RUBIN'S CONJECTURE ON LOCAL UNITS IN THE ANTICYCLOTOMIC TOWER AT INERT PRIMES: $p = 3$ CASE

XIAOJUN YAN AND XIUWU ZHU

Abstract. We prove Rubin's conjecture on the structure of local units in the anticyclotomic $\mathbb{Z}_p$-extension of unramified quadratic extension of $\mathbb{Q}_p$ in $p = 3$ case by extending Burungale-Kobayashi-Ota's work.

Contents

1. Introduction

1.1. **Background.** Iwasawa theory is a basic tool to study the growth of the Mordell-Weil rank of elliptic curves in a tower of number fields and its relation to special L-value. For an elliptic curve E over $\mathbb{Q}$ with complex multiplication by an imaginary quadratic field K, 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. If p splits in K, then this module is torsion, and its characteristic ideal is generated by the two-variable Katz p-adic L-function attached to E (cf. [18]). However, if p inerts in K, this module is non-torsion, since the rank of the module of local units is twice that of the module of elliptic units.

Let Λ be the Iwasawa algebra for the anticyclotomic $\mathbb{Z}_p$-extension of an unramified quadratic extension of $\mathbb{Q}_p$. Rubin considered the Λ-module V, the anticyclotomic projection of local units of $\mathbb{Z}_p^2$-extension of K, and defined two rank 1 free submodules $V^{\pm}$. He conjectured (cf. [13]) that

$$V = V^+ \oplus V^-.$$

The projection of every elliptic unit lies in V^{ϵ}, where ϵ is the sign of $L(E/\mathbb{Q}, s)$. Under the conjecture, Rubin constructed a p-adic L-function, which generates the quotient of V^{ϵ} by the image of elliptic units. Moreover, Agboola-Howard [1] formulated and proved an Iwasawa main conjecture that involves Rubin's p-adic L-function under Rubin's conjecture.

Rubin proposed a criterion under which the conjecture is true in the case $p \geq 5$. His criterion involves the existence of following global objects:

Date: July 13, 2025.

(R1) a CM elliptic curve with good supersingular reduction at p whose central L-value is p-indivisible,
(R2) a Heegner point over imaginary quadratic fields with p inert which is locally p-indivisible.

He proved that there are primes p with density 1 at which (R1) exists. In [3], using the results of [7], Burungale-Kobayashi-Ota verified the existence of a modified (R1) for primes $p > 3$. For (R2), Rubin verified that it exists for $5 \le p \le 1000$ and $p \not\equiv 1 \pmod{12}$ by using the computation of Stephen (unpublished, but similar to [2]). However, in general, it is difficult to verify the local p-indivisibility of Heegner points. Burungale-Kobayashi-Ota consider formal CM points and the modular parametrization of elliptic curves instead of Heegner points. They constructed such formal CM points when $p > 3$, and proved Rubin's conjecture in the case $p > 3$.

In this paper, we prove Rubin's conjecture for the case $p = 3$ by constructing special formal CM points in this case following Burungale-Kobayashi-Ota's approach. As an application, we complete the proof of Agboola-Howard's main conjecture when $p = 3$. The result has various potential applications such as extending the p-adic Waldspurger formula presented in [5] to the prime $p = 3$, [6] on Kato's epsilon-conjecture and [4] on vanishing of μ-invariants on Rubin's p-adic L-function.

In the case $p = 3$, we remark that Rubin's criterion also works and it may be verified by some computational methods.

1.2. **Statement.** Let p be a prime. Let Φ be the unramified quadratic extension of $\mathbb{Q}_p$ and $\mathcal{O}$ be its ring of integers. Let $\mathcal{F}_{/\mathcal{O}}$ be a Lubin-Tate formal group with parameter $\pi := -p$. Let $\Phi_n = \Phi(\mathcal{F}[\pi^{n+1}])$ for $0 \le n \le \infty$. Then we have an isomorphism $\kappa : \mathrm{Gal}(\Phi_\infty/\Phi) \xrightarrow{\sim} \mathcal{O}^\times$, $\sigma \mapsto \kappa(\sigma)$ where $\sigma(v) = [\kappa(\sigma)^{-1}](v)$ for all $v \in \mathcal{F}[\pi^\infty]$. Let Δ be the torsion subgroup of $\mathrm{Gal}(\Phi_\infty/\Phi)$. Let $\Theta_n = \Phi_n^\Delta$ for all $n \le \infty$.

1.2.1. *Coleman power series and Coates-Wiles homomorphism.* For a finite extension F of $\mathbb{Q}_p$, we denote $U(F)$ its group of local principal units. Define

$$U_\infty = \left(\varprojlim (U(\Phi_n) \otimes_{\mathbb{Z}_p} \mathcal{O})\right)^{\kappa|_\Delta}, \quad U_\infty^* = U_\infty \otimes_{\mathcal{O}} T_\pi \mathcal{F}^{\otimes -1} = \mathrm{Hom}_{\mathcal{O}}(T_\pi\mathcal{F}, U_\infty),$$

where $T_\pi\mathcal{F} = \varprojlim \mathcal{F}[\pi^{n+1}]$ is the π-adic Tate module of $\mathcal{F}$. Wintenberger showed that U_∞^* is a rank 2 free $\mathcal{O}[[\mathrm{Gal}(\Phi_\infty/\Phi_0)]]$-module (cf. [17]).

Consider the Coates-Wiles logarithmic derivatives

$$\delta : U_\infty^* \to \mathcal{O}, \quad x = u \otimes a \otimes v^{\otimes -1} \mapsto a \cdot \frac{f'(0)}{f(0)},$$

and

$$\delta_n : U_\infty^* \to \Phi_n, \quad x = u \otimes a \otimes v^{\otimes -1} \mapsto \frac{a}{\lambda'(v_n)} \cdot \frac{f'(v_n)}{f(v_n)},$$

where $u = (u_n)_n \in \varprojlim U(\Phi_n)$, $a \in \mathcal{O}$, $v = (v_n)_n \in T_\pi\mathcal{F}$ is a generator as $\mathcal{O}$-module, $f \in \mathcal{O}[[X]]^\times$ is the Coleman power series such that $f(v_n) = u_n$ and λ is the formal logarithm of $\mathcal{F}$ normalized by $\lambda'(0) = 1$.

For a finite character $\chi : \mathrm{Gal}(\Phi_\infty/\Phi) \to \overline{\mathbb{Q}}_p^\times$ which factor through $\mathrm{Gal}(\Phi_n/\Phi)$, we define

$$\delta_\chi : U_\infty^* \to \overline{\mathbb{Q}}_p, \quad x \mapsto \frac{1}{\pi^{n+1}} \sum_{\gamma \in \mathrm{Gal}(\Phi_n/\Phi)} \chi(\gamma)\delta_n(x)^\gamma.$$

It is independent of the choice of n. For $\sigma \in \mathrm{Gal}(\Phi_\infty/\Phi)$, we have $\delta_\chi(x^\sigma) = \chi(\sigma)^{-1}\delta_\chi(x)$.

