Annals of Mathematics **194** (2021), 943–966
https://doi.org/10.4007/annals.2021.194.3.8

Rubin's conjecture on local units in the anticyclotomic tower at inert primes

By Ashay A. Burungale, Shinichi Kobayashi, and Kazuto Ota

Abstract

We prove a fundamental conjecture of Rubin on the structure of local units in the anticyclotomic $\mathbb{Z}_p$-extension of the unramified quadratic extension of $\mathbb{Q}_p$ for $p \geq 5$ a prime.

Rubin's conjecture underlies Iwasawa theory of the anticyclotomic deformation of a CM elliptic curve over the CM field at primes p of good supersingular reduction, notably the Iwasawa main conjecture in terms of the p-adic L-function. As a consequence, we prove an inequality in the p-adic Birch and Swinnerton-Dyer conjecture for Rubin's p-adic L-function. Rubin's conjecture is also an essential tool in our exploration of the arithmetic of Rubin's p-adic L-function, which includes a Bertolini–Darmon–Prasanna type formula.

1. Introduction

Iwasawa theory for CM elliptic curves has a long history and continues to have significant arithmetic applications, needless to say, since the first general results towards the Birch and Swinnerton-Dyer conjecture by Coates–Wiles. Iwasawa theory is a p-adic theory and the behavior heavily depends on the nature of the prime p. Nowadays, for an ordinary prime p (or a Panchishkin prime in general; cf. [12, §3]), we have a guiding principle of Iwasawa theory for general motives and p-adic deformations (cyclotomic, Hida theoretic, several variables; cf. [12]). For the cyclotomic deformation, B. Perrin-Riou developed a general formalism of Iwasawa theory including non-ordinary primes (cf. [28]), and the (φ, Γ)-theory gives strong applications for this. Sometimes the signed Iwasawa theory initiated by R. Pollack and the second-named author also works well. However, apart from the cyclotomic deformation, the situation is still not

Keywords: CM elliptic curves, Iwasawa theory, local units, p-adic L-functions
AMS Classification: Primary: 11G07, 11G15, 11R23.
This work was partially supported by the NSF grant DMS 2001409, and the JSPS KAKENHI grants JP16K13742, JP17H02836, JP17K14173 and JP18J01237.

so satisfactory for non-ordinary (non-Panchishkin) deformations even for very basic cases such as Iwasawa theory for CM elliptic curves of the anticyclotomic deformation at inert (supersingular) primes. We point out that this is not merely a matter of formalism; in fact new interesting phenomena happen and an Iwasawa theory should reflect them.

Let E be an elliptic curve defined over $\mathbb{Q}$ with complex multiplication by an imaginary quadratic field K. We also assume that E has good reduction at p. Let $w_{E/\mathbb{Q}}$ be the root number of $E/\mathbb{Q}$. Let K_∞^{ac} be the anticyclotomic $\mathbb{Z}_p$-extension of K with the n-th layer K_n^{ac}. The behavior of the Mordell–Weil rank of $E(K_n^{\mathrm{ac}})$ is very interesting. If p splits in K (hence, E has good ordinary reduction above p), then $\mathrm{rank}_{\mathbb{Z}}\, E(K_n^{\mathrm{ac}})$ is bounded independently of n if $w_{E/\mathbb{Q}} = +1$, whereas $\mathrm{rank}_{\mathbb{Z}}\, E(K_n^{\mathrm{ac}}) = 2p^n + c$ for all n sufficiently large if $w_{E/\mathbb{Q}} = -1$ for c a constant. (In the latter exceptional case (cf. [24]) the Heegner hypothesis is not satisfied and the rational points on E are only indirectly related to Heegner points. Note that the rank should be even because of the CM action and the sign of the functional equation of the Hasse–Weil L-function of E/K being $+1$.) On the other hand, if p is inert in K (hence, E has good supersingular reduction above p), R. Greenberg noticed that root numbers vary in the anticyclotomic tower and observed

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

for all n sufficiently large, where ε_n is zero or two depending on the parity of n. In particular, new points of infinite order appear in every other layer of the anticyclotomic $\mathbb{Z}_p$-extension (cf. [11], [13]). More precisely, if $w_{E/\mathbb{Q}} = +1$, then ε_n for sufficiently large n is zero for odd n and two for even n. The reverse holds when $w_{E/\mathbb{Q}} = -1$. (The phenomenon was first observed in the early 80s (cf. [11, p. 247]). A proof appears in [1], [5].) In contrast, the Mordell–Weil rank is always bounded in the cyclotomic $\mathbb{Z}_p$-extension even for a supersingular prime p. (However, the behavior of the conjectural asymptotic order of the Tate–Shafarevich groups in the cyclotomic $\mathbb{Z}_p$-extension depends on the reduction type of E at p and is similar to the anticyclotomic case as above; cf. [22], [23], [26], [29].)

Rubin's conjecture. In [33], K. Rubin envisioned an Iwasawa theory reflecting such phenomena. In the split (ordinary) case, it is classical to study the module of local units modulo elliptic units attached to E in the $\mathbb{Z}_p^2$-extension of K, and it is shown that its characteristic ideal is generated by the two-variable Katz p-adic L-function attached to E. However, in the inert case, the rank of the module of local units is twice that of the module of elliptic units and the quotient is non-torsion.

Rubin considered a module V obtained as the (twisted) projection of local units in the $\mathbb{Z}_p^2$-extension of K to the anticyclotomic direction, and he defined

two free Λ-submodules $V^{\pm}$ of rank 1 of V. Here Λ is the Iwasawa algebra for the anticyclotomic $\mathbb{Z}_p$-extension of an unramified quadratic extension of $\mathbb{Q}_p$ and the local modules $V^{\square}$ depend only on p. In 1987 Rubin conjectured that

$$V = V^{+} \oplus V^{-} \tag{R}$$

(cf. [33, Conj. 2.2]). The conjecture is purely local, inherent to the prime p. Yet it is intertwined with a supersingular counterpart of the anticyclotomic Katz p-adic L-function. Indeed, the projection of elliptic units lives in V^{ε} where ε is the sign of the functional equation of $L(E/\mathbb{Q}, s)$. In [33] it was shown that the quotient of V^{ε} by the image of elliptic units is Λ-torsion and generated by a certain p-adic L-function $\mathscr{L}_E$, whose interpolation factors are non-zero under (R).

The aim of the present paper is to prove Rubin's conjecture (R) (cf. Theorem 2.1).

Intriguingly, Rubin's theory is a kind of signed Iwasawa theory preceding [22] and [30]. In fact, A. Agboola and B. Howard [1] reconsidered Rubin's theory in the context of the signed Iwasawa theory, and under Rubin's conjecture, they formulated and proved an Iwasawa main conjecture that involves Rubin's p-adic L-function $\mathscr{L}_E$ and also explained the rank formula of Greenberg. (The proof relies on the main conjecture for K [34].) We recall their Iwasawa main conjecture in Section 6, which is now unconditional (cf. Theorem 6.1). As a consequence, we prove an inequality in the rank part of the underlying p-adic Birch and Swinnerton-Dyer conjecture (cf. Theorem 2.4).

The strategy. In [33] Rubin envisaged a criterion under which the conjecture is true. The criterion is still elusive, yet its principle lies at the heart of our approach.

Rubin's criterion involves the existence of certain global objects:

(a) a CM elliptic curve with good supersingular reduction at p whose central L-value is p-indivisible;
(b) a Heegner point over imaginary quadratic fields with p inert that is locally p-indivisible.

The existence (a) and (b) implies (R).

After Rubin's work, there was an important development [10] towards (a). The p-indivisibility relies on (a variant of) the Manin–Mumford conjecture. The results of [10] exclude the set-up of the criterion, yet we slightly generalize the set-up so as to include more general L-values. This is the content of Section 3. (While the p-indivisibility [10] is not so recent, its relevance to Rubin's conjecture seems to be curiously overlooked.)

The essential difficulty is (b). Indeed, it was the fundamental obstruction, which resisted attempts at even partial progress towards the conjecture.

Despite an important recent advance [43], the local p-indivisibility of Heegner points seems to be still mysterious. Instead, we consider a variant of (b) and approach it by a new idea, which is surprisingly simple but decisive and the main content of our proof (cf. Sections 4 and 5). A primary insight is to replace the inherently global (b) with a variant that is more amenable to local tools. In Rubin's criterion, (b) assures the existence of an optimal system of local points of the Lubin–Tate formal group with parameter $-p$ in the anticyclotomic $\mathbb{Z}_p$-extension. It is actually the optimal system, rather than the Heegner point, that is crucial for the proof of Rubin's conjecture. For the cyclotomic $\mathbb{Z}_p$-extension, the construction of such a system of local points is the key of the signed Iwasawa theory in [22] and it is also the core of the theory of the Perrin-Riou exponential map [27]. The development of the Perrin-Riou theory, especially by using (φ,Γ)-theory, has been greatly influential; a striking instance is the p-adic Langlands program. It is highly desirable to develop such a general theory also for non-cyclotomic extensions and, in fact, there are some developments on (φ,Γ)-theory for Lubin–Tate extensions. Our prior attempts to construct the optimal system of local points related to (b) were actually via the (φ,Γ)-theory. However, the theory seems to be still incipient.

Departing the (φ,Γ)-environment, our new idea to construct the optimal system is geometric. Instead of Heegner points, we resort to formal CM points and the modular parametrization of elliptic curves. Formal CM points are local points of modular curves whose associated elliptic curves have formal complex multiplication: the endomorphism ring of its formal group is bigger than $\mathbb{Z}_p$. We employ the theory of quasi-canonical lifts by Gross [14] and the modular parametrization to construct the optimal system of local points in the Lubin–Tate formal group of height 2 (cf. Theorem 5.5).

Remark 1.1. The moduli of Lubin–Tate formal groups is also an essential tool in Tsuji's explicit reciprocity law [40] over imaginary quadratic fields with p inert. Katz pioneered the relevance of local moduli to CM Iwasawa theory (cf. [19], [20]); our method presents a new facet. We hope it to be merely a shadow of enriching interactions among local moduli and supersingular Iwasawa theory.

Horizon. Rubin's conjecture reveals unexplored vistas and inspires an advance in non-Panchishkin Iwasawa theory. Indeed, the proof of (R) has unexpectedly led us to new developments in supersingular Iwasawa theory. In retrospect, Rubin's conjecture perhaps constitutes the core of the emerging Perrin-Riou theory, thereby being central to the global arithmetic.

