ON THE UNRAMIFIED IWASA W A MODULE OF A $\mathbb{Z}_p$-EXTENSION GENERATED BY DIVISION POINTS OF A CM ELLIPTIC CURVE

TSUYOSHI ITOH

Abstract. We consider the unramified Iwasawa module $X(F_\infty)$ of a certain $\mathbb{Z}_p$-extension $F_\infty/F_0$ 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.

1. Introduction

1.1. Our questions. First at all, we explain the situation which we will treat. In this paper (except for Appendix [A]), 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 two distinct primes $p$ and $\overline{p}$ in $K$,
(C3) $E$ is an elliptic curve over $\mathbb{Q}$ which has complex multiplication by the ring $O_K$ of integers of $K$, and $E$ has good reduction at $p$.

In the following, we assume that $K$, $p$, $E$ satisfy (C1), (C2), (C3). Many authors treated this situation (or similar situations). See, e.g., [8], [4], [15], [54], [49], [50], [21, Section 5], [13], etc.

We shall recall several known facts (see, e.g., [8], [4], [21, pp.364–365], [13, Section 1]). Let $\psi$ be the Grössencharacter of $E$ over $K$, and put $\pi = \psi(p)$. Then, $\pi$ is a generator of the principal ideal $p$. For every non-negative integer $n$, let $E[\pi^{n+1}] \subset E(\overline{\mathbb{Q}})$ be the group of $\pi^{n+1}$-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 $p$ is totally ramified in $F_n/K$. We also put $F_\infty = \bigcup_n F_n$. It is known that

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

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

We denote by $L(F_\infty)/F_\infty$ the maximal unramified abelian pro-$p$ extension and $M(F_\infty)/F_\infty$ the maximal abelian pro-$p$ extension unramified outside the unique prime lying above $p$. We put $X(F_\infty) = \text{Gal}(L(F_\infty)/F_\infty)$ (the unramified Iwasawa module) and $\mathfrak{X}(F_\infty) = \text{Gal}(M(F_\infty)/F_\infty)$ (the $p$-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 $\Lambda$-module.

We note that $\mathfrak{X}(F_\infty)$ is also a finitely generated torsion $\Lambda$-module because the “$\mathfrak{p}$-adic analog” of Leopoldt’s conjecture holds for $F_0$ (see Section 2 for the detail). Recall
that a similar property holds for the “p-ramified Iwasawa module” of the cyclotomic $\mathbb{Z}_p$-extension of real abelian fields. (For these topics, see [19]). We also mention that $X(F_\infty)$ is finitely generated as a $\mathbb{Z}_p$-module (see [15], [51], [57]), and a similar fact for the p-ramified Iwasawa module of the cyclotomic $\mathbb{Z}_p$-extension of real abelian fields (with odd $p$) follows from Ferrero-Washington’s theorem [10] and Kummer duality. Furthermore, the main conjecture holds for this situation (see [19], [50]), and the statement is similar to that of the even part version of the main conjecture for abelian fields (rather than the odd part version). (Cf., e.g., [31], Appendix by Karl Rubin). Hence, it might be said that $F_\infty/F_0$ is close to the cyclotomic $\mathbb{Z}_p$-extension of real abelian fields in some sense. We would like to know how many properties these $\mathbb{Z}_p$-extensions have in common.

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 [18]). On the other hand, it is known that $X(F_\infty)$ can be infinite in general. We denote by $\text{rank}_\mathbb{Z} E(\mathbb{Q})$ the free rank of the Mordell-Weil group $E(\mathbb{Q})$.

**Theorem X** (see p.551, Remark of Rubin [18], pp.364–366 of Greenberg [21]). Assume that $K$, $p$, $E$ satisfy (C1), (C2), (C3). If $\text{rank}_\mathbb{Z} E(\mathbb{Q}) \geq 2$, then $X(F_\infty)$ is not finite.