1.2.2. *Anticyclotomic projection.* Let Ψ_∞ be the anticyclotomic $\mathbb{Z}_p$-extension of Φ and $G^- = \mathrm{Gal}(\Psi_\infty/\Phi)$ be its Galois group. Let $G^+ = \mathrm{Gal}(\Theta_\infty/\Psi_\infty)$. Let Ψ_n be the subextension of Ψ_∞/Φ of degree p^n. If χ is an anticyclotomic character, i.e., χ is a homomorphism $\mathrm{Gal}(\Psi_n/\Phi) \to \overline{\mathbb{Q}}_p^\times$ for some n, then $\delta_\chi((\sigma - 1)U_\infty^*)$ vanishes for all $\sigma \in \mathrm{Gal}(\Phi_\infty/\Psi_\infty)$. Set $V_\infty^* := U_\infty^*/\{(\sigma-1)u | \sigma \in \mathrm{Gal}(\Phi_\infty/\Psi_\infty), u \in U_\infty^*\}$. Then δ_χ factors through V_∞^*.

1.2.3. *Decomposition of Local Principal Units.* We say a non-trivial anticyclotomic character χ has conductor p^n if χ factors through $\mathrm{Gal}(\Phi_{n-1}/\Phi)$ but not through $\mathrm{Gal}(\Phi_{n-2}/\Phi)$, equivalently, χ factors through $\mathrm{Gal}(\Psi_{n-1}/\Phi)$ but not through $\mathrm{Gal}(\Psi_{n-2}/\Phi)$. We say that trivial character has conductor 1.

Let Ξ^+ (resp. Ξ^-) be the set of anticyclotomic characters whose conductors are even (resp. odd) powers of p. Define

$$V_\infty^{*,\pm} := \left\{ v \in V_\infty^* | \delta_\chi(v) = 0 \text{ for every } \chi \in \Xi^\mp \right\}.$$

Set $\Lambda = \mathcal{O}[[G^-]]$. It is known that V_∞^* is a free Λ-module of rank 2. We will show the following theorem.

Theorem 1.1. *Assume $p \geq 3$. We have*

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

Remark 1.2. Rubin conjectured and verified the direct decomposition for $5 \leq p \leq 1000$ and $p \not\equiv 1 \pmod{12}$(cf. [13]). Burungale, Kobayashi and Ota proved it for primes $p \geq 5$(cf. [3]). We modify Burungale-Kobayashi-Ota's proof to include the case $p = 3$.

1.3. **Strategy.** We know that $V_\infty^* \simeq \Lambda^2$ by [17]. Consider the anticyclotomic projections of elliptic units in V_∞^*. Their images under δ_χ are algebraic parts of L-values of Hecke character $\chi\varphi$ (Theorem 2.3,(1)). They vanish if the root number of $\chi\varphi$ is -1, which is the case if the root number $W(\varphi)$ of φ is 1 and the conductor of χ is an odd power of p, or $W(\varphi) = -1$ and the conductor of χ is an even power of p. Hence the root number of φ determines which of $V_\infty^{*,\pm}$ the elliptic units belong to (Theorem 2.3,(2)). Moreover, Rohrlich showed that there are all but finitely many anticyclotomic characters χ such that $L(\varphi\chi, 1) \neq 0$. This ensures the elliptic units above are nontrivial in $V_\infty^{\pm}$, so

$$\mathrm{rank}_\Lambda V_\infty^{*,\pm} \geq 1$$

(Theorem 2.1).

On the other hand, we have a perfect pairing

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

The annihilator of $V_\infty^{*,\pm}$ under this paring is $A^\pm \otimes \Phi/\mathcal{O}$, where

$$A^\pm := \{y \in \mathcal{F}(\Psi_\infty) | \lambda_\chi(y) = 0 \text{ for all } \chi \in \Xi^\pm\}.$$

These modules $A^\pm$ can be well studied (Proposition 3.2 and Lemma 3.1). We may found that $A^\pm \otimes \Phi/\mathcal{O}$ generate the whole $\mathcal{F}(\Psi_\infty) \otimes \Phi/\mathcal{O}$. Hence

$$V_\infty^{*,+} \cap V_\infty^{*,-} = 0 \text{ and } \mathrm{rank}_\Lambda V_\infty^{*,\pm} = 1.$$

Now its suffices to show that $V_\infty^*/V_\infty^{*,-}$ is isomorphic to $V_\infty^{*,+}$. This can be done if $V_\infty^*/V_\infty^{*,-}$ is free of rank 1 and there is $\xi \in V_\infty^{*,+} \otimes \mathcal{R}$ for some coefficient ring $\mathcal{R}$ such that $\delta_\chi(\xi) \in \mathcal{O}^\times \otimes \mathcal{R}$.

Burungale-Kobayashi-Ota considered the elliptic units of root number $+1$ twisted by an anticyclotomic character ν along $\mathbb{Z}_\ell$-extension for an auxiliary ℓ. Their images under δ_χ are algebraic parts of $L(1, \varphi\chi\nu)$. By the work of Finis [7], this ν can be well-chosen for the purpose that the algebraic parts of L-values do not vanish mod p. Hence there is $\xi_\nu \in V_\infty^{*,+} \otimes \mathcal{R}$ for some coefficient ring $\mathcal{R}$ such that

$$\delta_\chi(\xi_\nu) \in \mathcal{O}^\times \otimes \mathcal{R}$$

(Theorem 2.2).

The last step (see Theorem 4.1) is to show

$$(A^- \otimes \Phi/\mathcal{O})^{G^-} = \mathcal{F}(\Phi) \otimes \Phi/\mathcal{O}. \tag{1.1}$$

By the Nakayama Lemma, the Λ-module $V_\infty^*/V_\infty^{*,-}$ is free of rank 1, which completes the proof. To show Theorem 4.1, it suffices to prove

$$|\widehat{H}^0(G_n^-, A_n^-)| = |\mathcal{F}(\Phi)/\mathrm{N}_{n/0}(A_n^-)| \leq p^{n-1},$$

where $A_n^- = A^- \cap \mathcal{F}(\Psi_n)$. The key point is to construct points in A_n^- whose norm in A_0^- is locally p-indivisible (Theorem 4.6). Actually, we will construct points satisfying

(1) $y \in \mathcal{F}(\Phi) \backslash p\mathcal{F}(\Phi)$,
(2) $y_s \in \mathcal{F}(\Psi_s)$ such that $\mathrm{tr}_{s+1/s} y_{s+1} = -y_{s-1}$ for $s \geq 1$ and $\mathrm{tr}_{1/0} y_1 = -y$.
(3) $y_s \in A^-$ if s is odd.

