∞ be the anticyclotomic $\mathbb{Z}_p$-extension of Φ and Ψ_n the n-th layer. We put $G := \mathrm{Gal}(\Theta_\infty/\Phi) \cong \mathbb{Z}_p^2$, $G^- := \mathrm{Gal}(\Psi_\infty/\Phi) \cong \mathbb{Z}_p$ and $\Delta := \mathrm{Gal}(\Phi_\infty/\Theta_\infty) = \mathrm{Gal}(\Phi_0/\Phi) \cong (\mathcal{O}/p)^\times$. Fix a topological generator γ of G^-.

Let U_n be the group of principal units in Φ_n, that is, the group of elements in $\mathcal{O}_{\Phi_n}^\times$ congruent to one modulo the maximal ideal. Let

$$T^{\otimes -1} = \mathrm{Hom}_{\mathcal{O}}(T,\mathcal{O}), \qquad U_\infty^* = \big(\varprojlim_n (U_n \otimes_{\mathbb{Z}_p} T^{\otimes -1})\big)^\Delta,$$

where the superscript Δ means the Δ-invariants. Define the Iwasawa algebras

$$\Lambda_2 = \mathcal{O}[\![G]\!] \quad \text{and} \quad \Lambda = \mathcal{O}[\![G^-]\!].$$

It is known that U_∞^* is a free Λ_2-module of rank 2 (cf. [54]). A primary object is the anticyclotomic projection

$$V_\infty^* = U_\infty^* \otimes_{\Lambda_2} \Lambda.$$

Let $\delta_n : U_\infty^* \to \Phi_n$ be the Coates–Wiles homomorphism as in [12, §2]. For a finite character χ of $\mathrm{Gal}(\Phi_\infty/\Phi)$ of conductor dividing p^{n+1} and $u \in U_\infty^*$, let

$$\delta_\chi(u) = \frac{1}{\pi^{n+1}} \sum_{\sigma \in \mathrm{Gal}(\Phi_n/\Phi)} \chi(\sigma)\delta_n(u)^\sigma. \tag{2.1}$$

If χ factors through G^-, then δ_χ factors through V_∞^* (cf. [47, Lem. 2.1 (ii)]).

2.1.2. Rubin's conjecture. Let Ξ be the set of finite characters of G^-. Let

$$\Xi^+ = \{\chi \in \Xi \mid \mathrm{cond}^{\mathrm{r}}\chi \text{ is an even power of } p\},$$
$$\Xi^- = \{\chi \in \Xi \mid \mathrm{cond}^{\mathrm{r}}\chi \text{ is an odd power of } p\}.$$

Define

$$V_\infty^{*,\pm} := \{v \in V_\infty^* \mid \delta_\chi(v) = 0 \quad \text{for every } \chi \in \Xi^{\mp}\}. \tag{2.2}$$

Rubin showed that $V_\infty^{*,\pm}$ is a free Λ-module of rank one (cf. [47, Prop. 8.1]).

The following is central to the construction of local points.

Theorem 2.1. *(Rubin's conjecture) We have*

$$V_\infty^* = V_\infty^{*,+} \oplus V_\infty^{*,-}.$$

This was proposed by Rubin as [47, Conj. 2.2] and recently proved [12, Thm. 2.1].

2.2. Local cohomology

2.2.1. Kummer theory. We recast the modules of anticyclotomic local units in terms of the local Iwasawa cohomology.

Define a natural isomorphism of $\mathcal{O}[\![\mathrm{Gal}(\Phi_\infty/\Phi)]\!]$-modules

$$\varprojlim_n (U_n \otimes \mathcal{O}) \otimes T^{\otimes -1} \cong \varprojlim_n H^1(\Phi_n, T^{\otimes -1}(1)) \tag{2.3}$$

as the composite

$$\begin{aligned}\varprojlim_n (U_n \otimes \mathcal{O}) \otimes T^{\otimes -1} &\cong \varprojlim_n H^1(\Phi_n, \mathcal{O}(1)) \otimes T^{\otimes -1}\\ &\cong \varprojlim_n H^1(\Phi_n, \mathcal{O}/\pi^n(1)) \otimes T^{\otimes -1}\\ &\cong \varprojlim_n H^1(\Phi_n, T^{\otimes -1}(1)/\pi^n)\\ &\cong \varprojlim_n H^1(\Phi_n, T^{\otimes -1}(1)).\end{aligned}$$

Here, the first isomorphism is the Kummer map and the third is a consequence of the $\mathrm{Gal}(\Phi_\infty/\Phi_n)$-action on $\mathcal{O}(1) \otimes T^{\otimes -1}/\pi^n$ being trivial. The Δ-invariants of (2.3) give an isomorphism

$$U_\infty^* \cong \varprojlim_n H^1(\Theta_n, T^{\otimes -1}(1)) \tag{2.4}$$

of Λ_2-modules.

For a finite extension L of Φ, let

$$\exp_L^* : H^1(L, T^{\otimes -1}(1)) \to L \tag{2.5}$$

be the dual exponential map which arises from the identification of $\mathrm{Fil}^0 D_{\mathrm{dR}}(T^{\otimes -1}(1) \otimes \mathbb{Q}_p)$ with Φ so that the invariant differential $d\lambda$ corresponds to 1 (cf. [29, §1.2.4, Ch. II]).

By the explicit reciprocity law of Wiles (cf. [29, Thm. 2.1.7, Ch. II]), note that the following diagram

$$\begin{tikzcd} U_\infty^* \arrow[r] \arrow[d, "\pi^{-n-1}\delta_n"'] & \varprojlim_n H^1(\Theta_n, T^{\otimes -1}(1)) \arrow[d, "\exp^*_{\Theta_n}"] \\ \Phi_n \arrow[r, "="] & \Phi_n \end{tikzcd} \tag{2.6}$$

commutes, where the upper horizontal map is (2.4). The anticyclotomic projection induces an isomorphism

$$V_\infty^* \cong \varprojlim_n H^1(\Psi_n, T^{\otimes -1}(1)), \tag{2.7}$$

as well as a commutative diagram

$$\begin{tikzcd} V_\infty^* \arrow[r] \arrow[d, "\pi^{-n-1}\delta_n^{\mathrm{ac}}"'] & \varprojlim_n H^1(\Psi_n, T^{\otimes -1}(1)) \arrow[d, "\exp^*_{\Psi_n}"] \\ \Psi_n \arrow[r, "="] & \Psi_n, \end{tikzcd} \tag{2.8}$$

where $\delta_n^{\mathrm{ac}} := \mathrm{Tr}_{\Phi_n/\Psi_n} \circ \delta_n$. Hence, for a character χ of $\mathrm{Gal}(\Psi_n/\Phi)$ and $v = (v_m)_{m\geq 0} \in V_\infty^* = \varprojlim_m H^1(\Psi_m, T^{\otimes -1}(1))$ (cf. (2.7)), we have

$$\delta_\chi(v) = \sum_{\sigma \in \mathrm{Gal}(\Psi_n/\Phi)} \exp^*_{\Psi_n}(v_n^\sigma)\chi(\sigma). \tag{2.9}$$

Therefore, we may naturally identify $V_\infty^{*,\pm}$ with the module $\mathcal{H}^1_\pm$ introduced in (1.2), and Theorem 2.1 implies the decomposition (1.3) of $\varprojlim_m H^1(\Psi_m, T^{\otimes -1}(1))$.

Let $H^1_{\mathrm{f}}(\Psi_n, T)$ and $H^1_{\mathrm{f}}(\Psi_n, T^{\otimes -1}(1))$ denote the finite part of $H^1(\Psi_n, T)$ and $H^1(\Psi_n, T^{\otimes -1}(1))$, respectively.

Lemma 2.2.

(1) *The quotient by the ideal* $(\gamma^{p^n} - 1)\Lambda$ *induces an isomorphism*

$$V_\infty^*/(\gamma^{p^n} - 1) \cong H^1(\Psi_n, T^{\otimes -1}(1)). \tag{2.10}$$

(2) *The* $\mathcal{O}$*-module* $H^1_{\mathrm{f}}(\Psi_n, T^{\otimes -1}(1))$ *coincides with* $\ker(\delta_n^{\mathrm{ac}})$ *via (2.10).*

Proof.

(1) By definition, $V_\infty^*/(\gamma^{p^n} - 1)$ is isomorphic to $\varprojlim_m H^1(\Psi_m, T^{\otimes -1}(1))/(\gamma^{p^n} - 1)$. In light of the inflation-restriction sequence and [47, Prop. 4.5 (ii)], it follows that $\varprojlim_m H^1(\Psi_m, T^{\otimes -1}(1))/(\gamma^{p^n} - 1)$ is isomorphic to the Pontryagin dual of

$$H^0(\Psi_n, H^1(\Psi_\infty, \mathscr{F}[\pi^\infty])) \cong H^1(\Psi_n, \mathscr{F}[\pi^\infty]).$$

The local duality thus implies (2.10).

(2) Note that $H^1_{\mathrm{f}}(\Psi_n, T)$ coincides with the Kummer image of $\mathscr{F}(\mathfrak{m}_n)$ in $H^1(\Psi_n, T)$, and that $H^1_{\mathrm{f}}(\Psi_n, T^{\otimes -1}(1))$ coincides with the kernel of $\exp^*_{\Psi_n} : H^1(\Psi_n, T^{\otimes -1}(1)) \to \Psi_n$. Hence, by the commutative diagram (2.8), the proof concludes. $\square$

In the following, (2.10) will be often treated as an identification.

https://doi.org/10.1017/S147474802300021X Published online by Cambridge University Press

2.2.2. An optimal basis. We introduce a basis of the submodule of signed anticyclotomic local units and duality pairings, which will be used in the construction of local points.

We fix a Λ-basis $v_\pm$ of $V_\infty^{*,\pm}$ and regard it as an element of $\varprojlim_n H^1(\Psi_n, T^{\otimes -1}(1))$ via (2.7).

For $n \geq 0$, put $\Lambda_n = \mathcal{O}[\mathrm{Gal}(\Psi_n/\Phi)]$. Let $v_{\pm,n}$ denote the image of $v_\pm$ in $H^1(\Psi_n, T^{\otimes -1}(1))$ via (2.10). Let

$$(\ , \ )_n : H^1(\Psi_n, T) \times H^1(\Psi_n, T^{\otimes -1}(1)) \to \mathcal{O}$$

be the natural pairing.

Lemma 2.3.

(1) $\{v_{+,n}, v_{-,n}\}$ *is a* Λ_n*-basis of* $H^1(\Psi_n, T^{\otimes -1}(1))$.

(2) $(\ , \ )_n$ *is a perfect pairing.*

(3) $H^1_{\mathrm{f}}(\Psi_n, T)$ *and* $H^1_{\mathrm{f}}(\Psi_n, T^{\otimes -1}(1))$ *are orthogonal complements of each other under the pairing.*

Proof. The first assertion is a simple consequence of Theorem 2.1.

Note that $T^{\otimes -1}(1) \cong T^\tau$ as an $\mathcal{O}[G_\Phi]$-module, where T^τ denotes conjugation of T by the complex conjugate. Then, by [47, Prop. 4.5], $H^1(\Psi_n, T)$ and $H^1(\Psi_n, T^{\otimes -1}(1)) \cong H^1(\Psi_n, T)$ are $\mathcal{O}$-free, and we have natural identifications

$$H^1(\Psi_n, T) \otimes \Phi/\mathcal{O} = H^1(\Psi_n, T \otimes \Phi/\mathcal{O}), \ H^1(\Psi_n, T^{\otimes -1}(1)) \otimes \Phi/\mathcal{O} = H^1(\Psi_n, T^{\otimes -1}(1) \otimes \Phi/\mathcal{O}).$$

Hence, the local duality induces

$$H^1(\Psi_n, T) \cong \mathrm{Hom}_{\mathcal{O}}(H^1(\Psi_n, T^{\otimes -1}(1) \otimes \Phi/\mathcal{O}), \Phi/\mathcal{O}) = \mathrm{Hom}_{\mathcal{O}}(H^1(\Psi_n, T^{\otimes -1}(1)), \mathcal{O}),$$

where the isomorphism arises from the perfect pairing

$$H^1(\Psi_n, T) \times H^1(\Psi_n, T^{\otimes -1}(1) \otimes \Phi/\mathcal{O}) \to \Phi/\mathcal{O}.$$

It follows that the map $H^1(\Psi_n, T) \to \mathrm{Hom}_{\mathcal{O}}(H^1(\Psi_n, T^{\otimes -1}(1)), \mathcal{O})$ induced by $(\ , \ )_n$ is an isomorphism. By replacing T with $T^{\otimes -1}(1)$, the map $H^1(\Psi_n, T^{\otimes -1}(1)) \to \mathrm{Hom}_{\mathcal{O}}(H^1(\Psi_n, T), \mathcal{O})$ induced by $(\ , \ )_n$ is also an isomorphism, and hence, $(\ , \ )_n$ is perfect.

The assertion (3) then follows from the fact that $H^1_{\mathrm{f}}(\Psi_n, T) \otimes \mathbb{Q}_p$ is the orthogonal complement of $H^1_{\mathrm{f}}(\Psi_n, T^{\otimes -1}(1)) \otimes \mathbb{Q}_p$ under the base change of $(\ , \ )_n$, and vice versa. □

By Lemma 2.3, we have a perfect pairing

$$(\ , \ )_{\Lambda_n} : H^1(\Psi_n, T) \times H^1(\Psi_n, T^{\otimes -1}(1)) \to \Lambda_n, \quad (a, b) \mapsto \sum_{\sigma \in \mathrm{Gal}(\Psi_n/\Psi)} (a, b^\sigma)_n \sigma, \tag{2.11}$$

which is sesquilinear with respect to the involution ι of Λ_n induced by $\sigma \mapsto \sigma^{-1}$ for $\sigma \in \mathrm{Gal}(\Psi_n/\Phi)$. Let $\{v^\perp_{+,n}, v^\perp_{-,n}\} \subseteq H^1(\Psi_n, T)$ be the dual basis of $\{v_{-,n}, v_{+,n}\}$ with respect to $(\ , \ )_{\Lambda_n}$, that is,

$$\sum_{\sigma \in \mathrm{Gal}(\Psi_n/\Phi)} (v^\perp_{\pm,n}, v^\sigma_{\pm,n})_n \sigma = 0, \qquad \sum_{\sigma \in \mathrm{Gal}(\Psi_n/\Phi)} (v^\perp_{\pm,n}, v^\sigma_{\mp,n})_n \sigma = 1. \tag{2.12}$$

Note that $v^\perp_{\pm,n}$ depends on the choice of $v_\mp$ but is independent of $v_\pm$.

https://doi.org/10.1017/S147474802300021X Published online by Cambridge University Press

2.3. Local points

We introduce an optimal system of local points, which generate the signed submodules of the underlying Lubin–Tate group.

For $n \geq 0$, let $\Xi_n^{\pm}$ denote the set of $\chi \in \Xi^{\pm}$ factoring through $\mathrm{Gal}(\Psi_n/\Phi)$. For $\chi \in \Xi_n^{\pm}$, let

$$\lambda_\chi(x) = \frac{1}{p^n} \sum_{\sigma \in \mathrm{Gal}(\Psi_n/\Phi)} \chi^{-1}(\sigma)\lambda(x)^{\sigma}.$$

Define

$$\mathscr{F}(\mathfrak{m}_n)^{\pm} = \{x \in \mathscr{F}(\mathfrak{m}_n) |\ \lambda_\chi(x) = 0 \quad \text{for all } \chi \in \Xi_n^{\pm}\}.$$

We put

$$\omega_n^+ = \omega_n^+(\gamma) = \prod_{1 \leq k \leq n,\ k:\text{even}} \Phi_{p^k}(\gamma), \quad \omega_n^- = \omega_n^-(\gamma) = (\gamma - 1) \prod_{1 \leq k \leq n,\ k:\text{odd}} \Phi_{p^k}(\gamma) \in \mathbb{Z}[\gamma]$$

for $\Phi_{p^k}(X)$ the p^k-th cyclotomic polynomial, and we also put $\omega_0^+ = 1$ and $\omega_0^- = \gamma - 1$.

Definition 2.4 (local points). For $v_\pm$ and γ as above, let

$$c_n^{\pm} := c_n^{\pm}(v_\pm, \gamma) = \omega_n^{\mp} v_{\pm,n}^{\perp} \in H^1(\Psi_n, T).$$

Lemma 2.5. *For $n \geq 0$, $c_n^{\pm}$ lies in $H^1_{\mathrm{f}}(\Psi_n, T)$.*

Proof. It suffices to show that for a finite character χ of $\mathrm{Gal}(\Psi_n/\Phi)$, the image $\chi(c_n^{\pm})$ of $c_n^{\pm}$ under the natural map $H^1(\Psi_n, T) \to H^1(\Phi, V(\chi))$ lies in the finite part $H^1_{\mathrm{f}}(\Phi, V(\chi))$, where $V(\chi) := T \otimes \mathbb{Q}_p(\chi)$ denotes the twist of $T \otimes \mathbb{Q}_p$ by χ.

If $\chi \in \Xi^{\pm}$, then $\chi(\omega_n^{\mp}) = 0$, and so $\chi(c_n^{\pm}) \in H^1_{\mathrm{f}}(\Phi, V(\chi))$. If $\chi \in \Xi^{\mp}$, then $\delta_\chi(v_\pm) = 0$. Now, by Lemma 2.2 and (2.8), the image of $v_{\pm,n}$ under

$$H^1(\Psi_n, V^{\otimes -1}(1)) \to H^1(\Phi, V(\chi)^{\otimes -1}(1))$$

lies in the finite part, and it gives rise to a generator of $H^1_{\mathrm{f}}(\Phi, V(\chi)^{\otimes -1}(1))$ over $\Phi(\mathrm{Im}(\chi))$. Since $H^1_{\mathrm{f}}(\Phi, V(\chi))$ is the orthogonal complement of $H^1_{\mathrm{f}}(\Phi, V(\chi)^{\otimes -1}(1))$ with respect to the local duality, it thus follows that $\chi(c_n^{\pm})$ lies in the finite part. □

By Lemma 2.5, we may naturally regard $c_n^{\pm}$ as an element in $\mathscr{F}(\mathfrak{m}_n)$. In particular,

$$c_0^+ = (\gamma - 1) v_{+,0}^{\perp} = 0, \quad c_0^- = v_{-,0}^{\perp} \in \mathscr{F}(\Phi). \tag{2.13}$$

Salient features of the local points are given by the following.