In our next paper [5] we prove a Bertolini–Darmon–Prasanna (BDP) style formula for Rubin's p-adic L-function: a relationship between certain values of $\mathscr{L}_E$ (outside its defining range of interpolation) and rational points on E (cf. [3], [35]). The formula is based on our optimal system of local points. The

BDP formula in turn leads to a special case of the Birch and Swinnerton-Dyer conjecture: a p-converse to the Gross–Zagier and Kolyvagin theorem for E (cf. [7], [39], [43]). The general formalism of p-adic L-functions still excludes the case of Rubin's p-adic L-function. In [4] we determine the valuation of its "p-adic periods," which gives an asymptotic behavior of the anticyclotomic p-adic variation of the central L-values, where (R) is again a key. In [6] Kato's local ε-conjecture (for the anticyclotomic CM deformation) is shown to be yet another consequence of (R).

Our approach to local points has a potential for generalization on Shimura varieties. (In light of Shimura curve parametrizations over totally real fields, a natural generalization will appear in a subsequent work.) It may also offer an insight to the development of (φ,Γ)-theory for Lubin–Tate extensions. In the near future we plan to investigate a counterpart of Rubin's conjecture — in the enigmatic case — when the prime p ramifies in the CM field.

Acknowledgement. The authors thank Adebisi Agboola, Ye Tian, Chris Skinner and Wei Zhang for instructive comments. They also thank[1] Naomi Jochnowitz and Jeremy Rouse for helpful exchanges. They are grateful to the referee for valuable suggestions.

The authors would like to express their sincere gratitude to Karl Rubin for his inspiring oeuvre, the influence of which is transparent.

2. **The main theorem**

First, following [33], we explain Rubin's conjecture precisely.

Let $p \geq 5$ be a prime, and let Φ be the unique unramified quadratic extension of $\mathbb{Q}_p$ with integer ring $\mathcal{O}$. We fix a Lubin–Tate formal group $\mathscr{F}$ over $\mathcal{O}$ for the uniformizing parameter $\pi := -p$. For $n \geq -1$, 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 $\Phi_\infty = \cup_n \Phi_n$. The Galois action on the π-adic Tate module $T_\pi\mathscr{F}$ defines a natural isomorphism

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

We put $\Delta := \mathrm{Gal}(\Phi_0/\Phi) \cong (\mathcal{O}/\pi\mathcal{O})^\times$ and note $\mathrm{Gal}(\Phi_\infty/\Phi) \cong \Delta \times \mathrm{Gal}(\Phi_\infty/\Phi_0)$ canonically. Let ω denote the Teichmüller character; i.e., the restriction of κ to Δ via the preceding isomorphism. By the action of $\mathrm{Gal}(\Phi/\mathbb{Q}_p)$, we have a canonical decomposition $\mathrm{Gal}(\Phi_\infty/\Phi_0) \cong G^+ \oplus G^-$, $G^\pm \cong \mathbb{Z}_p$, where G^+ (resp. G^-) is the maximal subgroup of $\mathrm{Gal}(\Phi_\infty/\Phi_0)$ on which $\mathrm{Gal}(\Phi/\mathbb{Q}_p)$ acts via the trivial (resp. non-trivial) character. The group G^+ is naturally isomorphic to the Galois group of the cyclotomic $\mathbb{Z}_p$-extension of Φ, and the group

[1] It is the first author's pleasure to thank Peter Handke.

G^- is the Galois group of the anticyclotomic $\mathbb{Z}_p$-extension Ψ_∞ of Φ. The anticyclotomic $\mathbb{Z}_p$-extension Ψ_∞ is also characterized as the maximal dihedral pro-p-extension of $\mathbb{Q}_p$ in Φ_∞. We call a finite character of $\mathrm{Gal}(\Phi_\infty/\Phi)$ that factors through G^- an anticyclotomic character. By our convention, a non-trivial anticyclotomic character χ has conductor p^{n+1} if χ factors through $\mathrm{Gal}(\Phi_n/\Phi)$ but not through $\mathrm{Gal}(\Phi_{n-1}/\Phi)$ and the trivial one has conductor 1.

For a natural number n, let U_n be the group of principal units in Φ_n — that is, the group of units in the integer ring of Φ_n that are congruent to 1 modulo the maximal ideal. We define

$$\tilde{U}_\infty = \varprojlim_n (U_n \otimes_{\mathbb{Z}_p} \mathcal{O}), \qquad U_\infty = \tilde{U}_\infty^\omega,$$

where the inverse limit is taken with respect to the norm maps, and the superscript ω means the part where Δ acts by ω. Define the Iwasawa algebras

$$\Lambda_2 = \mathcal{O}[\![\mathrm{Gal}(\Phi_\infty/\Phi_0)]\!] \quad \text{and} \quad \Lambda = \mathcal{O}[\![G^-]\!].$$

It is known that U_∞ is a free Λ_2-module of rank 2. Our primary object is the quotient module

$$V_\infty = U_\infty/(\sigma - \kappa(\sigma))U_\infty,$$

where σ is a generator of G^+. (The ideal $(\sigma - \kappa(\sigma))$ in Λ_2 does not depend on the choice of σ.) Then V_∞ is a Λ-module free of rank 2. For a Λ_2-module M, we define $M^* := M \otimes_{\mathcal{O}} T_\pi \mathscr{F}^{\otimes -1} = \mathrm{Hom}_{\mathcal{O}}(T_\pi \mathscr{F}, M)$, and let the Galois group act diagonally. (We let M^* denote the conventional M_* for notational simplicity.) Hence, M^* is isomorphic to M but the Galois action is twisted by κ^{-1}. Then U_∞^* is the fixed part of $\tilde{U}_\infty^*$ by Δ and V_∞^* is the anticyclotomic quotient $U_\infty^*/(\sigma - 1)$.

Now we recall the Coates–Wiles logarithmic derivatives

$$\delta : U_\infty^* \to \mathcal{O}, \qquad \delta_n : U_\infty^* \to \Phi_n.$$

For an element $x \in U_\infty^*$, we write $x = u \otimes a \otimes v^{\otimes -1}$ where $u = (u_n)_n \in \varprojlim_n U_n$, $a \in \mathcal{O}$ and a generator $v = (v_n)_n \in T_\pi \mathscr{F}$ as an $\mathcal{O}$-module. (In [33] the p-adic Tate module is used instead of the π-adic Tate module.[2] Hence the generator v_n in [33, §2] differs by $(-1)^n$ from ours.) Then consider the Coleman power series $f \in \mathcal{O}[\![X]\!]^\times$ such that $f(v_n) = u_n$ and define

$$\delta(x) = a\frac{f'(0)}{f(0)}, \quad \delta_n(x) = \frac{a}{\lambda'(v_n)}\frac{f'(v_n)}{f(v_n)},$$

where λ is the formal logarithm of $\mathscr{F}$. It is straightforward to check that these maps are well defined and Galois equivariant. That is, $\delta_n(\gamma x) = \delta_n(x)^\gamma$ for

[2]The change is essential, as otherwise, the Coleman theory *does not* hold. There are sign errors in [33] because of this. In the following we modify some definitions of [33] appropriately without remarks.

$\gamma \in \mathrm{Gal}(\Phi_\infty/\Phi)$. For a finite character $\chi : \mathrm{Gal}(\Phi_\infty/\Phi) \to \overline{\mathbb{Q}}_p^\times$, let n be so that χ factors through $\mathrm{Gal}(\Phi_n/\Phi)$ and put

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

(The definition does not depend on the choice of n.) For $\beta \in \mathrm{Gal}(\Phi_\infty/\Phi)$, we have $\delta_\chi(x^\beta) = \chi(\beta)^{-1}\delta_\chi(x)$. In particular, if $\beta = \sigma \in G^+$ and χ is anticyclotomic, then $\delta_\chi((\sigma - 1)U_\infty^*) = 0$. Hence for an anticyclotomic χ, the map δ_χ defines a map on V_∞^*. Let Ξ^+ (resp. Ξ^-) be the set of anticyclotomic characters whose conductors are even (resp. odd) power of p.

Define

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

(Note that $V_\infty^{*,\epsilon}$ is a twist of V_∞^ϵ in [33, p. 406].) Rubin showed $V_\infty^{*,\pm} \cong \Lambda$ and $V_\infty^{*,+} \cap V_\infty^{*,-} = \{0\}$ (cf. [33, Prop. 8.1], a sketch of the argument is given in Section 4), and conjectured

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

(cf. [33, Conj. 2.2]).

The main result of this paper is the following:

THEOREM 2.1. *Rubin's conjecture is true, that is,* $V_\infty^* = V_\infty^{*,+} \oplus V_\infty^{*,-}$.

As in [33, Lem. 10.1], we have the following.

COROLLARY 2.2. *Let* $\epsilon \in \{+,-\}$ *and* $v \in V_\infty^{*,\epsilon}$ *be a generator. Then for all* $\chi \in \Xi^\epsilon$, *we have* $\delta_\chi(v) \neq 0$.

Remark 2.3. Rubin proved his conjecture for primes $p : 5 \leq p \leq 1001$ and $p \not\equiv 1 \bmod 12$ (cf. [33, p. 418]), which is the prior result towards the conjecture.

As another corollary of Rubin's conjecture, we present the following result towards a p-adic Birch and Swinnerton-Dyer conjecture in Section 6. For simplicity, let the notation and assumptions be as in the introduction. Let φ be the Hecke character associated to the CM elliptic curve E. Let $\mathscr{L}_E \in \Lambda$ be the Rubin p-adic L-function, as defined in Section 6.0.1, which interpolates the algebraic part of special values $L(\varphi\chi, 1)$ for $\chi \in \Xi^\epsilon$.

THEOREM 2.4. *We have*

$$\operatorname{rank} E(K_n^{\mathrm{ac}})^\chi \leq \begin{cases} \operatorname{ord}_\chi \mathscr{L}_E & (\chi \in \Xi^\epsilon), \\ \operatorname{ord}_\chi \mathscr{L}_E + 1 & (\chi \in \Xi^{-\epsilon}) \end{cases}$$

for p^n *the conductor of* χ.

In [5] we show that the equality holds in the above if $\mathrm{ord}_{s=1}L(\varphi\chi, s) \leq 1$.