Hence, under Greenberg’s conjecture, $F_\infty/F_0$ is different from the cyclotomic $\mathbb{Z}_p$-extension of a real abelian fields on this point.

We also note that “weak forms” of Greenberg’s conjecture are considered by several authors (see [27], [24], [43], [2], [33], [34], [11], etc.). Based on these studies, we shall consider the following questions. These are analogs of weak forms of Greenberg’s conjecture treated in [33], [34] (see also [35]). We denote by $X(F_\infty)_{\text{fin}}$ the maximal finite $\Lambda$-submodule of $X(F_\infty)$.

- When $X(F_\infty)$ is not trivial, is $X(F_\infty)_{\text{fin}}$ not trivial?
- When $X(F_\infty)$ is not trivial, is $\text{Gal}(M(F_\infty)/L(F_\infty))$ not trivial?

**Remark 1.1.1.** In [25, Appendix A], similar questions for “tamely ramified Iwasawa modules” of the cyclotomic $\mathbb{Z}_p$-extension of a totally real field are considered. See also [12].

**Remark 1.1.2.** It is known that $X(F_\infty)$ does not have a non-trivial finite $\Lambda$-submodule (see [19], p.94]). Hence if $X(F_\infty)_{\text{fin}}$ is not trivial, then $\text{Gal}(M(F_\infty)/L(F_\infty))$ is also not trivial (cf., e.g., [33, Lemme 2.1]).

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

**Theorem Y** (see Lemma 35 of Coates-Wiles [8]). Assume that $K$, $p$, $E$ satisfy (C1), (C2), (C3). If $\text{rank}_\mathbb{Z} E(\mathbb{Q}) \geq 1$, then $\text{Gal}(M(F_\infty)/L(F_\infty))$ is not trivial.

Strictly speaking, it was assumed that $p \geq 5$ in [8]. However, one can also show the same assertion for $p = 3$ similarly. This fact seems well known (see [48], (11.6) Proposition], [21]). See also Section 1,3 for analogs of Theorems X and Y for the case when $p = 2$.

Let $\phi$ be the isomorphism $\text{Gal}(F_\infty/K) \rightarrow \mathbb{Z}_p^\times$ which satisfy $P^\sigma = \phi(\sigma)P$ for all $P \in E[\pi^{n+1}]$ and $\sigma \in \text{Gal}(F_\infty/K)$ (see, e.g., [21], p.364, [13]). Let $\chi$ be the restriction of $\phi$ on $\Delta$. We denote by $X(F_\infty)_{\chi}$ (resp. $X(F_\infty)^\chi$) the $\chi$-part of $X(F_\infty)$ (resp. $X(F_\infty)$). (For a $\mathbb{Z}_p[\Delta]$-module $M$ appeared later, we also write $M^\chi$ for its $\chi$-part $M^\chi$.) $X(F_\infty)_{\chi}$ and $X(F_\infty)^\chi$ are also considered as $\Lambda$-modules. In this paper, we mainly treat the $\chi$-part version of the above questions.
Questions. Assume that $K$, $p$, $E$ satisfy (C1), (C2), (C3).

(Q1) When $X(F_{\infty})^\chi$ is not trivial, is $X(F_{\infty})_{\fin}^\chi$ not trivial?
(Q2) When $X(F_{\infty})^\chi$ is not trivial, is $\text{Gal}(M(F_{\infty})/L(F_{\infty}))^\chi$ not trivial?

Remark 1.1.3. Let $A(F_0)$ be the Sylow $p$-subgroup of the ideal class group of $F_0$. Since $\mathfrak{P}$ is the only prime which ramifies in $F_{\infty}/F_0$ and it is totally ramified, the $\Gamma$-coinvariant quotient $(X(F_{\infty})^\chi)^\Gamma$ is isomorphic to $A(F_0)^\chi$ (see, e.g., [50, Theorem 5.1]). From this, we see that $X(F_{\infty})^\chi$ is trivial if and only if $A(F_0)^\chi$ is trivial.