Lemma 2.6. *Let $n \geq 1$.*

(1) *If $(-1)^{n+1} = \pm 1$, then*

$$\mathrm{Tr}_{n+1/n} c_{n+1}^{\pm} = c_{n-1}^{\pm}, \quad c_n^{\pm} = \mathrm{Res}_{n,n-1} c_{n-1}^{\pm}$$

for $\mathrm{Tr}_{n+1/n} : \mathscr{F}(\mathfrak{m}_{n+1}) \to \mathscr{F}(\mathfrak{m}_n)$ the trace map and $\mathrm{Res}_{n,n-1} : H^1(\Psi_{n-1}, T) \to H^1(\Psi_n, T)$ the restriction.

(2) *We have $c_n^{\pm} \in \mathscr{F}(\mathfrak{m}_n)^{\pm}$.*

https://doi.org/10.1017/S147474802300021X Published online by Cambridge University Press

Proof.

(1) First, note that an element x of $H^1(\Psi_n,T)$ is determined by the two elements $(x,v^\sigma_{+,n})_{\Lambda_n}$ and $(x,v^\sigma_{-,n})_{\Lambda_n} \in \Lambda_n$.

By definition,

$$(\mathrm{Tr}_{n+1/n} c^\pm_{n+1}, v_{\pm,n})_{\Lambda_n} = (c^\pm_n, v_{\pm,n})_{\Lambda_n} = (\mathrm{Res}_{n,n-1} c^\pm_{n-1}, v_{\pm,n})_{\Lambda_n} = 0.$$

As $(c^\pm_n, v_{\mp,n})_{\Lambda_n} = \omega^\mp_n$, it suffices to show that

$$(\mathrm{Tr}_{n+1/n} c^\pm_{n+1}, v_{\mp,n})_{\Lambda_n} = (c^\pm_{n-1}, v_{\mp,n})_{\Lambda_n} = \omega^\mp_n.$$

Since $\omega^\mp_{n+1} = \omega^\mp_n$, we have

$$(\mathrm{Tr}_{n+1/n} c^\pm_{n+1}, v_{\mp,n})_{\Lambda_n} \equiv (c^\pm_{n+1}, v_{\mp,n})_{\Lambda_{n+1}} \equiv \omega^\mp_n \bmod (\gamma^{p^n} - 1).$$

Since $\omega^\mp_n = \omega^\mp_{n-1}\Phi_n(\gamma)$ and $\{v_{\mp,n}\}_n$ is norm compatible,

$$\begin{aligned}(c^\pm_{n-1}, v_{\mp,n})_{\Lambda_n} &\equiv \sum_{\sigma\in\mathrm{Gal}(\Psi_n/\Phi)} (c^\pm_{n-1}, v^\sigma_{\mp,n-1})_{n-1}\sigma \equiv \omega^\mp_{n-1} \sum_{\sigma\in\mathrm{Gal}(\Psi_n/\Phi)} (v^\perp_{\pm,n-1}, v^\sigma_{\mp,n-1})_{n-1}\sigma \\ &\equiv \omega^\mp_{n-1} \sum_{\sigma\in\mathrm{Gal}(\Psi_n/\Psi_{n-1})} \sigma \equiv \omega^\mp_{n-1}\Phi_{n-1}(\gamma) = \omega^\mp_n.\end{aligned}$$

Therefore, the assertion follows.

(2) This is a simple consequence of (1). □

2.3.2. The $\pm$-subgroups.

Theorem 2.7. *Let $n \geq 0$.*

(a) *As Λ_n-modules, we have $\mathscr{F}(\mathfrak{m}_n) = \mathscr{F}(\mathfrak{m}_n)^+ \oplus \mathscr{F}(\mathfrak{m}_n)^-$.*
(b) *$\mathscr{F}(\mathfrak{m}_n)^\pm$ is generated by $c^\pm_n$.*

Proof. By definition,

$$\sum_{\sigma\in\mathrm{Gal}(\Psi_n/\Phi)} (c^\pm_n, v^\sigma_{\mp,n})_n\sigma = \omega^\mp_n \in \Lambda_n. \tag{2.14}$$

(a) Let $x \in \mathscr{F}(\mathfrak{m}_n)$ and consider

$$\sum_{\sigma\in\mathrm{Gal}(\Psi_n/\Phi)} (x, v^\sigma_{\mp,n})_n\sigma,$$

which lives[3] in $\omega^\mp_n\Lambda_n$. Thus, by (2.14), there exists $h_\pm(\gamma) \in \Lambda_n$ such that

$$\sum_{\sigma\in\mathrm{Gal}(\Psi_n/\Phi)} (x - h_\pm(\gamma)c^\pm_n, v^\sigma_{\mp,n})_n\sigma = 0.$$

[3]This follows by considering evaluation at finite characters.

https://doi.org/10.1017/S147474802300021X Published online by Cambridge University Press

Now, for $y := h_+(\gamma)c_n^+ + h_-(\gamma)c_n^-$, we have

$$\sum_{\sigma\in\mathrm{Gal}(\Psi_n/\Phi)} (x-y,u^\sigma)_n\sigma = 0$$

for arbitrary $u \in H^1(\Psi_n, T^{\otimes -1}(1))$. Hence, $x = y$.

(b) If $x \in \mathscr{F}(\mathfrak{m}_n)^\pm$, then

$$\sum_{\sigma\in\mathrm{Gal}(\Psi_n/\Phi)} (x,v^\sigma_{\pm,n})_n\sigma = 0.$$

Thus, we may choose $h_\mp$ as above to be 0. □

Remark 2.8. The local points are also elemental to Iwasawa theory of the $\mathbb{Z}_p$-anticyclotomic deformation of a non-CM elliptic curve over imaginary quadratic fields with p inert (cf. [9]).

3. Rubin *p*-adic *L*-function and global points

The main results are Theorems 3.9 and 3.16.

3.0.1. Notation

Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$. Fix $\iota_\infty : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and $\iota_p : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$.

For a number field L, let $G_L = \mathrm{Gal}(\overline{\mathbb{Q}}/L)$. For a finite dimensional $\mathbb{Q}_p$-vector space V endowed with a continuous G_L-action and v a prime of L, the Bloch–Kato subgroup is given by

$$H^1_{\mathrm{f}}(L_v,V) = \begin{cases} \ker\left(H^1(L_v,V) \to H^1(L_v, V\otimes B_{\mathrm{crys}})\right) & (v \mid p), \\ \ker\left(H^1(L_v,V) \to H^1(L_v^{\mathrm{ur}},V)\right) & (v \nmid p). \end{cases}$$

If M denotes V or a $\mathbb{Z}_p$-lattice in V, then the Bloch–Kato Selmer group is defined as

$$H^1_{\mathrm{f}}(L,M) = \ker\left(H^1(L,M) \to \prod_v \frac{H^1(L_v,V)}{H^1_{\mathrm{f}}(L_v,V)}\right).$$

For an extension N/L of number fields, let $\mathrm{Ind}_L^N(\cdot)$ denote the induction $\mathrm{Ind}_{G_L}^{G_N}(\cdot)$.

For an abelian variety A, let $T_p(A)$ denote the p-adic Tate module and put $V_p(A) = T_p(A)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$.

3.1. Elements of Selmer groups

3.1.1. The set-up. Let K be an imaginary quadratic field of discriminant $-D_K < 0$ and H the Hilbert class field. Suppose

$$p \text{ is inert in } K. \tag{inr}$$

Let K_∞ be the anticyclotomic $\mathbb{Z}_p$-extension of K and K_n the n-th layer. Let G^- also denote $\mathrm{Gal}(K_\infty/K)$.

https://doi.org/10.1017/S147474802300021X Published online by Cambridge University Press

Let φ be a Hecke character over K of infinity type (1,0) such that the Hecke character $\varphi \circ N_{H/K}$ is associated to a $\mathbb{Q}$-curve E over H which has good reduction at each prime of H above p. In particular, E satisfies the Shimura condition. Fix a minimal Weierstrass model of E over $\mathcal{O}_{H,\mathfrak{p}} \cap H = \mathcal{O}_\Phi \cap H$ for $\mathfrak{p} \mid p$ the prime of H arising via ι_p and let ω be the Néron differential. Pick a non-zero $b_E \in H^1(E(\mathbb{C}),\mathbb{Z}_{(p)}) \cong \mathbb{Z}_{(p)} \otimes \mathcal{O}_K$ and define a CM period $\Omega \in \mathbb{C}^\times$ by

$$\mathrm{per}_{E/H}(\omega) = \Omega b_E$$

for $\mathrm{per}_{E/H} : \mathrm{coLie}(E) \to H^1(E(\mathbb{C}),\mathbb{Q}) \otimes_K \mathbb{C}$ the period map.

In this section, let $\mathcal{O}$ denote the integer ring of a finite extension of Φ which contains the Hecke field $K(\varphi(\widehat{K}^\times))$ for $\widehat{K} := K \otimes \varprojlim_m \mathbb{Z}/m\mathbb{Z}$. Let $\mathfrak{f}$ be the conductor of φ. Let T be the p-adic Galois representation of G_K associated to φ, which is an $\mathcal{O}$-module free of rank one so that its restriction to G_H is $T_pE \otimes_{\mathcal{O}_\Phi} \mathcal{O}$. Since

$$\hat{E} \cong \mathscr{F}$$

as formal groups over $\mathcal{O}_\Phi$, the results in §2 may be utilized by replacing $\mathscr{F}$ with $\hat{E}$ and identifying T_pE with $T_\pi E$ via

$$(t_n)_n \mapsto ((-1)^n t_n)_n.$$

We put $T^{\otimes -1} = \mathrm{Hom}_{\mathcal{O}}(T,\mathcal{O})$ and note that $T^{\otimes -1}(1)$ is identified with the complex conjugation of T as follows. Let τ be the complex conjugation. We have a natural decomposition

$$T \otimes_{\mathbb{Z}_p} \mathcal{O} = T_pE \otimes_{\mathcal{O}_\Phi} (\mathcal{O}_\Phi \otimes_{\mathbb{Z}_p} \mathcal{O}) = T \times (T_pE \otimes_{\mathcal{O}_\Phi,\tau} \mathcal{O}),$$

where $\otimes_{\mathcal{O}_\Phi,\tau}$ is the tensor product with respect to the map $\mathcal{O}_\Phi \to \mathcal{O}$ induced by τ and the natural inclusion. This decomposition and the base change of the Weil pairing over $\mathcal{O}$ induce a perfect $\mathcal{O}$-bilinear pairing

$$T \times (T_pE \otimes_{\mathcal{O}_\Phi,\tau} \mathcal{O}) \to \mathcal{O}(1).$$

Thus, we may naturally identify $T^{\otimes -1}(1)$ with $T_pE \otimes_{\mathcal{O}_\Phi,\tau} \mathcal{O}$. Since $\varphi(\tau(\mathfrak{a})) = \overline{\varphi(\mathfrak{a})}$ for an integral ideal $\mathfrak{a}$ of $\mathcal{O}_K$ relatively prime to $\mathfrak{f}$ (cf. [27, Lem. 11.1.1]), $T_pE \otimes_{\mathcal{O}_\Phi,\tau} \mathcal{O}$ is naturally identified with the complex conjugation T^τ of the G_K-representation T. Hence, we have a natural isomorphism of $\mathcal{O}[G_K]$-modules $T^{\otimes -1}(1) \cong T^\tau$, which induces an isomorphism $H^1(K_n,T^{\otimes -1}(1)) \cong H^1(K_n,T^\tau)$. Since the complex conjugation gives rise to an isomorphism $H^1(K_n,T^\tau) \cong H^1(K_n,T)^\iota$ of Λ-modules, we often identify

$$H^1(K_n,T^{\otimes -1}(1)) = H^1(K_n,T)^\iota, \tag{3.1}$$

where $\iota : \Lambda \to \Lambda$ denotes the involution induced by $g \mapsto g^{-1}$ for $g \in G^-$ and for a Λ-module M, we put $M^\iota = M \otimes_{\Lambda,\iota} \Lambda$.

3.1.2. Construction of Selmer elements. Based on elliptic units, we associate a Selmer element to a Hecke character.

The following existence is due to Coates and Wiles [20] (cf. [46], [30, Prop. 15.9]).

Proposition 3.1. *There exists an elliptic unit*

$$z = (z_n)_n \in \varprojlim_n H^1(K_n, T^{\otimes -1}(1)) \tag{3.2}$$

associated to b_E *such that for a character* χ *of* $\mathrm{Gal}(K_n/K)$*, we have*

$$\sum_{\sigma \in \mathrm{Gal}(K_n/K)} \chi(\sigma) \exp^*_{K_n}(\mathrm{loc}_p(z_n^\sigma)) = \frac{L_{p\mathfrak{f}}(\overline{\varphi}\chi, 1)}{\Omega}\omega. \tag{3.3}$$

Here,

$$\exp^*_{K_n} : H^1(K_n \otimes_K K_p, T^{\otimes -1}(1)) \to D^0_{\mathrm{cris}}(V^{\otimes -1}(1)) \otimes_K K_n = (\mathrm{coLie}(E_{/K_p}) \otimes_{K_p} \mathcal{O}[1/p]) \otimes_K K_n$$

is the dual exponential map, $K_p = K \otimes \mathbb{Q}_p = \Phi$*, and*

$$\mathrm{loc}_p : H^1(K_n, T^{\otimes -1}(1)) \to H^1(K_n \otimes_K K_p, T^{\otimes -1}(1)) = \prod_{w|p} H^1(\Psi_n, T^{\otimes -1}(1))$$

is the localization as w *varies over the places of* K_n *above* p.

We put $\mathcal{O}_\chi = \mathcal{O}[\mathrm{Im}(\chi)]$ and let $\mathcal{O}(\chi)$ denote the $\mathcal{O}[G_K]$-module with the underlying space $\mathcal{O}_\chi$ and the G_K-action being χ. For an $\mathcal{O}[G_K]$-module M, let $M(\chi) = M \otimes_{\mathcal{O}} \mathcal{O}(\chi)$ and

$$M^\chi = \{m \in M \otimes \mathcal{O}_\chi \mid gm = \chi(g)m \quad \text{for all } g \in G_K\}.$$

Definition 3.2 (Selmer element). For a character χ of $\mathrm{Gal}(K_n/K)$, let $z_\chi \in H^1(K_n, T^{\otimes -1}(1))^{\chi^{-1}}$ denote the image of the elliptic unit z_n under the composite

$$\begin{aligned} H^1(K_n, T^{\otimes -1}(1)) &\xrightarrow{\cong} H^1(K_n, T^{\otimes -1}(1)(\chi)) \to H^1(K, T^{\otimes -1}(1)(\chi)) \\ &\xrightarrow{\cong} H^0(K, H^1(K_n, T^{\otimes -1}(1)(\chi))) = H^1(K_n, T^{\otimes -1}(1))^{\chi^{-1}}. \end{aligned} \tag{3.4}$$

Here, the second and third maps are corestriction and restriction, respectively.

Note that

$$z_\chi = \sum_{\sigma \in \mathrm{Gal}(K_n/K)} \chi(\sigma) z_n^\sigma. \tag{3.5}$$

Since $(H^1(K_n, T)^\iota)^{\chi^{-1}} = H^1(K_n, T)^\chi$ by (3.1), we regard

$$z_\chi \in H^1(K_n, T)^\chi.$$

Lemma 3.3. *If* $L(\varphi\chi^{-1}, 1) = 0$*, then* $z_\chi \in H^1_{\mathrm{f}}(K_n, T)^\chi$.

Proof. By definition and [30, Prop. 15.9], z_χ lies in the image of

$$\varprojlim_m H^1(K(\mathfrak{f}p^m), T^{\otimes -1}(1)) \to H^1(K_n, T^{\otimes -1}(1)),$$

where $K(\mathfrak{f}p^m)$ denotes the ray class field of K of conductor $\mathfrak{f}p^m$.

For a prime $v \nmid p$ of K_n and a prime $w \mid v$ of $\cup_{m \geq 1} K(\mathfrak{f}p^m)$, note that the completion of $\cup_m K(\mathfrak{f}p^m)$ at w contains the maximal pro-p unramified extension of $K_{n,v}$, and so

https://doi.org/10.1017/S147474802300021X Published online by Cambridge University Press

$\mathrm{loc}_v(z_\chi) \in H^1_{\mathrm{f}}(K_{n,v}, T^{\otimes -1}(1))$. Since $L(\varphi\chi^{-1}, 1) = 0$, by the explicit reciprocity law (3.3) and (3.5),

$$\exp^*_{K_n}(\mathrm{loc}_p(z_\chi)) = 0.$$

As the Bloch–Kato subgroup $\oplus_{v|p} H^1_{\mathrm{f}}(K_{n,v}, T^{\otimes -1}(1))$ coincides with the kernel of $\exp^*_{K_n}$, the proof concludes. □

3.2. Global points

3.2.1. Mordell–Weil groups over $\mathbb{Q}$. In this subsection, for sufficiently large n with $(-1)^{n+1} = -W(\varphi)$ and χ an anticyclotomic character of conductor p^{n+1}, the Selmer element z_χ is shown to arise from a rational point.

Let χ be a finite character of $\mathrm{Gal}(K_\infty/K)$ and $f_\chi \in S_2(\Gamma_0(D_K N_{K/\mathbb{Q}}(\mathfrak{f}\mathfrak{c}_\chi)))$ the theta series attached to $\varphi\chi^{-1}$, where $\mathfrak{c}_\chi$ denotes the conductor of χ. In particular, $L(f_\chi, s) = L(\varphi\chi^{-1}, s)$. Let F_χ denote the Hecke field. Fix an abelian variety A_χ over $\mathbb{Q}$ of dimension $[F_\chi : \mathbb{Q}]$ with an $\mathcal{O}_{F_\chi}$-action so that

$$L(A_\chi, s) = \prod_{\sigma: F_\chi \hookrightarrow \overline{\mathbb{Q}}} L(f^\sigma_\chi, s).$$

In this subsection, $\mathcal{O}$ is enlarged to also contain the image of χ, and $\mathfrak{m}$ denotes the maximal ideal.

We begin with a preliminary.

Lemma 3.4. *We have*

$$\mathrm{Ind}^K_{\mathbb{Q}}(T^{\otimes -1}(1)(\chi)) \otimes_{\mathcal{O}} \mathcal{O}/\mathfrak{m} \cong \mathrm{Ind}^K_{\mathbb{Q}}(T(\chi^{-1})) \otimes_{\mathcal{O}} \mathcal{O}/\mathfrak{m},$$

which is an irreducible $G_{\mathbb{Q}}$-representation.

Proof. Note that $T^{\otimes -1}(1)(\chi) \cong T(\chi^{-1})^\tau$ as an $\mathcal{O}[G_K]$-module, and so the first assertion follows.