Remark 2.5. The theorem is an anticyclotomic variant of Kato's result towards the cyclotomic p-adic Birch and Swinnerton-Dyer conjecture (cf. [18, §18]).

Notation. Let $\overline{\mathbb{Q}}$ be an algebraic closure, and fix an embedding $\iota_\infty : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. Throughout, let $p \geq 5$ be a prime, $\overline{\mathbb{Q}}_p$ an algebraic closure, and fix an embedding $\iota_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$.

3. Hecke L-values

The main result of this section is Theorem 3.4.

3.0.1. *An auxiliary imaginary quadratic field.*

LEMMA 3.1. *There exists an imaginary quadratic field K such that*

(a) $\left(\frac{2}{D_K}\right) = +1$, *where* $-D_K < 0$ *is the discriminant of* K;
(b) p *is inert in* K;
(c) $p \nmid h_K$.

Proof. Pick an integer $1 \leq m \leq p-1$ with $(-m/p) = -1$, and let $0 \leq k \leq 7$ be the integer: $m + kp \equiv 7 \bmod 8$. Write $-(m + kp) = dn^2$ for d square-free.

Notice $d \equiv 1 \bmod 8$, and $(d/p) = -1$; i.e., (a) and (b) hold for $K = \mathbb{Q}(\sqrt{d})$.

In view of the convexity bound for $L(1, \chi_d)$ (for example, [25, Lem. 8.16]) and the Dirichlet class number formula, we have

$$h(d) \leq \frac{\sqrt{|d|}}{\pi}(2 + \log|d|) < \frac{\sqrt{8p}}{\pi}(2 + \log 8p).$$

(Note that here $\pi = 3.14\cdots$, which is a contrast with the preceding notation.) Thus, $h(d) < p$ unless $p \leq 47$, and (c) holds. For $p \leq 47$, the assertion is readily seen. □

Remark 3.2. We are grateful to Jeremy Rouse for the above argument. The existence of such infinitely many imaginary quadratic fields is due to Jochnowitz [16].

In the rest of this section K denotes an imaginary quadratic field satisfying assertions (b) and (c) of Lemma 3.1. (D_K is allowed to be even, and we do not assume the validity of the assertion (a) of Lemma 3.1 until Theorem 3.4.) For a non-zero integral ideal $\mathfrak{g}$ of K, we denote by $K(\mathfrak{g})$ the ray class field of K of conductor $\mathfrak{g}$. Let H denote the Hilbert class field $K(1)$ and $N_{H/K}$ denote the norm. Note that the completion of H in $\mathbb{C}_p$ is Φ since the prime p in K splits completely in H.

Let φ be a Hecke character over K with infinity type $(1, 0)$ of conductor $\mathfrak{f} = \mathfrak{f}_\varphi$ such that the Hecke character $\varphi \circ N_{H/K}$ over H is associated to an

elliptic curve E over H with complex multiplication by $\mathcal{O}_K$. We assume that E is a $\mathbb{Q}$-curve in the sense of Gross and has good reduction at every prime of H above p. We note that if φ is a canonical Hecke character (as in the proof of Theorem 3.4 below), such an E always exists. Then, E satisfies the Shimura condition (cf. [32, (1.1)]), and

(3.1) ∘ for $\alpha \in K^\times \cap \mathcal{O}_K$ such that $\alpha \equiv 1 \bmod \mathfrak{f} : \varphi(\alpha\mathcal{O}_K) = \alpha$,

(3.2) ∘ for an ideal $\mathfrak{a}$ prime to $\mathfrak{f} : \varphi(\overline{\mathfrak{a}}) = \overline{\varphi(\mathfrak{a})}$,

where $\overline{z}$ denotes the complex conjugate of z.

3.0.2. *Elliptic units: a variant.* Let $l \geq 5$ be a prime split in K such that l is relatively prime to $h_K\mathfrak{f}$ and

$$p \nmid (l-1). \tag{3.3}$$

Let $\mathfrak{X}_l$ be the set of Hecke characters ν over K of finite order that factor through the Galois group of the anticyclotomic $\mathbb{Z}_l$-extension of K. In particular, the conductor and order of ν are powers of l. We note that for $\nu \in \mathfrak{X}_l$, the root number $W(\overline{\varphi}\nu)$ of $\overline{\varphi}\nu$ coincides with the root number $W(\varphi)$ of φ (cf. [11, p. 247]).

In the following we employ elliptic units to construct a certain local element related to the special values of the Hecke L-function $L(\overline{\varphi}\nu, s)$ and its twists by finite characters of $\mathrm{Gal}(\Phi_\infty/\Phi_0)$ (cf. Proposition 3.3). The case where ν is trivial corresponds to the elliptic unit ξ_E in [33, Th. 3.2], that appears in Rubin's strategy [33, §8] to investigate $V_\infty^{*,+}$ and $V_\infty^*/V_\infty^{*,-}$ under the *assumption* of the p-indivisibility of the algebraic part of the special value $L^{\mathrm{alg}}(\varphi, 1)$. In Theorem 3.4 we utilize our local elements for a ν such that $L^{\mathrm{alg}}(\overline{\varphi}\nu, 1)$ *is* p-indivisible.

We fix a smooth Weierstrass model of the elliptic curve E over $\mathcal{O} \cap H$ and by considering a Galois conjugate of E over H if necessary, we may assume that the period lattice L attached to the Néron differential ω is given by $\Omega\mathcal{O}_K$ for some $\Omega \in \mathbb{C}^\times$. We fix such an Ω. Let $\mathcal{R}$ be the integer ring of a finite extension of Φ containing the image of φ. (In the following we may further enlarge $\mathcal{R}$.) Let T be the p-adic Galois representation associated to φ : a free $\mathcal{R}$-module of rank one, the G_K-action via φ, and the restriction to G_H being $T_\pi E \otimes \mathcal{R}$. (In the case $h_K = 1$, note that T is isomorphic to $T_\pi E \otimes \mathcal{R}$ as a G_K-module.) We put $V = T \otimes \mathbb{Q}_p$ and $V^{\otimes -1} = \mathrm{Hom}_{\mathcal{R}[\frac{1}{p}]}(V, \mathcal{R}[\frac{1}{p}])$, the latter being identified with $V_{\mathcal{R}[\frac{1}{p}]}(\varphi)$ in [18, §15.8].

For a non-zero integral ideal $\mathfrak{g}$ of K contained in $\mathfrak{f}$, by [18, Prop. 15.9] (with $\gamma = \mathrm{per}_\varphi(\omega)/\Omega$), there exists

$$\mathbf{z}_\mathfrak{g} = (z_{p^n\mathfrak{g}})_n \in \varprojlim_n H^1(K(\mathfrak{g}p^n), T^{\otimes -1}(1))$$

such that for $n \geq 0$ and a character χ of $\mathrm{Gal}(K(\mathfrak{g}p^n)/K)$,

$$\sum_{\sigma \in \mathrm{Gal}(K(\mathfrak{g}p^n)/K)} \chi(\sigma) \exp^*_{K(\mathfrak{g}p^n)}(\mathrm{loc}_p(z^{\sigma}_{p^n\mathfrak{g}})) = \frac{L_{p\mathfrak{g}}(\overline{\varphi}\chi, 1)}{\Omega}\omega. \tag{3.4}$$

Here $\mathrm{loc}_p : H^1(K(\mathfrak{g}p^n), -) \to H^1(K(\mathfrak{g}p^n) \otimes_K K_p, -)$ denotes the localization map ($K_p := K \otimes \mathbb{Q}_p \cong \Phi$),

$$\begin{aligned}\exp^*_{K(\mathfrak{g}p^n)} : H^1(K(\mathfrak{g}p^n) \otimes K_p, T^{\otimes -1}(1)) &\to D^0_{\mathrm{dR}}(V^{\otimes -1}(1)|_{G_{K_p}}) \otimes_K K(\mathfrak{g}p^n) \\ &= \mathcal{R} \otimes_{\mathcal{O}_H} \mathrm{coLie}(E) \otimes_K K(\mathfrak{g}p^n)\end{aligned}$$

is the dual exponential, and $L_{p\mathfrak{g}}(\overline{\varphi}\chi, s) := \sum_{\mathfrak{c}} \overline{\varphi}\chi(\mathfrak{c}) N_{K/\mathbb{Q}}(\mathfrak{c})^{-s}$ the Hecke L-function; $\mathfrak{c}$ ranges over all integral ideals of K relatively prime to $p\mathfrak{g}$.

Note that there exists a canonical isomorphism

$$\varprojlim_n H^1(K(\mathfrak{g}p^n), \mathbb{Z}_p(1)) \otimes T^{\otimes -1} \cong \varprojlim_n H^1(K(\mathfrak{g}p^n), T^{\otimes -1}(1)) \tag{3.5}$$

of $\mathcal{R}[\![\mathrm{Gal}(K(\mathfrak{g}p^{\infty})/K)]\!]$-modules. For $n \geq -1$, let $M_{n,m} \subseteq K(\mathfrak{f}l^m p^{n+1})$ denote the composite of $H(E[p^{n+1}])$ and the m-th layer L_m of the anticyclotomic $\mathbb{Z}_l$-extension of K.