Note that Theorems X and Y actually give the results for the $\chi$-part. (See [8, p.250], [48, p.551, Remark], [21, p.365].)

Theorem Z. Assume that $K$, $p$, $E$ satisfy (C1), (C2), (C3).

(i) If $\text{rank}_\mathbb{Z} E(\mathbb{Q}) \geq 2$, then $X(F_{\infty})^\chi$ is not finite.
(ii) If $\text{rank}_\mathbb{Z} E(\mathbb{Q}) \geq 1$, then $\text{Gal}(M(F_{\infty})/L(F_{\infty}))^\chi$ is not trivial.

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

1.2. Organization of the present paper. Our purposes of this paper are giving several criteria for (Q1), (Q2), and confirming these questions for specific elliptic curves. In Section 2 we will give the criteria.

We shall give examples in Section 3. First, we remark that the examples given in Fukuda-Komatsu’s paper [13] are also examples for our questions (Section 3.2). We also give an example for (Q2) in Section 3.3. These examples are elliptic curves of the form $y^2 = x^3 - dx$ with $p = 5$. In Section 3.4 we shall treat the elliptic curves of the form $y^2 = x^3 - 264d^2x + 1694d^3$ with $p = 3$. Consequently, for the question (Q1), we found that the following cases actually exist.

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

On the other hand, for most of the cases which we examined, (Q2) has an affirmative answer (see, e.g., Section 3.4). In particular, there are examples such that (Q2) has an affirmative answer and (Q1) has a negative answer.

In Appendix [A], we will treat the case when $p = 2$. We shall consider similar questions (Q1t), (Q2t), and we will show that these questions are equivalent.

1.3. Changes from the previous version. (This subsection is written only in the arXiv version.) The main change from arXiv:2001.04687v6 (abbreviated as v6) is that the contents of Appendix A of v6 was moved to Section 2. Theorem A.1.1 of v6 was moved to Remark [22,5]. Note that the proof was slightly modified, and the result was extended to the case when $p \geq 3$. Example A.3.1 was moved to Section 3.3. As a consequence, Appendix B of v6 was renamed to Appendix A of this version. Moreover various texts were modified mainly to shorten this paper.

2. Criteria for the questions (Q1) and (Q2)

2.1. Preliminaries. Let the notation be as in Section [1]. We also define the following notation:

- $K_p$ : the completion of $K$ at $p$,
- $(F_0)_\mathfrak{P}$ : 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 $\mathcal{U}^1$,

By class field theory, we see that

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

Note that 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 $F_0$ (for the name of this conjecture, we followed [19]). Recall that this holds true since $F_0/K$ is an abelian extension (see [5] and [13]).

We fix a topological generator $\gamma$ of $\Gamma$, and we shall identify $\Lambda$ with $\mathbb{Z}_p[[T]]$ ($\gamma \mapsto 1 + T$).

For a finitely generated torsion $\Lambda$-module $Y$, $Y^\Gamma$ denotes the $\Gamma$-invariant submodule of $Y$, $Y_\Gamma$ denotes the $\Gamma$-coinvariant quotient of $Y$, and $\text{Char}_\Lambda Y$ denotes the characteristic ideal of $Y$. For a finite group $B$, let $|B|$ be the order of $B$.

Since the $\{\mathfrak{p}\}$-adic analog of Leopoldt’s conjecture holds for $F_0$, we see that $\mathcal{X}(F_\infty)^\chi_\Gamma$ is finite. From this, we can deduce that the a generator of $\text{Char}_\Lambda \mathcal{X}(F_\infty)^\chi$ is not divisible by $T$ (the same result holds for $X(F_\infty)^\chi$). Moreover, $(\mathcal{X}(F_\infty)^\chi)^\Gamma$ is trivial since $\mathcal{X}(F_\infty)^\chi$ does not have a non-trivial finite $\Lambda$-module. We can also show that $(X(F_\infty)^\chi)^\Gamma = (X(F_\infty)^\chi_{\text{fin}})^\Gamma$. The following isomorphisms and exact sequences play important roles in this section.

