Riv. Mat. Univ. Parma, Vol. **14** (2023), 153-171

Tsuyoshi Itoh

On the unramified Iwasawa module of a $\mathbb{Z}_p$-extension generated by division points of a CM elliptic curve

Abstract. We consider the unramified Iwasawa module $X(F_\infty)$ of a certain $\mathbb{Z}_p$-extension F_∞/F_0 generated by division points of an elliptic curve with complex multiplication. This $\mathbb{Z}_p$-extension has properties similar to those of the cyclotomic $\mathbb{Z}_p$-extension of a real abelian field, however, it is already known that $X(F_\infty)$ can be infinite. That is, an analog of Greenberg's conjecture for this $\mathbb{Z}_p$-extension fails. In this paper, we mainly consider analogs of weak forms of Greenberg's conjecture.

Keywords. Non-cyclotomic $\mathbb{Z}_p$-extension, Iwasawa module, CM elliptic curve.

Mathematics Subject Classification: 11R23, 11G05, 11G15.

1 - Introduction

1.1 - *Our questions*

In this paper (except for Section 4), we shall consider the following situation:

(C1) K is an imaginary quadratic field whose class number is 1,

(C2) p is an odd prime number which splits in two distinct primes $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ in K,

(C3) E is an elliptic curve over $\mathbb{Q}$ which has complex multiplication by the ring of integers O_K of K, and E has good reduction at p.

In Sections 1–3, we shall always work under the following

Received: September 7, 2022; accepted in revised form: March 28, 2023.
This work was partly supported by JSPS KAKENHI Grant Number JP15K04791.

Assumption. K, p, and E satisfy (C1), (C2), and (C3).

We recall several known facts (see, e.g., [**6**], [**3**], [**17**, pp.364–365], [**10**, Section 1]). Let ψ be the Grössencharacter of E over K, and put $\pi = \psi(\mathfrak{p})$. Then, π is a generator of the principal ideal $\mathfrak{p}$. For every non-negative integer n, let $E[\pi^{n+1}] \subset E(\overline{\mathbb{Q}})$ be the group of π^{n+1}-division points of E. We put $F_n = K(E[\pi^{n+1}])$ for every n. Then F_n/K is an abelian extension, and $\mathfrak{p}$ is totally ramified in F_n/K. We also put $F_\infty = \bigcup_n F_n$. It is known that

$$\mathrm{Gal}(F_\infty/K) \cong \Delta \times \Gamma,$$

where $\Delta \cong \mathrm{Gal}(F_0/K)$ is a cyclic group of order $p-1$ and $\Gamma = \mathrm{Gal}(F_\infty/F_0)$ is topologically isomorphic to the additive group $\mathbb{Z}_p$. We often identify Δ with $\mathrm{Gal}(F_0/K)$ via the natural restriction map. Let $\mathfrak{P}$ be the unique prime of F_0 lying above $\mathfrak{p}$. Note that F_∞/F_0 is a $\mathbb{Z}_p$-extension which is unramified outside $\mathfrak{P}$.

We denote by $L(F_\infty)$ (resp. $M(F_\infty)$) the maximal abelian unramified (resp. unramified outside $\mathfrak{p}$) pro-p-extension of F_∞. We put $X(F_\infty) = \mathrm{Gal}(L(F_\infty)/F_\infty)$ (the unramified Iwasawa module) and $\mathfrak{X}(F_\infty) = \mathrm{Gal}(M(F_\infty)/F_\infty)$ (the $\mathfrak{p}$-ramified Iwasawa module). We also put $\Lambda = \mathbb{Z}_p[[\Gamma]]$. Then, it is well known that $X(F_\infty)$ is a finitely generated torsion Λ-module. We note that $\mathfrak{X}(F_\infty)$ is also a finitely generated torsion Λ-module (see [**15**, p.94]).

The $\mathbb{Z}_p$-extension F_∞/F_0 and the cyclotomic $\mathbb{Z}_p$-extension of real abelian fields have several similar properties. It is conjectured that the unramified Iwasawa module of the cyclotomic $\mathbb{Z}_p$-extension is finite for every totally real field (Greenberg's conjecture [**14**]). On the other hand, the following result is known. We denote by $\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q})$ the rank of the Mordell-Weil group $E(\mathbb{Q})$.

Theorem X (see Rubin [**37**, p.551, Remark], Greenberg [**17**, pp.364–366]). *If* $\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) \geq 2$, *then* $X(F_\infty)$ *is not finite.*

Hence, the analog of Greenberg's conjecture does not hold in general for F_∞/F_0. Let us then consider the analog of "weak forms" of Greenberg's conjecture. The following questions are the analog of conjectures treated in [**25**], [**26**]. We denote by $X(F_\infty)_{\mathrm{fin}}$ the maximal finite Λ-submodule of $X(F_\infty)$.

- Does either $X(F_\infty) = 0$ or $X(F_\infty)_{\mathrm{fin}} \neq 0$ hold?
- Does either $\mathfrak{X}(F_\infty) = 0$ or $\mathrm{Gal}(M(F_\infty)/L(F_\infty)) \neq 0$ hold?

It is known that $\mathfrak{X}(F_\infty)$ does not have non-trivial finite Λ-submodules (see [**15**, p.94]). Hence if $X(F_\infty)_{\mathrm{fin}} \neq 0$, then $\mathrm{Gal}(M(F_\infty)/L(F_\infty)) \neq 0$. Thus an affirmative answer for (Q1) implies that the same holds for (Q2) (but not vice versa).

Remark 1.1.1. In [**20**, Appendix A], similar assertions for “tamely ramified Iwasawa modules” of the cyclotomic $\mathbb{Z}_p$-extension of a totally real field are considered. See also [**9**].

Actually, it is already known that the second question has an affirmative answer for a large family of elliptic curves.

Theorem Y (see Coates-Wiles [**6**, Lemma 35]). *If* $\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) \geq 1$, *then* $\mathrm{Gal}(M(F_\infty)/L(F_\infty)) \neq 0$.

Strictly speaking, in [**6**] the authors assumed $p \geq 5$. However, one can also show the same assertion for $p = 3$ similarly (see [**37**, (11.6) Proposition], [**17**, pp.364–365]).

Let ϕ be the isomorphism $\mathrm{Gal}(F_\infty/K) \to \mathbb{Z}_p^\times$ which satisfies $P^\sigma = \phi(\sigma)P$ for all $P \in E[\pi^{n+1}]$ and $\sigma \in \mathrm{Gal}(F_\infty/K)$ (see, e.g., [**17**, p.364], [**10**, p.541]). Let χ be the restriction of ϕ on Δ. For any $\mathbb{Z}_p[\Delta]$-module M, we define its χ-part M^χ as

$$\{m \in M \mid m^\delta = \chi(\delta)m \text{ for every } \delta \in \Delta\}.$$

Both $X(F_\infty)^\chi$ and $\mathfrak{X}(F_\infty)^\chi$ are also considered as Λ-modules. We define $X(F_\infty)^\chi_{\mathrm{fin}}$ similarly. In this paper, we mainly treat the χ-part version of the above questions.

Questions.

(Q1) Does either $X(F_\infty)^\chi = 0$ or $X(F_\infty)^\chi_{\mathrm{fin}} \neq 0$ hold?

(Q2) Does either $\mathfrak{X}(F_\infty)^\chi = 0$ or $\mathrm{Gal}(M(F_\infty)/L(F_\infty))^\chi \neq 0$ hold?

Note that Theorems X and Y actually give the results for the χ-part. (See [**6**, p.250], [**37**, p.551, Remark], [**17**, p.365].)

Theorem Z.

(i) *If* $\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) \geq 2$, *then* $X(F_\infty)^\chi$ *is not finite.*

(ii) *If* $\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) \geq 1$, *then* $\mathrm{Gal}(M(F_\infty)/L(F_\infty))^\chi \neq 0$.