As for the irreducibility, in light of the proof of [30, Lem. 15.20], it suffices to show that for a finite character χ of $\mathrm{Gal}(K_\infty/K)$, there exists an integral ideal $\mathfrak{b}$ of K relatively prime to $p\mathfrak{f}$ such that

$$(\varphi\chi^{-1}(\mathfrak{b}) - \varphi\chi^{-1}(\bar{\mathfrak{b}}))N_{K/\mathbb{Q}}(\mathfrak{b}) \in \mathcal{O}^\times. \tag{3.6}$$

We put $\mathfrak{b} = (1 + f\sqrt{-D_K})\mathcal{O}_K$ for $f = N_{K/\mathbb{Q}}(\mathfrak{f}) \in \mathbb{Z}$. As p is inert in K, note that p is relatively prime to $N_{K/\mathbb{Q}}(\mathfrak{b}) = 1 + f^2 D_K$, i.e. $N_{K/\mathbb{Q}}(\mathfrak{b}) \in \mathcal{O}^\times$. Since $p \nmid f D_K$ and $1 + f\sqrt{-D_K} \equiv 1 \bmod \mathfrak{f}$, we have $\varphi(\mathfrak{b}) - \varphi(\bar{\mathfrak{b}}) = 2f\sqrt{-D_K} \in \mathcal{O}^\times$, and so $\varphi(\mathfrak{b})\gamma_{\mathfrak{b}} - \varphi(\bar{\mathfrak{b}})\gamma_{\bar{\mathfrak{b}}} \in \Lambda^\times$, from which (3.6) follows. (Here, $\gamma_{\mathfrak{a}} \in G^-$ denotes the element which corresponds via the Artin map to an integral ideal $\mathfrak{a}$ of K relatively prime to $p\mathfrak{f}$.) □

Put $V = T \otimes \mathbb{Q}_p \cong \mathcal{O}[1/p]$ and $V_p(A) = T_p(A_\chi) \otimes \mathbb{Q}_p \cong (F_\chi \otimes \mathbb{Q}_p)^{\oplus 2}$. We embed F_χ into $\mathcal{O}[1/p]$ via ι_p and notice an abstract isomorphism

$$\mathrm{Ind}^K_{\mathbb{Q}}(V(\chi^{-1})) \cong V_p(A_\chi) \otimes_{F_\chi \otimes \mathbb{Q}_p} \mathcal{O}[1/p],$$

https://doi.org/10.1017/S147474802300021X Published online by Cambridge University Press

which follows from considering the action of Frobenius elements. By Lemma 3.4, there exists an isomorphism $\mathrm{Ind}_{\mathbb{Q}}^{K}(T(\chi^{-1})) \cong T_p(A_\chi) \otimes_{\mathcal{O}_{F_\chi} \otimes \mathbb{Z}_p} \mathcal{O}$ of $\mathcal{O}[G_{\mathbb{Q}}]$-modules, and so we have an identification

$$H^1_{\mathrm{f}}(\mathbb{Q}, T_p(A_\chi) \otimes \mathcal{O}) \cong H^1_{\mathrm{f}}(K, T(\chi^{-1})). \tag{3.7}$$

Proposition 3.5. *Suppose that* $\mathrm{ord}_{s=1} L(\varphi\chi^{-1}, s) = r \in \{0,1\}$. *Then,* $\mathrm{rank}_{\mathcal{O}_{F_\chi}} A_\chi(\mathbb{Q}) = r$ *and the Tate–Shafarevich group* $Ш(A_{\chi/\mathbb{Q}})$ *is finite. In particular, if* $r = 1$*, we have*

$$A_\chi(\mathbb{Q}) \otimes \mathbb{Z}_p = H^1_{\mathrm{f}}(\mathbb{Q}, T_p(A_\chi)) \cong \mathcal{O}_{F_\chi} \otimes \mathbb{Z}_p.$$

Proof. Since $\mathrm{ord}_{s=1} L(f_\chi, s) = r$, by the main result of [8], there exists an imaginary quadratic field L such that

(i) $\mathrm{ord}_{s=1} L(f_{\chi/L}, s) = 1$ and

(ii) the pair (f_χ, L) satisfies the Heegner hypothesis.

Then, the Gross–Zagier formula [28], [55] implies that the Heegner point $y_L \in A_\chi(L)$ is non-torsion, and so the assertion is due to Kolyvagin [35] (see also [40]). As for the "in particular" part, note that $A_\chi(\mathbb{Q})$ is p-torsion-free by Lemma 3.4. □

Remark 3.6. The $r = 0$ case is due to Coates–Wiles [20] and Rubin [46], [48].

Let z_χ still denote the element of $H^1(K, T(\chi^{-1})) = H^1(K, T^{\otimes -1}(1)(\chi))$ which corresponds via (3.4) to the element z_χ as in (3.5). Suppose $L(\varphi\chi^{-1}, 1) = 0$. Then, by Lemma 3.3, we have $z_\chi \in H^1_{\mathrm{f}}(K, T(\chi^{-1}))$. Let

$$y_\chi \in H^1_{\mathrm{f}}(\mathbb{Q}, T_p(A_\chi) \otimes \mathcal{O})$$

denote the corresponding element via (3.7). An immediate consequence of Proposition 3.5 is the following.

Corollary 3.7. *If* $\mathrm{ord}_{s=1} L(\varphi\chi^{-1}, s) = 1$*, then* y_χ *arises from* $A_\chi(\mathbb{Q}) \otimes_{\mathcal{O}_{F_\chi}} \mathcal{O}$.

If $\mathrm{ord}_{s=1}(L(\varphi\chi^{-1}, s)) = 1$, then y_χ will be shown to be non-torsion (cf. Corollary 3.18). In our case, the latter is equivalent to being non-zero[4] by Lemma 3.4.

Remark 3.8. For any sufficiently large integer n with $(-1)^{n+1} = -W(\varphi)$ and χ a character of $\mathrm{Gal}(K_n/K)$ of conductor p^{n+1}, Rohrlich proved that $\mathrm{ord}_{s=1} L(\varphi\chi^{-1}, s) = 1$ (cf. [45]).

3.2.2. Anticyclotomic Mordell–Weil groups. This independent subsection presents an anticyclotomic variation of the Mordell–Weil groups.

For the identity Hecke character $\mathbb{1} =: 1$, we put $A = A_1$, $f = f_1$ and $F = F_1$. Let χ be a finite character of $\mathrm{Gal}(K_\infty/K)$ and n denote the maximum $\max\{0, \mathrm{ord}_p(\mathfrak{c}_\chi) - 1\}$. If $n = 0$, put $Ш(A_{/K_{n-1}}) = \{0\}$.

[4] A given element, such as y_χ, may a priori be zero.

https://doi.org/10.1017/S147474802300021X Published online by Cambridge University Press

Theorem 3.9. *Suppose that* $\mathrm{ord}_{s=1}L(\varphi\chi^{-1},s) = r \in \{0,1\}$.

(a) *We have*

$$\mathrm{rank}_{\mathcal{O}_\chi} A(K_n)^\chi = r[F:\mathbb{Q}],$$
$$(A(K_n)\otimes\mathbb{Z}_p)^\chi = H^1_{\mathrm{f}}(K_n, T_p(A))^\chi.$$

(b) *In particular, the quotient*

$$Ш(A_{/K_n})[p^\infty]/\mathrm{Im}\left(Ш(A_{/K_{n-1}})[p^\infty] \to Ш(A_{/K_n})[p^\infty]\right)$$

is finite.

Proof. Let B_n denote the Weil restriction $\mathrm{Res}_{K_n/K}(A_{/K_n})$ of A over K_n. By considering the Galois action on valued points of B_n, note that the Galois group $\mathrm{Gal}(K_n/K)$ embeds into $\mathrm{End}\,B_n$, which in turn implies

$$\mathrm{End}\,B_n = (\mathrm{End}\,A)[\mathrm{Gal}(K_n/K)]$$

as algebras (cf. [23, Thm. 3]).

In light of the decomposition $\mathbb{Q}[\mathrm{Gal}(K_n/K)] \cong \mathbb{Q}[\gamma]/(\Phi_{p^n}(\gamma)) \times \mathbb{Q}[\mathrm{Gal}(K_{n-1}/K)]$ and factorisation of the underlying L-functions, we have an isogeny

$$B_n \sim A_n \times B_{n-1} \tag{3.8}$$

of abelian varieties over K. Here, A_n is the abelian variety defined as a product of copies of A_χ with $\dim(A_n) = [F:\mathbb{Q}](p^n - p^{n-1})$. Note that the set of K-rational points is given by

$$A(K_n)\otimes\mathbb{Q} \cong (A_n(K)\otimes\mathbb{Q}) \oplus (A(K_{n-1})\otimes\mathbb{Q}).$$

Now, we consider $\mathrm{Gal}(K_n/K)$-action which leads to

$$(\gamma^{p^{n-1}} - 1)A(K_n)\otimes\mathbb{Q} \cong A_n(K)\otimes\mathbb{Q}, \tag{3.9}$$

and

$$(\gamma^{p^{n-1}} - 1)\left(T_p(Ш(A_{/K_n}))\otimes\mathbb{Q}_p\right) \cong T_p(Ш(A_{n/K}))\otimes\mathbb{Q}_p. \tag{3.10}$$

In light of the Gross–Zagier formula [28], [55] and Proposition 3.5, we have

$$\mathrm{rank}_{\mathbb{Z}}(A_n(\mathbb{Q})) = r(p^n - p^{n-1})[F:\mathbb{Q}], \quad Ш(A_{n/\mathbb{Q}})^\vee \otimes \mathbb{Q} = \{0\}, \tag{3.11}$$

and so

$$\mathrm{rank}_{\mathbb{Z}}(A_n(K)) = 2r(p^n - p^{n-1})[F:\mathbb{Q}], \quad Ш(A_{n/K})^\vee \otimes \mathbb{Q} = \{0\}. \tag{3.12}$$

Hence, in conjunction with (3.10), it follows that

$$\prod_{\chi_1}\left(T_p(Ш(A_{/K_n}))\otimes\mathbb{Q}_p\right)^{\chi_1} \cong (\gamma^{p^{n-1}} - 1)T_p(Ш(A_{/K_n}))\otimes\mathbb{Q}_p(\mu_{p^n}) = \{0\}, \tag{3.13}$$

where χ_1 ranges over the conjugates of χ.

(a) Recall the short exact sequence

$$0 \to (A(K_n)\otimes_{\mathbb{Z}}\mathbb{Z}_p)^\chi \to H^1_{\mathrm{f}}(K_n, T_p(A))^\chi \to T_p(Ш(A_{/K_n}))^\chi.$$

https://doi.org/10.1017/S147474802300021X Published online by Cambridge University Press

Now, as $T_p(\text{Ш}(A_{/K_n}))$ is p-torsion-free, (3.13) readily implies the second asserted equality of part (a).

Since p is unramified in K, observe $K[\gamma]/\Phi_{p^n}(\gamma)$ is a field with $\dim_K(K[\gamma]/\Phi_{p^n}(\gamma)) = p^n - p^{n-1}$. Naturally, $(\gamma^{p^{n-1}} - 1)A(K_n) \otimes \mathbb{Q}$ is a $K[\gamma]/\Phi_{p^n}(\gamma)$-vector space. So, in view of (3.9) and (3.12), it follows that

$$(\gamma^{p^{n-1}} - 1)A(K_n) \otimes \mathbb{Q} \cong (K[\gamma]/(\Phi_{p^n}(\gamma)))^{\oplus [F:\mathbb{Q}]}.$$

Hence, the evaluation at χ yields the first asserted equality of part (a).

(b) In view of (3.13), we have

$$\begin{aligned} T_p(\text{Ш}(A_{/K_n})) \otimes \mathbb{Q}_p &= \big(T_p(\text{Ш}(A_{/K_n})) \otimes \mathbb{Q}_p\big)^{\mathrm{Gal}(K_n/K_{n-1})} \\ &= \mathrm{Im}(T_p(\text{Ш}(A_{/K_{n-1}})) \to T_p(\text{Ш}(A_{/K_n}))) \otimes \mathbb{Q}_p, \end{aligned}$$

i.e. part (b) holds. □

Remark 3.10. The above argument is a variation of Rubin's argument for [3, Prop. A.8].

Corollary 3.11. *Suppose E is defined over K. Then, for any sufficiently large n,*

$$\mathrm{rank}_{\mathbb{Z}} E(K_n) - \mathrm{rank}_{\mathbb{Z}} E(K_{n-1}) = \varepsilon_n p^{n-1}(p-1).$$

Here, if $W(\varphi) = +1$, then $\varepsilon_n = 0$ (resp. 2) for n odd (resp. even) and the reverse in the case $W(\varphi) = -1$.

Proof. This is a simple consequence of Theorem 3.9 (a) and Remark 3.8. □

The corollary implies that new points of infinite order appear in the alternate anticyclotomic layers. As shown in Corollary 3.18 below, these points correspond to the Selmer elements y_χ.

Remark 3.12.

(i) Corollary 3.11 is originally due to Greenberg (unpublished, cf. [26, (1.10)]).

(ii) An analogue of Corollary 3.11 for Selmer groups appears in [2, Thm. A].

3.3. Rubin p-adic L-function and global points

The section presents a Rubin type special value formula for the Rubin p-adic L-function, which is a result towards the question (Q).

Assume that

$$p \nmid h_K. \tag{cp}$$

Then, the Galois group $\mathrm{Gal}(K_\infty/K)$ is naturally identified with $\mathrm{Gal}(\Psi_\infty/\Phi)$. For $n \geq 0$, let $\mathfrak{p}$ denote the prime of K_n above p.

3.3.1. Rubin p-adic L-function. Let ε be the sign of the root number $W(\varphi)$ of the functional equation of the Hecke L-function $L(\varphi, s)$. In light of (2.8) and (3.3), the image of $\mathrm{loc}_{\mathfrak{p}}(z) \in \varprojlim_n H^1(K_{n,\mathfrak{p}}, T^{\otimes -1}(1))$ in V_∞^* via (2.7) lives in $V_\infty^{*,\varepsilon}$.

https://doi.org/10.1017/S147474802300021X Published online by Cambridge University Press

Following [47, §10], we introduce the following.

Definition 3.13. A Rubin p-adic L-function $\mathscr{L} := \mathscr{L}_{b_E,v_\varepsilon} \in \Lambda$ is defined by

$$\mathscr{L}_{b_E,v_\varepsilon} \cdot v_\varepsilon = \mathrm{loc}_{\mathfrak{p}}(z) \in V^{*,\varepsilon} = \Lambda v_\varepsilon. \tag{3.14}$$

For an anticyclotomic character χ, let $\mathscr{L}(\chi)$ denote the evaluation at χ. For $\chi \in \Xi^\varepsilon$ (resp. $\chi \in \Xi^{-\varepsilon}$), note that $W(\varphi\chi) = +1$ (resp. $W(\varphi\chi) = -1$, cf. [24, p. 247]).

Lemma 3.14. *For $\chi \in \Xi^\varepsilon$, we have*

$$\mathscr{L}(\chi) = \frac{1}{\delta_{\chi^{-1}}(v_\epsilon)} \cdot \frac{L_{\mathfrak{p}\mathfrak{f}}(\overline{\varphi\chi},1)}{\Omega}.$$

Proof. The non-vanishing of $\delta_{\chi^{-1}}(v_\varepsilon)$ is a consequence of Theorem 2.1 and [47, Lem. 10.1]. Hence, the assertion follows by (2.8) and (3.3). □

3.3.2. A Rubin type formula. The subsection explores $\mathscr{L}(\chi)$ for $\chi \in \Xi^{-\varepsilon}$.

Let $\lambda_E : \hat{E}(\Psi_n) \otimes_{\mathcal{O}_\Phi} \mathcal{O} \to \Psi_n \otimes \mathcal{O}$ denote the homomorphism induced by the logarithm associated to $\hat{E}$. For a character χ of $\mathrm{Gal}(\Psi_n/\Psi)$ and $c \in \hat{E}(\Psi_n)$, let

$$\lambda_{E,\chi}(c) = p^{-n} \sum_{\sigma \in \mathrm{Gal}(\Psi_n/\Phi)} \chi^{-1}(\sigma)\lambda_E(c^\sigma).$$

Recall that $T|_{G_{K_\mathfrak{p}}}$ is identified with $T_p(E) \otimes \mathcal{O}$.

As in (3.1), we identify

$$H^1(\Psi_n,T)^\iota = H^1(\Psi_n,T^{\otimes -1}(1)), \quad \varprojlim_m H^1(\Psi_m,T)^\iota = \varprojlim_m H^1(\Psi_m,T^{\otimes -1}(1)), \tag{3.15}$$

by which an element v of $H^1(\Psi_n,T^{\otimes -1}(1))$ will be regarded as an element of $H^1(\Psi_n,T)$. In view of the identifications the pairings $(\ ,\ )_{\Lambda_m}$ in (2.11) induce a perfect pairing

$$(\ ,\ )_\Lambda : \varprojlim_m H^1(\Psi_m,T) \times \varprojlim_m H^1(\Psi_m,T) \to \Lambda,$$

which is Λ-bilinear (as the pairing (2.11) is sesquilinear). In the following, we regard $(\ ,\ )_n$ and $(\ ,\ )_{\Lambda_n}$ as pairings on $H^1(\Psi_n,T) \times H^1(\Psi_n,T)$.

Lemma 3.15. *We have*

$$(v_\pm, v_\mp)_\Lambda \in \Lambda^\times \text{ and } (v_\pm, v_\pm)_\Lambda = 0.$$

Proof. As for the first assertion, by Nakayama's lemma, it suffices to show that $(v_{+,0}, v_{-,0})_0 \in \mathcal{O}^\times$.

In view of Theorem 2.1,

$$V_\infty^*/(\gamma-1) = V_\infty^{*,+}/(\gamma-1) \oplus V_\infty^{*,-}/(\gamma-1) = \mathcal{O}v_{+,0} \oplus \mathcal{O}v_{-,0}, \tag{3.16}$$

https://doi.org/10.1017/S147474802300021X Published online by Cambridge University Press

where $v_{\pm,0}$ is the image of $v^{\pm}$ in $V_\infty^*/(\gamma-1)$. Note that $H^1_{\mathrm{f}}(\Phi,T)\cong\mathscr{F}(\mathfrak{m}_0)\cong\mathcal{O}$, and so by (3.16),

$$H^1_{\mathrm{f}}(\Phi,T)=V_\infty^{*,-}/(\gamma-1).$$

As $\delta_0(v_-)=0$, observe $v_{-,0}\in H^1_{\mathrm{f}}(\Phi,T)$ by Lemma 2.2. Recall $(\quad,\quad)_0$ is perfect and $H^1_{\mathrm{f}}(\Phi,T)$ is a maximal isotropic subgroup. Hence, (3.16) implies that $(v_{+,0},v_{-,0})_0\in\mathcal{O}^\times$.