Choose a supersingular CM elliptic curve E which has good supersingular reduction at p. Then $\widehat{E} \simeq \mathcal{F}$ over $\mathcal{O}$, where $\widehat{E}$ is the formal group associated to E. Rubin considered the Heegner points in A_n^-, which are the images of some CM points on $X_0(N)(\mathcal{O})$ under the modular parametrization map

$$\pi : X_0(N) \to E_{/\mathcal{O}}.$$

If the bottom layer is p-indivisible, then we are done. Unfortunately, we do not know the p-divisibility of it.

The idea of Burungale-Kobayashi-Ota is to construct formal CM points instead. There are supersingular points on $X_0(N)(\mathcal{O})$ which may not be CM but fake CM, i.e., the formal group of the "representative" elliptic curve has an $\mathcal{O}$-action. We call such points formal CM points. Similar to the construction of Heegner points, Gross constructed a system of compatible formal CM points on $\widehat{E}(\Psi_n)$.

Now we need to find a "good" supersingular point on $X_0(N)(\mathcal{O})$ which leads to the p-indivisibility in the bottom layer. We may choose a point on $X_0(N)(\mathbb{F}_{p^2})$ such that

(1) the point "represents" a supersingular elliptic curve with a level structure
(2) under modular parametrization $\overline{\pi} : X_0(N) \to E$ the point is unramified and maps to $\overline{O}$

Taking formal completion of π over $\mathcal{O}$ along these two points, we get an isomorphism $\widehat{X_0(N)} \simeq \widehat{E}$. Choose $Q \in \widehat{E}(\mathfrak{m}) \backslash p\widehat{E}(\mathfrak{m})$, where $\mathfrak{m}$ is the maximal ideal of $\mathcal{O}$. Let $P \in X_0(N)(\mathcal{O})$ be the preimage of Q. Then the point P "represents" a fake CM elliptic curve A with a level structure. This elliptic curve A is what we want. Noting that $X_0(N)$ is not fine moduli, we need replace $X_0(N)$ by $X(\Gamma_0(N) \cap \Gamma_1(M))$ and modify the above argument.

Acknowledgement. We would like to thank Professor Ashay A. Burungale and Professor Ye Tian for their insightful discussions. We also appreciate the valuable suggestions provided by the anonymous referee.

2. Hecke L-values and elliptic units

In this section, we recall the proof of the following two theorems given in [13] and [3].

Theorem 2.1. $\operatorname{rank}_\Lambda V_\infty^{*;\pm} \geq 1$.

Theorem 2.2. *There exists an element $\xi \in V_\infty^{*;+}$ such that $\delta(\xi) \in \mathcal{O}^\times$.*

The basic ideas involve using the relation of elliptic units and Hecke L-values, and properties of Hecke L-values proved by Rohrlich [12] and Finis [7].

Firstly, we choose an auxiliary imaginary quadratic field. By [3, Lemma 3.4], there exist infinitely many imaginary quadratic fields K of odd discriminants such that

(1) $\left(\frac{2}{D_K}\right) = +1$ where $-D_K < 0$ is the discriminant of K;
(2) p inerts in K and is prime to h_K.

In the rest of our paper, K is an imaginary quadratic field satisfying (2). We do not assume that K satisfies (1) except in the proof of Theorem 2.2. 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 $H = K(1)$ be the Hilbert class field of K.

Let φ be a Hecke character over K with infinity type $(1, 0)$ of $\mathfrak{f}_\varphi$ such that $\varphi \circ \mathrm{N}_{H/K}$ corresponds to an elliptic curve $E_{/H}$ which is CM by $\mathcal{O}_K$, is isogenous to all its $\mathrm{Gal}(H/\mathbb{Q})$-conjugate and is good at primes above p. We note that if φ is a canonical Hecke character (in the sense of [11]), such an E always exists.

We fix a smooth Weierstrass model of the elliptic curve E over $\mathcal{O} \cap H$ and we may assume the period lattice L attached to the Néron differential ω is given by $\Omega\mathcal{O}_K$ for some $\Omega \in \mathbb{C}^\times$. Fix such Ω.

Let $\ell \geq 5$ be a prime such that ℓ splits in K, $\ell \nmid h_K$ and $p \nmid \ell - 1$. Let $\mathfrak{X}_\ell$ be the set of finite Hecke characters that factor through the anticyclotomic $\mathbb{Z}_\ell$-extension of K.

Theorem 2.3. *Let $\nu \in \mathfrak{X}_\ell$ be a character of order ℓ^m. Let $\mathcal{R}$ be the integer ring of the finite extension of Φ generated by the image of φ and ν. Then there exists a $\xi_\nu \in U_\infty^* \otimes \mathcal{R}$ such that*

(1) *the following holds*
$$\delta(\xi_\nu) = \frac{L_{\mathfrak{f}\ell}(\overline{\varphi}\nu, 1)}{\Omega}, \quad \delta_\chi(\xi_\nu) = \frac{L_{\mathfrak{f}\ell p}(\overline{\varphi}\nu\chi, 1)}{\Omega},$$
for all finite characters χ of $\mathrm{Gal}(\Phi_\infty/\Phi_0)$;
(2) *the anticyclotomic projection of ξ_ν lies in $V_\infty^{*;\epsilon} \otimes \mathcal{R}$ where ϵ is the root number of φ.*

Proof. As above, we choose an imaginary quadratic field K, a prime p that inerts in K and is prime to h_K, a $\mathbb{Q}$-curve E and the associated Hecke character φ. Besides, we choose an auxiliary prime ℓ. Let $T = T_\pi E$.

(1) Consider the elliptic units $z_{\mathfrak{f}\ell^m} = (z_{\mathfrak{f}\ell^m p^n})_n \in \varprojlim_n H^1(K(\mathfrak{f}\ell^m p^n), T^{\otimes -1}(1))$. Let
$$M_n = H(E[p^{n+1}])L_m \subset K(\mathfrak{f}\ell^m p^{n+1})$$

where L_m is the m-th layer of anticyclotomic $\mathbb{Z}_\ell$-extension of K. Let ν be an anticyclotomic Hecke character over K of order ℓ^m. Consider the composition of the following maps

$$\begin{aligned}
&\varprojlim_n H^1(K(\mathfrak{f}\ell^m p^{n+1}), T^{\otimes -1}(1)) \xrightarrow{\text{cores}} \varprojlim_n H^1(M_n, T^{\otimes -1}(1)) \\
&\xrightarrow{\text{loc}_p} \varprojlim_n H^1(M_n \otimes K_p, T^{\otimes -1}(1)) \xrightarrow{\nu} \varprojlim_n H^1(H(E[p^{n+1}]) \otimes K_p, T^{\otimes -1}(1)) \otimes \mathcal{R} \\
&\xrightarrow{\text{pr}} \varprojlim_n H^1(\Phi_n, T^{\otimes -1}(1)) \otimes \mathcal{R} \to \left(\varprojlim_n H^1(\Phi_n, T^{\otimes -1}(1))\right)^{\Delta} \otimes \mathcal{R} \simeq U^*_\infty \otimes \mathcal{R}.
\end{aligned}$$

Let $\xi_\nu \in U^*_\infty \otimes \mathcal{R}$ be the image of $z_{\mathfrak{f}\ell^m p^{n+1}}$ under the above map. Then we have

$$\delta_\chi(\xi_\nu) = \frac{L_{\mathfrak{f}\ell p}(\overline{\varphi}\chi\nu, 1)}{\Omega}$$

for all finite characters χ of $\mathrm{Gal}(\Phi_\infty/\Phi_0)$.