Hence, (Q2) has an affirmative answer if $\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) \geq 1$.

1.2 - *Organization of the present paper*

Our purpose in this paper is to give criteria for (Q1) and (Q2), and prove these statements for specific elliptic curves.

We will give the criteria in Section 2, and examples in Section 3. We treat the elliptic curves of the form $y^2 = x^3 - dx$ with $p = 5$ in Section 3.2, and $y^2 = x^3 - 264d^2x + 1694d^3$ with $p = 3$ in Section 3.3. For (Q1), we found that the following cases exist.

- $X(F_\infty)^\chi$ is infinite and $X(F_\infty)^\chi_{\mathrm{fin}} = 0$ (i.e., (Q1) has a negative answer).
- $X(F_\infty)^\chi$ is infinite and $X(F_\infty)^\chi_{\mathrm{fin}} \neq 0$.
- $X(F_\infty)^\chi$ is non-trivial and finite.

On the other hand, for most of the cases we examined, (Q2) has an affirmative answer, and no negative examples for (Q2) are found at this time.

In Section 4, we will treat the case $p = 2$. We shall consider similar questions (Q1t), (Q2t) and give a partial result.

2 - Criteria for questions (Q1) and (Q2)

2.1 - *Preliminaries*

Let the notation be as in Section 1. We also define the following notation:

- $K_\mathfrak{p}$: the completion of K at $\mathfrak{p}$,
- $(F_0)_\mathfrak{P}$: the completion of F_0 at $\mathfrak{P}$,
- $O_\mathfrak{P}$: the valuation ring of $(F_0)_\mathfrak{P}$,
- $\mathcal{U}^i = 1 + \mathfrak{P}^i O_\mathfrak{P}$ (for $i = 1, 2$),
- $E(F_0)^1$: the group of units of F_0 which are congruent to 1 modulo $\mathfrak{P}$,
- $\mathcal{E}^1$: the closure of $E(F_0)^1$ in $\mathcal{U}^1$,

We fix a topological generator γ_0 of Γ, and we shall identify Λ with $\mathbb{Z}_p[[T]]$ ($\gamma_0 \mapsto 1 + T$). For a finitely generated torsion Λ-module Y, let Y^Γ be the Γ-invariant submodule of Y, Y_Γ the Γ-coinvariant quotient of Y, $\mathrm{Char}_\Lambda Y$ the characteristic ideal of Y, and Y_{fin} the maximal finite Λ-submodule of Y. For a finite group B, we denote by $|B|$ the order of B.

Let $M(F_0)$ (resp. $L(F_0)$) be the maximal abelian pro-p-extension unramified outside $\mathfrak{P}$ (resp. maximal abelian unramified p-extension) of F_0. By class field theory, we see that

$$\mathrm{Gal}(M(F_0)/L(F_0)) \cong \mathcal{U}^1/\mathcal{E}^1.$$

The $\mathfrak{P}$-adic analog of Leopoldt's conjecture for F_0 asserts that the $\mathbb{Z}_p$-rank of $\mathcal{E}^1$ is equal to the free rank of the group of global units of F_0, and this holds true since F_0/K is an abelian extension (see [**15**, p.94]). This implies that $\mathrm{Gal}(M(F_0)/F_\infty)$ is finite. Let $A(F_0)$ be the Sylow p-subgroup of the ideal class group of F_0. By taking the χ-parts, we obtain the exact sequence

$$0 \to (\mathcal{U}^1/\mathcal{E}^1)^\chi \to \mathrm{Gal}(M(F_0)/F_0)^\chi \to A(F_0)^\chi \to 0. \tag{1}$$

We note that the isomorphisms

$$\mathfrak{X}(F_\infty)^\chi_\Gamma \cong \mathrm{Gal}(M(F_0)/F_0)^\chi \quad \text{and} \quad X(F_\infty)^\chi_\Gamma \cong A(F_0)^\chi \tag{2}$$

hold. The first one is obtained from the isomorphism $\mathrm{Gal}(M(F_0)/F_0)^\chi \cong \mathrm{Gal}(M(F_0)/F_\infty)^\chi$ (cf. the proof of [**31**, Lemma 2]), and the second one follows from the fact that $\mathfrak{P}$ is the only prime which ramifies in F_∞/F_0 and it is totally ramified (see, e.g., [**39**, Theorem 5.1]). From the above facts, we see that $\mathfrak{X}(F_\infty)^\chi_\Gamma$ is finite. We also note that $X(F_\infty)^\chi = 0$ if and only if $A(F_0)^\chi = 0$.

The following results are the analog of those given in the proof of [**30**, Proposition 2], and they can be obtained by imitating the arguments. By using the structure theorem of finitely generated torsion Λ-module and the fact that $\mathfrak{X}(F_\infty)^\chi_{\mathrm{fin}} = 0$, we obtain an injective Λ-module homomorphism $\mathfrak{X}(F_\infty)^\chi \to \mathfrak{E}$ with finite cokernel, where $\mathfrak{E}$ is an elementary torsion Λ-module (see [**44**, p.351]). Since $\mathfrak{X}(F_\infty)^\chi_\Gamma$ is finite, we see that $\mathfrak{E}_\Gamma$ is also finite. Therefore, $\mathrm{Char}_\Lambda\, \mathfrak{X}(F_\infty)^\chi$ is prime to $T\Lambda$, and the same result also holds for $\mathrm{Char}_\Lambda\, X(F_\infty)^\chi$. It can be shown that $\mathfrak{E}^\Gamma = 0$, and hence $(\mathfrak{X}(F_\infty)^\chi)^\Gamma = 0$. By applying the same argument to $X(F_\infty)^\chi/X(F_\infty)^\chi_{\mathrm{fin}}$, we can also show that $(X(F_\infty)^\chi)^\Gamma = (X(F_\infty)^\chi_{\mathrm{fin}})^\Gamma$. Moreover, from the well known exact sequence involving Γ-invariants and Γ-coinvariants, we obtain the exact sequence

$$0 \to (X(F_\infty)^\chi)^\Gamma \to \mathrm{Gal}(M(F_\infty)/L(F_\infty))^\chi_\Gamma \to \mathfrak{X}(F_\infty)^\chi_\Gamma \to X(F_\infty)^\chi_\Gamma \to 0. \tag{3}$$

Remark 2.1.1. Let $(\mathcal{U}^1/\mathcal{E}^1)_{\mathrm{tor}}$ be the $\mathbb{Z}_p$-torsion subgroup of $\mathcal{U}^1/\mathcal{E}^1$. By using the argument given in [**8**, Section 4], we can show that

$$\mathrm{Gal}(M(F_0)/L(F_0)F_\infty) \cong (\mathcal{U}^1/\mathcal{E}^1)_{\mathrm{tor}}.$$

Hence, for the question on the non-triviality of $\mathrm{Gal}(M(F_\infty)/L(F_\infty))$, it also seems significant to study $(\mathcal{U}^1/\mathcal{E}^1)_{\mathrm{tor}}$ (more generally, a similar object for F_n). See also the proof of Theorem 4.1.1 (ii).

Remark 2.1.2. Concerning the above remark, the works [**1**], [**13**] may be helphul to study $(\mathcal{U}^1/\mathcal{E}^1)_{\mathrm{tor}}$. The author would like to thank Christian Maire for giving a comment about this and related topics.

2.2 - *Criteria for (Q2)*

Lemma 2.2.1 (cf. e.g., [**31**, Lemma 2]). *If* $(\mathcal{U}^1/\mathcal{E}^1)^\chi \neq 0$, *then* $\mathrm{Gal}(M(F_\infty)/L(F_\infty))^\chi \neq 0$.