Let $\nu \in \mathfrak{X}_l$ be a Hecke character of order l^m. We define ξ_ν as the image of $\mathbf{z}_{\mathfrak{f}l^m}$ under the composite

$$\begin{aligned}&\varprojlim_n H^1(K(\mathfrak{f}l^m p^{n+1}), T^{\otimes -1}(1)) \\ &\quad\to \varprojlim_n H^1(K(\mathfrak{f}l^m p^{n+1}), \mathbb{Z}_p(1)) \otimes T^{\otimes -1} \\ &\quad\to \varprojlim_n H^1(M_{n,m}, \mathbb{Z}_p(1)) \otimes T^{\otimes -1} \\ &\quad\to \varprojlim_n H^1(M_{n,m} \otimes_K K_p, \mathbb{Z}_p(1)) \otimes T^{\otimes -1} \\ &\quad= \varprojlim_n H^1\left(H(E[p^{n+1}]) \otimes_K K_p, \mathbb{Z}_p(1)\right) \otimes T^{\otimes -1} \otimes \mathcal{R}[\mathrm{Gal}(L_m/K)] \\ &\quad\xrightarrow{\nu} \varprojlim_n H^1\left(H(E[p^{n+1}]) \otimes_K K_p, \mathbb{Z}_p(1)\right) \otimes T^{\otimes -1} \\ &\quad= \varprojlim_n H^1\left(\Phi_n, \mathbb{Z}_p(1)\right) \otimes T^{\otimes -1} \otimes \mathcal{R}[\mathrm{Gal}(H/K)] \\ &\quad\to \varprojlim_n H^1\left(\Phi_n, \mathbb{Z}_p(1)\right) \otimes T^{\otimes -1} \\ &\quad\to \left(\varprojlim_n H^1\left(\Phi_n, \mathbb{Z}_p(1)\right) \otimes T^{\otimes -1}\right)^{\Delta} \\ &\quad\cong U^*_{\infty} \otimes \mathcal{R},\end{aligned}$$

with $\mathcal{R}$ being enlarged to contain the image of ν. Here the first arrow is via (3.5), the second one is the corestriction map, and the third localization. The

first equality is a consequence of $p\mathcal{O}_K$ being completely split in the ring class fields and $M_{n,m} = H(E[p^{n+1}]) \otimes_K L_m$ (as $l \nmid h_K$). The fourth arrow with ν is the evaluation at $\nu : \mathrm{Gal}(L_m/K) \to \mathcal{R}^\times$, the fifth one is induced by the natural projection $\mathcal{R}[\mathrm{Gal}(H/K)] \to \mathcal{R}$, and the sixth one the projection to the Δ-invariants. The last isomorphism arises from the Kummer map. Note that the above composite is $\mathrm{Gal}(\Phi_\infty/\Phi_0)$-equivariant, where $\mathrm{Gal}(\Phi_\infty/\Phi_0)$ is identified with $\mathrm{Gal}(K(\mathfrak{f}p^\infty)/K(\mathfrak{f}p))$.

So, in light of (3.4) and the explicit reciprocity law of Wiles (cf. [17, Th. 2.1.7, Ch. II]), for a finite character χ of $\mathrm{Gal}(\Phi_\infty/\Phi_0)$,

$$\delta_\chi(\xi_\nu) = \frac{L_{l^m p\mathfrak{f}}(\overline{\varphi}\nu\chi, 1)}{\Omega}. \tag{3.6}$$

Here $\mathrm{Gal}(\Phi_\infty/\Phi_0)$ is identified with the Galois group of the $\mathbb{Z}_p^2$-extension of K (as $p \nmid h_K$), and we identify $\mathscr{F}$ with the formal group $\hat{E}$ of E so that the invariant differential of $\mathscr{F}$ corresponds to ω. In particular,

$$\delta(\xi_\nu) = \frac{L_{l^m\mathfrak{f}}(\overline{\varphi}\nu, 1)}{\Omega}. \tag{3.7}$$

We now have the following:

PROPOSITION 3.3. *Let $\nu \in \mathfrak{X}_l$ be a character of order l^m. Then, the element $\xi_\nu \in U_\infty^* \otimes \mathcal{R}$ satisfies the following assertions*:

(1) *We have $\delta(\xi_\nu) = \Omega^{-1} L_{l^m\mathfrak{f}}(\overline{\varphi}\nu, 1)$.*
(2) *For a finite character χ of $\mathrm{Gal}(\Phi_\infty/\Phi_0)$, we have $\delta_\chi(\xi_\nu) = \Omega^{-1} L_{l^m p\mathfrak{f}}(\overline{\varphi}\nu\chi, 1)$.*
(3) *If we denote by ϵ the sign of the root number $W(\varphi) \in \{\pm 1\}$ of φ, then the anticyclotomic projection of ξ_ν lies in $V_\infty^{*,\epsilon} \otimes \mathcal{R}$*

Proof. It only remains to consider (3). In view of (2), the assertion amounts to the following: for a character χ of G^- of conductor $p^{n+1} > 1$ with $(-1)^{n+1} = -W(\varphi)$, we have $W(\overline{\varphi}\nu\chi) = -1$.

Since ν is anticyclotomic, we have $\overline{\varphi}\nu(p\mathcal{O}_K) = -p$ (cf. [33, Lem. 3.1]). From (3.2), the conductor $\mathfrak{f}l^m$ of $\overline{\varphi}\nu$ is fixed by the complex conjugation, and then $\chi(\mathfrak{f}l^m) = 1$ as χ is of odd order. Thus, by the same argument as in the proof of [33, Cor. 3.3] or as in [11, p. 247], we have $W(\overline{\varphi}\nu\chi) = (-1)^{n+1} W(\overline{\varphi}\nu) = (-1)^{n+1} W(\overline{\varphi}) = -1$. □

3.0.3. *An optimal unit.*

THEOREM 3.4. *There exists an element $\xi^* \in V_\infty^{*,+}$ such that $\delta(\xi^*) \in \mathcal{O}^\times$.*

Proof. Let K be as in Lemma 3.1. Let φ as above be a canonical Hecke character over K (cf. [31]). In particular,

(3.8)
the conductor $\mathfrak{f}_\varphi$ of φ is divisible only by primes of K ramified in $K/\mathbb{Q}$.

From Lemma 3.1(a), $W(\varphi) = +1$ (cf. [31] or [41, (5.0)]).

Let $l \geq 5$ be a split prime as in (3.3). By [10, Th. 1.1, (2)], for all but finitely many $\nu \in \mathfrak{X}_l$,

$$\Omega^{-1} L_{\mathfrak{f}}(\overline{\varphi}\nu, 1) \in \mathcal{W}^{\times}, \tag{3.9}$$

where $\mathcal{W}$ is the integer ring of a finite extension of Φ containing the image of ν. Here we utilize (3.8) and note that for an inert prime $q \neq p$, the invariants $\mu_p(\overline{\varphi}_q \nu_q)$ and $b_p(\overline{\varphi}_p \nu_p, w(p))$ of op. cit. vanish in our case (cf. the paragraph above [op. cit., Th. 1.1]). From now, fix a ν as in (3.9) and let l^m be the conductor.

By Proposition 3.3 and (3.9), there exists an element $\xi_\nu \in V_\infty^{*,+} \otimes \mathcal{W}$ such that we have

$$\delta(\xi_\nu) \in \mathcal{W}^{\times}. \tag{3.10}$$

Since $V_\infty^{*,+} \cong \Lambda$, (3.10) implies that any generator ξ^* of $V_\infty^{*,+}$ satisfies $\delta(\xi^*) \in \mathcal{O}^{\times}$. □

4. **The Kummer duality**

In this section we follow [33, §5], to which the reader may refer for details. For $n \leq \infty$, let $\Theta_n = \Phi_n^{\Delta}$ and $\Psi_n = \Theta_n^{G^+}$. As usual, the Kummer sequence

$$0 \longrightarrow \mathscr{F}_{\pi^{n+1}} \longrightarrow \mathscr{F}(\overline{\Phi}) \xrightarrow{\pi^{n+1}} \mathscr{F}(\overline{\Phi}) \longrightarrow 0$$

gives rise to an exact sequence

$$0 \longrightarrow \mathscr{F}(\Theta_n)/\pi^{n+1} \longrightarrow H^1(\Theta_n, \mathscr{F}_{\pi^{n+1}}) \longrightarrow H^1(\Theta_n, \mathscr{F}(\overline{\Phi}))_{\pi^{n+1}} \longrightarrow 0. \tag{4.1}$$

Since $\varprojlim_n \mathscr{F}(\Theta_n) = \{0\}$ (cf. [15]), we have $\varinjlim_n H^1(\Theta_n, \mathscr{F}(\overline{\Phi}))_{\pi^{n+1}} = \{0\}$ by the Tate duality. Hence (4.1) induces an isomorphism

$$\begin{aligned} \mathscr{F}(\Theta_\infty) \otimes_{\mathcal{O}} \Phi/\mathcal{O} &\cong H^1(\Theta_\infty, \mathscr{F}_{p^\infty}) \\ &\cong \mathrm{Hom}(\mathrm{Gal}(\overline{\Phi}/\Phi_\infty), \mathscr{F}_{p^\infty})^{\Delta} \cong \mathrm{Hom}_{\mathcal{O}}(U_\infty, \mathscr{F}_{p^\infty}), \end{aligned}$$

where the last isomorphism is given by local class field theory. In other words, we have the Kummer pairing

$$\langle\ ,\ \rangle : \mathscr{F}(\Theta_\infty) \otimes_{\mathcal{O}} \Phi/\mathcal{O} \ \times\ U_\infty^* \longrightarrow \Phi/\mathcal{O}.$$

Since $\varinjlim_n H^1(\Psi_n, \mathscr{F}(\overline{\Phi}))_{\pi^{n+1}} = \{0\}$, this pairing induces a non-degenerate pairing

$$\langle\ ,\ \rangle : \mathscr{F}(\Psi_\infty) \otimes_{\mathcal{O}} \Phi/\mathcal{O} \ \times\ V_\infty^* \longrightarrow \Phi/\mathcal{O}$$

(cf. [33, Prop. 5.4]).

Let λ be the formal logarithm of $\mathscr{F}$. For any character χ of G^-, define a map $\lambda_\chi : \mathscr{F}(\Psi_\infty) \to \Phi_\infty$ by

$$\lambda_\chi(y) := \frac{1}{p^n} \sum_{\gamma \in \mathrm{Gal}(\Psi_n/\Phi)} \chi^{-1}(\gamma)\lambda(y)^\gamma,$$

where n is any integer so that $y \in \mathscr{F}(\Psi_n)$ and the conductor of χ divides p^{n+1}. Then for a symbol $\epsilon = \pm$, define

$$A^\epsilon := \{y \in \mathscr{F}(\Psi_\infty) \mid \lambda_\chi(y) = 0 \quad \text{for all } \chi \in \Xi^\epsilon\}.$$

It is not difficult to see that

$$\mathscr{F}(\Psi_\infty) \otimes_{\mathcal{O}} \Phi/\mathcal{O} = A^+ \otimes_{\mathcal{O}} \Phi/\mathcal{O} + A^- \otimes_{\mathcal{O}} \Phi/\mathcal{O}, \qquad \mathrm{rank}_{\mathcal{O}} A^\pm = \infty \tag{4.2}$$

(cf. [33, Lem. 5.5]). The explicit reciprocity by Wiles computes the Kummer pairing as

$$\langle y \otimes \pi^{-n}, x \rangle = \frac{1}{\pi^{m+1+n}} \mathrm{Tr}_{\Phi_m/\Phi}(\delta_m(x)\lambda(y)) \in \Phi/\mathcal{O}$$

for $y \in \mathscr{F}(\Theta_n)$, $x \in U_\infty^*$ and a sufficiently large m for n. Then it is shown that the orthogonal complement of $A^\pm \otimes \Phi/\mathcal{O}$ with respect to the Kummer pairing is $V_\infty^{*,\pm}$. In other words, we have a non-degenerate Galois compatible pairing

$$\langle\ ,\ \rangle : A^\pm \otimes_{\mathcal{O}} \Phi/\mathcal{O}\ \times\ V_\infty^*/V_\infty^{*,\pm} \longrightarrow \Phi/\mathcal{O}.$$

Then (4.2) implies that $V_\infty^{*,+} \cap V_\infty^{*,-} = \{0\}$ and $\mathrm{rank}_\Lambda V_\infty^{*,\pm} \le 1$.