(2) For character χ of G^- of conductor p^{n+1}, Greenberg ([8, p.247]) showed that $W(\overline{\varphi}\nu\chi) = W(\overline{\varphi}\chi) = (-1)^{n+1}W(\overline{\varphi})$ if p is odd and $\ell \nmid \mathfrak{f}$, . Therefore $L(\overline{\varphi}\nu\chi, 1) = 0$ if $(-1)^{n+1}W(\varphi) = -1$ and the theorem follows from (1).

□

Proof of Theorem 2.1. By [12], for all but finitely many anticyclotomic characters ρ,

$$L(1, \rho\varphi) \neq 0, \text{ if } W(\varphi\rho) = 1.$$

If ρ is of conductor p^n and φ is of root number ϵ, then $W(\varphi\rho) = (-1)^n\epsilon$. Thus there exist infinitely many anticyclotomic characters ρ such that $L(1, \varphi\rho) \neq 0$. Hence $\delta_\chi(\xi) \neq 0$ for the elliptic units ξ associated to φ by the theorem above. Since $V^*_\infty \simeq \Lambda^2$ is torsion-free, we have $\mathrm{rank}_\Lambda V^{*,\pm}_\infty \geq 1$. □

Proof of Theorem 2.2. Suppose that φ is canonical. We have $W(\varphi) = +1$ (cf. [11]). Then by [7], for all but finitely many $\nu \in \mathfrak{X}_\ell$, one has

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

Fix a ν, Theorem 2.3 shows that there is a $\xi_\nu \in V^{*,+}_\infty \otimes \mathcal{R}$ such that $\delta(\xi_\nu) \in \mathcal{R}^\times$. It implies that there exists an element of $V^{*,+}_\infty$ whose image under δ belongs to $\mathcal{O}^\times$. □

3. Kummer pairing

We recall the construction of the Kummer pairing

$$\langle\ ,\ \rangle : (\mathcal{F}(\Psi_\infty) \otimes_{\mathcal{O}} \Phi/\mathcal{O}) \times V^*_\infty \to \Phi/\mathcal{O}.$$

Note that $\Theta_n = \Phi_n^\Delta$ for all $n \leq \infty$. The Kummer sequence

$$0 \to \mathcal{F}[\pi^{n+1}] \to \mathcal{F}(\overline{\Phi}) \xrightarrow{\pi^{n+1}} \mathcal{F}(\overline{\Phi}) \to 0$$

gives us an exact sequence

$$0 \to \mathcal{F}(\Theta_n)/\pi^{n+1}\mathcal{F}(\Theta_n) \to H^1(\Theta_n, \mathcal{F}[\pi^{n+1}]) \to H^1(\Theta_n, \mathcal{F}(\overline{\Phi}))[\pi^{n+1}] \to 0.$$

Hazewinkel [9] showed that $\cap_n \mathrm{N}_n \mathcal{F}(\Theta_n) = 0$ if $\mathcal{F}$ is a Lubin-Tate formal group of height 2 over $\mathcal{O}$. Hence $\varprojlim \mathcal{F}(\Theta_n) = 0$ and its Tate duality ([15]) $\varinjlim H^1(\Theta_n, \mathcal{F}(\overline{\Phi}))_{p^{n+1}}$ is also zero. Taking direct limit of the above exact sequences, we have

$$\mathcal{F}(\Theta_n) \otimes \Phi/\mathcal{O} \simeq H^1(\Theta_\infty, \mathcal{F}[\pi^\infty]) \simeq \mathrm{Hom}(\mathrm{Gal}(\overline{\Phi}/\Phi_\infty), \mathcal{F}[\pi^\infty])^\Delta \simeq \mathrm{Hom}_{\mathcal{O}}(U_\infty, \mathcal{F}[\pi^\infty]),$$

where the last isomorphism is given by local class field theory. Therefore we have a perfect pairing

$$\langle\ ,\ \rangle : (\mathcal{F}(\Theta_\infty) \otimes \Phi/\mathcal{O}) \times U^*_\infty \to \Phi/\mathcal{O}.$$

Since $\mathcal{F}(\Theta_\infty)$ has no p-torsion, the exact sequence

$$0 \to \mathcal{F}(\Theta_\infty) \to \mathcal{F}(\Theta_\infty) \otimes_{\mathcal{O}} \Phi \to \mathcal{F}(\Theta_\infty) \otimes \Phi/\mathcal{O} \to 0$$

induces an isomorphism $(\mathcal{F}(\Theta_\infty) \otimes \Phi/\mathcal{O})^{G^+} \simeq \mathrm{Hom}_{\mathcal{O}}(V_\infty, \mathcal{F}[\pi^\infty])$. However, we have that

$$(\mathcal{F}(\Theta_\infty) \otimes \Phi/\mathcal{O})^{G^+} / (\mathcal{F}(\Psi_\infty) \otimes \Phi/\mathcal{O}) \simeq H^1(G^+, \mathcal{F}(\Theta_\infty)) \subset H^1(\Psi_\infty, \mathcal{F}(\overline{\Phi})) = \varinjlim H^1(\Psi_n, \mathcal{F}(\overline{\Phi})) = 0.$$

Here the reason for the last equality is similar to $\varinjlim H^1(\Psi_n, \mathcal{F}(\overline{\Phi})) = 0$. Hence we have a perfect paring

$$\langle\ ,\ \rangle : (\mathcal{F}(\Psi_\infty) \otimes_{\mathcal{O}} \Phi/\mathcal{O}) \times V^*_\infty \to \Phi/\mathcal{O}.$$

By Wiles' explicit reciprocity law ([16]), the pairing can be described as

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

with $y\in\mathcal{F}(\Psi_n)$, $x\in V_\infty^*$ and some sufficiently large m.

For any anticyclotomic character χ of conductor dividing p^{n+1}, let

$$\lambda_\chi:\mathcal{F}(\Psi_\infty)\to\Phi_\infty,\quad y\mapsto\frac{1}{\pi^n}\sum_{\gamma\in\mathrm{Gal}(\Psi_n/\Phi)}\chi^{-1}(\gamma)\lambda(y)^\gamma,\quad y\in\mathcal{F}(\Psi_n).$$

Denote

$$A^\pm:=\{y\in\mathcal{F}(\Psi_\infty)|\lambda_\chi(y)=0\text{ for all }\chi\in\Xi^\pm\}.$$

We recall the following properties of λ_χ.