Proof. Using (1), (2), (3), we see that $\mathrm{Gal}(M(F_\infty)/L(F_\infty))^\chi = 0$ implies $(\mathcal{U}^1/\mathcal{E}^1)^\chi = 0$. □

Proposition 2.2.2.

(i) *If* $\mathcal{E}^1$ *is contained in* $\mathcal{U}^2$, *then* $\mathrm{Gal}(M(F_\infty)/L(F_\infty))^\chi \neq 0$.

(ii) *If* $\mathcal{U}^1$ *contains a primitive* p*-th root of unity, then* $\mathrm{Gal}(M(F_\infty)/L(F_\infty))^\chi \neq 0$.

Proof. There is a $\mathbb{Z}_p[\Delta]$-module isomorphism

$$E[\pi] \cong \mathcal{U}^1/\mathcal{U}^2. \tag{4}$$

(See [**40**, Lemma 10.4]. Note that there the author assumed $p > 7$, however we can show that this assertion holds for $p \geq 3$. See also [**6**, Lemma 9].) Then, (i) follows from this isomorphism and Lemma 2.2.1.

We prove (ii). Assume that $\mathcal{U}^1$ contains a primitive p-th root of unity ζ_p. That is, $(F_0)_{\mathfrak{P}}$ is isomorphic to $\mathbb{Q}_p(\zeta_p)$ (see also the proof of [**6**, Lemma 12]). Since $\zeta_p\mathcal{U}^2$ generates $\mathcal{U}^1/\mathcal{U}^2$, it follows that ζ_p is contained in $(\mathcal{U}^1)^\chi$ by (4). We claim that $\mathcal{E}^1$ does not contain ζ_p. Note that the global field F_0 does not contain a primitive p-th root of unity because E has good reduction at p, see, e.g., [**40**, Corollary 3.17]. The claim follows combining this fact and the validity of the $\mathfrak{P}$-adic analog of Leopoldt's conjecture (see, e.g., [**13**, Lemma 3.1 and Corollary 3.2]), and it implies that $(\mathcal{U}^1/\mathcal{E}^1)^\chi \neq 0$. □

Remark 2.2.3. Assume that $\mathcal{U}^1$ does not contain any primitive p-th root of unity. In this case, $(\mathcal{U}^1)^\chi$ is a free $\mathbb{Z}_p$-module of rank 1. Hence, by using (4), we see $(\mathcal{U}^1)^\chi/((\mathcal{U}^1)^\chi)^p \cong \mathcal{U}^1/\mathcal{U}^2$. From this, we can see that $(\mathcal{U}^1/\mathcal{E}^1)^\chi = 0$ if and only if there is a (global) unit u of F_0 such that $u^{p-1} \not\equiv 1 \pmod{\mathfrak{P}^2}$.

Remark 2.2.4. Let $\widetilde{E}(\mathbb{F}_p)$ be the group of $\mathbb{F}_p$-rational points of the reduction of E at p. Assume that $|\widetilde{E}(\mathbb{F}_p)|$ is divisible by p. Then we can see that $\psi(\mathfrak{p}) + \overline{\psi(\mathfrak{p})} \equiv 1 \pmod{p}$, where ψ is the Grössencharacter of E over K (see, e.g., [**43**, Chapter II, Corollary 10.4.1 (b)]). By using the argument given in the proof of [**6**, Lemma 12], we see that $(F_0)_{\mathfrak{P}}$ contains a primitive p-th root of unity. Hence (Q2) has an affirmative answer by Proposition 2.2.2 (ii).

Remark 2.2.5. Let $L(E/\mathbb{Q},s)$ (resp. $L(E/K,s)$) be the complex L-function of E over $\mathbb{Q}$ (resp. over K). We assume that $L(E/\mathbb{Q},1)\neq 0$. In this situation, we can show that if the p-rank of $A(F_0)^\chi$ is odd then (Q2) has an affirmative answer. We give an outline of the proof. We first note that $L(E/K,1)$ is also not equal to 0, and then $E(K)$ is finite (see, e.g., [**6**, p.251], the proof of [**24**, Corollary 3.2]). Let $S_\pi(E/K)\subset H^1(\mathrm{Gal}(\overline{K}/K),E[\pi])$ be the Selmer group relative to π, and $S'_\pi(E/K)$ the enlarged Selmer group relative to π (see, e.g., [**34**, p.32], [**40**, Definition 6.3]). We may assume that $|\widetilde{E}(\mathbb{F}_p)|\not\equiv 0 \pmod p$ (see Remark 2.2.4). Under this assumption, we can show that $S'_\pi(E/K)\cong S_\pi(E/K)$ (see [**34**, p.35]). Note that

$$S'_\pi(E/K)\cong \mathrm{Hom}(\mathrm{Gal}(M(F_0)/F_0)^\chi, E[\pi]).$$

(See [**40**, Theorem 6.5]. In our situation, this holds even when $p=3$.) We claim that the p-rank of $S'_\pi(E/K)$ is even. Let $Ш(E/K)$ (resp. $Ш(E/\mathbb{Q})$) be the Tate-Shafarevich group of E/K (resp. $E/\mathbb{Q}$). We denote by $Ш(E/K)[\pi]$ the π-torsion subgroup of $Ш(E/K)$ (we also define $Ш(E/K)[p]$, $Ш(E/K)[\overline{\pi}]$, and $Ш(E/\mathbb{Q})[p]$ similarly). In our situation, it is known that both $|Ш(E/K)|$ and $|Ш(E/\mathbb{Q})|$ are finite ([**37**]). Then, by a result of Cassels (see, e.g., [**42**, Chapter X, Theorem 4.14]), the p-rank of $Ш(E/\mathbb{Q})$ is even. Moreover, we can show that $S_\pi(E/K)\cong Ш(E/K)[\pi]$ in our situation. We write $K=\mathbb{Q}(\sqrt{d})$ with a negative square-free integer d. Let E^d be the quadratic twist of E by d. We have the following:

$$Ш(E/K)[p]\cong Ш(E/\mathbb{Q})[p]\oplus Ш(E^d/\mathbb{Q})[p]$$

(see, e.g., [**27**, Lemma 3.1]),

$$Ш(E/\mathbb{Q})[p]\cong Ш(E^d/\mathbb{Q})[p]$$

(this was suggested by an anonymous referee of an earlier manuscript, and the author express his gratitude to him/her),

$$Ш(E/K)[p]\cong Ш(E/K)[\pi]\oplus Ш(E/K)[\overline{\pi}],\quad |Ш(E/K)[\pi]|=|Ш(E/K)[\overline{\pi}]|$$

(cf. the argument given in [**16**, p.260]). By using these results, we see that the p-rank of $Ш(E/K)[\pi]$ is even. The claim follows. Hence the p-ranks of $S'_\pi(E/K)$ and of $\mathrm{Gal}(M(F_0)/F_0)^\chi$ are even as well. Therefore if the p-rank of $A(F_0)^\chi$ is odd, then $A(F_0)^\chi$ is not isomorphic to $\mathrm{Gal}(M(F_0)/F_0)^\chi$ and $(\mathcal{U}^1/\mathcal{E}^1)^\chi\neq 0$.

2.3 - *Criteria for (Q1)*

Proposition 2.3.1. *If* $(\mathcal{U}^1/\mathcal{E}^1)^\chi=0$ *and* $\mathrm{rank}_{\mathbb{Z}}E(\mathbb{Q})\geq 1$*, then* $X(F_\infty)^\chi_{\mathrm{fin}}\neq 0$.

Proof. We first recall that $\mathrm{Gal}(M(F_\infty)/L(F_\infty))^\chi \neq 0$ by Theorem Z (ii).

The essential idea of the following argument was given to the author by Satoshi Fujii (concerning his work [**8**, Section 4]). We mention that a similar idea also can be found in, e.g., [**2**, Théorème 2.1].