We now consider the second assertion. For any $\chi\in\Xi^{\mp}$, note that $\delta_\chi(v_\pm)=0$, i.e. the image of $v_\pm$ under $\varprojlim_m H^1(\Phi_m,T)\to H^1(\Phi,V(\chi^{-1}))$ lies in the finite part $H^1_{\mathrm{f}}(\Phi,V(\chi^{-1}))$. Since $H^1_{\mathrm{f}}(\Phi,V(\chi^{-1}))$ is the orthogonal complement of itself under $(\quad,\quad)_n$, we have $\chi((v_\pm,v_\pm)_\Lambda)=0$. This implies $(v_\pm,v_\pm)_\Lambda=0$ as $\Xi^{\mp}$ is an infinite set. $\square$

From now, we fix v_+,v_- so that

$$(v_+,v_-)_\Lambda=1,$$

and then $v^{\perp}_{\pm,n}$ in (2.12) is identified with $v_{\pm,n}$ via (3.15).

The main result of this subsection is the following.

Theorem 3.16. *Let K be an imaginary quadratic field and $p\geq 5$ a prime satisfying (inr) and (cp). Let E be a $\mathbb{Q}$-curve with complex multiplication by $\mathcal{O}_K$ with good reduction at p, φ the associated Hecke character of K and ε the sign of the root number. Let $\mathscr{L}$ be the Rubin p-adic L-function as in (3.14).*

(a) *Let $\chi\in\Xi^{-\varepsilon}$ be a Hecke character with conductor p^{n+1}. Let $z_{\chi^{-1}}\in H^1(K_n,T_pE)^{\chi^{-1}}$ be the image of a system of elliptic units of E (cf. §3.1.2). Then,*

$$z_{\chi^{-1}}\in H^1_{\mathrm{f}}(K_n,T_pE)^{\chi^{-1}}$$

and we have[5]

$$\mathscr{L}(\chi)=\delta_{\chi^{-1}}(v_{-\varepsilon})\cdot\lambda_E(\mathrm{loc}_{\mathfrak{p}}(z_{\chi^{-1}}))=\frac{\omega_n^{-\varepsilon}(\chi(\gamma))}{\tau(\chi,\lambda_E(c_n^{\varepsilon}))}\cdot\lambda_E(\mathrm{loc}_{\mathfrak{p}}(z_{\chi^{-1}})),$$

where $\tau(\chi,\alpha):=\sum_{\sigma\in\mathrm{Gal}(K_n/K)}\chi(\sigma)\alpha^\sigma$.

(b) *If $\varepsilon=-1$, then*

$$\mathscr{L}(\mathbb{1})=\frac{1}{\lambda_E(v_{-,0})}\cdot\lambda_E(\mathrm{loc}_{\mathfrak{p}}(z_0)).$$

Proof. (a) By Definition 3.13, note that

$$\sum_{\sigma\in\mathrm{Gal}(K_n/K)}(v^{\perp}_{-\varepsilon,n},z_n^{\sigma})_n\sigma=\mathscr{L}(\gamma^{-1})\bmod(\gamma^{p^n}-1),$$

where z_n also denotes $\mathrm{loc}_{\mathfrak{p}}(z_n)$.

[5]Note that $\lambda_{E,\chi}(c_n^{\varepsilon})$ is non-zero by Theorem 2.7 (b).

https://doi.org/10.1017/S147474802300021X Published online by Cambridge University Press

In view of the explicit reciprocity law of Wiles (cf. [53]) and [47, Lem. 5.5], we have

$$\sum_{\sigma\in\mathrm{Gal}(K_n/K)}(v^{\perp}_{-\varepsilon,n},z_n^{\sigma})_n\chi^{-1}(\sigma)=(v^{\perp}_{-\varepsilon,n},\sum_{\sigma}z_n^{\sigma}\chi^{-1}(\sigma))_n$$
$$=\mathrm{Tr}_{\Psi_n(\mathrm{Im}(\chi))/\Phi(\mathrm{Im}(\chi))}\left[\exp^*(v^{\perp}_{-\varepsilon,n}),\log\left(\sum_{\sigma}z_n^{\sigma}\chi^{-1}(\sigma)\right)\right]$$
$$=\left[\sum_{\sigma\in\mathrm{Gal}(\Psi_n/\Phi)}\exp^*(\sigma v^{\perp}_{-\varepsilon,n})\chi(\sigma),\log\left(\sum_{\sigma}z_n^{\sigma}\chi^{-1}(\sigma)\right)\right]$$
$$=\delta_{\chi^{-1}}(v_{-\varepsilon})\cdot\lambda_E(z_{\chi^{-1}})$$

(see also [47, p. 413]). Here,

$$[\ \ ,\ \ ]:D_{\mathrm{dR}}(V)\otimes_{\Phi}\Psi_n\times D_{\mathrm{dR}}(V^{\otimes -1}(1))\otimes_{\Phi}\Psi_n\to\mathcal{O}[1/p]\otimes_{\Phi}\Psi_n$$

denotes the natural pairing, $\exp^*$ is the dual exponential map, and the last equality follows from (2.9) and the fact that $\sigma v^{\perp}_{-\varepsilon,n}$ corresponds to $\sigma^{-1}v_{-\varepsilon,n}$ under (3.15). Hence,

$$\mathscr{L}(\chi(\gamma))=\delta_{\chi^{-1}}(v_{-\varepsilon})\cdot\lambda_E(z_{\chi^{-1}}) \tag{3.17}$$

However,

$$\sum_{\sigma\in\mathrm{Gal}(K_n/K)}(\sigma c_n^{\varepsilon},v_{-\varepsilon,n})_n\sigma=\omega_n^{-\varepsilon}(\gamma)\bmod(\gamma^{p^n}-1),$$

and so

$$\delta_{\chi^{-1}}(v_{-\varepsilon})\cdot p^n\lambda_{E,\chi^{-1}}(c_n^{\varepsilon})=\omega_n^{-\varepsilon}(\chi(\gamma)).$$

Hence, (3.17) concludes the proof.

(b) This just follows by letting $n=0$ and $\chi=\mathbb{1}$ in the above argument. □

Remark 3.17.

(i) In view of Theorem 3.16 (b), if $\varepsilon=-1$, then

$$\mathscr{L}(\mathbb{1})=p^{-1}\lambda_E(\mathrm{loc}_{\mathfrak{p}}(z_0)) \tag{3.18}$$

up to an element in $\mathcal{O}^{\times}$.

(ii) One may seek a Coleman integration approach to Theorem 3.16. The preliminary study of a p-adic Eisenstein series in [5] maybe relevant.

(iii) A natural problem is to investigate a special value formula $\mathscr{L}(\chi)$ for anticyclotomic characters χ of infinity type $(j,-j)$ with $j>0$. It will be investigated in a forthcoming paper.

Corollary 3.18. *Let χ be a primitive character of* $\mathrm{Gal}(K_n/K)$ *so that* $\mathrm{ord}_{s=1}L(\varphi\chi,s)=1$. *Then,* $y_{\chi^{-1}}\in A_{\chi^{-1}}(\mathbb{Q})\otimes\mathcal{O}_{\chi}$, *as in Corollary 3.7, has the following properties.*

https://doi.org/10.1017/S147474802300021X Published online by Cambridge University Press

(i) $y_{\chi^{-1}}$ *is nontorsion.*

(ii) *We have*

$$\mathscr{L}(\chi) = d_\chi \cdot \lambda_{A_{\chi^{-1}}}(y_{\chi^{-1}})$$

for a non-zero $d_\chi \in \mathcal{O}_\chi[1/p]$ *and* $\lambda_{A_{\chi^{-1}}}$ *a formal group logarithm of the Néron model of* $A_{\chi^{-1}}$ *over* $\mathbb{Z}_{(p)}$.

Proof. The following is based on Iwasawa main conjectures [2], [12], to which we refer for notation.

Let ε denote the sign of the root number $W(\varphi)$. By [2, Thm. 3.6], the Selmer group $\mathscr{X}_\infty^\varepsilon$ has Λ-rank one. Let $\mathscr{X}_{\rm str}$ be the Pontryagin dual of the strict Selmer group $S_{\rm str} := \mathrm{Sel}_{\rm str}(K_\infty, V/T)$ (cf. [2, §2] or (4.1) below). Let $\mathscr{X}_{\rm rel}$ be defined analogously.

In light of Proposition 3.5 and [2, Thm. 5.2], the latter being the main conjecture[6], the χ^{-1}-specialization of $\mathrm{char}_\Lambda(\mathscr{X}^\varepsilon_{\infty,\rm tor})$ is non-zero, where $\mathrm{char}_\Lambda(\cdot)$ denotes the characteristic ideal. Observe that Proposition 3.5 also implies that the χ^{-1}-specialization of $\mathrm{char}_\Lambda(\mathscr{X}_{\rm str})$ is non-zero and then so is the χ^{-1}-specialization of $\mathrm{char}_\Lambda(\mathscr{X}_{\mathrm{rel},\Lambda-\rm tor})$ (cf. [2, Thm. 4.1]). Hence, in view of [2, (4.1), (4.4)], it follows that $z_{\chi^{-1}}$ is non-torsion, and the proof concludes by Theorem 3.16 (b). □

Remark 3.19.

(i) By Lemma 3.4, $A_\chi(\mathbb{Q}) \otimes \mathcal{O}_\chi$ is p-torsion-free.

(ii) If $\mathrm{ord}_{s=1} L(\varphi, s) = 1$, then

$$\mathscr{L}(\mathbb{1}) = p^{-1}\lambda_A(y_{\mathbb{1}}) \tag{3.19}$$

up to an element in $\mathcal{O}^\times$.

4. Rubin p-adic L-function and rational points

The main results are Theorems 4.8 and 4.18, and Proposition 4.14.

4.0.1. Notation

Let the setup be as in §3.3. In particular, $f \in S_2(\Gamma_0(N))$ denotes the theta series associated to the Hecke character φ. Let $F \subset \mathbb{C}$ denote the Hecke field of f.

Let $A_{/\mathbb{Q}}$ be a GL_2-type abelian variety so that

$$L(A,s) = \prod_{\sigma: F \hookrightarrow \mathbb{C}} L(f^\sigma, s)$$

(cf. §B.1). Let L denote the subfield of $\mathbb{C}$ generated by $\varphi(\widehat{K}^\times)$ over K, a finite extension of K containing F. As in §3, let $\mathcal{O}$ be the integer ring of the completion $L_\mathfrak{p}$ at the prime $\mathfrak{p}$ compatible with the embedding ι_p. Let $\lambda_f : A(\mathbb{Q}_p) \to F_\mathfrak{p}$ be a formal group logarithm arising from the differential attached to the newform f as in §A.3.

[6]This is an underlying Iwasawa main conjecture, whose proof relies on Rubin's conjecture (cf. Theorem 2.1).

https://doi.org/10.1017/S147474802300021X Published online by Cambridge University Press

Put $V(f) = V_p(A) \otimes_{F\otimes\mathbb{Q}_p} F_\mathfrak{p} \cong F_\mathfrak{p}^{\oplus 2}$ and $V_{L_\mathfrak{p}}(f) = V(f) \otimes_{F_\mathfrak{p}} L_\mathfrak{p}$. Our normalisation differs from [30]; namely, our $V_{L_\mathfrak{p}}(f)$ is isomorphic to $V_{L_\mathfrak{p}}(f)(1)$ of [30, §8.3] as a $G_\mathbb{Q}$-representation.

Replacing A by an isogeny, we may assume that A has $\mathcal{O}_F$-multiplication. For $W = A[\mathfrak{p}^\infty]$ (resp. V/T) and a finite extension M of $\mathbb{Q}$ (resp. K), define

$$\mathrm{Sel}_{\mathrm{str}}(M,W) = \ker\left(H^1(M,W) \to \prod_{v|p} H^1(M_v,W) \times \prod_{v\nmid p} \frac{H^1(M_v,W)}{H^1_{\mathrm{f}}(M_v,W)}\right). \tag{4.1}$$

Put $\mathrm{Sel}_{\mathrm{str}}(K_\infty,V/T) = \varinjlim_n \mathrm{Sel}_{\mathrm{str}}(K_n,V/T)$.

4.1. p-adic Beilinson formula: a first form

4.1.1.

Theorem 4.1. *Let $A_{/\mathbb{Q}}$ be a GL_2-type CM abelian variety. Let K be the corresponding imaginary quadratic field and F the Hecke field. Suppose that the root number of the associated CM newform is -1. Let $p \geq 5$ be a prime of good non-ordinary reduction for $A_{/\mathbb{Q}}$ with $p \nmid h_K$ and $\mathscr{L}$ the Rubin p-adic L-function as in (3.14). Then, there exists a rational point $P \in A(\mathbb{Q})$ with the following properties.*

(a) *We have*

$$\mathscr{L}(\mathbb{1}) = \frac{c}{\lambda_E(v_{-,0})} \cdot \lambda_f(P)^2$$

for some $c \in L^\times$.

(b) *P is non-torsion if and only if $\mathrm{ord}_{s=1} L(A,s) = [F:\mathbb{Q}]$.*

4.1.2. Tools of the proof.

We outline the strategy.

Elliptic units and Beilinson–Kato elements. The following link between zeta elements is a key.

Theorem 4.2. *Let $z = (z_n) \in \varprojlim_n H^1(K_n,T)$ be the elliptic unit as in (3.2) under the identification (3.1) and $z_f \in H^1(\mathbb{Q},V(f))$ a Beilinson–Kato element associated to the newform f. Then, under the identification (4.2), we have*

$$z_0 = z_f$$

up to an element in $L^\times$.

Proof. This is [30, (15.16.1)]. □

Beilinson-Kato elements and rational points. The following connects Beilinson-Kato elements with Heegner points.

Theorem 4.3. *If $L(f,1) = 0$, then there exists a rational point $P \in A(\mathbb{Q})$ with the following properties.*

https://doi.org/10.1017/S147474802300021X Published online by Cambridge University Press

(a) *We have*

$$\lambda_f(\mathrm{loc}_p(z_f)) = c_P\left(1 - \frac{a_p(f)}{p} + \frac{1}{p}\right)\lambda_f(P)^2$$

for some $c_P \in F^\times$ *and* $a_p(f)$ *the* p*-th Fourier coefficient of* f*.*

(b) P *is non-torsion if and only if* $\mathrm{ord}_{s=1} L(f,s) = 1$.

(c) *If the equivalent conditions in (b)hold, then*

$$c_P = \frac{L'(f,1)}{\Omega_f \langle P,P\rangle_\infty}$$

for $\langle , \rangle_\infty$ *the Néron-Tate height pairing.*

This is an evidence towards a conjecture of Perrin-Riou [42]. We refer to Appendix B for details (cf. Theorem B.3).

p-adic Gross-Zagier formula. Theorem 4.3 is based on the following interrelation between p-adic logarithm of a Heegner point and central derivative $\mathscr{L}'_{p,\gamma}(f,1)$ of the cyclotomic p-adic L-function $\mathscr{L}_{p,\gamma}(f,s)$ for $\gamma \in \{\alpha,\beta\}$ a root of the Hecke polynomial at p.

Theorem 4.4. *Suppose that the root number of* $L(f,s)$ *is* -1*. Then, there exists a point* $P \in A(\mathbb{Q})$ *and a non-zero constant* $c_P \in \mathbb{Q}$ *such that*

$$\left(1 - \frac{1}{\alpha}\right)^{-2}\mathscr{L}'_{p,\alpha}(f,1) - \left(1 - \frac{1}{\beta}\right)^{-2}\mathscr{L}'_{p,\beta}(f,1) = c_P\frac{(\beta-\alpha)}{[\omega_f,\varphi\omega_f]}\lambda_f(P)^2.$$

Moreover, P *is non-torsion if and only if* $\mathrm{ord}_{s=1}L(f,s) = 1$*, and*

$$c_P = \frac{L'(f,1)}{\Omega_f\langle P,P\rangle_\infty}.$$

This is a variant of the p-adic Gross–Zagier formula [32] (cf. Appendix A). In combination with Proposition B.4, it yields Theorem 4.3.

4.1.3. Proof of Theorem 4.1. The approach is based on Theorem 3.16 (b) and a link between elliptic units and Heegner points (cf. Theorems 4.2 and 4.3).

Proof. Fix an isomorphism $\mathrm{Ind}_{\mathbb{Q}}^K(V) \cong V_{L_\mathfrak{p}}(f)$ of $G_{\mathbb{Q}}$-representations and let

$$H^1(K,V) \cong H^1(\mathbb{Q}, V_{L_\mathfrak{p}}(f)) \tag{4.2}$$

be the induced identification. Let

$$z_f \in H^1(\mathbb{Q}, V(f))$$

be a Beilinson–Kato element as in [30, Thm. 12.5], which depends on a choice of an element in $H^1(A(\mathbb{C}),\mathbb{Q}) \cong F$ (cf. §B.2).

Since the root number of f is -1, $L(f,1)=0$, and so $\mathrm{loc}_p(z_f)\in H^1_{\mathrm{f}}(\mathbb{Q}_p,V(f))$ by Kato's reciprocity law [30, Thm. 12.5 (1)]. Now in view of Theorems 3.16 and 4.2, it follows that

$$\mathscr{L}(\mathbb{1})=\frac{1}{\lambda_E(v_{-,0})}\lambda_f(\mathrm{loc}_p(z_f)) \tag{4.3}$$

up to an element in $L^\times$. Hence, Theorem 4.3 concludes the proof. □

Remark 4.5. Theorem 4.1 concerns an anticyclotomic p-adic L-value, yet its proof relies on central derivative of cyclotomic p-adic L-functions.

4.2. p-adic Beilinson formula: a refined form

The main result is Theorem 4.8.

To consider a refinement of Theorem 4.1, we first specify an abelian variety A in the associated isogeny class (cf. §4.2.1), leading to an explicit form of Theorem 4.2 (cf. Proposition 4.12).

4.2.1. A CM abelian variety.

We begin with a preliminary (cf. [27, §5.1]).

Lemma 4.6. *Let E be a CM elliptic curve as in §3.1.1 and $j\in H$ denote its j-invariant. Then the following holds.*

(1) $[H:\mathbb{Q}(j)]=2$,

(2) $\mathbb{Q}(j)$ *has at least one real place and*

(3) $H=\mathbb{Q}(j)K$.