Lemma 3.1 ([13, Lemma 5.5])**.**

(1) *If $y\in\mathcal{F}(\Psi_\infty)$, χ is a finite character of G^- and $\sigma\in G^-$, then $\lambda_\chi(y^\sigma)=\chi(\sigma)\lambda_\chi(y)$;*
(2) *If $y\in\mathcal{F}(\Psi_n)$ and the conductor of χ is greater than p^{n+1}, then $\lambda_\chi(y)=0$;*
(3) *If $y\in\mathcal{F}(\Psi_\infty)$, then $\lambda(y)=\sum\lambda_\chi(y)$, summing over all finite characters χ of G^-;*
(4) *If $m\geq n$, $y\in\mathcal{F}(\Psi_m)$ and χ is a character of $\mathrm{Gal}(\Psi_n/\Phi)$, then $\lambda_\chi(\mathrm{N}_{m/n}y)=p^{m-n}\lambda_\chi(y)$.*
(5) *$A^+\cap A^-=0$;*
(6) *$(A^+\otimes\Phi/\mathcal{O})+(A^-\otimes\Phi/\mathcal{O})=\mathcal{F}(\Psi_\infty)\otimes\Phi/\mathcal{O}$.*

Proposition 3.2 ([13, Proposition 5.6])**.** *Under the Kummer pairing $(\mathcal{F}(\Psi_\infty)\otimes_{\mathcal{O}}\Phi/\mathcal{O})\times V_\infty^*\to\Phi/\mathcal{O}$, the annihilator of $V_\infty^{*,\pm}$ is $A^\pm\otimes\Phi/\mathcal{O}$.*

Proof. If $y\in\mathcal{F}(\Psi_\infty)$ and $x\in V_\infty^*$, then the above formula and Lemma 3.1 yields

$$\begin{aligned}\langle y\otimes\pi^{-n},x\rangle&=\pi^{-1-m-n}\operatorname{Tr}_{\Phi_m/\Phi}(\delta_m(x)\lambda(y))=\pi^{-1-m-n}\sum_\gamma\delta_m(x)^\gamma\lambda(y^\gamma)\\&=\pi^{-1-m-n}\sum_\gamma\delta_m(x)^\gamma\sum_\chi\lambda_\chi(y^\gamma)=\sum_\chi\pi^{-1-m-n}\sum_\gamma\delta_m(x)^\gamma\chi(\gamma)\lambda_\chi(y)\\&=\sum_\chi\delta_\chi(x)\lambda_\chi(y).\end{aligned}$$

By definition, $V_\infty^{*,\pm}$ annihilate $A^\pm\otimes\Phi/\mathcal{O}$.

Now suppose that $x\in V_\infty^*$ and x annihilates $A^\pm\otimes\Phi/\mathcal{O}$ and $\chi\in\Xi^\mp$. Choose $y\in A^\pm$ such that $\lambda_\chi(y)\neq0$. Then the above computation shows that

$$\sum_\rho\delta_\rho(x)\lambda_\rho(y^\gamma)=0$$

for every γ. Thus

$$\pi^n\delta_\chi(x)\lambda_\chi(y)=\sum_\rho\sum_\gamma\chi^{-1}(\gamma)\delta_\rho(x)\lambda_\rho(y^\gamma)=0.$$

Hence $\delta_\chi(x)=0$, i.e., $x\in V_\infty^{*,\pm}$. □

Now we have the following corollary by Lemma 3.1 (6) and Proposition 3.2.

Corollary 3.3. $V_\infty^{*,+}\cap V_\infty^{*,-}=0$.

4. Local points

In this section, we will prove the following theorem.

Theorem 4.1. *We have*

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

Corollary 4.2. *The Λ-module $V_\infty^*/V_\infty^{*,-}$ is free of rank one.*

Proof. Note that

$$\mathcal{F}(\Phi)\otimes\Phi/\mathcal{O}\simeq(A^-\otimes\Phi/\mathcal{O})^{G^-}\simeq\mathrm{Hom}\left((V_\infty^*/V_\infty^{*,-})/(\gamma-1),\Phi/\mathcal{O}\right)$$

where γ is the topological generator of G^-. Hence $(V_\infty^*/V_\infty^{*,-})/(\gamma-1)\simeq\mathcal{O}$ generated by one element. By Nakayama's lemma, $V_\infty^*/V_\infty^{*,-}$ is also generated by one element. Hence the Λ-module $V_\infty^*/V_\infty^{*,-}$ is free of rank one. □

We will construct a system of local points in $\mathcal{F}(\Psi_n)$, which can be used to show that $(A^- \otimes \Phi/\mathcal{O})^{G^-}$ is isomorphic to the divisible module $\mathcal{F}(\Phi) \otimes \Phi/\mathcal{O}$. So the dual module (under Kummer pairing) $V_\infty^*/V_\infty^{*,-}$ is free.

Let E be an elliptic curve over $\mathbb{Q}$ with good supersingular reduction at p. Consider the modular parametrization $\pi : X_0(N) \to E$ over $\mathbb{Q}$. We may assume π is strong Weil by choosing E in its isogeny class. By the Néron mapping property, π extends to a morphism between smooth models over $\mathbb{Z}_p$.

4.1. **A special supersingular elliptic curve.**

Lemma 4.3 ([3, Lemma 5.1])**.** *Let $q = p^2$ and $\overline{A}$ be an elliptic curve over $\mathbb{F}_q$ with $a_q(\overline{A}) = \pm 2p$.*

1. *Any finite subgroup $\overline{A}(\overline{\mathbb{F}}_q)$ is defined over $\mathbb{F}_q$.*
2. *For A an elliptic curve over $\mathcal{O}$ which is a lift of $\overline{A}$, the associated formal group $\widehat{A}$ is Lubin-Tate with parameter $\mp p$.*

Lemma 4.4. *If $p \geq 3$, there is a supersingular point with $a_{p^2} = \pm 2p$ in $X_0(N)(\mathbb{F}_{p^2})$ which is unramified under $\overline{\pi} : X_0(N)_{\mathbb{F}_{p^2}} \to \overline{E}$.*

Proof. See [3] for $p > 3$. We give a proof for $p = 3$. Let S_{ram} be the set of points of $X_0(N)$ which are ramified under $\overline{\pi}$. By Hurwitz formula [10, Chapter 7, Theorem 4.16]

$$\#S_{ram} \leq 2g - 2,$$

where g is the genus of $X_0(N)$. Let $\mu = N\prod_{p|N}(1 + p^{-1})$ be the degree of natural projection $X_0(N) \to X(1)$. By genus formula

$$g = 1 + \frac{\mu}{12} - \frac{\varepsilon_2}{4} - \frac{\varepsilon_3}{3} - \frac{\varepsilon_\infty}{2},$$

where ε_2 (resp. ε_3) is the number of elliptic points of period 2 (resp. 3) in $X_0(N)$, and ε_∞ the number of cusp of $X_0(N)$. Hence

$$\#S_{ram} \leq \frac{\mu}{6} - \frac{\varepsilon_2}{2} - \frac{2\varepsilon_3}{3} - \varepsilon_\infty < \frac{\mu}{6}.$$