Since $(\mathcal{U}^1/\mathcal{E}^1)^\chi = 0$, we see that $\mathfrak{X}(F_\infty)^\chi_\Gamma \cong X(F_\infty)^\chi_\Gamma$ by using (2) and (1). Recall also that $(\mathfrak{X}(F_\infty)^\chi)^\Gamma = 0$. From these facts and (3), we see that

$$(X(F_\infty)^\chi)^\Gamma \cong \mathrm{Gal}(M(F_\infty)/L(F_\infty))^\chi_\Gamma.$$

Since $\mathrm{Gal}(M(F_\infty)/L(F_\infty))^\chi \neq 0$, we can show that $\mathrm{Gal}(M(F_\infty)/L(F_\infty))^\chi_\Gamma \neq 0$ using Nakayama's lemma. Then, $(X(F_\infty)^\chi_{\mathrm{fin}})^\Gamma = (X(F_\infty)^\chi)^\Gamma \neq 0$. □

Corollary 2.3.2. *If $(\mathcal{U}^1/\mathcal{E}^1)^\chi = 0$, $\mathrm{rank}_\mathbb{Z} E(\mathbb{Q}) = 1$, and $|A(F_0)^\chi| = p$, then $X(F_\infty)^\chi$ is non-trivial and finite.*

Proof. Since $|A(F_0)^\chi| = p$, we see that $X(F_\infty)^\chi_{\mathrm{fin}} = 0$ or $X(F_\infty)^\chi = X(F_\infty)^\chi_{\mathrm{fin}}$ (this can be shown by using the same idea given in the first paragraph of the proof of [**29**, Theorem 2]). Under the assumption of this corollary, the former case never occurs by Proposition 2.3.1. □

For the triviality of $X(F_\infty)^\chi_{\mathrm{fin}}$, we obtain the following result (cf. [**20**, Sections 1–4]). Let κ be the restriction of ϕ on Γ (see Section 1.1). Put $r = \mathrm{rank}_\mathbb{Z} E(\mathbb{Q})$. It is known that $\mathrm{Char}_\Lambda X(F_\infty)^\chi$ is contained in $(T+1-\kappa(\gamma_0))^{r-1}\Lambda$ (see [**17**, p.366]).

Proposition 2.3.3. *Let the notation be as above. If $r \geq 2$ and $|A(F_0)^\chi| = p^{r-1}$, then $X(F_\infty)^\chi_{\mathrm{fin}} = 0$ and $\mathrm{Char}_\Lambda X(F_\infty)^\chi = (T+1-\kappa(\gamma_0))^{r-1}\Lambda$.*

Proof. Let $f(T)$ be a generator of $\mathrm{Char}_\Lambda X(F_\infty)^\chi$. It is well known that

$$\frac{|(X(F_\infty)^\chi)^\Gamma|}{|X(F_\infty)^\chi_\Gamma|} = |f(0)|_p,$$

where $|\cdot|_p$ denotes the normalized p-adic (multiplicative) absolute value (see, e.g., [**44**, Exercise 13.12]).

Recall that $X(F_\infty)^\chi_\Gamma \cong A(F_0)^\chi$ and $(X(F_\infty)^\chi)^\Gamma = (X(F_\infty)^\chi_{\mathrm{fin}})^\Gamma$. As noted above, $f(T)$ is divisible by $(T+1-\kappa(\gamma_0))^{r-1}$. Hence, if $|A(F_0)^\chi| = p^{r-1}$, then $(X(F_\infty)^\chi_{\mathrm{fin}})^\Gamma = 0$ and $\mathrm{Char}_\Lambda X(F_\infty)^\chi = (T+1-\kappa(\gamma_0))^{r-1}\Lambda$. Note that the triviality of $(X(F_\infty)^\chi_{\mathrm{fin}})^\Gamma$ implies the triviality of $X(F_\infty)^\chi_{\mathrm{fin}}$. □

Remark 2.3.4. If E and p satisfy the assumptions of the above Proposition 2.3.3, then [**10**, Conjecture 1.2] holds for E and p. However, we mention that this does not imply the validity of [**10**, Conjecture 1.1].

3 - Examples for questions (Q1) and (Q2)

3.1 - *Software used in the example computations*

The author used PARI/GP [**33**] to compute the ideal class groups, units, values of L-functions, etc. For the computation of the rank of elliptic curves given in Section 3.3, the author used Sage [**41**], in particular, `mwrank` [**7**]. In the computation on Sage, the article [**21**] was very helpful. The author also would like to thank Iwao Kimura for giving comments.

3.2 - *Examples with $K = \mathbb{Q}(\sqrt{-1})$ and $p = 5$*

In this subsection, we put $K = \mathbb{Q}(\sqrt{-1})$ and $p = 5$. An example treated in Fukuda-Komatsu [**10**] gives a negative answer for (Q1).

Example 3.2.1 (see Fukuda-Komatsu [**10**, Section 4.1]). Let E be an elliptic curve defined by the Weierstrass equation

$$y^2 = x^3 + 99x.$$

Then K, p, E satisfy (C1), (C2), (C3). It is known that $\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q})$ is 2 ([**3**, Table des valeurs des $\lambda(l^*_{\mathfrak{p},i})$: I]), and then $X(F_\infty)^\chi$ is not finite by Theorem Z (i). It is also known that $|A(F_0)| = 5$, hence the infiniteness of $X(F_\infty)^\chi$ implies that $|A(F_0)^\chi| = 5$. By Proposition 2.3.3, we see that $X(F_\infty)^\chi_{\mathrm{fin}} = 0$. Then, this is a negative example for (Q1). On the other hand, (Q2) has an affirmative answer by Theorem Z (ii). Note also that Proposition 2.3.3 gives an alternative proof of the fact (already confirmed in [**10**]) that $\mathrm{Char}_\Lambda X(F_\infty)^\chi = (T + 1 - \kappa(\gamma_0))\Lambda$.

Remark 3.2.2. In [**10**, Sections 4.2, 4.3], Fukuda and Komatsu gave examples of elliptic curves of the form $y^2 = x^3 - dx$ which satisfy that $X(F_\infty)^\chi$ is finite. Although it is not explicitly written there, these examples seem to satisfy $X(F_\infty)^\chi \neq 0$. The author confirmed this fact for two of them ($d = -1331, -2197$) by checking $A(F_0)^\chi \neq 0$.

We give an example for (Q2) with $\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) = 0$ and $X(F_\infty)^\chi \neq 0$.

Example 3.2.3. Let E be an elliptic curve defined by the Weierstrass equation

$$y^2 = x^3 - 307^2 x.$$

It is known that $L(E/\mathbb{Q}, 1) \neq 0$ (see [**36**, Theorem 1]), and the author checked that $|A(F_0)| = |A(F_0)^\chi| = 5$. Then the criterion given in Remark 2.2.5 is applicable, and hence this is a non-trivial example in which (Q2) has an affirmative answer. Note that one can also check the non-triviality of $(\mathcal{U}^1/\mathcal{E}^1)^\chi$ by using a more direct method (Remark 2.2.3). We also remark that Proposition 2.2.2 (ii) is not applicable for this example.

Remark 3.2.4. Concerning Remark 3.2.2 and Example 3.2.3, the author computed $|A(F_0)^\chi|$ with a help of PARI/GP and several known results. An explicit Kummer generator of F_0 over K is given in [**10**, p.547]. One way to check $A(F_0)^\chi \neq 0$ is to observe the Δ-action on an ideal class. For the case of Remark 3.2.2, the author also used another method referring to the data given in [**3**, Table des valeurs des $\lambda(l^*_{\mathfrak{p},i})$: I] and computing the ideal class group of the quadratic intermediate field of F_0/K. For Example 3.2.3, the full Birch and Swinnerton-Dyer conjecture holds for E (see [**38**, p.26, Theorem]), and there is another way of checking $A(F_0)^\chi \neq 0$ by computing the analytic order of $\text{Ш}(E/\mathbb{Q})$. (See Remark 2.2.5. See also the proof of [**40**, Corollary 6.10].)