1. $\mathcal{X}(F_\infty)^\chi_\Gamma \cong \text{Gal}(M(F_0)/F_0)^\chi$ and $X(F_\infty)^\chi_\Gamma \cong A(F_0)^\chi$.
2. $0 \to (\mathcal{U}^1/\mathcal{E}^1)^\chi \to \text{Gal}(M(F_0)/F_0)^\chi \to A(F_0)^\chi \to 0$.
3. $0 \to (X(F_\infty)^\chi)^\Gamma \to \text{Gal}(M(F_\infty)/L(F_\infty))^\chi \to \mathcal{X}(F_\infty)^\chi_\Gamma \to X(F_\infty)^\chi_\Gamma \to 0$.

For the results given in this paragraph, note that similar results hold for the case of the cyclotomic $\mathbb{Z}_p$-extension of real abelian fields, and one can also show our results quite similarly. See, e.g., [38], [11], [39], [40], [1], [3], [1].

Remark 2.1.1. Note that $L(F_0)_{F_\infty}/F_\infty$ is the maximal unramified subextension of $M(F_0)/F_\infty$ in our situation, and \text{Gal}(M(F_0)/L(F_0)/F_\infty) is isomorphic to the $\mathbb{Z}_p$-torsion subgroup of $\mathcal{U}^1/\mathcal{E}^1$ (this can be shown by using the same argument given in [11 Section 4]). Hence, for the question on the non-triviality of \text{Gal}(M(F_\infty)/L(F_\infty)), it seems significant to study the $\mathbb{Z}_p$-torsion subgroup of $\mathcal{U}^1/\mathcal{E}^1$ (more generally, a similar object of $F_\infty$). Christian Maire gave a remark on the earlier studies on the structure of the $\mathbb{Z}_p$-torsion subgroup of the “group of (semi) local units modulo the completion of the group of global units”. In particular, studying analogous objects of the “Kummer-Leopoldt constant” and the “$p$-adic normalized regulator” (see [1], [17]) may be useful. See also Appendix [A].

2.2. Criteria for (Q2).

Lemma 2.2.1 (cf. e.g., [27], [11]). Assume that $K$, $p$, $E$ satisfy (C1), (C2), (C3). If $(\mathcal{U}^1/\mathcal{E}^1)^\chi$ is not trivial, then $\text{Gal}(M(F_\infty)/L(F_\infty))^\chi$ is not trivial.

Proof. This proposition can be obtained by using the same argument given in the proof of [11, Lemma 2], which treats the case of the cyclotomic $\mathbb{Z}_p$-extension of real abelian fields. (See also [27], Theorem 3.) In fact, by using [11], [2], [3], we can see that the triviality of $\text{Gal}(M(F_\infty)/L(F_\infty))^\chi$ implies the triviality of $(\mathcal{U}^1/\mathcal{E}^1)^\chi$. □
Proposition 2.2.2. Assume that $K$, $p$, $E$ satisfy (C1), (C2), (C3).

(i) If $\mathcal{E}^1$ is contained in $\mathcal{U}^2$, then $\text{Gal}(M(F_\infty)/L(F_\infty))^\chi$ is not trivial.

(ii) If $\mathcal{U}^1$ contains a primitive $p$th root of unity, then $\text{Gal}(M(F_\infty)/L(F_\infty))^\chi$ is not trivial.

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

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

(See [51] Lemma 10.4. Note that it was assumed that $p > 7$ at [51] Section 10, however, we can show that this assertion holds for $p \geq 3$. See also [8] Lemma 9.) Then, (i) follows from this isomorphism and Lemma 2.2.1.