The elliptic curve

$$\overline{A}_{/\mathbb{F}_3} : y^2 = x^3 - x$$

is supersingular and $j(\overline{A}) = 0 = 1728$. Note that $\overline{A}(\mathbb{F}_3) = \{O, (0,0), (1,0), (-1,0)\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\overline{A}(\mathbb{F}_9) \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, and $a_3(\overline{A}) = 0, a_9(\overline{A}) = -6$. Since $p \nmid N$, the group $\overline{A}[N]$ is isomorphic to $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ and thus has μ cyclic subgroup of order N, which we denote by $\{C_1(N), \cdots, C_\mu(N)\}$ (they are defined over $\mathbb{F}_9$). Since $\#\mathrm{Aut}(\overline{A}) = 12$ ([14, Theorem III.10.1]) and -1 induces an isomorphism of pairs $(\overline{A}, C_i(N)) \to (\overline{A}, C_i(N))$, there are at least $\frac{\mu}{6}$ isomorphism classes of pair $(\overline{A}, C_i(N))$. Hence there is a supersingular point with $a_9 = -6$ in $X_0(N)(\mathbb{F}_9)$ which is unramified under $\overline{\pi} : X_0(N) \to \overline{E}$. □

4.2. **A formal CM point.**

By Lemma 4.4, we can choose a supersingular point $\overline{P}$ of $X_0(N)_{\mathbb{F}_q}$ unramified under $\overline{\pi}$, representing an elliptic curve $\overline{A}$ with $a_{p^2} = \pm 2p$ and a $\Gamma_0(N)$-level structure. In particular, when $p = 3$, $\overline{A}$ is chosen to be $y^2 = x^3 - x$. We assume that $\overline{\pi}(\overline{P}) = \overline{O}$ by replacing $\overline{\pi}$ with $\#E(\mathbb{F}_{p^2})\overline{\pi}$. In this subsection, for a properly chosen E, we construct a lift $P \in X_0(N)(\mathcal{O})$ of $\overline{P}$ representing an elliptic curve A over $\mathcal{O}$ and a $\Gamma_0(N)$-level structure, such that $\pi(P) \in \widehat{E}(\mathfrak{m}) \backslash p\widehat{E}(\mathfrak{m})$, where $\mathfrak{m}$ be the maximal ideal of $\mathcal{O}$. For $p > 3$, the construction details can be found in [3]. From now on, we assume $p = 3$.

Lemma 4.5. *Let $\overline{A} : y^2 = x^3 - x$ be the supersingular elliptic curve over $\mathbb{F}_3$. There are infinitely many integers N such that*

1. *N is the conductor of a CM elliptic curve $E_{/\mathbb{Q}}$ which is good at 2, 3 and satisfies $a_3(E) = 0$;*
2. *for a $\Gamma_0(N)$-structure $C(N)$ of $\overline{A}$, the automorphism group of $(\overline{A}, C(N))$ over $\overline{\mathbb{F}}_3$ is $\{\pm 1\}$.*

Proof. Let X be the set of integers satisfying conditions a) and b) in the lemma, and Y the set of integers N satisfying the following conditions:

a) N is conductor of a CM elliptic curve $E_{/\mathbb{Q}}$ which is good at 2, 3 and satisfies $a_3 = 0$;
b) $\varphi(N) > \#(\ker(g + 1) \cup \ker(g - 1))$;
c) -3 is not a square in $\mathbb{Z}/N\mathbb{Z}$.

We claim that Y is an infinite set and $Y \subset X$. It completes the proof.

We first show that Y is an infinite set. Choose a CM elliptic curve $E_{/\mathbb{Q}}$ which has good reduction at $2, 3$ and satisfies $a_3 = 0$ (for example, $E_{/\mathbb{Q}} : y^2 + y = x^3 - 38x + 90$). Let N_E be its conductor. By Dirichlet's theorem on arithmetic progressions, there are infinitely many primes $\ell \equiv 5 \pmod{12}$ prime to N_E and satisfying $\varphi(\ell^2 N) > \#(\ker(g+1) \cup \ker(g-1))$. Let E^ℓ be the quadratic twists of E by prime ℓ. It is a CM elliptic curve with conductor $\ell^2 N_E$ and satisfies $a_3 = 0$. Hence $\ell^2 N_E \in Y$, which implies that Y is a infinite set.

Now we show that $Y \subset X$. Let N be an integer satisfying b) and c). Since $\#\mathrm{Aut}(\overline{A}) = 12$, it suffices to prove that for any $g \in \mathrm{Aut}(\overline{A})\backslash\{\pm 1\}$ of order 2 or 3, the actions of g on N-cyclic subgroup of $\overline{A}$ are not stable. If not, i.e., there is $g \in \mathrm{Aut}(\overline{A})\backslash\{\pm 1\}$ of order 2 or 3 and an N-cyclic subgroup $C(N)$, such that for any primitive elements $\alpha \in C(N)$, $g\alpha = n\alpha$ for some $n \in \mathbb{Z}/N\mathbb{Z}$. It follows that $n^2\alpha = g^2\alpha = \alpha$ or $n^3\alpha = g^3\alpha = \alpha$ (depends on the order of g). Thus $0 \equiv n^2 - 1 \equiv (n-1)(n+1) \pmod{N}$ or $0 \equiv n^3 - 1 \equiv (n-1)(n^2+n+1) \pmod{N}$. Since -3 is not a square in $\mathbb{Z}/N\mathbb{Z}$, we have $n \equiv 1$ or -1. So all primitive elements $\alpha \in C(N)$ must belong to $\ker(g-1) \cup \ker(g+1)$, which contradicts condition b).

□

Choose a point ξ of order 4 in $\overline{A}(\mathbb{F}_{p^2}) \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Let $X(\Gamma_0(N), \Gamma_1(4))$ be the modular curve with $\Gamma_0(N)$ and $\Gamma_1(4)$-level structure. Then $X(\Gamma_0(N), \Gamma_1(4))$ is a fine moduli space. Consider

$$\begin{array}{ccc}
X(\Gamma_0(N),\Gamma_1(4))(\mathbb{F}_{p^2}) & & \overline{P}' = (\overline{A}, C(N), \xi)\ . \\
\downarrow{\scriptstyle \overline{\pi}'} & & \downarrow \\
X_0(N)(\mathbb{F}_{p^2}) & & \overline{P} = (\overline{A}, C(N)) \\
\downarrow{\scriptstyle \overline{\pi}} & & \downarrow{\scriptstyle \text{unramified}} \\
E(\mathbb{F}_{p^2}) & & \overline{O}
\end{array}$$

We choose E as in Lemma 4.5. Then the automorphism group of $(\overline{A}, C(N))$ is $\{\pm 1\}$. Hence $\#{\overline{\pi}'}^{-1}(\overline{P}) = \deg \overline{\pi}' = [\mathrm{GL}_2(\mathbb{Z}) : \Gamma_1(4)]/2$, and therefore $\overline{\pi}'$ is unramified at $\overline{P}'$. The formal completion of $\pi \circ \pi' : X(\Gamma_0(N), \Gamma_1(4)) \to E$ (on integral models) at $\overline{P}'$ is an isomorphism ([10, Chapter 4, Proposition 3.26]).