3.3 - *Examples with* $K = \mathbb{Q}(\sqrt{-11})$ *and* $p = 3$

Let $E^d_\circ$ be an elliptic curve defined by the Weierstrass equation

$$y^2 = x^3 - 264d^2x + 1694d^3,$$

where d is a non-zero square-free integer. We put $K = \mathbb{Q}(\sqrt{-11})$ and $p = 3$. It is well known that $E^d_\circ$ has complex multiplication by O_K (see, e.g., [**19**]). Note also that $E^d_\circ$ has good reduction at $p = 3$ if and only if $d \equiv 0 \pmod 3$ (see [**19**]). We also note that $E^d_\circ$ and $E^{-11d}_\circ$ are isomorphic over K. Hence, in the remaining part of this subsection, we assume

(D1) d is a square-free integer satisfying $d \equiv 0 \pmod 3$ and $d \not\equiv 0 \pmod{11}$.

Then, under (D1), K, p, $E^d_\circ$ satisfy (C1), (C2), (C3). We choose $\mathfrak{p}$ as the prime generated by $(-1-\sqrt{-11})/2$. We put $d' = d/3$, then

$$F_0 = K\left(\sqrt{d'\,(11 - \sqrt{-11})}\right).$$

This can be obtained using an explicit endomorphism given in [**35**, Theorem 3]. (However, it seems that the multiplication by $(-1+\sqrt{-11})/2$ endomorphism given in [**35**, Theorem 3] is actually the multiplication by $(-1-\sqrt{-11})/2$ endomorphism.)

Let $\overline{\mathfrak{p}}$ be the conjugate of $\mathfrak{p}$. Then, $\overline{\mathfrak{p}}$ is unramified in F_0. Moreover, we can see that $\overline{\mathfrak{p}}$ splits completely in F_0 if and only if $d' \equiv 1 \pmod 3$ (i.e., $d \equiv 3 \pmod 9$). We also note that $\mathcal{U}^1$ contains a primitive third root of unity if and only if $\overline{\mathfrak{p}}$ splits completely in F_0. Hence, by Proposition 2.2.2 (ii), we have the following result.

- If $d \equiv 3 \pmod 9$, then (Q2) has an affirmative answer for $E_\circ^d$.

Let $L(E_\circ^d/\mathbb{Q}, s)$ be the complex L-function of $E_\circ^d$ over $\mathbb{Q}$. We note that if $d > 0$, then the root number of $E_\circ^d$ is -1 (see [**18**, Theorem 19.1.1]) and $L(E_\circ^d/\mathbb{Q}, 1) = 0$.

We shall give several examples for the case $d \equiv 6 \pmod 9$. First, we shall consider (Q2). For this question, we can use Theorem Z (ii) and Proposition 2.2.2. Recall that if $d \equiv 6 \pmod 9$ then $\mathcal{U}^1$ does not contain a primitive third root of unity. We can check whether $(\mathcal{U}^1/\mathcal{E}^1)^\chi = 0$ or not by using the method stated in Remark 2.2.3.

Example 3.3.1. Assume that $d > 0$ and $d \equiv 6 \pmod 9$. In the range $1 < d < 3000$, the following values satisfy $|A(F_0)^\chi| \neq 1$.

$$\begin{aligned} d = \ & 78, 87, 141, 177, 186, 195, 213, 285, 357, 366, \\ & 393, 447, 501, 510, 537, 609, 699, 717, 753, 807, \\ & 843, 861, 870, 915, 942, 969, 987, 1005, 1149, 1167, \\ & 1203, 1230, 1293, 1365, 1374, 1482, 1545, 1554, 1635, 1662, \\ & 1689, 1707, 1779, 1842, 1851, 1887, 1923, 1959, 2085, 2121, \\ & 2139, 2202, 2247, 2301, 2346, 2454, 2463, 2481, 2490, 2562, \\ & 2571, 2589, 2634, 2679, 2715, 2769, 2877, 2922, 2949, 2967, 2985. \end{aligned} \tag{5}$$

Recall that $L(E_\circ^d/\mathbb{Q}, 1) = 0$ in this situation. Hence, if $L'(E_\circ^d/\mathbb{Q}, 1) \neq 0$, we see that $\operatorname{rank}_{\mathbb{Z}} E_\circ^d(\mathbb{Q}) = 1$ ([**37**, Corollary C]). For the above values, the condition $L'(E_\circ^d/\mathbb{Q}, 1) \neq 0$ is satisfied except for the cases $d = 141, 807, 2121$. Moreover, for these 3 values, the author checked that $\operatorname{rank}_{\mathbb{Z}} E_\circ^d(\mathbb{Q}) = 3$. Hence, for the values of d listed above, (Q2) has an affirmative answer by Theorem Z (ii). For $d = 141, 807, 2121$, it can be checked that $(\mathcal{U}^1/\mathcal{E}^1)^\chi \neq 0$, and hence Lemma 2.2.1 is applicable.

Example 3.3.2. Assume that $d < 0$ and $d \equiv 6 \pmod 9$. In the range $-3000 < d < 0$, the following 48 values of d satisfy $|A(F_0)^\chi| \neq 1$.

$$\begin{aligned} d = \ & -2955, -2910, -2874, -2847, -2757, -2730, -2703, -2649, \\ & -2613, -2559, -2514, -2478, -2469, -2433, -2361, -2298, \\ & -2271, -2262, -2154, -2109, -2010, -1974, -1965, -1758, \\ & -1731, -1695, -1623, -1461, -1281, -1263, -1227, -1137, \\ & -1119, -1110, -1065, -1038, -1002, -993, -678, -651, \\ & -489, -399, -390, -327, -255, -174, -93, -21. \end{aligned} \tag{6}$$

The 45 values different from $-2910, -2361, -1731$ satisfy $(\mathcal{U}^1/\mathcal{E}^1)^\chi \neq 0$, then (Q2) has an affirmative answer for these values. From the computation of approximate values, we can expect that $L(E_\circ^d/\mathbb{Q},1)=0$ for several values in the above list (see Example 3.3.4). In particular, for the case $d=-2361$, we will later see that $\operatorname{rank}_{\mathbb{Z}} E_\circ^d(\mathbb{Q})=2$, and hence this is also an affirmative example for (Q2).

Next, we consider (Q1).

Example 3.3.3. We go back to the situation treated in Example 3.3.1. For the values given in (5), $\operatorname{rank}_{\mathbb{Z}} E_\circ^d(\mathbb{Q})\geq 1$. Moreover, if $(\mathcal{U}^1/\mathcal{E}^1)^\chi=0$ then (Q1) has an affirmative answer by Proposition 2.3.1. Among the values in (5), the following ones satisfy $(\mathcal{U}^1/\mathcal{E}^1)^\chi=0$.

$$\begin{aligned} d=\ & 78,87,186,195,213,285,393,447,501,510,537,609,699,717,\\ & 753,861,870,915,969,987,1005,1167,1230,1293,1365,1482,\\ & 1545,1635,1662,1707,1779,1842,1851,1887,1923,1959,2085,\\ & 2139,2247,2454,2463,2481,2562,2571,2634,2679,2715,2769,\\ & 2877,2922,2967,2985. \end{aligned}$$

Note that all of these values satisfy $\operatorname{rank}_{\mathbb{Z}} E_\circ^d(\mathbb{Q})=1$. In addition, if $|A(F_0)^\chi|=3$, then $X(F_\infty)^\chi$ is non-trivial and finite by Corollary 2.3.2. In the above list, the condition $|A(F_0)^\chi|=3$ is satisfied except for the cases $d=1167,1482,2247$.