We shall prove (ii). Assume that $\mathcal{U}^1$ contains a primitive $p$th root of unity $\zeta_p$. That is, $(F_0)_p$ is isomorphic to $\mathbb{Q}_p(\zeta_p)$ (see also the proof of [51] Lemma 12). Since $\zeta_p\mathcal{U}^2$ generates $\mathcal{U}^1/\mathcal{U}^2$, it follows that $\zeta_p$ is contained in $(\mathcal{U}^1)^\chi$. We claim that $\mathcal{E}^1$ does not contain $\zeta_p$. Note that the global field $F_0$ does not contain a primitive $p$th root of unity. (If it contains, then both primes of $K$ lying above $p$ ramifies. However, it cannot be occurred because $E$ has good reduction at $p$. See, e.g., [51] Corollary 3.17.) By combining this fact and the validity of the $\{\mathfrak{p}\}$-adic analog of Leopoldt’s conjecture, the claim can be shown (cf. also, e.g., [17] Lemma 3.1 and Corollary 3.2). By this claim, we see that $(\mathcal{U}^1/\mathcal{E}^1)^\chi$ is not trivial.

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. By using this fact and (1), we can see that $(\mathcal{U}^1/\mathcal{E}^1)^\chi$ is trivial if and only if there is a (global) unit $u$ of $F_0$ such that $u^{p-1} \equiv 1 \pmod{\mathfrak{p}^2}$.

Remark 2.2.4. Let $\tilde{E}(\mathbb{F}_p)$ be the group of $\mathbb{F}_p$-rational points of the reduction of $E$ at $p$. Assume that $|\tilde{E}(\mathbb{F}_p)|$ is divisible by $p$. Then we can see that $\psi(p) + \overline{\psi(p)} \equiv 1 \pmod{p}$, where $\psi$ is the Grössencharacter of $E$ over $K$ (see, e.g., [55] Chapter II, Corollary 10.4.1 (b)). By using the argument given in the proof of [8] 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., [8], [32]). Let $S_\pi(E/K)(\subset H^1(\text{Gal}(\bar{K}/K), E[\pi]))$ be the Selmer group relative to $\pi$, and $S_\pi'(E/K)$ the enlarged Selmer group relative to $\pi$ (see, e.g., [45] p.32, [51] Definition 6.3). We may assume that $\tilde{E}(\mathbb{F}_p) \not\equiv 0 \pmod{p}$ (see Remark 2.2.4). Under this assumption, we can show that $S_\pi'(E/K) \cong S_\pi(E/K)$ (see also [45] p.35). Note that

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

(See [51] 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 $\text{III}(E/K)$ (resp. $\text{III}(E/\mathbb{Q})$) be the Tate-Shafarevich group of $E/K$ (resp. $E/\mathbb{Q}$). We denote by $\text{III}(E/K)[\pi]$ the $\pi$-torsion subgroup of $\text{III}(E/K)$ (we also define $\text{III}(E/K)[p]$, $\text{III}(E/K)[\bar{\pi}]$, and $\text{III}(E/\mathbb{Q})[p]$ similarly). In our situation, it is known that both $|\text{III}(E/K)|$ and $|\text{III}(E/\mathbb{Q})|$ are finite (Rubin [48]). Then, by the result of Cassels (see, e.g., [54] Chapter X, Theorem 4.14], the $p$-rank of $\text{III}(E/\mathbb{Q})$ is
even. Moreover, we can show that $S_{\pi}(E/K) \cong \III(E/K)[\pi]$ 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 can obtain the following:

$$
\III(E/K)[p] \cong \III(E/Q)[p] \oplus \III(E^d/Q)[p]
$$

(see, e.g., [36] Lemma 3.1, the argument given in [32]),

$$
\III(E/Q)[p] \cong \III(E^d/Q)[p]
$$

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

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

(cf. the argument given in [20] p.260). By using these results, we see that the $p$-rank of $\III(E/K)[\pi]$ is even. The claim follows, and hence if the $p$-rank of $A(F_0)^{\chi}$ is odd, then $A(F_0)^{\chi}$ is not isomorphic to $\Gal(M(F_0)/F_0)^{\chi}$ (and $(U^1/E^1)^{\chi}$ is not trivial).