Take a point

$$Q \in \widehat{E}(\mathfrak{m}) \backslash p\widehat{E}(\mathfrak{m}).$$

Then there is a point $P' \in X(\Gamma_0(N), \Gamma_1(4))(\mathcal{O})$ over $\overline{P}'$ sent to Q by $\pi \circ \pi'$. As $X(\Gamma_0(N), \Gamma_1(4))$ is a fine moduli space, there is 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 4.3. In particular, A is a formal CM elliptic curve. Let P be the image of P' in $X_0(N)$.

4.3. **Construction of local points.** Since $\widehat{A}$ is Lubin-Tate, the module $T = T_pA = \mathcal{O}t$ is a free $\mathcal{O}$-module of rank 1. For $s \geq 0$, let $T_s = p^{-s}\mathbb{Z}_p t + T$, $C_s = T_s/T$. Let $A_s = A/C_s$, a quasi-canonical lift of conductor p^s of $\overline{A}$ with respect to A.

Let Ψ_s' be the fixed field of subgroup of $\mathrm{Gal}(\overline{\Phi}/\Phi)$ stabilizing T_s and $\Psi_\infty' = \cup \Psi_s'$. It's known that

$$\mathrm{Gal}(\Psi_s'/\Phi) = (\mathcal{O}/p^s\mathcal{O})^\times/(\mathbb{Z}/p^s\mathbb{Z})^\times, \quad \mathrm{Gal}(\Psi_\infty'/\Phi) \simeq \mathbb{Z}_p \times \mathbb{Z}/(p+1)\mathbb{Z}.$$

Let Δ' be the torsion subgroup of $\mathrm{Gal}(\Psi_\infty'/\Phi)$. The field Ψ_∞' contains the anticyclotomic $\mathbb{Z}_p$-extension Ψ_∞. The field Ψ_s lies in Ψ_{s+1}'.

Then $A_s/\mathcal{O}_{\Psi_s'}$ and the canonical level structure induced from that of A define a point $z_s \in X_0(N)(\mathcal{O}_{\Psi_s'})$. Let $x_s = \pi(z_s)$. Let

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

$$
\begin{tikzcd}
 & \Psi'_\infty \\
\Psi_\infty \arrow[ur, dash, "\Delta'"] \arrow[d, dash] & \Psi'_{s+1} \arrow[u, dash] \arrow[d, dash] \\
\Psi_s \arrow[ur, dash] \arrow[d, dash] & \Psi'_1 \\
\Phi = \Psi_0 \arrow[ur, dash] &
\end{tikzcd}
$$

Theorem 4.6. *There is a system of local points $y_s \in \mathcal{F}(\Psi_s)$ and $y \in \mathcal{F}(\Phi)\backslash p\mathcal{F}(\Phi)$, such that*

$$\mathrm{Tr}_{s+1/s}\, y_{s+1} = a_p y_s - y_{s-1}, \quad s \geq 1$$

and

$$\mathrm{Tr}_{1/0}\, y_1 = a_p y_0 - y, \qquad \textit{and } y_0 = a_p x_0,$$

where $a_p = a_p(E)(= 0)$. Moreover, $y_s \in A^+$ if s is even, and $y_s \in A^-$ if s is odd.

Proof. Identify $\mathcal{F}$ with $\widehat{E}$. Consider the action of the Hecke operator T_p on x_s. There are two types of lattice containing T_s with index p:

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

The first type is of form σx_{s+1} and permuted by the action of $\mathrm{Gal}(\Psi'_{s+1}/\Psi'_s)$ and the second type is equivalent 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 $a_p(E)$ on E, we have the desired relation.

For the proof of $y_s \in A^{\pm}$, consider the anticyclotomic character χ of conductor p^{k+1} for $k \geq 1$. If $s < k$, then $\lambda_\chi(y_s) = 0$. If $s \geq k$, then $\lambda_\chi(\mathrm{N}_{s/k} y_s) = p^{s-k}\lambda_\chi(y_s)$. But if $2 \nmid s-k$, we have

$$\lambda_\chi(\mathrm{N}_{s/k} y_s) = \lambda_\chi\left(-(-p)^{(s-k-1)/2} y_{k-1}\right) = 0,$$

i.e. $\lambda_\chi(y_s) = 0$, hence $y_s \in A^-$ if s is odd. Similarly, if χ is trivial and s is even,

$$p^s \lambda_\chi(y_s) = \lambda_\chi(\mathrm{N}_{n/0} y_s) = \lambda_\chi\left((-p)^{n/2} y_0\right) = 0.$$

Hence $y_s \in A^+$ if s is even. $\square$

4.4. **Proof of Theorem 4.1.** Write $G_n^- = \mathrm{Gal}(\Psi_n/\Phi)$. For any $\mathcal{O}[G_n^-]$-module Z, denote the Herbrand quotient of Z by $h_n(Z)$, i.e.,

$$h_n(Z) := |\widehat{H}^0(G_n^-, Z)|/|H^1(G_n^-, A^-)|.$$

We know that $h_n(Z_1/Z_2) = h_n(Z_1)/h_n(Z_2)$ and $h_n(Z) = 1$ if Z is finite. Let $A_n^- = A^- \cap \mathcal{F}(\Psi_n)$. The exact sequence

$$0 \to A^- \to A^- \otimes \Phi \to A^- \otimes \Phi/\mathcal{O} \to 0$$

gives the $\mathcal{O}[G^-]$-mod isomorphism

$$H^1\left(G^-, A^-\right) \simeq \left(A^- \otimes \Phi/\mathcal{O}\right)^{G^-} / \left((A^-)^{G^-} \otimes \Phi/\mathcal{O}\right) \simeq \left(A^- \otimes \Phi/\mathcal{O}\right)^{G^-} / \left(\mathcal{F}(\Phi) \otimes \Phi/\mathcal{O}\right).$$

Note that for odd n, we have $h_n(A_n^-) = p^{n-1}$ ([13, Lemma 7.1]), hence

$$|H^1(G_n^-, A_n^-)| = |\widehat{H}^0(G_n^-, A_n^-)|/h_n(A_n^-) = p^{-(n-1)}|(A_n^-)^{G_n^-} / \mathrm{Tr}_n A_n^-| \leq [\mathcal{F}(\Phi) : \mathcal{O}y] = 1.$$

Therefore, $H^1(G^-, A^-) = \varinjlim H^1(G_n^-, A_n^-) = 0$, i.e. $(A^- \otimes \Phi/\mathcal{O})^{G^-} = \mathcal{F}(\Phi) \otimes \Phi/\mathcal{O}$.