5. **Local points**

The main results are Theorems 5.5 and 5.8, while the decisive notion is Definition 5.4.

5.0.1. *The set-up.* Let $p \ge 5$ be a prime. As before, let $\mathscr{F}$ be the Lubin–Tate formal group over $\mathcal{O}$ with the parameter $-p$. We take an elliptic curve E defined over $\mathbb{Q}$ with good reduction at p with $a_p(E) = 0$. Such an E exists, for example, [9, Th. 14.18]. The formal group $\hat{E}$ is isomorphic to $\mathscr{F}$ over $\mathcal{O}$.

Consider a modular parametrization $\pi : X_0(N) \to E$ over $\mathbb{Q}$. (Just in this section, the letter π does *not* denote the uniformizer $-p$.) Changing E by isogeny if necessary, we may assume π is strong Weil and N is the conductor of E. The morphism π extends to a morphism between smooth models over $\mathbb{Z}_p$ by the Néron mapping property. We consider the reduction map $\overline{\pi} : X_0(N)_{\mathbb{F}_p} \to \overline{E}$ over $\mathbb{F}_p$ for $\overline{E}$ the reduction of E. This map is separable since the Manin constant is p-indivisible for the strong Weil parametrization.

We will use the following lemmas to choose a certain unramified point for $\overline{\pi}$, which corresponds to a supersingular elliptic curve with Frobenius trace $a_{p^2} = \pm 2p$.

LEMMA 5.1. *Let $q = p^2$ and $\overline{A}$ be an elliptic curve over $\mathbb{F}_q$ with*

$$a_q(\overline{A}) := 1 + q - \sharp\overline{A}(\mathbb{F}_q) = \pm 2p.$$

(i) *Any finite subgroup of $\overline{A}(\overline{\mathbb{F}}_q)$ is defined over $\mathbb{F}_q$.*
(ii) *Let A be an elliptic curve over $\mathcal{O}$ that is a lift of $\overline{A}$. Then the Honda type of the associated formal group $\hat{A}$ is $\pm x^2 + p$. In particular, $\hat{A}$ is Lubin–Tate with parameter $\mp p$.*

Proof.

(i) Let C be such a subgroup. Since $\overline{A}$ is supersingular, the order of C is prime to p. We may assume that C has order l^n for a prime $l \neq p$. Let φ_q be the q-th Frobenius. Then by assumption,

$$(\varphi_q \mp p)^2 = \varphi_q^2 - a_q(\overline{A})\varphi_q + q = 0$$

on $T_l(\overline{A})$. Hence $\varphi_q = \pm p$ on $T_l(\overline{A})$. In particular, C is fixed by φ_q, which is nothing but the Galois action of the Frobenius of $\mathbb{F}_q$.

(ii) By (i), we have $\varphi_q = \pm p$ as an endomorphism of $\overline{A}$. In particular, the q-th Frobenius action on the Dieudonné module of $\overline{A}$ is just multiplication by $\pm p$. The assertion follows from this. □

In the rest of the section we often identify $X(1)$ with $\mathbb{P}^1$ via the j-invariant.

LEMMA 5.2. (i) *The number of ramification points of $\overline{\pi}$ is bounded by*

$$2g_N - 2 \leq \frac{\mu}{6} = \frac{1}{6} N \prod_{l|N} (1 + l^{-1}),$$

where g_N is the genus of $X_0(N)$ and μ is the degree of the natural map $X_0(N) \to X(1)$.

(ii) *The number of supersingular points in $X_0(N)(\mathbb{F}_{p^2})$ that correspond to supersingular elliptic curves over $\mathbb{F}_{p^2}$ with the Frobenius trace $a_{p^2} = 2p$ or $-2p$ and the j-invariant different from 0 and 1728 is at least*

$$\mu\left(\lfloor\frac{p-1}{12}\rfloor - \frac{3}{2} + \left(\frac{-3}{p}\right) + \frac{1}{2}\left(\frac{-1}{p}\right)\right).$$

In particular, there is a supersingular point with $a_{p^2} = 2p$ or $-2p$ in $X_0(N)(\mathbb{F}_{p^2})$ over $X(1)(\mathbb{F}_{p^2}) \setminus \{0, 1728\}$ that is unramified for $\overline{\pi}$ if $p \equiv 1 \bmod 12$ or $p \geq 31$.

(iii) *If $p \equiv 2 \bmod 3$, there are at least $\mu/3$ supersingular points with $j = 0$. If $p \equiv 3 \bmod 4$, there are at least $\mu/2$ supersingular points with $j = 1728$. In particular, there is a supersingular point with $a_{p^2} = 2p$ or $-2p$ in $X_0(N)(\mathbb{F}_{p^2})$ that is unramified for $\overline{\pi}$.*

Remark 5.3. In view of Remark 2.3, to prove Rubin's conjecture, one may assume $p \equiv 1 \bmod 12$ or $p \geq 31$. Accordingly, the reader may skip Lemma 5.2(iii), which perhaps streamlines some of the following arguments.

Proof. (i): This just follows from the Riemann–Hurwitz formula and the genus formula of $X_0(N)$ (cf. [38, Prop. 1.40, 1.43]).

(ii), (iii): Recall that the supersingular points in $X(1)(\overline{\mathbb{F}}_p)$ are defined over $\mathbb{F}_{p^2}$. By the mass formula of Eichler and Deuring, the number of supersingular points in $X(1)(\overline{\mathbb{F}}_p)$ is $m+\delta+\epsilon$, where $m \in \mathbb{N} \cup \{0\}$ and $\epsilon, \delta \in \{0,1\}$ are uniquely determined by $p-1 = 12m + 4\delta + 6\epsilon$. Note that $\delta \neq 0$ (resp. $\epsilon \neq 0$) if and only if $j = 0$ (resp. $j = 1728$) is supersingular. More precisely, let $N(t)$ be the number of isomorphism classes of supersingular elliptic curves having exactly p^2+1-t points defined over $\mathbb{F}_{p^2}$. Then

$$N(t) = \begin{cases} \frac{1}{12}\left(p+6-4\left(\frac{-3}{p}\right)-3\left(\frac{-1}{p}\right)\right) & (t=\pm 2p), \\ 1-\left(\frac{-3}{p}\right) & (t=\pm p), \\ 1-\left(\frac{-1}{p}\right) & (t=0). \end{cases}$$

(See, for example, [37, Th. 4.6]. Over $\mathbb{F}_{p^2}$, one must count the number of twists.)

Recall that the morphism $Y_0(N)_{\mathbb{F}_p} \to Y(1)_{\mathbb{F}_p}$ is étale if $j \neq 0, 1728$. (Indeed, one may simply apply [21, Cor. 8.4.5] for the $\Gamma_1(N)$-problem.) Since p is relatively prime to 6, the ramification index of $\overline{\pi}$ at elliptic points is 2 or 3. So there are μ points in the fiber of each supersingular point in $X(1)$ except $j = 0, 1728$, and at least $\mu/3$ or $\mu/2$ points when $j = 0$ or 1728 respectively.

Let x be a supersingular point in $X(1)(\overline{\mathbb{F}}_p)$ represented by a supersingular elliptic curve $\overline{A}$ defined over $\mathbb{F}_{p^2}$ with $a_{p^2}(\overline{A}) = \pm 2p$. A point $y \in X_0(N)(\overline{\mathbb{F}}_p)$ in the fiber of x for the projection $X_0(N) \to X(1)$ corresponds to an isomorphism class over $\overline{\mathbb{F}}_p$ of a pair $(\overline{A}, C)$ with a cyclic subgroup C of order N of $\overline{A}$. By Lemma 5.1(i), the subgroup C is defined over $\mathbb{F}_{p^2}$. Hence $y \in X_0(N)(\mathbb{F}_{p^2})$.

If $\left(\frac{-3}{p}\right) = -1$ (resp. $\left(\frac{-1}{p}\right) = -1$), then $j = 0$ (resp. $j = 1728$) is supersingular. The supersigular elliptic curve $\overline{A}$ with $j = 0$ or 1728 can be defined over $\mathbb{F}_p$, thus, $t = -2p$ since $a_p(\overline{A}) = 0$. If

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) = 1,$$

any supersingular elliptic curve over $\mathbb{F}_{p^2}$ satisfies $t = \pm 2p$. The assertion follows from these facts. □

A formal CM point. Consider a supersingular point $\overline{P}$ of $X_0(N)(\mathbb{F}_{p^2})$ unramified for $\overline{\pi}$, represented by an elliptic curve $\overline{A}$ with $a_{p^2} = \pm 2p$ and a $\Gamma_0(N)$-level structure, which exists by Lemma 5.2(ii), (iii). By composing $\overline{\pi}$ with the

multiplication by $\sharp E(\mathbb{F}_{p^2})$, we may assume that $\overline{P}$ is sent to the origin $\overline{O}$ of $\overline{E}$. Note that since E is supersingular, $\sharp E(\mathbb{F}_{p^2})$ is prime to p and hence $\overline{P}$ is still an unramified point.

Fix a torsion point of $\overline{A}(\mathbb{F}_{p^2})$ of order M where M is taken so that the $\Gamma_1(M)$-moduli is fine and $\sharp\Gamma_0(M)/\Gamma_1(M)$ is prime to p. This is possible since $\sharp\overline{A}(\mathbb{F}_{p^2}) = (p \pm 1)^2$. Let $X_0(N; M)$ be the modular curve with $\Gamma_0(N)$ and $\Gamma_1(M)$-level structures. Unlike $X_0(N)$, it is a fine moduli space.