We provide now several negative examples for (Q1).

Example 3.3.4. As noted in Example 3.3.2, for several values of d in (6), we can expect $L(E_\circ^d/\mathbb{Q},1)$ to be 0 from its approximate value. Such values are the following:

$$\begin{aligned} d=\ & -2874,-2847,-2730,-2703,-2649,-2514,-2361,-2271,\\ & -2154,-1974,-1965,-1758,-1119,-1002,-651,-489,\\ & -399,-390,-255,-174,-21. \end{aligned}$$

The author checked that $\operatorname{rank}_{\mathbb{Z}} E_\circ^d(\mathbb{Q})=2$ for all of the above values. Hence, for these values, we see that $X(F_\infty)^\chi$ is infinite by Theorem Z (i). Moreover, if $|A(F_0)^\chi|=3$, then $X(F_\infty)^\chi_{\mathrm{fin}}=0$ and $\operatorname{Char}_\Lambda X(F_\infty)^\chi=(T+1-\kappa(\gamma_0))\Lambda$ by Proposition 2.3.3. In the above list, we have $|A(F_0)^\chi|=3$ except for the cases $d=-2703,-2361$.

Example 3.3.5. We consider $d=141,807,2121$. Recall that $\operatorname{rank}_{\mathbb{Z}} E_\circ^d(\mathbb{Q})=3$ for these values (see Example 3.3.1). Moreover, it can be checked that $|A(F_0)^\chi|=9$ for all of these values. Then we see that $X(F_\infty)^\chi_{\mathrm{fin}}=0$ and $\operatorname{Char}_\Lambda X(F_\infty)^\chi=(T+1-\kappa(\gamma_0))^2\Lambda$ by Proposition 2.3.3.

The above Example 3.3.5 gives examples of rank 3 elliptic curves for which [**10**, Conjecture 1.2] is valid.

Remark 3.3.6. We can also find examples satisfying $X(F_\infty)^\chi$ is infinite and $X(F_\infty)^\chi_{\mathrm{fin}} = 0$ for the case $d \equiv 3 \pmod 9$. For instance, $d = -159, -114, -51$.

We provide a final positive example for (Q1) where $X(F_\infty)^\chi$ is infinite and $X(F_\infty)^\chi_{\mathrm{fin}} \neq 0$.

Example 3.3.7. We consider $d = -2361$. Recall that $\mathrm{rank}_{\mathbb{Z}} E_\circ^{-2361}(\mathbb{Q}) = 2$, and hence $X(F_\infty)^\chi$ is infinite (Example 3.3.4). In this case, $(\mathcal{U}^1/\mathcal{E}^1)^\chi = 0$ (Example 3.3.2). Thus, by Proposition 2.3.1, we see that $X(F_\infty)^\chi_{\mathrm{fin}} \neq 0$.

As a conclusion of this subsection, for the case of $E_\circ^d$ with an integer d satisfying (D1), we have confirmed the following:

- In the range $-3000 < d < 3000$, (Q2) has an affirmative answer except for the cases $d = -2910, -1731$ (for which our criteria do not apply). It is likely that (Q2) holds for these two values as well.
- Similar to the situation treated in Section 3.2, both affirmative and negative examples exist for (Q1).

4 - Similar questions for the case $p = 2$

4.1 - *Questions and results*

In this section, we fix $K = \mathbb{Q}(\sqrt{-7})$ and $p = 2$. For a non-zero square free integer d, let E_*^d be the elliptic curve over $\mathbb{Q}$ defined by the equation

$$y^2 = x^3 + 21dx^2 + 112d^2x.$$

It is well known that E_*^d has complex multiplication by O_K. This situation is well studied, and we recall several facts. Note that E_*^d has good reduction at 2 if and only if $d \equiv 1 \pmod 4$ (see, e.g., [**19**]). Moreover, if d is prime to 7, then E_*^d is isomorphic to E_*^{-7d} over K (see, e.g., [**42**, Chapter X], [**12**, Section 7], [**24**, Section 2]). Hence, we assume

(D2) d is a square-free integer satisfying $d \equiv 1 \pmod 4$ and $d \not\equiv 0 \pmod 7$.

Recall that $p = 2$ splits in K, and the class number of K is 1. Let $\mathfrak{p}$ be a prime of K lying above 2. We denote by ψ the Grössencharacter of E_*^d over K, and put $\pi = \psi(\mathfrak{p})$. We also put $F_n = K(E_*^d[\pi^{n+2}])$ for all $n \geq 0$. Note that this definition of F_n is slightly different from the case $p \geq 3$. Then F_0/K is a quadratic extension (see, e.g., [**12**, Section 2], [**4**]). It is known that F_n/K is totally ramified at $\mathfrak{p}$ (see, e.g., [**37**, (3.6)Proposition (i)], [**4**]). We denote by $\mathfrak{P}$ the unique prime of F_0 lying above $\mathfrak{p}$. We put $F_\infty = \bigcup_n F_n$, then F_∞/F_0 is a $\mathbb{Z}_2$-extension unramified outside $\mathfrak{P}$.

In the following, we choose $\mathfrak{p}$ as the prime generated by $(-1-\sqrt{-7})/2$. It is known that

$$F_0 = K(\sqrt{d\sqrt{-7}}) \tag{7}$$

(see [**4**, Lemma 2.2], however notice the difference in the choice of $\mathfrak{p}$).

We define the notation Γ, Λ, $X(F_\infty)$, $\mathfrak{X}(F_\infty)$, $M(F_\infty)$, $L(F_\infty)$, etc. as in previous sections. In this section, we shall consider the following:

Questions. Let the notation be as in the previous paragraphs, and assume that d satisfies (D2).

(Q1t) Does either $X(F_\infty) = 0$ or $X(F_\infty)_{\mathrm{fin}} \neq 0$ hold?

(Q2t) Does either $\mathfrak{X}(F_\infty) = 0$ or $\mathrm{Gal}(M(F_\infty)/L(F_\infty)) \neq 0$ hold?

Concerning the above questions, we shall show the following:

Theorem 4.1.1. *Assume that d satisfies* (D2).

(i) *If* $d \equiv 5 \pmod 8$, *then* (Q1t) *has an affirmative answer for* E_*^d.

(ii) *Suppose that* $d \equiv 1 \pmod 8$. *If* $\mathrm{Gal}(M(F_\infty)/L(F_\infty)) \neq 0$, *then* $X(F_\infty)_{\mathrm{fin}} \neq 0$.

Similar to the case $p \geq 3$, if (Q1t) has an affirmative answer then (Q2t) also has, because $\mathfrak{X}(F_\infty)_{\mathrm{fin}} = 0$ ([**15**, p.94]). For the case $d \equiv 1 \pmod 8$, if (Q2t) has an affirmative answer then (Q1t) also has. That is, the above theorem also says that the case "(Q2t) is affirmative but (Q1t) is negative" does not occur.

One can also show an analog of Theorem Y for this situation. That is, (Q2t) has an affirmative answer if $\mathrm{rank}_{\mathbb{Z}} E_*^d(\mathbb{Q}) \geq 1$. This can be shown by slightly modifying the argument given in [**6**], however, we omit the details. By combining this fact and Theorem 4.1.1, we obtain the following:

Corollary 4.1.2. *Assume that d satisfies* (D2). *If* $\mathrm{rank}_{\mathbb{Z}} E_*^d(\mathbb{Q}) \geq 1$, *then* (Q1t) *has an affirmative answer for* E_*^d.

Remark 4.1.3. The analog of Theorem X also holds for this setting. We can show this by modifying the method presented in [**11**] (see also [**37**, p.551, Remark]).