2.3. Criteria for $(Q1)$.

**Proposition 2.3.1.** Assume that $K$, $p$, $E$ satisfy $(C1)$, $(C2)$, $(C3)$. If $(U^1/E^1)^{\chi}$ is trivial and rank$_{\mathbb{Z}} E(Q) \geq 1$, then $X(F_{\infty})^{\chi}_{\text{fin}}$ is not trivial.

**Proof.** We first recall that $\Gal(M(F_{\infty})/L(F_{\infty}))^{\chi}$ is not trivial by Theorem Z (ii).

The essential idea of the following argument was given to the author by Satoshi Fujii (concerning his work [11] Section 4]). (Note that the same idea also can be found in [2] Théorème 2.1. See also [1] Proposition 4.) Since $(U^1/E^1)^{\chi}$ is trivial, we see that $\mathfrak{X}(F_{\infty})^{\chi} \cong X(F_{\infty})^{\chi}_{\text{fin}}$ by using (11) and (2). Recall also that $(\mathfrak{X}(F_{\infty})^{\chi})^F$ is trivial. From these facts and (3), we see that

$$
(X(F_{\infty})^{\chi})^F \cong \Gal(M(F_{\infty})/L(F_{\infty}))^{\chi}
$$

Since $\Gal(M(F_{\infty})/L(F_{\infty}))^{\chi}$ is not trivial, we can show that $\Gal(M(F_{\infty})/L(F_{\infty}))^{\chi}_{\text{fin}}$ is not trivial by using Nakayama’s lemma. Then, $(X(F_{\infty})^{\chi})^F = (X(F_{\infty})^{\chi}_{\text{fin}})^F$ is not trivial. The assertion has been shown.

**Corollary 2.3.2.** Assume that $K$, $p$, $E$ satisfy $(C1)$, $(C2)$, $(C3)$. If $(U^1/E^1)^{\chi}$ is trivial, rank$_{\mathbb{Z}} E(Q) = 1$, and $|A(F_0)^{\chi}| = p$, then $X(F_{\infty})^{\chi}$ is non-trivial and finite.

**Proof.** When $|A(F_0)^{\chi}| = p$, we see that $X(F_{\infty})^{\chi}_{\text{fin}}$ is trivial or $X(F_{\infty})^{\chi} = X(F_{\infty})^{\chi}_{\text{fin}}$ (see the proof of [39] Theorem 2). By Proposition 2.3.1, we see that the former case never occurs under the assumption of this corollary.

By using the argument given in the above proof, we can see that if $|A(F_0)^{\chi}| = p$ and $X(F_{\infty})^{\chi}$ is not finite, then $X(F_{\infty})^{\chi}_{\text{fin}}$ is trivial (cf. [25] Corollary 2.2]). Moreover, we can also show the following result (cf. Sections 1–4 of [25]).

Let $\kappa$ be the restriction of $\phi$ on $\Gamma$ (see Section 1.1). Put $r = \text{rank}_{\mathbb{Z}} E(Q)$. It is known that the characteristic ideal $\text{Char}_{\Lambda} X(F_{\infty})^{\chi}$ is contained in $(T + 1 - \kappa(\gamma_0))^{r-1}\Lambda$ (see [21], [13]).

**Proposition 2.3.3.** Let the notation be as above. Assume that $K$, $p$, $E$ satisfy $(C1)$, $(C2)$, $(C3)$. If $r \geq 2$ and $|A(F_0)^{\chi}| = p^{r-1}$, then $X(F_{\infty})^{\chi}_{\text{fin}}$ is trivial and $\text{Char}_{\Lambda} X(F_{\infty})^{\chi} = (T + 1 - \kappa(\gamma_0))^{r-1}\Lambda$. 
Proof. Let \( f(T) \) be a generator of \( \text{Char}_\Lambda X(F_\infty)^\chi \). It is well known that
\[
\frac{|(X(F_\infty)^\chi)^\Gamma|}{|X(F_\infty)^\chi|} = |f(0)|_p,
\]
where \(| \cdot |_p\) denotes the normalized \( p \)-adic (multiplicative) absolute value (see, e.g., [57, Exercise 13.12]).