Let $\overline{P'}$ be a point of $X_0(N; M)(\mathbb{F}_{p^2})$ above $\overline{P}$ with the $\Gamma_1(M)$-level structure by the fixed torsion point of order M. We may assume that $\overline{P'}$ is unramified for $X_0(N; M) \to X_0(N)$. (If $j(\overline{A}) \neq 0, 1728$, this is evident. If $j(\overline{A}) = 0$, p must be 2 modulo 3. Then we pick $N = 27$ as there is no elliptic point of order 3 in $X_0(27)$. If $j(\overline{A}) = 1728$, we pick $N = 32$.) Hence the formal completion of the morphism $\pi' : X_0(N; M) \to E$ (on integral models) at the closed points $\overline{P'}$ and $\overline{O}$ is an isomorphism. Let $\mathfrak{m}$ be the maximal ideal of $\mathcal{O}$. Take a point

$$Q \in \hat{E}(\mathfrak{m}) \setminus p\hat{E}(\mathfrak{m}). \tag{5.1}$$

Then there is a point $P' \in X_0(N; M)(\mathcal{O})$ over $\overline{P}'$ sent to Q by π. As $X_0(N; M)$ is a fine moduli space, there exists an elliptic curve A defined over $\mathcal{O}$ that represents P' by the moduli interpretation. The formal group $\hat{A}$ is Lubin–Tate by Lemma 5.1(ii). In particular, A is a formal CM elliptic curve. (It is called fake CM in [8, §3].) Let P be the image of P' in $X_0(N)$.

5.0.2. *An optimal system of local points.* Now we resort to Gross' theory of quasi-canonical lifts [14], [42] (the latter for non-algebraically closed residue field).

Since $\hat{A}$ is Lubin–Tate, the Tate module $T := T_pA$ is a free $\mathcal{O}$-module of rank 1. Put $V = T \otimes_{\mathcal{O}} \Phi$, and consider $\mathbb{Z}_p$-modules $T \subset T' \subset V$ such that T'/T is finite. We regard

$$C := T'/T \subset V/T = \hat{A}[p^\infty] = A[p^\infty].$$

Let Ψ' be the fixed field of the $\mathrm{Gal}(\overline{\Phi}/\Phi)$-action on C. Consider $A' = A/C$ as an abelian scheme defined over $\mathcal{O}'$, the integer ring of Ψ'. Then $\mathrm{End}(\hat{A}')$ is isomorphic to $\mathcal{O}$ or an order $\mathbb{Z}_p + p^s\mathcal{O}$ for a natural number s (cf. [14, p. 325]).

If we take a basis t of the $\mathcal{O}$-module T and put $T_s = p^{-s}\mathbb{Z}_p t + T$ as T', then $\mathrm{End}(\hat{A}') \cong \mathbb{Z}_p + p^s\mathcal{O}$. Following Gross, we call this A' a *quasi-canonical* lift of conductor p^s of $\overline{A}$ with respect to A (cf. [14, p. 325], [42, §4]). Denote A' by A_s and Ψ' by Ψ'_s for this choice. It is known that

$$\mathrm{Gal}(\Psi'_s/\Phi) \cong (\mathcal{O}/p^s\mathcal{O})^\times/(\mathbb{Z}/p^s\mathbb{Z})^\times$$

(cf. [14, Prop. 5.3], [42, Th. 1]). In particular, it is the local ring class field of degree $[\Phi'_s : \Phi] = p^{s-1}(p + 1)$. Let Ψ'_∞ be $\cup_s \Psi'_s$. Then $\mathrm{Gal}(\Psi'_\infty/\Phi) \cong$

$\mathbb{Z}_p \times \mathbb{Z}/(p+1)\mathbb{Z}$. Let Δ' be the torsion subgroup of $\mathrm{Gal}(\Psi'_\infty/\Phi)$. The field Ψ'_∞ contains the anticyclotomic $\mathbb{Z}_p$-extension Ψ_∞. The s-th layer Ψ_s of Ψ_∞ lies in Ψ'_{s+1}. Let $\mathrm{Tr}_{s+1/s} : \Psi_{s+1} \to \Psi_s$ denote the trace map. Then elliptic curve $A_s/\mathcal{O}_{\Psi'_s}$ and the canonical level structure induced from that of A define a point $z_s \in X_0(N)(\mathcal{O}_{\Psi'_s})$. Let x_s be the image of z_s by the modular parametrization π.

Definition 5.4. Let

$$y_s = \sum_{\sigma \in \Delta'} \sigma x_{s+1} \in \hat{E}(\mathfrak{m}_{\Psi_s}) \quad \text{and} \quad y = (p+1)Q \in \hat{E}(\mathfrak{m})$$

be a system of local points.

The salient features are the following:

THEOREM 5.5.

(i) $y \in \hat{E}(\mathfrak{m}) \setminus p\hat{E}(\mathfrak{m})$.

(ii) *The elements* $y_s \in \hat{E}(\mathfrak{m}_{\Psi_s})$ *satisfy*

$$\mathrm{Tr}_{s+1/s} y_{s+1} = -y_{s-1}$$

for $s \geq 1$ *and*

$$\mathrm{Tr}_{1/0} y_1 = -y \quad \textit{and} \quad y_0 = 0.$$

Proof. (i) just follows from our choice (5.1).

(ii) We consider the action of the Hecke operator T_p on x_s.

Let T' be a lattice containing $T_s = \frac{1}{p^s}\mathbb{Z}_p t + T$ with index p. First suppose that $s \geq 1$. There are two types of T':

$$\frac{1+ap^s}{p^{s+1}}\mathbb{Z}_p t + T \text{ for } a \in \{0, 1, \ldots, p-1\} \quad \text{or} \quad \frac{1}{p^s}\mathbb{Z}_p t + \frac{1}{p}T.$$

The first type is permuted by the action of $\mathrm{Gal}(\Psi'_{s+1}/\Psi'_s)$. So each lattice of this type is of the form σx_s with $\sigma \in \mathrm{Gal}(\Psi'_{s+1}/\Psi'_s)$. Note that each lattice of the second type is homothetic to the lattice $\frac{1}{p^{s-1}}\mathbb{Z}_p t + T$. Hence for $s \geq 1$, we have

$$T_p x_s = \sum_\sigma \sigma x_{s+1} + x_{s-1}.$$

Since T_p acts as $a_p(E) = 0$ on E, we have the desired relation. When $s = 0$, there exist $p+1$ lattices containing T with index p, which are permuted by Δ. Hence $T_p x = \sum_{\sigma \in \Delta} \sigma x_1$. The assertion follows. □

COROLLARY 5.6. *We have*

$$(A^- \otimes_{\mathcal{O}} \Phi/\mathcal{O})^{G^-} = \mathscr{F}(\Phi) \otimes_{\mathcal{O}} \Phi/\mathcal{O}.$$

In particular, $V_\infty/V_\infty^{*,-}$ *and* $V_\infty^{*,-}$ *are free* Λ*-modules of rank* 1.

Proof. The first assertion follows from Theorem 5.5 and [33, Prop. 7.4]. Strictly speaking, y in [33, Prop. 7.4] is a Heegner point but can be replaced by our y since this proposition is proved by using [33, Prop. 6.1], which corresponds to our Theorem 5.5.

Then by the Kummer duality and Nakayama's lemma, $V_\infty^*/V_\infty^{*,-}$ is generated as a Λ-module by a single element. Hence it is a free module of rank 1 or a torsion module. However, since $\mathrm{rank}_\Lambda(V_\infty^*/V_\infty^{*,-}) \geq 1$, the latter case does not happen. Since $\mathrm{rank}_\Lambda V_\infty^* = 2$ and Λ is a UFD, it is straightforward to show that the freeness of $V_\infty^*/V_\infty^{*,-}$ implies the freeness of $V_\infty^{*,-}$ (cf. [33, Lem. 4.1]). □

Remark 5.7. Since we employ a modular parametrization, the above construction is not purely local. In light of (potential) links with a generalization of the theory of (φ,Γ)-modules, a very interesting problem is to construct the optimal system of local points by a purely local method.

5.0.3. *Rubin's conjecture.*

THEOREM 5.8. *We have* $V_\infty^* = V_\infty^{*,+} \oplus V_\infty^{*,-}$.

Proof. We just recall Rubin's argument (cf. [33, Th. 8.4]).

Consider the Coates–Wiles derivative $\delta : V_\infty^*/V_\infty^{*,-} \to \mathcal{O}$. By Theorem 3.4, there exists an element $\xi \in V_\infty^{*,+}$ such that $\delta(\xi) \in \mathcal{O}^\times$. By Corollary 5.6, we may identify $V_\infty^*/V_\infty^{*,-}$ and Λ. Then the image of the maximal ideal of Λ by δ is in $p\mathcal{O}$. Therefore, ξ does not belong to the maximal ideal, and hence, it generates $V_\infty^*/V_\infty^{*,-}$. Thus, $V_\infty^* = V_\infty^{*,+} \oplus V_\infty^{*,-}$. □

6. **Arithmetic consequences**

In this section we first present consequences of Rubin's conjecture as in [1] and [33].[3] Then Section 6.0.3 concerns the underlying p-adic Birch and Swinnerton-Dyer conjecture.

Let K be an imaginary quadratic field where p remains to be a prime, and let H be the Hilbert class field of K. We assume that

$$p \nmid h_K. \tag{6.1}$$

Let φ and E be as in Section 3: φ is a Hecke character over K with infinity type $(1,0)$, and E is a $\mathbb{Q}$-curve in the sense of Gross such that the Hecke character $\varphi \circ N_{H/K}$ is associated to E, and E has good reduction at each prime of H above p. Then, $E \in \mathscr{E}$ in the notation of [33, §3], and in particular, E satisfies the Shimura condition. Let $\mathfrak{p}$ be the prime of H above p that is

[3] Unfortunately, the sign conventions in [1] and [33] are different. In [33] the parity is based on the conductor of characters, but in [1] it is based on the order of characters (cf. [1, Rem. 3.2]). Our conventions are consistent with [33].

compatible with the fixed embedding $\iota_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. We fix a Weierstrass model of E over $H \cap \mathcal{O}$ that is smooth at $\mathfrak{p}$, and by considering a Galois conjugate of E over H if necessary, we may assume that there exists a complex period $\Omega \in \mathbb{C}^\times$ of E such that $L = \mathcal{O}_K\Omega$, where L is the period lattice associated to the model.