Remark 4.1.4. As noted in [**12**, Section 7], it is known that $L(E_*^d, 1) = 0$ when $d < 0$ (recall that $d \not\equiv 0 \pmod 7$). Hence, $\operatorname{rank}_{\mathbb{Z}} E_*^d(\mathbb{Q})$ is expected to be positive for this case. We also mention that a sufficient condition to have $\operatorname{rank}_{\mathbb{Z}} E_*^d(\mathbb{Q}) = 1$ is given in [**5**, Theorem 1.4].

Remark 4.1.5. The $\mathbb{Z}_2$-rank of $\mathfrak{X}(F_\infty)$ was considered in [**4**], [**23**]. These results seem helpful for future research on our questions (Q1t), (Q2t).

4.2 - *Proof of Theorem 4.1.1*

Let the notation be as in Section 4.1. Recall that F_0/K is totally ramified at $\mathfrak{p}$, and $\mathfrak{P}$ is the unique prime of F_0 lying above $\mathfrak{p}$. Let $\mathrm{cl}(\mathfrak{P})$ be the ideal class of F_0 containing $\mathfrak{P}$. We note that the order of $\mathrm{cl}(\mathfrak{P})$ is equal to 1 or 2 because the class number of K is 1.

Lemma 4.2.1. *Assume that d satisfies* (D2). *If* $\mathrm{cl}(\mathfrak{P})$ *is not trivial, then* $X(F_\infty)_{\mathrm{fin}} \neq 0$.

Proof. For $n \geq 0$, let $A(F_n)$ be the Sylow 2-subgroup of the ideal class group of F_n, and D_n the subgroup of $A(F_n)$ consisting of the classes containing a power of the prime lying above $\mathfrak{P}$. Note that $\mathrm{cl}(\mathfrak{P})$ is contained in D_0. Assume that $\mathrm{cl}(\mathfrak{P})$ is not trivial.

In our situation, we can see that $|A(F_n)^{\mathrm{Gal}(F_n/F_0)}|$ is bounded with respect to n (cf. the proof of [**14**, Theorem 1]), and then $|D_n|$ is also bounded. From this, we can show that $\mathrm{cl}(\mathfrak{P})$ capitulates in F_n if n is sufficiently large (cf. [**14**, p.267]). Thus, by using [**28**, p.218, Proposition], we see that $X(F_\infty)_{\mathrm{fin}} \neq 0$. □

We also show the following lemma. This can be seen as the analog of [**32**, Lemma 2].

Lemma 4.2.2. *Assume that d satisfies* (D2). *If d has a rational prime divisor ℓ which satisfies $\ell \equiv \pm 3 \pmod 8$, then* $\mathrm{cl}(\mathfrak{P})$ *is not trivial.*

Proof. We put $\ell^* = \ell$ or $-\ell$ so that ℓ^* satisfies $\ell^* \equiv 1 \pmod 4$. Then $K(\sqrt{\ell^*})/K$ is unramified outside the primes lying above ℓ^*, and every prime of K lying above ℓ^* is totally ramified in $K(\sqrt{\ell^*})$.

We note that every prime of K lying above ℓ also ramifies in F_0. Since the prime of K lying above 7 is ramified in F_0, $K(\sqrt{\ell^*})$ and F_0 are disjoint. (See (7)).

Note that every prime of K lying above ℓ is tamely ramified in $F_0(\sqrt{\ell^*})$. Combining the above results, we see that $F_0(\sqrt{\ell^*})/F_0$ is unramified.

On the other hand, the rational prime 2 is inert in $\mathbb{Q}(\sqrt{\ell^*})$. Since 2 splits in K and $\mathfrak{p}$ ramifies in F_0, we see that $\mathfrak{P}$ is inert in the unramified quadratic extension $F_0(\sqrt{\ell^*})/F_0$. Then, by class field theory, $\mathrm{cl}(\mathfrak{P})$ is not trivial. $\square$

We now give a proof of Theorem 4.1.1 (i). Since $d \equiv 5 \pmod 8$, there is a rational prime divisor ℓ of d which satisfies $\ell \equiv \pm 3 \pmod 8$. Then the assertion follows from Lemmas 4.2.1 and 4.2.2.

In the rest of this subsection, we give a proof of Theorem 4.1.1 (ii). We define $(F_0)_{\mathfrak{P}}$, $\mathcal{U}^1$, $E(F_0)^1$, and $\mathcal{E}^1$ similar to the case $p \geq 3$ (see Section 2.1).

Lemma 4.2.3. *Assume that d satisfies* (D2) *and* $d \equiv 1 \pmod 8$. *If $\mathfrak{P}$ is principal, then $\mathcal{U}^1/\mathcal{E}^1$ has no non-trivial $\mathbb{Z}_2$-torsion element.*

Proof. We mention that a quite similar result in a slightly different situation was given in [**22**, Theorem 1 (2) and Lemma 5 (2)]. The field $\mathbb{Q}(\sqrt[4]{-q})$ with a prime number q satisfying $q \equiv 7 \pmod{16}$ was considered in [**22**]. Our case is $F_0 = \mathbb{Q}(\sqrt[4]{-7d^2})$ with $d \equiv 1 \pmod 8$. Our result can be also shown by using the same argument, and hence we only give an outline of the proof.

By taking a suitable generator γ of $\mathfrak{P}$, we can see that the group of units of F_0 is generated by -1 and $\eta = \gamma^2/2$ (see the proof of [**22**, Lemma 5]). Let $\mathrm{ord}_{\mathfrak{P}}(\cdot)$ be the normalized (additive) valuation at $\mathfrak{P}$, then

$$\mathrm{ord}_{\mathfrak{P}}(\eta^2 - 1) = 2 \qquad \text{and} \qquad \mathrm{ord}_{\mathfrak{P}}(\eta - 1) = \mathrm{ord}_{\mathfrak{P}}(-\eta - 1) = 1.$$

We can see that the torsion units of $\mathcal{U}^1$ are ± 1. (Note that $(F_0)_{\mathfrak{P}}$ is isomorphic to $\mathbb{Q}_2(\sqrt{3})$ when $d \equiv 1 \pmod 8$. See also [**22**].) From these facts, we can see that $\mathcal{U}^1/\mathcal{E}^1$ has no non-trivial $\mathbb{Z}_2$-torsion element. $\square$

We finish the proof of Theorem 4.1.1 (ii). If $\mathrm{cl}(\mathfrak{P})$ is not trivial, then $X(F_\infty)_{\mathrm{fin}} \neq 0$ by Lemma 4.2.1. Hence, in the following, we assume that $\mathrm{cl}(\mathfrak{P})$ is trivial. Similar to the proof of Proposition 2.3.1, we use the argument given in [**8**, Section 4]. Under the above assumption, we see that $\mathcal{U}^1/\mathcal{E}^1$ has no non-trivial $\mathbb{Z}_2$-torsion element by Lemma 4.2.3. From this, we see that $\mathfrak{X}(F_\infty)_\Gamma \cong X(F_\infty)_\Gamma$, and then

$$X(F_\infty)_{\mathrm{fin}}^\Gamma = X(F_\infty)^\Gamma \cong \mathrm{Gal}(M(F_\infty)/L(F_\infty))_\Gamma.$$

(We used the validity of the $\mathfrak{P}$-adic analog of Leopoldt's conjecture for F_0 and the fact that $\mathfrak{X}(F_\infty)_{\mathrm{fin}} = 0$.) The assertion follows from this. $\square$

Acknowledgments. This research was born out of the discussions with Satoshi Fujii. In particular, the ideas concerning the results of [**8**] were one of the motivations to start this study. The author thanks him. The author also wishes to express his gratitude to Takashi Fukuda for his kind responses to the inquiries about computation, and to Keiichi Komatsu for his encouragement. They also gave significant comments on an earlier manuscript. The author also would like to thank Jianing Li for sending a manuscript of a stronger version of [**22**] and giving information about his results. The author also would like to express his gratitude to the referee of an earlier manuscript (who seems different from the person mentioned in Remark 2.2.5). His/her comments motivated the author to improve the contents of this paper. Finally, the author would like to thank the referee of this journal for giving many suggestions to improve the exposition.