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

\[\square\]

Remark 2.3.4. If \( E \) and \( p \) satisfy the assumption of the above Proposition 2.3.3, then Conjecture 1.2 of [13] holds for \( E \) and \( p \). However, we mention that this does not imply the validity of Conjecture 1.1 of [13].

3. Examples for the questions (Q1) and (Q2)

3.1. Software used in the example calculation. The author used PARI/GP [14] (formerly 2.11.2 and finally version 2.13.1) mainly to compute the ideal class groups, units, values of \( L \)-functions, etc (all examples are computed (or recomputed) by using version 2.13.1). However, for the computation of the rank of elliptic curves, the author used Sage [52] (\texttt{mwrank} [2] was mainly used). In the computation on Sage, the article [26] was very helpful. The author also would like to express thanks to Iwao Kimura for giving comments.

3.2. Fukuda-Komatsu’s examples. In this subsection, we put \( K = \mathbb{Q}(\sqrt{-1}) \) and \( p = 5 \). We can find a negative example for (Q1) in Fukuda-Komatsu’s paper [13].

Example 3.2.1 (see Fukuda-Komatsu [13]). Let \( E \) be an elliptic curve defined by the Weierstrass equation
\[
y^2 = x^3 + 99x.
\]
Then \( K, p, E \) satisfy (C1), (C2), (C3). This case is treated in [13, Section 4.1]. Note that \( \text{rank}_K E(\mathbb{Q}) = 2 \) ([4, Table des valeurs des \( A(t_i^*) \): I]), and then \( X(F_\infty)^\chi \) is not finite by Theorem Z (i). It is also known that \( |A(F_0)^\chi| = 5 \), hence the infiniteness of \( X(F_\infty)^\chi \) implies that \( |A(F_0)^\chi| = 5 \). By Proposition 2.3.3 we see that \( X(F_\infty)^{\chi_\text{fin}} \) is trivial. Then, this is a negative example for (Q1). On the other hand, (Q2) has an affirmative answer for this case by Theorem Z (ii). Hence the assertion of (Q2) is actually weaker than that of (Q1). Note that Proposition 2.3.3 also gives an alternative proof of the fact (already confirmed in [13]) that \( \text{Char}_\Lambda X(F_\infty)^\chi = (T + 1 - \kappa(\gamma_0))\Lambda \).

In Sections 4.2 and 4.3 of [13], the examples such that \( X(F_\infty)^\chi \) is finite are also given. We shall introduce some of them.

Example 3.2.2 (see Fukuda-Komatsu [13]). Let \( E \) be an elliptic curve defined by the Weierstrass equation
\[
y^2 = x^3 + 1331x.
\]
Then \( K, p, E \) satisfy (C1), (C2), (C3). It is stated in [13, Section 4.2] that \( |A(F_0)| = 5 \) and \( X(F_\infty)^\chi \) is finite. Note that it is not explicitly stated that \( |A(F_0)^\chi| = 5 \) in [13]. (Although it seems that they had obtained this fact, the author also confirmed this fact.)
Hence we see that $X(F_\infty)^\chi$ is non-trivial and finite. Similarly, it is also stated in [13, Section 4.2] that
\[ y^2 = x^3 + 2197x \]
is also an example such that $X(F_\infty)^\chi$ is finite. For this case, it can be also checked that $|A(F_0)^\chi| = 5$, and hence $X(F_\infty)^\chi$ is non-trivial.