6.0.1. *Rubin's p-adic L-function.* As in [32] or Proposition 3.3, there exists an elliptic unit $\xi = \xi(E, \Omega) \in U_\infty^*$ such that

$$\delta(\xi) = \frac{L(\overline{\varphi}, 1)}{\Omega}$$

and for a non-trivial character χ of $\mathrm{Gal}(\Phi_\infty/\Phi_0)$ of finite order,

$$\delta_\chi(\xi) = \frac{L(\overline{\varphi}\chi, 1)}{\Omega}.$$

Here we identify $\mathrm{Gal}(\Phi_\infty/\Phi_0)$ with the Galois group of the $\mathbb{Z}_p^2$-extension of K (cf. (6.1)) and correct a minor sign error in [33, Th. 3.2] (cf. our modified definition of $(v_n)_n$ and δ_χ in Section 2).

Let $\epsilon \in \{+, -\}$ be the sign of the functional equation of the Hecke L-function $L(\varphi, s)$. Then it is known that the projection of $\xi(E, \Omega)$ on V_∞^* belongs to $V_\infty^{*,\epsilon}$ (cf. [33, Cor. 3.3]) Let $\mathscr{C}_\infty$ be the free Λ-submodule of $V_\infty^{*,\epsilon}$ generated by $\xi(E, \Omega) \in V_\infty^{*,\epsilon}$. We take a generator v_ϵ of the Λ-module $V_\infty^{*,\epsilon}$ and write

$$\xi(E, \Omega) = \mathscr{L}_p(\varphi, \Omega, v_\epsilon) \cdot v_\epsilon$$

for an element $\mathscr{L}_p(\varphi, \Omega, v_\epsilon) \in \Lambda$. We call it *Rubin's p-adic L-function* associated to φ. We sometimes omit the indices of $\mathscr{L}_p(\varphi, \Omega, v_\epsilon)$ and write its evaluation at an anticyclotomic character χ by $\mathscr{L}_p(\chi)$ for simplicity.

The interpolation property of Rubin's p-adic L-function is

$$\mathscr{L}_p(\chi) = \frac{1}{\delta_{\chi^{-1}}(v_\epsilon)} \cdot \frac{L(\overline{\varphi\chi}, 1)}{\Omega}$$

for non-trivial $\chi \in \Xi^\epsilon$. Here we utilize [33, Lem. 2.1 (iii)] (note we consider U_∞^* instead of U_∞) and $\delta_\chi(v_\epsilon) \neq 0$, which is a consequence of Rubin's conjecture (cf. Corollary 2.2). In particular, for $\chi \in \Xi^\epsilon$, $\mathscr{L}_p(\chi) \neq 0$ if and only if $L(\overline{\varphi\chi}, 1) \neq 0$.

6.0.2. *An Iwasawa main conjecture.* Now we present the results of [1].

Let K_∞ be the anticyclotomic $\mathbb{Z}_p$-extension of K. We identify G^- with $\mathrm{Gal}(K_\infty/K)$ and put $G_K := \mathrm{Gal}(\overline{\mathbb{Q}}/K)$. Let $\mathcal{R}$ be the ring of integers in a finite extension of Φ containing the image of the p-adic avatar $G_K \to \overline{\mathbb{Q}}_p^\times$ of φ. Let T be the free $\mathcal{R}$-module of rank one on which G_K acts by the p-adic avatar. We put $W = T \otimes_{\mathcal{O}} \Phi/\mathcal{O}$.

For simplicity, let p still denote the prime of the n-th layer K_n above p. We note that the completion $K_{n,p}$ at p coincides with Ψ_n and that $W \cong$

$\mathscr{F}[\pi^\infty] \otimes_{\mathcal{O}} \mathcal{R}$ as an $\mathcal{R}[\mathrm{Gal}(\overline{\mathbb{Q}}_p/\Phi)]$-module (cf. (6.1)). We define

$$H^1_\pm(K_{n,p}, W) \subseteq H^1(K_{n,p}, W) \cong H^1(\Psi_n, \mathscr{F}[\pi^\infty]) \otimes \mathcal{R}$$

to be the Kummer image of $\mathscr{F}^\pm(\Psi_n) \otimes \mathcal{R} \otimes \mathbb{Q}_p/\mathbb{Z}_p$, where

$$\mathscr{F}^\pm(\Psi_n) := \{y \in \mathscr{F}(\Psi_n) \mid \lambda_\chi(y) = 0 \text{ for all } \chi \in \Xi^\pm \text{ factoring through } \mathrm{Gal}(\Psi_n/\Psi)\}.$$

Note that $H^1_\pm(K_{n,p}, W)$ is independent of the choice of isomorphism $W \cong \mathscr{F}[\pi^\infty] \otimes \mathcal{R}$. The signed Selmer groups $\mathrm{Sel}_\pm(K_n, W)$ are defined by

$$\mathrm{Sel}_\pm(K_n, W) = \ker\left\{H^1(K_n, W) \to \frac{H^1(K_{n,p}, W)}{H^1_\pm(K_{n,p}, W)} \times \prod_{v \nmid p} H^1(K_{n,v}, W)\right\},$$

where v varies over the primes of K_n relatively prime to p. Note that for $v \nmid p$, since $H^1(K_{n,v}, T \otimes \mathbb{Q}_p) = \{0\}$ (cf. [2, Prop. 2.10]), the usual local condition $H^1_{\mathrm{f}}(K_{n,v}, W)$ coincides with $\{0\}$.

Let $\mathscr{X}^\pm_\infty$ be the Pontryagin dual of the signed Selmer group

$$\varinjlim_n \mathrm{Sel}_\pm(K_n, W).$$

In [1, Th. 3.6] it is shown that $\mathscr{X}^{-\epsilon}_\infty$ is a finitely generated torsion Λ-module. (Although in op. cit. E is defined over $\mathbb{Q}$ and hence the class number of K is assumed to be equal to one, by a similar argument one can prove the same assertion, where we assume only (6.1). Note again that our sign convention is opposite to that in op. cit.)

Finally, an Iwasawa main conjecture:

THEOREM 6.1. *The characteristic ideal of $\mathscr{X}^{-\epsilon}_\infty$ is generated by Rubin's p-adic L-function $\mathscr{L}_p(\varphi, \Omega, v_\epsilon)$.*

Proof. This is proved in [1] assuming Rubin's conjecture (cf. the paragraph after [op. cit., Th. 4.3]). Although in op. cit. E is defined over $\mathbb{Q}$, by a similar argument one can prove [op. cit., (4.2) and Th. 4.3] to deduce the theorem, where we assume only (6.1). □

6.0.3. *Towards a p-adic Birch and Swinnerton-Dyer conjecture.*

THEOREM 6.2. *Suppose that E is defined over K. Let χ be an anticyclotomic character of conductor p^n. Then we have*

$$\mathrm{rank}\, E(K_n)^\chi \leq \dim \mathrm{Sel}(K_n, V_pE)^\chi \leq \begin{cases} \mathrm{ord}_\chi \mathscr{L}_p & (\chi \in \Xi^\epsilon), \\ \mathrm{ord}_\chi \mathscr{L}_p + 1 & (\chi \in \Xi^{-\epsilon}). \end{cases}$$

Proof. The characteristic ideal of $\mathscr{X}^{-\epsilon}_\infty$ is contained in that of the strict Selmer group $\mathscr{X}^{\mathrm{str}}_\infty$. (The latter appears in [1], the notation being X_{str}, and the definition is as in [op. cit., pp. 613, 615].) Since the control theorem holds

for the strict Selmer group (cf. [36, Prop. 7.3.4]), standard arguments show that

$$\mathrm{ord}_\chi \mathscr{L}_p \geq \dim \mathrm{Sel}_{\mathrm{str}}(K_n, V_pE)^\chi \geq \dim \mathrm{Sel}(K_n, V_pE)^\chi - 1$$

(cf. Theorem 6.1).

Suppose $\chi \in \Xi^\epsilon$. Then we may consider the control theorem for $\mathscr{X}_\infty^{-\epsilon}$ at χ (cf. [1, Th. 5.2]). Hence by [1, Prop. 5.3],

$$\mathrm{ord}_\chi \mathscr{L}_p \geq \dim \mathrm{Sel}_{-\epsilon}(K_n, V_pE)^\chi = \dim \mathrm{Sel}(K_n, V_pE)^\chi. \qquad \square$$

Remark 6.3. In [5] we prove the rank part of the p-adic Birch and Swinnerton-Dyer conjecture (i.e., the equality in the above) if $\mathrm{ord}_{s=1} L(\varphi\chi, s) \leq 1$. Moreover, if $\mathrm{ord}_{s=1} L(\varphi, s) \leq 1$, the full p-adic Birch and Swinnerton-Dyer conjecture for φ is proven up to a p-adic unit.

References

[1] A. Agboola and B. Howard, Anticyclotomic Iwasawa theory of CM elliptic curves. II, *Math. Res. Lett.* **12** no. 5-6 (2005), 611–621. MR 2189225. Zbl 1130.11058. https://doi.org/10.4310/MRL.2005.v12.n5.a1.

[2] T. Arnold, Anticyclotomic main conjectures for CM modular forms, *J. Reine Angew. Math.* **606** (2007), 41–78. MR 2337641. Zbl 1138.11047. https://doi.org/10.1515/CRELLE.2007.034.

[3] M. Bertolini, H. Darmon, and K. Prasanna, Generalized Heegner cycles and p-adic Rankin L-series, *Duke Math. J.* **162** no. 6 (2013), 1033–1148, with an appendix by Brian Conrad. MR 3053566. Zbl 1302.11043. https://doi.org/10.1215/00127094-2142056.

[4] A. A. Burungale, S. Kobayashi, and K. Ota, A local invariant of Rubin and p-divisibility of anticyclotomic Hecke L-values at inert primes, in preparation.

[5] A. A. Burungale, S. Kobayashi, and K. Ota, p-adic L-functions and rational points on CM elliptic curves at inert primes, preprint.

[6] A. A. Burungale, S. Kobayashi, K. Ota, and S. Yasuda, Kato's ε-conjecture for anticyclotomic CM deformations at inert primes, in preparation.