References

[**1**] J. Assim and T. Nguyen Quang Do, *Sur la constante de Kummer-Leopoldt d'un corps de nombres*, Manuscripta Math. **115** (2004), 55–72.

[**2**] R. Badino and T. Nguyen Quang Do, *Sur les égalités du miroir et certaines formes faibles de la conjecture de Greenberg*, Manuscripta Math. **116** (2005), 323–340.

[**3**] D. Bernardi, C. Goldstein and N. Stephens, *Notes p-adiques sur les courbes elliptiques*, J. Reine Angew. Math. **351** (1984), 129–170.

[**4**] J. Choi and J. Coates, *Iwasawa theory of quadratic twists of* $X_0(49)$, Acta Math. Sin. (Engl. Ser.) **34** (2018). 19–28.

[**5**] J. Coates, Y. Li, Y. Tian and S. Zhai, *Quadratic twists of elliptic curves*, Proc. Lond. Math. Soc. **110** (2015), 357–394.

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

[**7**] J. E. Cremona, `mwrank` and `eclib`, `http://homepages.warwick.ac.uk/staff/J.E.Cremona/mwrank/index.html`.

[**8**] S. Fujii, *Some remarks on finite submodules of the unramified Iwasawa module of totally real fields*, Proc. Japan Acad. Ser. A Math. Sci. **96** (2020), 83–85.

[**9**] S. Fujii and T. Itoh, *Some remarks on pseudo-null submodules of tamely ramified Iwasawa modules*, J. Théor. Nombres Bordeaux **30** (2018), 533–555.

[**10**] T. Fukuda and K. Komatsu, $\mathbb{Z}_p$*-extensions associated to elliptic curves with complex multiplication*, Math. Proc. Cambridge Philos. Soc. **137** (2004), 541–550.

[**11**] T. Fukuda, K. Komatsu and S. Yamagata, *Iwasawa* λ*-invariants and Mordell-Weil ranks of abelian varieties with complex multiplication*, Acta Arith. **127** (2007), 305–307.

[**12**] C. D. Gonzalez-Avilés, *On the conjecture of Birch and Swinnerton-Dyer*, Trans. Amer. Math. Soc. **349** (1997), 4181–4200.

[13] G. Gras, *The p-adic Kummer-Leopoldt constant: normalized p-adic regulator*, Int. J. Number Theory **14** (2018), 329–337.

[14] R. Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. **98** (1976), 263–284.

[15] R. Greenberg, *On the structure of certain Galois groups*, Invent. Math. **47** (1978), 85–99.

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

[17] R. Greenberg, *Iwasawa theory – past and present*, Class field theory – its centenary and prospect (Tokyo, 1998), Adv. Stud. Pure. Math., **30**, Math. Soc. Japan, Tokyo, 2001, 335–385.

[18] B. H. Gross, *Arithmetic on elliptic curves with complex multiplication*, with an appendix by B. Mazur, Lecture Notes in Math., **776**, Springer, Berlin, 1980.

[19] T. Hadano, *Conductor of elliptic curves with complex multiplication and elliptic curves of prime conductor*, Proc. Japan Acad. **51** (1975), 92–95.

[20] T. Itoh, *Tamely ramified Iwasawa modules having no non-trivial pseudo-null submodules*, J. Théor. Nombres Bordeaux **30** (2018), 859–872.

[21] I. Kimura, *Sage for number theorists*, (Japanese. English summary), Algebraic number theory and related topics 2010, RIMS Kôkyûroku Bessatsu, **B32**, Research Institute for Mathematical Sciences (RIMS), Kyoto, 2012,125–144.

[22] J. Li, *On the* 2*-adic logarithm of units if certain totally imaginary quartic fields*, Asian J. Math. **25** (2021), 177–182.

[23] J. Li, *On the λ-invariant of Selmer groups arising from certain quadratic twists of Gross curves*, arXiv:2107.03027, preprint, 2021.

[24] R. L. Miller, *Proving the Birch and Swinnerton-Dyer conjecture for specific elliptic curves of analytic rank zero and one*, LMS J. Compt. Math. **14** (2011), 327–350.

[25] T. Nguyen Quang Do, *Sur la conjecture faible de Greenberg dans le cas abélien p-décomposé*, Int. J. Number Theory **2** (2006), 49–64.

[26] T. Nguyen Quang Do, *Sur une forme faible de la conjecture de Greenberg II*, Int. J. Number Theory **13** (2017), 1061–1070.

[27] K. Ono and M. A. Papanikolas, *Quadratic twists of modular forms and elliptic curves*, Number theory for the millennium, III (Urbana, IL, 2000), A K Peters, Natick, MA, 2002, 73–85.

[28] M. Ozaki, *A note on the capitulation in $\boldsymbol{Z}_p$-extensions*, Proc. Japan Acad. Ser. A Math. Sci. **71** (1995), 218–219.

[29] M. Ozaki, *On the cyclotomic unit group and the ideal class group of a real abelian number field II*, J. Number Theory **64** (1997), 223–232.

[30] M. Ozaki, *The class group of $\boldsymbol{Z}_p$-extensions over totally real number fields*, Tôhoku Math. J. (2) **49** (1997), 431–435.

[31] M. Ozaki and H. Taya, *A note on Greenberg's conjecture for real abelian number fields*, Manuscripta Math. **88** (1995), 311–320.

[32] M. Ozaki and H. Taya, *On the Iwasawa λ_2-invariants of certain families of real quadratic fields*, Manuscripta Math. **94** (1997), 437–444.

[33] The PARI-Group, *PARI/GP version* `2.13.1`, Univ. Bordeaux, 2021, `http://pari.math.u-bordeaux.fr/`.

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

[35] A. R. Rajwade, *Some formulae for elliptic curves with complex multiplication*, Indian J. Pure Appl. Math. **8** (1977), 379–387.

[36] M. J. Razar, *The non-vanishing of $L(1)$ for certain elliptic curves with no first descents*, Amer. J. Math. **96** (1974), 104–126.

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

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

[39] K. Rubin, *The one-variable main conjecture for elliptic curves with complex multiplication*, L-functions and arithmetic (Durham, 1989), London Math. Soc. Lecture Note Ser., **153**, Cambridge University Press, Cambridge, 1991, 353–371.

[40] K. Rubin, *Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer*, Arithmetic theory of elliptic curves (Cetraro, 1997), Lecture Notes in Math., **1716**, Springer-Verlag, Berlin, 1999, 167–234.

[41] The Sage Developers, *SageMath*, the Sage Mathematics Software System (Version 9.2), 2020, `https://www.sagemath.org`.

[42] J. H. Silverman, *The arithmetic of elliptic curves*, Grad. Texts in Math., **106**, Springer-Verlag, New York, 1986. Corrected 2nd printing, 1992.

[43] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Grad. Texts in Math., **151**, Springer-Verlag, New York, 1994. Corrected second printing, 1999.

[44] L. C. Washington, *Introduction to cyclotomic fields*, Second ed., Grad. Texts in Math., **83**, Springer-Verlag, New York, 1997.

Tsuyoshi Itoh
Division of Mathematics, Education Center
Faculty of Social Systems Science
Chiba Institute of Technology
2–1–1 Shibazono, Narashino
Chiba, 275–0023, Japan
e-mail: tsuyoshi.itoh@it-chiba.ac.jp