Suppose that

$$E \text{ is defined over } \mathbb{Q}(j). \tag{rt}$$

This holds if $j=j(\mathcal{O}_K)$ or, equivalently, $E(\mathbb{C})\cong\mathbb{C}/\mathcal{O}_K$ (cf. [27, (5.1.4) and Thm. 10.1.3]).

Fix a minimal Weierstrass model of E at $\mathfrak{p}$ over $\mathcal{O}_{H_\mathfrak{p}}\cap\mathbb{Q}(j)$ and let ω be the Néron differential.

Lemma 4.7. *The Weil restriction*

$$A:=\mathrm{Res}_{\mathbb{Q}(j)/\mathbb{Q}}(E)$$

is a GL_2*-type abelian variety associated to f.*

Proof. By [27, Thm. 15.2.5], A is a CM abelian variety[7] defined over $\mathbb{Q}$ which is simple over K. Since

$$L(A_{/\mathbb{Q}},s)=\prod_{\sigma:F\hookrightarrow\mathbb{C}}L(f^\sigma,s)$$

(cf. [27, Thm. 18.1.7]), the assertion follows. □

We now describe some structures on A arising from E.

[7] Note that A and $\mathbb{Q}(j)$ correspond to B and F of [27], respectively.

https://doi.org/10.1017/S147474802300021X Published online by Cambridge University Press

The canonical identification

$$H^1_{\mathrm{dR}}(A_{/\mathbb{Q}}) = H^1_{\mathrm{dR}}(E_{/\mathbb{Q}(j)})$$

is compatible with the Hodge filtration, via which the Néron differential ω of E gives an element ω_A of $\mathrm{coLie}(A_{/\mathbb{Q}})$. Since $H = \mathbb{Q}(j)K$, we have

$$\mathrm{coLie}(A_{/\mathbb{Q}}) \otimes_{\mathbb{Q}} L = \mathrm{coLie}(E_{/\mathbb{Q}(j)}) \otimes_{\mathbb{Q}} L = \mathrm{coLie}(E_{/H}) \otimes_K L.$$

So, the one-dimensional L-vector space $\mathrm{coLie}(A_{/\mathbb{Q}}) \otimes_F L$ leads to a one-dimensional subspace $S(\varphi)$ of $\mathrm{coLie}(E_{/H}) \otimes_K L$, namely its φ-part. This induces an identification

$$\mathrm{Ind}_{\mathbb{Q}}^K V = V_{L_{\mathfrak{p}}}(f), \tag{4.4}$$

which is the same as the identification [30, (15.11.2)] (recall that our $V_{L_{\mathfrak{p}}}(f)$ is isomorphic to the $L_{\mathfrak{p}}$-linear dual of that of [30]). In turn, $\lambda_E : H^1_{\mathrm{f}}(\Phi, V) \to L_{\mathfrak{p}}$ is identified with the logarithm map $\lambda_f : H^1_{\mathrm{f}}(\mathbb{Q}_p, V_{L_{\mathfrak{p}}}(f)) \to L_{\mathfrak{p}}$ associated to ω_A, where $\omega_A \in \mathrm{coLie}(A_{/\mathbb{Q}})$ is regarded as an element of $\mathrm{Fil}^0(D_{\mathrm{dR}}(V_{L_{\mathfrak{p}}}(f))) = \mathrm{coLie}(A_{/\mathbb{Q}}) \otimes_F L_{\mathfrak{p}}$.

Fix $b_A \in H^1(A(\mathbb{C}), \mathbb{Q})$ and define a period $\Omega_f \in \mathbb{R}^\times$ as in (B.3). Note that $u := \Omega_f / \Omega \in L^\times$.

4.2.2. Main result and applications.

Theorem 4.8. *Let $A_{/\mathbb{Q}}$ be a GL_2-type abelian variety associated to a CM newform f as in §4.2.1. Let K be the CM field and F the Hecke field. Suppose that (rt) holds and the root number of f equals -1. Let $p \geq 5$ be a prime of good non-ordinary reduction for $A_{/\mathbb{Q}}$ with $p \nmid h_K$ and $\mathscr{L}$ the Rubin p-adic L-function as in (3.14). Then there exists a rational point $P \in A(\mathbb{Q})$ with the following properties.*

(a) *We have*

$$\mathscr{L}(\mathbb{1}) = \mathscr{L}_{b_E, v_-}(\mathbb{1}) = u\left(1 + \frac{1}{p}\right)\frac{\lambda_f(P)^2}{\lambda_f(v_{-,0})} \cdot c_P$$

for some $c_P \in F^\times$.

(b) *P is non-torsion if and only if $\mathrm{ord}_{s=1} L(f,s) = 1$.*

(c) *If $\mathrm{ord}_{s=1} L(f,s) = 1$, then*

$$c_P = \frac{L'(f,1)}{\Omega_f \langle P, P \rangle_\infty}.$$

Part (a) leads to the following p-adic construction of a rational point of infinite order.

Corollary 4.9. *Let $E_{/\mathbb{Q}}$ be a CM elliptic curve with root number -1. Let $p \geq 5$ be a prime of good supersingular reduction for $E_{/\mathbb{Q}}$ and $\mathscr{L}_E$ the Rubin p-adic L-function as in (3.14). Suppose that $\mathrm{ord}_{s=1} L(E,s) = 1$, and the Birch–Swinnerton-Dyer formula is true for $E_{/\mathbb{Q}}$. Then,*

$$\exp_{E,\omega}\left(\#E(\mathbb{Q})_{\mathrm{tors}}\sqrt{\frac{\lambda_E(v_{-,0})\cdot\mathscr{L}(\mathbb{1})}{(1+p^{-1})u\prod_\ell c_\ell}}\right)\in E(\mathbb{Q})$$

is a rational point of infinite order, where c_ℓ denotes the Tamagawa number at ℓ.

Remark 4.10.

(i) The BSD formula is known to be true up to an element in $\mathbb{Z}[\frac{1}{\#\mathcal{O}_K^\times\cdot N}]^\times$ (cf. [32, Cor. 1.4]).

(ii) The rational point is independent of the choices involved, besides that of the square root.

(iii) Rubin initiated p-adic construction of rational points of infinite order (cf. [50, Thm. 10.4].)

Another application is the following variant of Corollary 3.11.

Corollary 4.11. *Let $E_{/\mathbb{Q}}$ be a CM elliptic curve and K the CM field. Let $p\geq 5$ be a prime of good supersingular reduction for $E_{/\mathbb{Q}}$ and K_n the n^{th}-layer of the anticyclotomic $\mathbb{Z}_p$-extension of K.*

(i) *If $L(E_{/\mathbb{Q}},1)/\Omega$ is a p-adic unit, then for all $n\geq 1$,*

$$\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_{p^\infty}(E_{/K_n})-\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_{p^\infty}(E_{/K_{n-1}})=\varepsilon_n p^{n-1}(p-1),$$

where $\varepsilon_n=0$ (resp. 2) for n odd (resp. even).

(ii) *Suppose that $\mathrm{ord}_{s=1}L(E_{/\mathbb{Q}},s)=1$ and there exists a rational point $P\in E(\mathbb{Q})$ whose image generates the $\mathbb{Z}_p$-module $E(\mathbb{Q}_p)/E(\mathbb{Q}_p)_{\mathrm{tor}}$. If*

$$L'(E_{/\mathbb{Q}},1)/\Omega\langle P,P\rangle_\infty$$

is a p-adic unit, then for all $n\geq 1$,

$$\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_{p^\infty}(E_{/K_n})-\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_{p^\infty}(E_{/K_{n-1}})=\varepsilon_n p^{n-1}(p-1),$$

where $\varepsilon_n=0$ (resp. 2) for n even (resp. odd).

In particular, if $Ш(E_{/K_n})$ is finite, then

$$\mathrm{rank}_{\mathbb{Z}}E(K_n)-\mathrm{rank}_{\mathbb{Z}}E(K_{n-1})=\varepsilon_n p^{n-1}(p-1).$$

Proof. We first consider the case (i).

Since $L(\bar{\varphi},1)/\Omega$ is a p-adic unit, note that $\varepsilon(\varphi)=+1$ and

$$\mathscr{L}\in\Lambda^\times.$$

For $\chi\in\Xi^+$, we then have $L(\varphi\chi,1)\neq 0$ and so $\mathrm{rank}_{\mathcal{O}_\chi}E(K_n)^{\chi^{-1}}=0$ by Theorem 3.9 (a) where n denotes $\max\{0,\mathrm{ord}_p(\mathfrak{c}_\chi)-1\}$. Now, let $\chi\in\Xi^-$. In view of Theorem 3.16,

$$\mathrm{loc}_\mathfrak{p}(z_{\chi^{-1}})\neq 0.$$

Hence, the image of z in S_{rel} is a $\Lambda_\mathfrak{q}$-basis for $S_{\mathrm{rel},\mathfrak{q}}$ up to tensoring with $\mathbb{Q}_p$, where S_{rel} denotes the relaxed compact Selmer group and $\mathfrak{q}$ the prime ideal of Λ corresponding

https://doi.org/10.1017/S147474802300021X Published online by Cambridge University Press

to the χ^{-1}-specialization. In turn, $\mathscr{X}_{\mathrm{str},\mathfrak{q}}$ is finite by [2, Prop. 3.3] and then so is $H^2(\mathcal{O}_K[\frac{1}{p}],T(\chi))$. Hence, Tate's Euler characteristic formula implies

$$\mathrm{rank}_{\mathcal{O}_\chi} H^1(\mathcal{O}_K[\frac{1}{p}],T(\chi)) = 1.$$

Since $z_{\chi^{-1}} \in H^1_{\mathrm{f}}(K,T(\chi))$ by Lemma 3.3, we conclude that $\mathrm{rank}_{\mathcal{O}_\chi} H^1_{\mathrm{f}}(\mathcal{O}_K[\frac{1}{p}],T(\chi)) = 1$. The assertion follows from this.

The case (ii) is similarly proven by using Theorem 4.8. □

4.2.3. Elliptic units and Beilinson–Kato elements.

Proposition 4.12. *Let $z = (z_n) \in \varprojlim_n H^1(K_n,T)$ be the elliptic unit as in (3.2) under the identification (3.1) and $z_{f,0} \in H^1(\mathbb{Q},V(f))$ the Beilinson–Kato element associated to the newform f as in (4.8). Then, under the identification (4.7), we have*

$$z_0 = u \cdot z_{f,0},$$

where $u := \Omega_f/\Omega \in L^\times$.

Proof. By [30, Lem. 15.11 (2)], there is a unique isomorphism

$$\mathrm{Ind}_{\mathbb{R}}^{\mathbb{C}} H^1(E(\mathbb{C}),\mathbb{Q}) \otimes_K L \cong H^1(A(\mathbb{C}),\mathbb{Q}) \otimes_F L \tag{4.5}$$

of $L[\mathrm{Gal}(\mathbb{C}/\mathbb{R})]$-modules such that the following diagram

$$\begin{tikzcd} S(\varphi) \arrow[r, "\mathrm{per}_\varphi"] \arrow[d, "="] & \mathrm{Ind}_{\mathbb{R}}^{\mathbb{C}}(H^1(E(\mathbb{C}),\mathbb{Q}) \otimes_K \mathbb{C}) \arrow[d, "(4.5)"] \\ \mathrm{coLie}(A/\mathbb{Q}) \otimes_F L \arrow[r, "\mathrm{per}_f"] & H^1(A(\mathbb{C}),\mathbb{Q}) \otimes_F \mathbb{C} \end{tikzcd} \tag{4.6}$$

commutes. Here, $H^1(A(\mathbb{C}),\mathbb{Q})$ is regarded as a $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$-module via the complex conjugation on $A(\mathbb{C})$, per_φ is the period map induced by that of E (cf. [30, §15.8]) and the right vertical map is the base change of (4.5) via $L \subseteq \mathbb{C}$.

Recall that $z \in \varprojlim_n H^1(K_n,T)$ is the image of an element $\mathbf{z}^{\mathrm{ell}} \in \varprojlim_n H^1(K(\mathfrak{f}p^n),T)$ associated to b_E as in [30, Prop. 15.9] under the corestriction map

$$\varprojlim_n H^1(K(\mathfrak{f}p^n),T) \to \varprojlim_n H^1(K_n,T),$$

where $\mathfrak{f}$ denotes the conductor of φ and $K(\mathfrak{f}p^n)$ the ray class field of K of conductor $\mathfrak{f}p^n$ (cf. [30, p. 254]). Let $\mathbb{Q}_n$ be the n-th layer of the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty$ of $\mathbb{Q}$. Let

$$z^{\mathrm{ell}} = (z_n^{\mathrm{ell}}) \in \varprojlim_n H^1(\mathbb{Q}_n,T(f)) \otimes L_{\mathfrak{p}}$$

denote the image of $\mathbf{z}^{\mathrm{ell}}$ under

$$\varprojlim_n H^1(K(\mathfrak{f}p^n),T) \otimes L_{\mathfrak{p}} \to \varprojlim_n H^1(K \otimes \mathbb{Q}_n,T) \otimes L_{\mathfrak{p}} = \varprojlim_n H^1(\mathbb{Q}_n,T(f)) \otimes L_{\mathfrak{p}}.$$

Here, the first map is induced by the corestriction maps with respect to $K\otimes\mathbb{Q}_n \subseteq K(\mathfrak{f}p^n)$, and the equality is a consequence of (4.4) and Shapiro's lemma.

Note that $b_E = \Omega^{-1}\mathrm{per}_\varphi(\omega)$ maps to $\Omega^{-1}\mathrm{per}_f(\omega_A)$ under (4.5) and $\mathbf{z}^{\mathrm{ell}}$ is associated to b_E. Thus, in light of (4.6) and [30, (15.16.1)], it follows that z^{ell} coincides with the system of Beilinson–Kato elements associated to

$$\Omega^{-1}\mathrm{per}_f(\omega_A) \in H^1(A(\mathbb{C}),\mathbb{Q})\otimes_F L.$$

Since $\mathbb{Q}_\infty$ is a totally real field, the last assertion in [30, Thm. 12.5 (1)] implies that z^{ell} also coincides with the system of Beilinson–Kato elements associated to

$$\Omega^{-1}2^{-1}(1+\iota)\mathrm{per}_f(\omega_A),$$

and that $\mathfrak{z}_f$ coincides with the one associated to

$$b_A^+ := 2^{-1}(1+\iota)b_A = \Omega_f^{-1}2^{-1}(1+\iota)\mathrm{per}_f(\omega_A)$$

(cf. (B.3)), where ι denotes the involution induced by the complex conjugation on $A(\mathbb{C})$.

Therefore, we have

$$z_0^{\mathrm{ell}} = uz_{f,0}.$$

Since $z_0 = z_0^{\mathrm{ell}}$ in $H^1(K,V) = H^1(\mathbb{Q},V_{L_\mathfrak{p}}(f))$, the proposition follows. □

4.2.4. Proof of Theorem 4.8. We proceed as in the proof of Theorem 4.1 (cf. §4.1.3). The additional ingredient is Proposition 4.12.

Proof. By (4.4) and Shapiro's lemma, we have an identification

$$H^1(K,V) = H^1(\mathbb{Q},V_{L_\mathfrak{p}}(f)). \tag{4.7}$$

Let $T(f)$ be a Galois stable $\mathcal{O}_{F_\mathfrak{p}}$-lattice of $V(f)$.

Let

$$\mathfrak{z}_f = (z_{f,n}) \in \varprojlim_n H^1(\mathbb{Q}_n,T(f))\otimes\mathbb{Q}_p \tag{4.8}$$

be the Beilinson–Kato element associated to b_A as in [30, Thm. 12.5 (1)] (since our $V_{L_\mathfrak{p}}(f)$ is a Tate twist of that in [30], $\mathfrak{z}_f$ is the corresponding twist of $\mathbf{z}_{b_A}^{(p)}$ as in [30]). In particular, $\mathfrak{z}_f$ satisfies the explicit reciprocity law (B.4).

Note that $L(f,1)=0$, and so by Proposition 4.12,

$$z_0 = uz_{f,0} \in H^1_{\mathrm{f}}(K,V\otimes L_\mathfrak{p}) = H^1_{\mathrm{f}}(\mathbb{Q},V_{L_\mathfrak{p}}(f)). \tag{4.9}$$

Hence, Theorem 4.8 is a consequence of Theorems 3.16 (b) and 4.3. □

Remark 4.13. For a given b_E or ω, note that $\lambda_f(v_{-,0})\Omega\cdot\mathscr{L}(\mathbb{1})$ is independent of the choices of Ω and v_-. Moreover, the right-hand side of Theorem 4.8 (a) is independent of the choice of b_A.

https://doi.org/10.1017/S147474802300021X Published online by Cambridge University Press

4.3. Towards a conjecture of Perrin-Riou: primes of bad reduction

The conjecture [42] intertwines Beilinson–Kato elements and global arithmetic (cf. §B.1).

For a weight two elliptic newform g and $z_g \in H^1(\mathbb{Q},V)$ an associated p-adic Beilinson–Kato element, the conjecture predicts

$$\mathrm{loc}_p(z_g) \neq 0 \iff \mathrm{ord}_{s=1} L(g,s) \leq 1.$$

(cf. (B.2)).

Proposition 4.14. *Let φ be a self-dual Hecke character of an imaginary quadratic field K of infinity type $(1,0)$. Let $p \geq 5$ be a prime so that (inr) holds and $p \nmid h_K \cdot \mathrm{cond}^{\mathrm{r}}\varphi$. Let K_∞ be the anticyclotomic $\mathbb{Z}_p$-extension of K. For a finite character χ of $\mathrm{Gal}(K_\infty/K)$, let g be the theta series associated to the Hecke character $\varphi\chi^{-1}$. Let z_g be an associated Beilinson–Kato element. Then,*

$$\mathrm{ord}_{s=1} L(g,s) = 1 \implies \mathrm{loc}_p(z_g) \neq 0.$$

Proof. By Corollary 3.18, the localisation of the Selmer element y_χ is non-torsion. This element is defined using elliptic units as in (3.4). Hence, the assertion is a consequence[8] of Theorem 4.2. □

Remark 4.15. For non-trivial χ, an abelian variety A_χ associated to g does not have semistable reduction at p. Accordingly, the proposition complements [7], [17] and Theorem B.3. It is perhaps the first evidence towards Perrin-Riou's conjecture at primes of non-semistable reduction.

4.4. *p*-converse to a theorem of Gross–Zagier and Kolyvagin

Let the setting be as in §4.1.