4.5. **Rubin's conjecture.**

Theorem 4.7. *Assuming $p \geq 3$, we have*

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

Proof. The Corollary 3.3, Theorem 2.2 and Corollary 4.2 complete the proof. □

5. Some applications

Recall that K is an imaginary quadratic field where p does not divide h_K and is inert in K. Let K_∞ be the anticyclotomic $\mathbb{Z}_p$-extension of K. We identify G^- with $\mathrm{Gal}(K_\infty/K)$. Let $\mathcal{R}$ be the ring of integers of a finite extension of Φ containing the image of $\widehat{\varphi}$. Let $T = \mathcal{R}(\widehat{\varphi})$ and $W = T \otimes_{\mathcal{O}} \Phi/\mathcal{O}$. The completion of K_n at the prime above p is identical to Ψ_n. Note that $W \simeq \mathcal{F}[\pi^\infty] \otimes \mathcal{R}$ as a $\mathcal{R}[G_\Phi]$-module. The exact sequence

$$0 \to \mathcal{F}[\pi^{n+1}] \to \mathcal{F}(\overline{\Phi}) \xrightarrow{\pi^{n+1}} \mathcal{F}(\overline{\Phi}) \to 0$$

gives the Kummer map $\mathcal{F}(\Psi_n)/\pi^{n+1} \to H^1(\Psi_n, \mathcal{F}[\pi^{n+1}])$. Hence we have

$$\mathcal{F}(\Psi_n) \otimes \mathcal{R} \otimes \mathbb{Q}_p/\mathbb{Z}_p \to H^1(\Psi_n, \mathcal{F}[\pi^\infty]) \otimes \mathcal{R} \simeq H^1(\Psi_n, W).$$

Let $H^1_\pm(\Psi_n, W) \subset H^1(\Psi_n, W)$ be the Kummer image of $\mathcal{F}^\pm(\Psi_n) \otimes \mathcal{R} \otimes \mathbb{Q}_p/\mathbb{Z}_p$ where

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

Let $H^1_\pm(\Psi_n, T) \subset H^1(\Psi_n, T)$ be the orthogonal complement of $H^1_\pm(\Psi_n, W)$ with respect to the local Tate pairing.

We define

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

Let $\mathcal{X}_*$ be the Pontryagin dual of $\varinjlim_n \mathrm{Sel}_*(K_n, W)$ for $* \in \{+, -\}$. In [1, Theorem 3.6] it is shown that $\mathcal{X}_\epsilon$ is a finitely generated torsion Λ-module.

Let E and φ be as defined in section 2. As in Theorem 2.3, there is a unit $\xi = \xi(E, \Omega) \in U_\infty^*$ such that

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

and

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

for a finite character χ of $\mathrm{Gal}(\Phi_\infty/\Phi_0)$. Let $\epsilon \in \{+, -\}$ be the sign of φ. It is known that the projection of ξ on V_∞^* belongs to $V_\infty^{*,\epsilon}$. Define $\mathcal{C}_\infty$ as the free Λ-submodule of $V_\infty^{*,\epsilon}$ generated by ξ. Take a generator v_ϵ of the Λ-module $V_\infty^{*,\epsilon}$ and write

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

for a power series $\mathcal{L}_p(\varphi, \Omega, v_\epsilon) \in \Lambda$. We call it Rubin's p-adic L-function associated with φ. We sometimes omit the indices of $\mathcal{L}_p(\varphi, \Omega, v_\epsilon)$ and write its evaluation at an anticyclotomic character χ by $\mathcal{L}_p(\chi)$ for simplicity. Rubin's p-adic L-function has the following interpolation property:

$$\mathcal{L}_p(\chi) = \frac{1}{\delta_\chi(v_\epsilon)} \frac{L(\overline{\varphi\chi}, 1)}{\Omega}$$

In analogy with [3], we have the following theorems.

Theorem 5.1. *Let $\epsilon = W(\varphi)$ be the sign of φ, then*

$$\mathrm{char}(\mathcal{X}_{-\epsilon}) = (\mathcal{L}_p).$$

Theorem 5.2. *Let χ be an anticyclotomic character of conductor p^n. Then we have*

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

Declarations

Ethical Approval. Not applicable.

Funding. Not applicable.

References

[1] A. Agboola and B. Howard. Anticyclotomic Iwasawa theory of CM elliptic curves II. *Mathematical Research Letters*, 12(5):611–622, 2005.

[2] B. J. Birch and N. M. Stephens. Computation of Heegner points. Modular forms, Symp. Durham/Engl. 1983, 13-41 (1984)., 1984.

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

[4] A. A. Burungale, W. He, S. Kobayashi, and K. Ota. Hecke l-values, definite shimura sets and mod ℓ non-vanishing. *arXiv preprint arXiv:2408.13932*, 2024.

[5] A. A. Burungale, S. Kobayashi, and K. Ota. p-adic l-functions and rational points on cm elliptic curves at inert primes. *Journal of the Institute of Mathematics of Jussieu*, 23(3):1417–1460, 2024.

[6] A. A. Burungale, S. Kobayashi, K. Ota, and S. Yasuda. Kato's epsilon conjecture for anticyclotomic cm deformations at inert primes. *Journal of Number Theory*, 2024.

[7] T. Finis. Divisibility of anticyclotomic L-functions and theta functions with complex multiplication. *Annals of mathematics*, pages 767–807, 2006.

[8] R. Greenberg. On the Birch and Swinnerton-Dyer conjecture. *Inventiones mathematicae*, 72(2):241–265, 1983.

[9] M. Hazewinkel. On norm maps for one dimensional formal groups III. 1977.

[10] Q. Liu. Algebraic geometry and arithmetic curves, 2006.

[11] D. E. Rohrlich. Root numbers of Hecke L-functions of CM fields. *American Journal of Mathematics*, 104(3):517–543, 1982.

[12] D. E. Rohrlich. On L-functions of elliptic curves and anticyclotomic towers. *Inventiones mathematicae*, 75(3):383–408, 1984.

[13] K. Rubin. Local units, elliptic units, Heegner points and elliptic curves. *Inventiones mathematicae*, 88(2):405–422, 1987.

[14] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106. Springer, 2009.

[15] J. Tate. WC-groups over p-adic fields. *Séminaire Bourbaki*, 4:265–277, 1957.

[16] A. Wiles. Higher explicit reciprocity laws. *Annals of Mathematics*, 107(2):235–254, 1978.

[17] J.-P. Wintenberger. Structure galoisienne de limites projectives d'unités locales. *Compositio Mathematica*, 42(1):89–103, 1980.

[18] R. I. Yager. On two variable p-adic L-functions. *Annals of Mathematics*, 115(2):411–449, 1982.

Beijing Institute of Mathematical Sciences and Applications, Beijing 101408, China.

Department of Mathematics and Yau Mathematical Sciences Center, Tsinghua University;
Email address: `xjyan95@amss.ac.cn`

Beijing Institute of Mathematical Sciences and Applications, Beijing 101408, China.

Department of Mathematics and Yau Mathematical Sciences Center, Tsinghua University;
Email address: `xwzhu@bimsa.cn`