[7] A. A. Burungale and Y. Tian, p-converse to a theorem of Gross-Zagier, Kolyvagin and Rubin, *Invent. Math.* **220** no. 1 (2020), 211–253. MR 4071412. Zbl 1452.11068. https://doi.org/10.1007/s00222-019-00929-7.

[8] R. Coleman and K. McMurdy, Fake CM and the stable model of $X_0(Np^3)$, *Doc. Math.* no. Extra Vol. (2006), 261–300. MR 2290590. Zbl 1155.11030.

[9] D. A. Cox, *Primes of the Form $x^2 + ny^2$. Fermat, Class Field Theory and Complex Multiplication*, *A Wiley-Interscience Publication*, John Wiley & Sons, Inc., New York, 1989. MR 1028322. Zbl 0701.11001.

[10] T. Finis, Divisibility of anticyclotomic L-functions and theta functions with complex multiplication, *Ann. of Math.* (2) **163** no. 3 (2006), 767–807. MR 2215134. Zbl 1111.11047. https://doi.org/10.4007/annals.2006.163.767.

[11] R. Greenberg, On the Birch and Swinnerton-Dyer conjecture, *Invent. Math.* **72** no. 2 (1983), 241–265. MR 0700770. Zbl 0546.14015. https://doi.org/10.1007/BF01389322.

[12] R. Greenberg, Iwasawa theory and p-adic deformations of motives, in *Motives* (*Seattle*, *WA*, 1991), *Proc. Sympos. Pure Math.* **55**, Amer. Math. Soc., Providence, RI, 1994, pp. 193–223. MR 1265554. Zbl 0819.11046. https://doi.org/10.1090/pspum/055.2/1265554.

[13] R. Greenberg, Introduction to Iwasawa theory for elliptic curves, in *Arithmetic algebraic geometry* (*Park City*, *UT*, 1999), *IAS/Park City Math. Ser.* **9**, Amer. Math. Soc., Providence, RI, 2001, pp. 407–464. MR 1860044. Zbl 1002.11048. https://doi.org/10.1090/pcms/009/06.

[14] B. H. Gross, On canonical and quasi-canonical liftings, *Invent. Math.* **84** no. 2 (1986), 321–326. MR 0833193. Zbl 0597.14044. https://doi.org/10.1007/BF01388810.

[15] M. Hazewinkel, On norm maps for one dimensional formal groups. III, *Duke Math. J.* **44** no. 2 (1977), 305–314. MR 0439851. Zbl 0371.14024. https://doi.org/10.1215/S0012-7094-77-04412-X.

[16] N. Jochnowitz, Congruences between modular forms of half integral weights and implications for class numbers and elliptic curves, preprint.

[17] K. Kato, Lectures on the approach to Iwasawa theory for Hasse-Weil L-functions via B_{dR}. I, in *Arithmetic Algebraic Geometry* (Trento, 1991), *Lecture Notes in Math.* **1553**, Springer, Berlin, 1993, pp. 50–163. MR 1338860. Zbl 0815.11051. https://doi.org/10.1007/BFb0084729.

[18] K. Kato, p-adic Hodge theory and values of zeta functions of modular forms, in *Cohomologies p-adiques et Applications Arithmétiques. III*, *Astérisque* **295**, Math. Soc. France, Paris, 2004, pp. ix, 117–290. MR 2104361. Zbl 1142.11336. Available at http://www.numdam.org/item/AST_2004__295__117_0/.

[19] N. M. Katz, p-adic L-functions, Serre-Tate local moduli, and ratios of solutions of differential equations, in *Proceedings of the International Congress of Mathematicians. Volume* 1 (Helsinki, 1978), Acad. Sci. Fennica, Helsinki, 1980, pp. 365–371. MR 0562628. Zbl 0439.12010. Available at https://www.mathunion.org/fileadmin/ICM/Proceedings/ICM1978.1/ICM1978.1.ocr.pdf.

[20] N. M. Katz, Divisibilities, congruences, and Cartier duality, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **28** no. 3 (1981), 667–678 (1982). MR 0656042. Zbl 0559.14032.

[21] N. M. Katz and B. Mazur, *Arithmetic Moduli of Elliptic Curves*, *Ann. of Math. Stud.* **108**, Princeton Univ. Press, Princeton, NJ, 1985. MR 0772569. Zbl 0576.14026. https://doi.org/10.1515/9781400881710.

[22] S.-i. Kobayashi, Iwasawa theory for elliptic curves at supersingular primes, *Invent. Math.* **152** no. 1 (2003), 1–36. MR 1965358. Zbl 1047.11105. https://doi.org/10.1007/s00222-002-0265-4.

[23] M. Kurihara, On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction. I, *Invent. Math.* **149** no. 1 (2002), 195–224. MR 1914621. Zbl 1033.11028. https://doi.org/10.1007/s002220100206.

[24] B. Mazur, Modular curves and arithmetic, in *Proceedings of the International Congress of Mathematicians*, *Vol.* 1, 2 (Warsaw, 1983), PWN, Warsaw, 1984, pp. 185–211. MR 0804682. Zbl 0597.14023.

[25] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, third ed., *Springer Monogr. Math.*, Springer-Verlag, Berlin, 2004. MR 2078267. Zbl 1159.11039. https://doi.org/10.1007/978-3-662-07001-7.

[26] A. G. Nasybullin, Elliptic curves with supersingular reduction over Γ-extensions, *Uspehi Mat. Nauk* **32** no. 2(194) (1977), 221–222. MR 0472830. Zbl 0366.14004. Available at http://mi.mathnet.ru/eng/umn/v32/i2/p221.

[27] B. Perrin-Riou, Théorie d'Iwasawa des représentations p-adiques sur un corps local, *Invent. Math.* **115** no. 1 (1994), 81–161, with an appendix by Jean-Marc Fontaine. MR 1248080. Zbl 0838.11071. https://doi.org/10.1007/BF01231755.

[28] B. Perrin-Riou, *Fonctions L p-adiques des Représentations p-adiques*, *Astérisque* **229**, Math. Soc. France, Paris, 1995. MR 1327803. Zbl 0845.11040.

[29] B. Perrin-Riou, Arithmétique des courbes elliptiques à réduction supersingulière en p, *Experiment. Math.* **12** no. 2 (2003), 155–186. MR 2016704. Zbl 1061.11031. https://doi.org/10.1080/10586458.2003.10504490.

[30] R. Pollack, On the p-adic L-function of a modular form at a supersingular prime, *Duke Math. J.* **118** no. 3 (2003), 523–558. MR 1983040. Zbl 1074.11061. https://doi.org/10.1215/S0012-7094-03-11835-9.

[31] D. E. Rohrlich, Root numbers of Hecke L-functions of CM fields, *Amer. J. Math.* **104** no. 3 (1982), 517–543. MR 0658544. Zbl 0503.12008. https://doi.org/10.2307/2374152.

[32] K. Rubin, Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer, *Invent. Math.* **64** no. 3 (1981), 455–470. MR 0632985. Zbl 0506.14039. https://doi.org/10.1007/BF01389277.

[33] K. Rubin, Local units, elliptic units, Heegner points and elliptic curves, *Invent. Math.* **88** no. 2 (1987), 405–422. MR 0880958. Zbl 0623.14006. https://doi.org/10.1007/BF01388915.

[34] K. Rubin, The "main conjectures" of Iwasawa theory for imaginary quadratic fields, *Invent. Math.* **103** no. 1 (1991), 25–68. MR 1079839. Zbl 0737.11030. https://doi.org/10.1007/BF01239508.

[35] K. Rubin, p-adic L-functions and rational points on elliptic curves with complex multiplication, *Invent. Math.* **107** no. 2 (1992), 323–350. MR 1144427. Zbl 0770.11033. https://doi.org/10.1007/BF01231893.

[36] K. Rubin, *Euler Systems*, *Ann. of Math. Stud.* **147**, Princeton Univ. Press, Princeton, NJ, 2000, Hermann Weyl Lectures. The Institute for Advanced Study. MR 1749177. Zbl 0977.11001. https://doi.org/10.1515/9781400865208.

[37] R. Schoof, Nonsingular plane cubic curves over finite fields, *J. Combin. Theory Ser. A* **46** no. 2 (1987), 183–211. MR 0914657. Zbl 0632.14021. https://doi.org/10.1016/0097-3165(87)90003-3.

[38] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, *Publ. Math. Soc. Japan* **11**, Princeton Univ. Press, Princeton, NJ, 1994, reprint of the 1971 original, Kanô Memorial Lectures, 1. MR 1291394. Zbl 0872.11023.

[39] C. Skinner, A converse to a theorem of Gross, Zagier, and Kolyvagin, *Ann. of Math.* (2) **191** no. 2 (2020), 329–354. MR 4076627. Zbl 1447.11071. https://doi.org/10.4007/annals.2020.191.2.1.

[40] T. Tsuji, Explicit reciprocity law and formal moduli for Lubin-Tate formal groups, *J. Reine Angew. Math.* **569** (2004), 103–173. MR 2055715. Zbl 1055.14047. https://doi.org/10.1515/crll.2004.022.

[41] T. Yang, On CM abelian varieties over imaginary quadratic fields, *Math. Ann.* **329** no. 1 (2004), 87–117. MR 2052870. Zbl 1088.11048. https://doi.org/10.1007/s00208-004-0511-8.

[42] J.-K. Yu, On the moduli of quasi-canonical liftings, *Compositio Math.* **96** no. 3 (1995), 293–321. MR 1327148. Zbl 0866.14029. Available at http://www.numdam.org/item?id=CM_1995__96_3_293_0.

[43] W. Zhang, Selmer groups and the indivisibility of Heegner points, *Camb. J. Math.* **2** no. 2 (2014), 191–253. MR 3295917. Zbl 1390.11091. https://doi.org/10.4310/CJM.2014.v2.n2.a2.

(Received: April 1, 2021)
(Revised: July 6, 2021)

California Institute of Technology, Pasadena, CA and
The University of Texas at Austin, Austin, TX
E-mail: ashayburungale@gmail.com

Kyushu University, Fukuoka, Japan
E-mail: kobayashi@math.kyushu-u.ac.jp

Graduate School of Science, Osaka University, Toyonaka, Osaka, Japan
E-mail: kazutoota@math.sci.osaka-u.ac.jp