4.4.1. Preliminary.

Proposition 4.16. *Suppose that $L(\varphi,1) = 0$. Then, the element $\mathrm{loc}_p(z_0) \in H^1_{\mathrm{f}}(K_p,V)$ is non-zero if and only if $\mathrm{ord}_{s=1} L(\varphi,s) = 1$.*

Proof. This is a consequence of Theorems 4.2 and 4.3. □

4.4.2. *p*-converse.

Theorem 4.17. *Let $A_{/\mathbb{Q}}$ be a GL_2-type CM abelian variety. Let K be the CM field and F the Hecke field. Suppose that (rt) holds and $\mathcal{O}_F \hookrightarrow \mathrm{End}A$. Let $p \geq 5$ be a prime of good non-ordinary reduction for $A_{/\mathbb{Q}}$ with $p \nmid h_K$, and $\mathfrak{p}$ a prime of F above p. If $\mathrm{Sel}_{\mathrm{str}}(\mathbb{Q},A[\mathfrak{p}^\infty])$ is finite, then*

$$\mathrm{ord}_{s=1} L(A,s) = [F:\mathbb{Q}] \cdot \mathrm{corank}_{\mathcal{O}_{F,\mathfrak{p}}} \mathrm{Sel}_{\mathfrak{p}^\infty}(A).$$

[8] The theorem is stated for CM elliptic newforms with good reduction at p, but it holds for any prime p (cf. [30, (15.16.1)]).

https://doi.org/10.1017/S147474802300021X Published online by Cambridge University Press

Proof. We have $A(\mathbb{Q}_p)\otimes_{\mathcal{O}_F} F_{\mathfrak{p}}/\mathcal{O}_{F_{\mathfrak{p}}} \cong F_{\mathfrak{p}}/\mathcal{O}_{F_{\mathfrak{p}}}$. So the exact sequence

$$0 \to \mathrm{Sel}_{\mathrm{str}}(\mathbb{Q}, A[\mathfrak{p}^\infty]) \to \mathrm{Sel}_{\mathfrak{p}^\infty}(A) \to A(\mathbb{Q}_p)\otimes_{\mathcal{O}_F} F_{\mathfrak{p}}/\mathcal{O}_{F_{\mathfrak{p}}} \tag{4.10}$$

and the finiteness of $\mathrm{Sel}_{\mathrm{str}}(\mathbb{Q}, A[\mathfrak{p}^\infty])$ imply that

$$\mathrm{corank}_{\mathcal{O}_{F,\mathfrak{p}}} \mathrm{Sel}_{\mathfrak{p}^\infty}(A) \le 1. \tag{4.11}$$

Observe[9]

$$\begin{aligned} \mathrm{Sel}_{\mathrm{str}}(K_\infty, V/T)^\vee \otimes \mathbb{Q}_p/(\gamma-1) &\cong \mathrm{Sel}_{\mathrm{str}}(K, V/T)^\vee \otimes \mathbb{Q}_p \\ &\cong \mathrm{Sel}_{\mathrm{str}}(\mathbb{Q}, A[\mathfrak{p}^\infty])^\vee \otimes_{\mathcal{O}_{F_{\mathfrak{p}}}} L_{\mathfrak{p}} \\ &= \{0\}. \end{aligned} \tag{4.12}$$

Thus, $z_0 \in H^1(K,T)$ is non-torsion by [2, Prop. 3.3 (ii)].

We now show

$$0 \ne \mathrm{loc}_{\mathfrak{p}}(z_0) \in H^1(K_{\mathfrak{p}}, V). \tag{4.13}$$

To begin, $\mathrm{Sel}_{\mathrm{str}}(K,V/T)$ is finite by (4.12). Put

$$p^a = |\mathrm{Sel}_{\mathrm{str}}(K,V/T)|.$$

Since $z_0 \in H^1(K,T)$ is non-torsion, pick an integer m such that $p^{-m+a}z_0 \in H^1(K,V)$ does not lie in the image of $H^1(K,T)$. Suppose that $\mathrm{loc}_{\mathfrak{p}}(z_0) = 0 \in H^1(K_{\mathfrak{p}},V)$. Then, as z_0 is unramified outside $\mathfrak{p}$, the image w_m of $p^{-m}z_0$ in $H^1(K,V/T)$ lies in $\mathrm{Sel}_{\mathrm{str}}(K,V/T)$ and so does $p^a w_m$. However,

$$p^a w_m = 0 \in H^1(K,V/T).$$

This contradiction yields (4.13).

- The case $W(\varphi) = +1$. In view of (3.3) and (4.13), we have $L(\varphi,1) \ne 0$. Hence, by the theorem of Coates-Wiles [20] and Rubin [46],
$$\mathrm{ord}_{s=1} L(A,s) = [F:\mathbb{Q}]\cdot \mathrm{corank}_{\mathcal{O}_{F,\mathfrak{p}}} \mathrm{Sel}_{\mathfrak{p}^\infty}(A) = 0.$$
- The case $W(\varphi) = -1$. In view of (4.13) and Lemma 3.3, the image of $p^{-m}z_0$ in $H^1(K,V/T)$ gives a non-zero element of $\mathrm{Sel}(K,V/T)$ for a sufficiently large m. By (4.11), it then follows that
$$\mathrm{corank}_{\mathcal{O}_{F,\mathfrak{p}}} \mathrm{Sel}_{\mathfrak{p}^\infty}(A) = 1.$$
Hence, the assertion is a consequence of Proposition 4.16. □

Finally, we have the following p-converse.

Theorem 4.18. *Let $A_{/\mathbb{Q}}$ be a GL_2-type CM abelian variety. Let K be the CM field and F the Hecke field. Suppose that (rt) holds and $\mathcal{O}_F \hookrightarrow \mathrm{End}A$. Let $p \ge 5$ be a prime of good non-ordinary reduction for $A_{/\mathbb{Q}}$ with $p \nmid h_K$, and $\mathfrak{p}$ a prime of F above p. Suppose either of the following.*

[9] Recall that $\mathrm{Ind}_{\mathbb{Q}}^K(V) \cong T_p(A)\otimes_{\mathcal{O}_F\otimes\mathbb{Z}_p} L_{\mathfrak{p}}$.

https://doi.org/10.1017/S147474802300021X Published online by Cambridge University Press

(a) $\mathrm{corank}_{\mathcal{O}_{F,\mathfrak{p}}} \mathrm{Sel}_{\mathfrak{p}^\infty}(A) = 1$ *and* $\mathrm{loc}_p : \mathrm{Sel}_{\mathfrak{p}^\infty}(A) \to A(\mathbb{Q}_p) \otimes_{\mathcal{O}_F} F_\mathfrak{p}/\mathcal{O}_{F_\mathfrak{p}}$ *is a non-zero map.*

(b) $\mathrm{corank}_{\mathcal{O}_{F,\mathfrak{p}}} \mathrm{Sel}_{\mathfrak{p}^\infty}(A) = 1$ *and* $\text{Ш}(A)[\mathfrak{p}^\infty]$ *is finite.*

Then,

$$\mathrm{ord}_{s=1} L(A,s) = [F:\mathbb{Q}].$$

Proof.

(a) In view of the assumption and (4.10), $\mathrm{Sel}_{\mathrm{str}}(\mathbb{Q}, A[\mathfrak{p}^\infty])$ is finite. So, the assertion directly follows from Theorem 4.17.

(b) Recall the exact sequence

$$0 \to A(\mathbb{Q}) \otimes_{\mathcal{O}_F} F_\mathfrak{p}/\mathcal{O}_{F_\mathfrak{p}} \to \mathrm{Sel}_{\mathfrak{p}^\infty}(A) \to \text{Ш}(A)[\mathfrak{p}^\infty] \to 0. \tag{4.14}$$

So, by the assumption, we have $A(\mathbb{Q}) \otimes_{\mathcal{O}_F} F_\mathfrak{p}/\mathcal{O}_{F_\mathfrak{p}} \cong F_\mathfrak{p}/\mathcal{O}_{F_\mathfrak{p}}$. Hence,

$$\mathrm{loc}_\mathfrak{p} : A(\mathbb{Q}) \otimes_{\mathcal{O}_F} F_\mathfrak{p}/\mathcal{O}_{F_\mathfrak{p}} \to A(\mathbb{Q}_p) \otimes_{\mathcal{O}_F} F_\mathfrak{p}/\mathcal{O}_{F_\mathfrak{p}}$$

is a non-zero map. □

Remark 4.19. The p-converse was initiated by Skinner and Zhang (cf. [52], [56]). The above approach is a variant of [52], yet it does not rely on the parity conjecture.

Appendix A. *p*-adic height pairings and logarithms

A basic reference is [33, §3.2]. See also [32], [42] for elliptic curves.

A.1. *p*-adic height pairings on abelian varieties

We fix an embedding $\iota_p : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$. Let F be a finite extension of $\mathbb{Q}$. We choose a continuous homomorphism $\ell_F : \mathbb{A}_F^\times / F^\times \to \mathbb{Q}_p$ and denote by $\ell_{F,v}$ or ℓ_v the v-th component for a place v of F (note that $\ell_v = 0$ if v is archimedean). The important example is the cyclotomic logarithm. Let $\log_p$ be the p-adic logarithm on $\mathbb{Z}_p^\times$ such that $\log_p p = 0$. We define the cyclotomic logarithm $\ell_{F,v}^c$ on $F_v^\times$ at a non-archimedean place v by

$$\ell_{F,v}^c(x) = \begin{cases} -\log_p |x|_v = v(x)\log_p \mathbf{N}(v) & \text{if} \quad v \nmid p \\ -\log_p \mathbf{N}_{F_v/\mathbb{Q}_p}(x) & \text{if} \quad v \mid p, \end{cases}$$

where $\mathbf{N}(v)$ is the number of elements of the residue field of F at v and we normalize as $v(\pi) = 1$ for a uniformizer π at v of F. We define the cyclotomic logarithm ℓ_F^c by $\ell_F^c := \sum_v \ell_{F,v}^c$. Then, $\ell_F^c(x) = 0$ for $x \in F^\times$ and it defines a homomorphism $\mathbb{A}_F^\times / F^\times \to \mathbb{Q}_p$.

Let A be an abelian variety defined over F with good reduction at all places over p and let $A^\vee$ be its dual. For simplicity, we also assume that F is unramified at all places over p. Let L be a finite extension of $\mathbb{Q}_p$, which plays as the coefficient field. We choose a splitting of the Hodge filtration of $M_v(A) \otimes_{\mathbb{Q}_p} L$ for each place v over p. Here, $M_v(A)$ is the weakly admissible filtered φ-module of A over F_v with Hodge-Tate weight $\{0,1\}$ (the Hodge-Tate weight of the cyclotomic character is normalized as -1). In other words, we fix an L-vector subspace N_v of $M_v(A) \otimes_{\mathbb{Q}_p} L$ which is complementary to $\mathrm{Fil}^1 M_v(A) \otimes_{\mathbb{Q}_p} L$. We put $N := (N_v)_{v|p}$.

https://doi.org/10.1017/S147474802300021X Published online by Cambridge University Press

Let $\mathfrak{a} = \sum_i n_i(P_i)$ be a zero cycle on A of degree 0 defined over F_v and let D be an algebraically trivial divisor over F_v prime to the support of $\mathfrak{a}$. Then, for a place $v \nmid p$, there is a canonical way to define the local height pairing $\langle D, \mathfrak{a}\rangle_{\ell_v} \in \mathbb{Q}_p$ characterized by certain standard functorial properties (cf. [33, Proposition 9]. The pairing is independent of the choice N). For a place v over p, depending on the choice of N_v, we can define the local p-adic height pairing $\langle D, \mathfrak{a}\rangle_{\ell_v, N_v} \in L$. We recall the definition below.

The global p-adic height pairing is defined as the sum of local p-adic height pairings:

$$\langle\, ,\rangle_{\ell_F, N} : A^\vee(F) \times A(F) \to L, \quad (d,a) \mapsto \sum_{v \nmid p} \langle D, \mathfrak{a}\rangle_{\ell_v} + \sum_{v | p} \langle D, \mathfrak{a}\rangle_{\ell_v, N_v}.$$

Here, D is an algebraically trivial divisor that represents d, and $\mathfrak{a}$ is a zero cycle $\sum n_i[P_i]$ of degree zero with $\sum n_i P_i = a$. We choose D and $\mathfrak{a}$ so that they have no point in common. The global pairing does not depend on the choice of D, $\mathfrak{a}$.

A.1.1. The local p-adic height at $v|p$. We assume that $v|p$. As before, let $\mathfrak{a} = \sum_i n_i(P_i)$ be a zero cycle on A of degree 0 defined over F_v and let D be an algebraically trivial divisor over F_v prime to the support of $\mathfrak{a}$. Let $\mathscr{A}/\mathcal{O}_{F_v}$ be the smooth model of A/F_v and let $\mathscr{A}^\vee$ be the smooth model of $A^\vee$. Then, the rational equivalence class of D defines a point in $A^\vee(F_v) = \mathscr{A}^\vee(\mathcal{O}_{F_v}) = \mathrm{Ext}^1_{fppf}(\mathscr{A}, \mathbb{G}_m)$. Hence, we have an exact sequence as fppf sheaves

$$1 \longrightarrow \mathbb{G}_m \longrightarrow \mathscr{X}_D \longrightarrow \mathscr{A} \longrightarrow 1, \tag{A.1}$$

where $\mathscr{X}_D$ is a smooth separated commutative group scheme over $\mathcal{O}_{F_v}$. Over $\mathrm{Spec}\, F_v$, this exact sequence is isomorphic to

$$1 \longrightarrow \mathbb{G}_m \longrightarrow X_D \longrightarrow A \longrightarrow 1, \tag{A.2}$$

where X_D is the line bundle associated to $\mathcal{O}_A(D)$ minus zero section which has a group law since D is algebraically equivalent to zero. Hence, attached to D, there is a geometric section $s_D : A \setminus |D| \to X_D$ which is canonical up to a translation by an element of $\mathbb{G}_m$. We identify $\mathscr{X}_D \otimes F_v$ with X_D.

We define a local section

$$s_{D,N_v} : \mathscr{A}(\mathcal{O}_{F_v}) \otimes_{\mathbb{Z}_p} L \longrightarrow \mathscr{X}_D(\mathcal{O}_{F_v}) \otimes_{\mathbb{Z}_p} L.$$

First, we identify

$$\mathscr{A}(\mathcal{O}_{F_v}) \hat{\otimes} L = \mathrm{Hom}_{F_v \otimes L}(\mathrm{Fil}^1 M_{\mathscr{A},L}, F_v \otimes L) = \mathrm{Hom}_L(\mathrm{Fil}^1 M_{\mathscr{A},L}, L),$$

and so for $\mathscr{X}_D(\mathcal{O}_{F_v})$. Here, $M_{\mathscr{A},L} = M_v(A) \otimes_{\mathbb{Q}_p} L$ is the filtered φ-module with coefficients in $F_v \otimes_{\mathbb{Q}_p} L$ associated to $\mathscr{A}/\mathcal{O}_{F_v}$. Hence, it suffices to construct an L-linear map

$$\mathrm{Fil}^1 M_{\mathscr{X}_D,L} \to \mathrm{Fil}^1 M_{\mathscr{A},L}.$$

Since $M_{\mathscr{A},L}$ and $M_{\mathbb{G}_m,L}$ have different Frobenius eigenvalues, the exact sequence

$$0 \longrightarrow M_{\mathscr{A},L} \longrightarrow M_{\mathscr{X}_D,L} \longrightarrow M_{\mathbb{G}_m,L} \longrightarrow 0 \tag{A.3}$$

splits as $F_v \otimes L[\varphi]$-modules. Hence, we have a left splitting $M_{\mathscr{X}_D,L} \to M_{\mathscr{A},L}$. By composing it to the projection $M_{\mathscr{A},L} \to \mathrm{Fil}^1 M_{\mathscr{A},L}$ by N_v, we obtain the map $t_{D,N_v} : M_{\mathscr{X}_D,L} \to \mathrm{Fil}^1 M_{\mathscr{A},L}$. By the restriction to $\mathrm{Fil}^1 M_{\mathscr{X}_D,L}$, we obtain the desired map.

The local height pairing at $v|p$ is defined as

$$\langle D,\mathfrak{a}\rangle_{\ell_v,N_v} := \ell_v\left(\prod_i (s_D(P_i)/s_{D,N_v}(P_i))^{n_i}\right) \in L$$

(we write the group law on X_D multiplicatively. Note that the image of $s_D/s_{D,N_v}$ lives in $\mathbb{G}_m$).

A.2. The dependence of the p-adic height on the splitting

Suppose that $N' = (N'_v)_{v|p}$ is another splitting. Then,

$$\langle d,a\rangle_{\ell_F,N'} - \langle d,a\rangle_{\ell_F,N} = \sum_{v|p} \ell_v\left(\prod_i (s_{D,N_v}(P_i)/s_{D,N'_v}(P_i))^{n_i}\right). \tag{A.4}$$

Note that the image of $s_{D,N_v}/s_{D,N'_v}$ lives in $\mathcal{O}_{F_v}^\times \otimes_{\mathbb{Z}_p} L \subset \mathscr{X}_D(\mathcal{O}_{F_v}) \otimes_{\mathbb{Z}_p} L$. We also remark that $s_{D,N_v}/s_{D,N'_v}$ does not depend on the choice of D for d (the geometric section s_D depends on the choice of the divisor D for d). The map $s_{D,N_v}/s_{D,N'_v}$ is induced by the map

$$\ell_{d,N_v.N'_v} : \mathrm{Fil}^1 M_{\mathbb{G}_m,L} \to \mathrm{Fil}^1 M_{\mathscr{A},L}, \quad \omega_{\mathbb{G}_m} \mapsto t_{D,N_v}(\omega^H_{\mathbb{G}_m}) - t_{D,N'_v}(\omega^H_{\mathbb{G}_m}).$$

Here, $\omega^H_{\mathbb{G}_m} \in \mathrm{Fil}^1 M_{\mathscr{X}_D,L}$ is a lift of $\omega_{\mathbb{G}_m}$ under

$$0 \longrightarrow \mathrm{Fil}^1 M_{\mathscr{A},L} \longrightarrow \mathrm{Fil}^1 M_{\mathscr{X}_D,L} \longrightarrow \mathrm{Fil}^1 M_{\mathbb{G}_m,L} \longrightarrow 0$$

(note that t_{N_v} is identity on $\mathrm{Fil}^1 M_{\mathscr{A},L}$). We note that the image of d by the logarithm $\lambda_{\omega_{A^\vee}}$ for $\omega_{A^\vee} \in \mathrm{Fil}^1 M_{\mathscr{A}^\vee}$ is given by

$$[\omega_{A^\vee}, (\omega^H_{\mathbb{G}_m} - \omega^\varphi_{\mathbb{G}_m})].$$

Here, $\omega^\varphi_{\mathbb{G}_m} \in M_{\mathscr{X}_D,L}$ is the lift of $\omega_{\mathbb{G}_m}$ compatible with the action of φ under (A.3), and $[\,,\,]$ is the de Rham pairing on $M_{\mathscr{A}^\vee}$ and $M_{\mathscr{A}}$. Let $\omega_1^\vee, \ldots, \omega_g^\vee$ be a basis of $\mathrm{Fil}^1 M_{\mathscr{A}^\vee}$ and $\eta_1, \ldots, \eta_g$ a basis of a complementary subspace of $\mathrm{Fil}^1 M_{\mathscr{A}}$ such that $[\omega_i^\vee, \eta_j] = \delta_{ij}$ (the Kronecker Delta). Then, we have

$$\omega^H_{\mathbb{G}_m} = \omega^\varphi_{\mathbb{G}_m} + \sum_i c_i \omega_i + \sum_i \lambda_{\omega_i^\vee}(d)\eta_i$$

for some $c_i \in F_v$. Hence,

$$\ell_{d,N_v.N'_v}(\omega_{\mathbb{G}_m}) = \sum_i \lambda_{\omega_i^\vee}(d)(t_{N_v}(\eta_i) - t_{N'_v}(\eta_i)), \tag{A.5}$$

where $t_{N_v} : M_{\mathscr{A}} \to \mathrm{Fil}^1 M_{\mathscr{A}}$ is a splitting by N_v.

https://doi.org/10.1017/S147474802300021X Published online by Cambridge University Press

Suppose that $\omega_{\mathbb{G}_m}$ is the canonical invariant differential of $\mathbb{G}_m$. Then, the map

$$\lambda_{d,N_v,N'_v} := \log\circ(s_{D,N_v}/s_{D,N'_v}) : \ A(F_v) \longrightarrow F_v \otimes_{\mathbb{Q}_p} L$$

is the logarithm map defined by the invariant differential $\ell_{d,N_v.N'_v}(\omega_{\mathbb{G}_m}) \in \mathrm{Fil}^1 M_{\mathscr{A},L}$. Hence,

$$\langle d,a\rangle_{\ell_F,N'} - \langle d,a\rangle_{\ell_F,N} = \sum_{v|p} \ell_v\left(\exp\circ\lambda_{d,N_v,N'_v}(a)\right). \tag{A.6}$$

The difference between global p-adic height pairing is measured by logarithms on A.

Proposition A.1. *Assume that $N_v \cap N'_v = \{0\}$. Then, $s_{D,N_v} = s_{D,N'_v}$ if and only if D is torsion in $A^\vee$.*

Proof. D is torsion if and only if (A.3) splits as filtered φ-modules. In such a case, t_{D,N_v} does not depend on the choice of N_v. Assume that $s_{D,N_v} = s_{D,N'_v}$. Then, ℓ_{d,N_v,N'_v} $(\omega_{\mathbb{G}_m}) = 0$. Then, we have

$$\omega^H_{\mathbb{G}_m} - \omega^\varphi_{\mathbb{G}_m} - t_{D,N_v}(\omega^H_{\mathbb{G}_m}) = \omega^H_{\mathbb{G}_m} - \tilde{\omega}_{\mathbb{G}_m} - t_{D,N'_v}(\omega'_{\mathbb{G}_m}) \in N_v \cap N'_v.$$

Hence, by our assumption, we have

$$\omega^\varphi_{\mathbb{G}_m} = \omega^H_{\mathbb{G}_m} - t_{D,N_v}(\omega^H_{\mathbb{G}_m}) \in \mathrm{Fil}^1 M_{\mathscr{X}_D,L}.$$

This means that (A.3) splits as filtered φ-modules. □

A.3. Applications for modular abelian varieties

Let f be a normalized eigen newform of weight 2 for $\Gamma_0(M)$ with $p \nmid M$. Let A_f be a modular abelian variety defined over $\mathbb{Q}$ associated to f. We fix a polarization of A_f compatible with the Hecke action and identify objects on A_f and $A_f^\vee$ by the pullback after tensoring L if necessary (e.g. differential forms, rational points). Let K_f be the Hecke field of f. We apply our theory for $A = A_f/F$ for a number field F unramified over p and L containing K_f and roots of the Hecke eigen polynomial of f at p. Then, we have the decomposition

$$M_{\mathscr{A}/F_v,L} = \bigoplus_{\sigma\in\mathrm{Gal}(K_f/\mathbb{Q})} M_{f^\sigma}$$

as filtered φ-modules by the Hecke action. Here, M_{f^σ} is a filtered φ-module of dimension 2 as $F_v \otimes_{\mathbb{Q}_p} L$-vector space and $\mathrm{Fil}^1 M_{f^\sigma} = F_v \otimes_{\mathbb{Q}_p} L\omega_{f^\sigma}$, where ω_{f^σ} is the differential form on $X_0(N)$ associated to f^σ. Let α and β be distinct roots of the Hecke eigen polynomial of f at p in L. (cf. [21].) We consider a splitting N_α (resp. N_β) of the Hodge filtration of M_f generated by $\beta\omega_f - \varphi\omega_f$ (resp. $\alpha\omega_f - \varphi\omega_f$). Note that if $F = \mathbb{Q}$, N_α is an α-eigenspace of the Frobenius. We extend them (arbitrary) to splittings for $M_{\mathscr{A}/F_v,L}$, which are also denoted by N_α and N_β. Then, by (A.6), we have

$$\langle d,a\rangle_{\ell_F^c,N_\alpha} - \langle d,a\rangle_{\ell_F^c,N_\beta} = -\mathrm{Tr}_{F/\mathbb{Q}}\lambda_{d,N_\alpha,N_\beta}(a)$$

https://doi.org/10.1017/S147474802300021X Published online by Cambridge University Press

for the cyclotomic height pairing (here, $\mathrm{Tr}_{F/\mathbb{Q}}\lambda_{d,N_\alpha,N_\beta}(a) := \sum_{\sigma:F\hookrightarrow\mathbb{C}_p}\lambda_{d^\sigma,N_\alpha,N_\beta}(a^\sigma)$). We put $A(F)_f$ for the f-part of $A(F)\otimes L$ be the Hecke action. Let $\lambda_f : A(F)_f \to \mathbb{C}_p$ be the logarithm associated to ω_f.

Theorem A.2. *Assume that $[\varphi\omega_f,\omega_f]\neq 0$. Then, we have*

$$\langle d,a\rangle_{\ell^c_F,N_\alpha} - \langle d,a\rangle_{\ell^c_F,N_\beta} = \frac{(\beta-\alpha)}{[\omega_f,\varphi\omega_f]}\mathrm{Tr}_{F/\mathbb{Q}}(\lambda_f(d)\lambda_f(a))$$

for $d,a\in A(F)_f$ (note that A is self-dual). In particular,

$$\langle a,a\rangle_{\ell^c_F,N_\alpha} - \langle a,a\rangle_{\ell^c_F,N_\beta} = \frac{(\beta-\alpha)}{[\omega_f,\varphi\omega_f]}\mathrm{Tr}_{F/\mathbb{Q}}\lambda_f(a)^2.$$

Proof. Put $\eta_f := \frac{1}{[\omega_f,\varphi\omega_f]}\varphi\omega_f$ and extend ω_f, η_f to a symplectic basis of $M_{\mathscr{A}/F_v}$. Since $\beta\omega_f - \varphi\omega_f \in N_\alpha$, we have $t_{N_\alpha}(\eta) = \frac{\beta}{[\omega_f,\varphi\omega_f]}\omega_f$. Hence, the assertion follows from (A.5) and (A.6). □

Corollary A.3. *Assume that $[\varphi\omega_f,\omega_f]\neq 0$. The pairing $\langle\,,\,\rangle_{\ell^c_{\mathbb{Q}},N_\alpha}$ or $\langle\,,\,\rangle_{\ell^c_{\mathbb{Q}},N_\beta}$ is non-trivial. In particular, if the Hecke polynomial at p is irreducible over the p-adic completion of K_f, the height pairing $\langle\,,\,\rangle_{\ell^c_{\mathbb{Q}},N_\alpha}$ is non-trivial.*

Proof. This follows from Theorem A.2 since λ_f is non-trivial. The pairings $\langle\,,\,\rangle_{\ell^c_{\mathbb{Q}},N_\alpha}$ and $\langle\,,\,\rangle_{\ell^c_{\mathbb{Q}},N_\beta}$ are conjugate if α and β are. □

Corollary A.4. *The p-adic Gross-Zagier formula of f holds for inert primes if f is non-ordinary at p. (cf. [33, Theorem 3])*

Proof. We first show that $[\varphi\omega_f,\omega_f]\neq 0$. We have a strongly divisible lattice D in M_f by the Fontaine-Laffaille theory. Suppose that $[\varphi\omega_f,\omega_f]=0$. Then, $\mathrm{Fil}^1 D$ is stable by φ. Hence, $\varphi(\mathrm{Fil}^1 D)\subset \mathrm{Fil}^1 D\cap pD = p\mathrm{Fil}^1 D$. This implies that one of the eigenvalues α, β is divisible by p, which contradicts the non-ordinary assumption. By Corollary A.3, choose α for which $\langle\,,\,\rangle_{\ell^c_{\mathbb{Q}},N_\alpha}$ is non-trivial. Then, see a remark after [33, Theorem 3]. □

Corollary A.5. *Let p be a non-ordinary (good) prime for f. Suppose that* $\mathrm{ord}_{s=1}L(f,s) = 1$ *and the Iwasawa main conjecture for f is true for p. Then, the p-part of the full Birch and Swinnerton-Dyer conjecture (Bloch-Kato's tamagawa number conjecture) is true for f.*

Proof. Take α so that $\langle\,,\,\rangle_{\ell^c_{\mathbb{Q}},N_\alpha}$ is non-trivial. Then, the assertion follows from similar arguments as [33, Corollary 1.3 (iii)]. □

Let

$$\mathscr{H}_L = \left\{\sum_{n\geq 0} a_n(\gamma-1)^n \in L[[\gamma-1]] \,\middle|\, \lim_n |a_n|_p n^{-1} = 0\right\},$$

where $|\cdot|_p$ is the multiplicative valuation of L normalized by $|p|_p = 1/p$. For $|\alpha|_p > 1/p$, let $L_{p,\alpha}(f)\in\mathscr{H}_L$ be the cyclotomic p-adic L-function as in [30, Theorem 16.2]. Fixing a real period Ω_f of f, we have the following interpolation property. For a finite character χ of $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ of conductor $p^n > 1$,

$$L_{p,\alpha}(f)(\chi) = \frac{p^n}{\alpha^n \tau(\chi^{-1}, \zeta_{p^n})} \cdot \frac{L(f, \chi^{-1}, 1)}{\Omega_f},$$

where $\zeta_{p^n} = e^{2\pi i/p^n}$, and for the trivial character

$$L_{p,\alpha}(f)(\mathbb{1}) = (1-\alpha^{-1})^2 \cdot \frac{L(f,1)}{\Omega_f}.$$

If $|\beta|_p > 1/p$, then replacing α with β, we see the interpolation property of $L_{p,\beta}(f)$.

Define

$$\mathscr{L}'_{p,\alpha}(f,1) = \lim_{s\to 1} L_{p,\alpha}(f)((\chi^{\mathrm{cyc}})^{s-1})/(s-1),$$

where $\chi^{\mathrm{cyc}} : \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \to 1 + p\mathbb{Z}_p$ is the cyclotomic character. We similarly define $\mathscr{L}'_{p,\beta}(f,1)$.

Theorem A.6. *Let p be a non-ordinary (good) prime for f. Suppose that the root number of $L(f,s)$ is -1. Then, there exists a point $P \in A(\mathbb{Q})_f$ and a non-zero constant $c_P \in \mathbb{Q}$ such that*

$$\left(1-\frac{1}{\alpha}\right)^{-2} \mathscr{L}'_{p,\alpha}(f,1) - \left(1-\frac{1}{\beta}\right)^{-2} \mathscr{L}'_{p,\beta}(f,1) = c_P \frac{(\beta-\alpha)}{[\omega_f, \varphi\omega_f]} \lambda_f(P)^2.$$

Moreover, P is non-torsion if and only if $\mathrm{ord}_{s=1} L(f,s) = 1$, and in such a case $c_P = \frac{L'(f,1)}{\Omega_f \langle P,P\rangle_\infty}$, where $\langle , \rangle_\infty$ is the Néron-Tate height pairing.

Proof. By [8], there exists an imaginary quadratic field K satisfying the Heegner hypothesis and $L(f\otimes\varepsilon,1) \neq 0$ for the quadratic character ε associated to K. Let z be a Heegner point associated to K. Since $L(f\otimes\varepsilon,1)\neq 0$, the Heegner point z lives in $A(\mathbb{Q})\otimes\mathbb{Q}$ up to a torsion element. Then, by Theorem A.2 for $F = K$ and by the p-adic Gross-Zagier formula, we have

$$\left(1-\frac{1}{\alpha}\right)^{-4} \mathscr{L}'_{p,\alpha}(f/K,1) - \left(1-\frac{1}{\beta}\right)^{-4} \mathscr{L}'_{p,\beta}(f/K,1) = 2u^{-2} \frac{(\beta-\alpha)}{[\omega_f, \varphi\omega_f]} \lambda_f(z)^2, \tag{A.7}$$

where $\mathscr{L}_{p,-}(f/K,s)$ is the p-adic L-function of f over K (cf. [32], [33]) and $u = \sharp\mathcal{O}_K^\times/2$. By the classical Gross-Zagier formula, z is non-torsion if and only if $\mathrm{ord}_{s=1}L(f,s) = 1$. Then, as in the proof of [32, Corollary 1.3], we have the desired formula from (A.7) by using the complex and the p-adic Gross-Zagier formulae. □

Appendix B. Perrin-Riou conjecture

Rubin's formula [50] inspired the eponymous conjecture [42, §3.3.2], which primarily concerns the arithmetic of Beilinson-Kato elements.

https://doi.org/10.1017/S147474802300021X Published online by Cambridge University Press

B.1. The conjecture

Let $f \in S_2(\Gamma_0(N))$ be an elliptic newform and $F \subseteq \mathbb{C}$ the Hecke field. Let A be an associated GL_2-type abelian variety over $\mathbb{Q}$; that is, A is a simple, $[F:\mathbb{Q}]$-dimensional abelian variety equipped with a homomorphism $F \to \mathrm{End}(A) \otimes \mathbb{Q}$ of $\mathbb{Q}$-algebras such that

$$L(A,s) = \prod_{\sigma: F \hookrightarrow \overline{\mathbb{Q}}} L(f^\sigma, s).$$

Let p be a prime number and $\mathfrak{p}$ the prime of the Hecke field F over p arising from the fixed embedding $\iota_p : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$. Let $V(f) \cong F_{\mathfrak{p}}^{\oplus 2}$ denote the $\mathfrak{p}$-th component of the Galois representation $T_p(A) \otimes \mathbb{Q}_p \cong \prod_{v|p} F_v^{\oplus 2}$. Let $z_f \in H^1(\mathbb{Q}, V(f))$ be a Beilinson-Kato element as in [30, Theorem 12.5]. By Kato's reciprocity law [30, Theorem 12.5 (1)],

$$\mathrm{loc}_p(z_f) \in H^1_{\mathrm{f}}(\mathbb{Q}_p, V(f)) \iff L(f,1) = 0. \tag{B.1}$$

After Kato, if $L(f,1) \neq 0$, then z_f is inherent to the arithmetic of f (cf. [30, Theorem 14.5]). If $L(f,1) = 0$, then Perrin-Riou [42, §3.3.2] (for elliptic curves) conjectured the Beilinson-Kato element z_f to be still intertwined with the arithmetic as follows.

Conjecture B.1. *Let $f \in S_2(\Gamma_0(N))$ be an elliptic newform and $A_{/\mathbb{Q}}$ an associated GL_2-type abelian variety. Suppose that $L(f,1) = 0$. Let p be a prime. Then, there exists a rational point $P \in A(\mathbb{Q})$ with the following properties.*

(a) *We have*

$$\lambda_f(\mathrm{loc}_p(z_f)) = c\lambda_f(P)^2$$

for some $c \in F^\times$ and $\lambda_f : H^1_{\mathrm{f}}(\mathbb{Q}_p, V(f)) \to F_{\mathfrak{p}}$ the logarithm map associated to a non-zero element $\omega_A \in \mathrm{coLie}(A)$.

(b) *P is non-torsion if and only if $\mathrm{ord}_{s=1} L(f,s) = 1$.*

The conjecture implies

$$\mathrm{loc}_p(z_f) \neq 0 \iff \mathrm{ord}_{s=1} L(f,s) = 1. \tag{B.2}$$

B.2. The non-ordinary case

We prove Perrin-Riou's Conjecture B.1 at the primes of good non-ordinary reduction. The main result is Theorem B.3, which shows a refinement of the conjecture.

B.2.1. Backdrop. Let the setting be as in §B.1.

Fix an element $b_A \in H^1(A(\mathbb{C}), \mathbb{Q})$ such that $b_A^+ := 2^{-1}(1+\iota)b_A \neq 0$ for ι the involution of $H^1(A(\mathbb{C}), \mathbb{Q})$ induced by the complex conjugation c on $A(\mathbb{C})$. Fix a non-zero element $\omega_A \in \mathrm{coLie}(A) \cong F$. Define $\Omega_f \in \mathbb{R}$ by

$$\frac{1+\iota}{2} \mathrm{per}_f(\omega_A) = \Omega_f b_A^+, \tag{B.3}$$

where $\mathrm{per}_f : \mathrm{coLie}(A) \to H^1(A(\mathbb{C}), \mathbb{Q}) \otimes_F \mathbb{C}$ denotes the F-linear map induced by the period map of A. (Since ω_A is defined over $\mathbb{Q}$, note that $\mathrm{per}_f(\omega_A)$ lies in the $(\iota \otimes c)$-fixed

https://doi.org/10.1017/S147474802300021X Published online by Cambridge University Press

part of $H^1(A(\mathbb{C}),\mathbb{Q})\otimes_F\mathbb{C}$, and so $\Omega_f\in\mathbb{R}$.) Fix a polarization of A which is compatible with the F-action. Let $T(f)$ be a Galois stable $\mathcal{O}_{F_\mathfrak{p}}$-lattice of $V(f)$.

Let

$$\mathfrak{z}_f=(z_{f,n})\in\varprojlim_n H^1(\mathbb{Q}_n,T(f))\otimes\mathbb{Q}_p$$

be the Beilinson-Kato element associated to b_A as in [30, Thm. 12.5 (1)]. The following explicit reciprocity law is due to Kato [30, Thm. 12.5].

Proposition B.2. *For a finite character χ of $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$, we have*

$$\sum_{\sigma\in\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})}\chi(\sigma)\exp_n^*(\mathrm{loc}_{\tilde{\mathfrak{p}}}(z_{f,n}^\sigma))=\frac{L(f,\chi,1)}{\Omega_f}\omega_A. \tag{B.4}$$

Here,

$$\exp_n^*:H^1(\mathbb{Q}_{n,\tilde{\mathfrak{p}}},V(f))\to\mathrm{Fil}^0(D_{\mathrm{dR}}(V(f)))\otimes_{\mathbb{Q}_p}\mathbb{Q}_{n,\tilde{\mathfrak{p}}}=\mathrm{coLie}(A)\otimes_F F_\mathfrak{p}\otimes_{\mathbb{Q}_p}\mathbb{Q}_{n,\tilde{\mathfrak{p}}}$$

is the dual exponential map and $\tilde{\mathfrak{p}}$ the prime of $\mathbb{Q}_n$ over p.

B.2.2. The theorem.

Theorem B.3. *Let $f\in S_2(\Gamma_0(N))$ be an elliptic newform and p a prime of good non-ordinary reduction. Then, an explicit form of Conjecture B.1 is true: if $L(f,1)=0$, then there exists a rational point $P\in A(\mathbb{Q})$ with the following properties.*

(a) *We have*

$$\lambda_f(\mathrm{loc}_p(z_f))=c_P\left(1-\frac{a_p(f)}{p}+\frac{1}{p}\right)\lambda_f(P)^2$$

for some $c_P\in F^\times$, and $z_f:=z_{f,0}$, $a_p(f)$ the p-th Fourier coefficient of f, and $\lambda_f: H^1_{\mathrm{f}}(\mathbb{Q}_p,V(f))\to F_\mathfrak{p}$ the logarithm map associated to ω_A.

(b) *P is non-torsion if and only if $\mathrm{ord}_{s=1}L(f,s)=1$.*

(c) *If the equivalent conditions in (b)hold, then*

$$c_P=\frac{L'(f,1)}{\Omega_f\langle P,P\rangle_\infty}$$

for $\langle,\rangle_\infty$ the Néron-Tate height pairing.

Our proof is based on the following link between the logarithm of $\mathrm{loc}_p(z_f)\in H^1_{\mathrm{f}}(\mathbb{Q}_p,V(f))$ and the first derivatives of the p-adic L-functions.

Proposition B.4. *Let α and β be the roots of the Hecke polynomial $X^2-a_p(f)X+p$ of f. Then, we have*

$$\lambda_f(\mathrm{loc}_p(z_f))=\frac{1-a_p(f)+p}{\beta-\alpha}[\omega_A,\varphi\omega_A]_{D_{\mathrm{cris}}(V(f))}\cdot\left((1-\alpha^{-1})^2\mathscr{L}'_{p,\alpha}(f,1)-(1-\beta^{-1})^2\mathscr{L}'_{p,\beta}(f,1)\right),$$

where $\mathscr{L}'_{p,\alpha}(f,1)$ *and* $\mathscr{L}'_{p,\beta}(f,1)$ *are the derivatives of the cyclotomic p-adic L-functions as in §A.3, and*

$$[\ ,\ ]_{D_{\mathrm{cris}}(V(f))} : D^0_{\mathrm{cris}}(V(f)) \times D_{\mathrm{cris}}(V(f))/D^0_{\mathrm{cris}}(V(f)) \to D_{\mathrm{cris}}(\mathbb{Q}_p(1)) \otimes F_{\mathfrak{p}} \cong F_{\mathfrak{p}}$$

is the natural pairing induced by the de Rham pairing. Here, under the last isomorphism, the basis of $D_{\mathrm{cris}}(\mathbb{Q}_p(1))$ *associated to* $(\zeta_{p^n})_n = (e^{2\pi i/n})_n$ *corresponds to* $1 \in F_{\mathfrak{p}}$, *and* $D^0_{\mathrm{cris}}(V(f))$ *denotes* $\mathrm{Fil}^0 D_{\mathrm{cris}}(V(f))$.

Proof. Define $\omega_\alpha, \omega_\beta \in D := D_{\mathrm{cris}}(V(f)) \otimes_{F_{\mathfrak{p}}} F_{\mathfrak{p}}(\alpha)$ by

$$\omega_\alpha = \beta^{-1}\omega_A - \varphi\omega_A, \quad \omega_\beta = \alpha^{-1}\omega_A - \varphi\omega_A$$

for φ the Frobenius map of D. Then, ω_α and ω_β are non-zero elements such that $\varphi\omega_\alpha = \alpha^{-1}\omega_\alpha$ and $\varphi\omega_\beta = \beta^{-1}\omega_\beta$. Here, we note that D coincides with $M_f \otimes D_{\mathrm{cris}}(\mathbb{Q}_p(1))$ in subsection A.3 with $L = F_{\mathfrak{p}}(\alpha)$.

Following [42, §3.1.3], define[10] $L_p(f) \in \mathscr{H}_{F_{\mathfrak{p}}(\alpha)} \otimes_{F_{\mathfrak{p}}(\alpha)} D$ by

$$L_p(f) = \frac{p}{\alpha - \beta} \cdot \left(L_{p,\alpha}(f)\omega_\alpha - L_{p,\beta}(f)\omega_\beta\right)$$

and $\mathscr{L}'_p(f,1) = \lim_{s\to 1} L_p(f)((\chi^{\mathrm{cyc}})^{s-1})/(s-1) \in D$.

Then, by [42, Proposition 2.2.2] and (B.4), we have

$$\begin{aligned}\log_f(\mathrm{loc}_p(z_f)) &\equiv (1-p^{-1}\varphi^{-1})(1-\varphi)^{-1}\mathscr{L}'_p(f,1)\\ &\equiv \frac{p}{\alpha-\beta}(1-p^{-1}\alpha)(1-\alpha^{-1})^{-1}\mathscr{L}'_{p,\alpha}(f,1)\omega_\alpha - \frac{p}{\alpha-\beta}(1-p^{-1}\beta)(1-\beta^{-1})^{-1}\mathscr{L}'_{p,\beta}(f,1)\omega_\beta\\ &\equiv \frac{1-a_p(f)+p}{\beta-\alpha}\left((1-\alpha^{-1})^2\mathscr{L}'_{p,\alpha}(f,1) - (1-\beta^{-1})^2\mathscr{L}'_{p,\beta}(f,1)\right)\varphi\omega_A \quad \bmod \mathrm{Fil}^0 D.\end{aligned}$$

Here, $\log_f : H^1_{\mathrm{f}}(\mathbb{Q}_p, V(f)) \to D_{\mathrm{cris}}(V(f))/D^0_{\mathrm{cris}}(V(f))$ denotes the Bloch-Kato logarithm of $V(f)$. Considering the product with ω_A, the proposition follows. □

We now return to Theorem B.3.

Proof of Theorem B.3. Since $D_{\mathrm{cris}}(V(f)) \cong M_f \otimes D_{\mathrm{cris}}(\mathbb{Q}_p(1))$, note that $p[\omega_A, \varphi\omega_A]_{D_{\mathrm{cris}}(V(f))}$ coincides with $[\omega_A, \varphi\omega_A]$ in Theorem A.6.

Hence, the assertion is a consequence of Theorem A.6 and Proposition B.4. □

Remark B.5.

(i) A recent progress towards Conjecture B.1 appears in [7], [17], [19]. The key tools are (variants of) the Beilinson-Flach element and the BDP formula. In the non-ordinary case, these results assume additional hypotheses such as p odd, while our independent approach treats the general non-ordinary case.

(ii) Theorem B.3 is a tool in the proof of yet another CM p-converse (cf. [15]), and in turn, a result towards the cube sum problem (cf. [1]).

[10] Note that $\omega_A = \frac{p}{\alpha-\beta}(\omega_\alpha - \omega_\beta)$.

https://doi.org/10.1017/S147474802300021X Published online by Cambridge University Press

Acknowledgement. It is a pleasure to thank Chris Skinner for stimulating discussions. We are grateful to the referee for valuable suggestions.

The paper owes its very existence to prescient works [47], [50] by Karl Rubin. The authors would like to express their sincere gratitude to him.

This work was partially supported by the NSF grant DMS 2001409 and the JSPS KAKENHI grants JP17H02836, JP18H05233, JP22H00096, JP17K14173, JP21K13774.

Competing Interests. The author declares none.

References

[1] L. Alpoge, M. Bhargava and A. Shnidman, 'Integers expressible as the sum of two rational cubes', Preprint, arXiv:2210.10730.

[2] A. Agboola and B. Howard, 'Anticyclotomic Iwasawa theory of CM elliptic curves II', *Math. Res. Lett.* **12**(5-6) (2005), 611–621.

[3] A. Agboola and B. Howard, 'Anticyclotomic Iwasawa theory of CM elliptic curves', *Ann. Inst. Fourier (Grenoble)* **56**(4) (2006), 1001–1048.

[4] F. Andreatta and A. Iovita, 'Katz type p-adic L-functions for primes p non-split in the CM field', Preprint, arXiv:1905.00792.

[5] K. Bannai, H. Furusho and S. Kobayashi, 'p-adic Eisenstein-Kronecker series for CM elliptic curves and the Kronecker limit formulas', *Nagoya Math. J.* **219** (2015), 269–302.

[6] M. Bertolini, H. Darmon and K. Prasanna, 'Generalised Heegner cycles and p-adic Rankin L-series', *Duke Math. J.* **162**(6), 1033–1148.

[7] M. Bertolini, H. Darmon and R. Venerucci, 'Heegner points and Beilinson–Kato elements: A conjecture of Perrin-Riou', *Adv. Math.* **398**(108172) (2022), 50 pp.

[8] D. Bump, S. Friedberg and J. Hoffstein, 'Nonvanishing theorems for L-functions of modular forms and their derivatives', *Invent. Math.* **102**(3) (1990), 543–618.

[9] A. Burungale, K. Buyukboduk and A. Lei, Anticyclotomic Iwasawa theory of abelian varieties of GL_2-type at non-ordinary primes, Preprint, arXiv:2211.03722.

[10] A. Burungale, F. Castella, C. Skinner and Y. Tian, 'p^∞-Selmer groups and rational points on CM elliptic curves', *Ann. Math. Qué.* **46**(2) (2022), 325–346.

[11] A. Burungale, F. Castella, C. Skinner and Y. Tian, 'p-converse to a theorem of Gross–Zagier and Kolyvagin: CM elliptic curves over totally real fields', Preprint.

[12] A. Burungale, S. Kobayashi and K. Ota, 'Rubin's conjecture on local units in the anticyclotomic tower at inert primes', *Ann. of Math. (2)* **194**(3) (2021), 943–966.

[13] A. Burungale, S. Kobayashi and K. Ota, 'The p-adic valuation of local resolvents, generalized Gauss sums and anticyclotomic Hecke L-values of imaginary quadratic fields at inert primes', Preprint.

[14] A. Burungale, S. Kobayashi, K. Ota and S. Yasuda, 'Kato's epsilon conjecture for anticyclotomic CM deformations at inert primes', *Preprint.*

[15] A. Burungale and C. Skinner, 'A p-converse theorem for CM elliptic curves', Preprint, arXiv:2210.10730.

[16] A. Burungale, C. Skinner and Y. Tian, 'The Birch and Swinnerton-Dyer conjecture: A brief survey', *Proc. Sympos. Pure Math.* vol. 104 (Amer. Math. Soc., Providence, RI, 2021), 11–29.

[17] A. Burungale, C. Skinner and Y. Tian, 'Elliptic curves and Beilinson–Kato elements: Rank one aspects', Preprint.

[18] A. Burungale and Y. Tian, 'p-converse to a theorem of Gross–Zagier, Kolyvagin and Rubin', *Invent. Math.* **220**(1) (2020), 211–253.

[19] K. Buyukboduk, R. Pollack and S. Sasaki, 'p-adic Gross–Zagier formula at critical slopes and a conjecture of Perrin-Riou', Preprint.

[20] J. Coates and A. Wiles, 'On the conjecture of Birch and Swinnerton-Dyer', *Invent. Math.* **39**(3) (1977), 223–251.

[21] R. Coleman and B. Edixhoven, 'On the semi-simplicity of the U_p-operator on modular forms', *Math. Ann.* **310**(1) (1998), 119–127.

[22] P. Colmez, 'Fonctions L p-adiques', *Séminaire Bourbaki* vol. 41 (1998/99), Astérisque No. 266 (2000), Exp. No. 851, 3, 21–58.

[23] C. Diem and N. Naumann, 'On the structure of Weil restrictions of abelian varieties', *J. Ramanujan Math. Soc.* **18**(2) (2003), 153–174.

[24] R. Greenberg, 'On the Birch and Swinnerton-Dyer conjecture', *Invent. Math.* **72**(2) (1983), 241–265.

[25] R. Greenberg, 'Iwasawa theory and p-adic deformations of motives', *Motives* (Seattle, WA, 1991), 193–223, *Proc. Sympos. Pure Math.* vol. 55, part 2, (Amer. Math. Soc., Providence, RI, 1994).

[26] R. Greenberg, 'Introduction to Iwasawa theory for elliptic curves', *Arithmetic Algebraic Geometry* (Park City, UT, 1999), 407–464, *IAS/Park City Math. Ser.* vol. 9 (Amer. Math. Soc., Providence, RI, 2001).

[27] B. Gross, Arithmetic on elliptic curves with complex multiplication, *Lecture Notes in Mathematics* vol. 776 (Springer, Berlin, 1980), iii+95.

[28] B. Gross and D. Zagier, 'Heegner points and derivatives of L-series', *Invent. Math.* **84**(2) (1986), 225–320.

[29] K. Kato, 'Lectures on the approach to Iwasawa theory for Hasse-Weil L -functions via $B_{\mathrm{d}R}$. I', *Arithmetic Algebraic Geometry* (Trento, 1991), *Lecture Notes in Math.* vol. 1553 (Springer, Berlin, 1993), 50–163.

[30] K. Kato, 'p-adic Hodge theory and values of zeta functions of modular forms', in *Cohomologies p-adiques et applications arithmétiques III*, Astérisque vol. 295 (2004), 117–290.

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

[32] S. Kobayashi, 'The p -adic Gross–Zagier formula for elliptic curves at supersingular primes', *Invent. Math.* **191**(3) (2013), 527–629.

[33] S. Kobayashi, 'The p-adic height pairing on abelian varieties at non-ordinary primes', in *Iwasawa Theory 2012* vol. 7 (Springer, Berlin, 2014), 265–290.

[34] S. Kobayashi, 'A p-adic interpolation of generalized Heegner cycles and integral Perrin-Riou twist I', *Ann. Math. Qué*, To appear.

[35] V. Kolyvagin, Euler systems, *The Grothendieck Festschrift* vol. II, *Progr. Math.* vol. 87, (Birkhauser Boston, Boston, MA, 1990), 435–483.

[36] D. Kriz, 'A new p-adic Maass–Shimura operator and supersingular Rankin–Selberg p -adic L-functions', Preprint, arXiv:1805.03605.

[37] Y. Liu, S.-W. Zhang and W. Zhang, 'A p-adic Waldspurger formula', *Duke Math. J.* **167**(4) (2018), 743–833.

[38] B. Mazur, Modular curves and arithmetic, in *Proceedings of the International Congress of Mathematicians* vol. 1-2 (Warsaw, 1983), 185–211.

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

[40] J. Nekovář, 'The Euler system method for CM points on Shimura curves. L-functions and Galois representations', *London Math. Soc. Lecture Note Ser.* vol. 320 (Cambridge Univ. Press, Cambridge, 2007), 471–547.

[41] B. Perrin-Riou, 'Théorie d'Iwasawa p-adique locale et globale', *Invent. Math.* **99**(2) (1990), 247–292.

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

[43] B. Perrin-Riou, 'Théorie d'Iwasawa des représentations p-adiques sur un corps local', *Invent. Math.* **115**(1) (1994), 81–161.

[44] B. Perrin-Riou, *Fonctions Lp-adiques des représentations p-adiques*, Astérisque No. **229** (1995), 198 pp.

[45] D. Rohrlich, 'On L-functions of elliptic curves and anticyclotomic towers', *Invent. Math.* **75**(3) (1984), 383–408.

[46] K. Rubin, 'Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer', *Invent. Math.* **64**(3) (1981), 455–470.

[47] K. Rubin, 'Local units, elliptic units, Heegner points and elliptic curves', *Invent. Math.* **88**(2) (1987), 405–422.

[48] K. Rubin, 'Tate–Shafarevich groups and L-functions of elliptic curves with complex multiplication', *Invent. Math.* **89**(3) (1987), 527–559.

[49] K. Rubin, 'The "main conjectures" of Iwasawa theory for imaginary quadratic fields', *Invent. Math.* **103**(1) (1991), 25–68.

[50] K. Rubin, 'p-adic L-functions and rational points on elliptic curves with complex multiplication', *Invent. Math.* **107**(2) (1992), 323–350.

[51] K. Rubin, 'p-adic variants of the Birch and Swinnerton-Dyer conjecture for elliptic curves with complex multiplication', p-adic monodromy and the Birch and Swinnerton-Dyer conjecture, *Contemp. Math.* vol. 165 (Boston, MA, 1991) (Amer. Math. Soc., Providence, RI, 1994), 71–80.

[52] C. Skinner, 'A converse to a theorem of Gross, Zagier and Kolyvagin', *Ann. of Math.* **191**(2) (2020), 329–354.

[53] A. Wiles, 'Higher explicit reciprocity laws', *Ann. of Math. (2)* **107**(2) (1978), 235–254.

[54] J.-P. Wintenberger, 'Structure galoisienne de limites projectives d'unités locales', *Compositio Math.* **42**(1) (1980/81), 89–103.

[55] X. Yuan, S.-W. Zhang and W. Zhang, 'The Gross–Zagier formula on Shimura curves', in *Annals of Mathematics Studies* vol. 184 (Princeton University Press, Princeton, NJ, 2013), x+256.

[56] W. Zhang, 'Selmer groups and the indivisibility of Heegner points', *Camb. J. Math.* **2**(2) (2014), 191–253.