Remark 3.2.3. In the computation concerning Example 3.2.2 (and below Example 3.3), the author used an explicit Kummer generator of $F_0$ over $K$ written in [13, p.547] to obtain a defining polynomial of $F_0$. For the curves given in Example 3.2.2, the author checked that $|A(F_0)^\chi| = 5$ by using the following two ways. One is computing the $\Delta$-action for a generator of $A(F_0)$. The other is comparing the information on the $\chi^j$-part of $\chi(F_\infty)$ given in [1, Table des valeurs des $\lambda(l^*_p;i)$: I] and ideal class group of the quadratic subextension of $F_0/K$.

In their computation, Fukuda-Komatsu [13] used the $p$-adic $L$-function and the “Ichimura-Sumida type” criterion for elliptic units to determine the characteristic polynomials. Their method is also a powerful tool to confirm our questions. For example, our Corollary 2.3.2 is not applicable for the cases of $y^2 = x^3 + 1331x$ and $y^2 = x^3 + 2197x$. However, the “Ichimura-Sumida type” criterion seems to need the information on the elliptic units of higher layers of $F_\infty/F_0$ in general. Our criteria only need the information on $F_0$, which can be easily computed by using existing software (at least when $p = 3$). Hence, our criteria seem suitable to confirm various examples (see Section 3.1).

We also note that if an explicit generator $f(T)$ of $\text{Char}_A X(F_\infty)^\chi$ is known, we can check whether $X(F_\infty)^{\chi_{\text{fin}}}$ is trivial or not by comparing $|A(F_0)^\chi|$ and $|f(0)|_p$. (See the proof of Proposition 2.3.3. See also [25].)

3.3. Example for (Q2) with $K = \mathbb{Q}(\sqrt{-1})$ and $p = 5$. Here we give an example for (Q2) such that $\text{rank}_{\mathbb{Z}} E(\mathbb{Q}) = 0$ and $X(F_\infty)^\chi$ is non-trivial.

Example 3.3.1. We put $K = \mathbb{Q}(\sqrt{-1})$ and $p = 5$. Let $E$ be an elliptic curve defined by the Weierstrass equation
\[ y^2 = x^3 - 307^2x. \]
In this case, it is known that $L(E/\mathbb{Q},1) \neq 0$ (see [47, Theorem 1]). The author checked that $|A(F_0)^\chi| = 5$. Then, the criterion given in Remark 2.2.5 is applicable, and hence this is a non-trivial example such that (Q2) has an affirmative answer. We also remark that Proposition 2.2.2(ii) is not applicable for this example. However, the author also checked the non-triviality of $(U^1/E^1)^\chi$ by using a more direct method (Remark 2.2.3).

Remark 3.3.2. For the above example, the order of $A(F_0)$ is 5. Although the fact $|A(F_0)^\chi| = 5$ can be confirmed by observing the $\Delta$-action, we can also check this by using the following way. In this situation, we can see that if $|\text{III}(E/\mathbb{Q})|$ is divisible by 5, then $A(F_0)^{\chi_{\text{fin}}}$ is not trivial. (See Remark 2.2.5. See also the proof of [51, Corollary 6.10].) We also note that the full Birch and Swinnerton-Dyer conjecture holds for $E$ (see [49, p.26, Theorem]). Then, by computing the analytic order of $\text{III}(E/\mathbb{Q})$, we can confirm that $A(F_0)^\chi$ is not trivial, and hence $|A(F_0)^\chi| = 5$. 


3.4. **Examples with** $K = \Q(\sqrt{-11})$ **and** $p = 3$. Let $E_0^d$ 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 $K = \Q(\sqrt{-11})$ and $p = 3$. It is well known that $E_0^d$ has complex multiplication by $O_K$ (see, e.g., [23]). Note also that $E_0^d$ has good reduction at $p = 3$ if and only if $d \equiv 0 \pmod{3}$ (see [23]). We also note that $E_0^d$ and $E_0^{-11d}$ are isomorphic over $K$. Hence, in the remaining part of this subsection, we assume that $d$ satisfies the following condition.

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

Then, under (D1), $K$, $p$, $E_0^d$ satisfy (C1), (C2), (C3). We choose $p$ as a prime generated by $(-1 - \sqrt{-11})/2$. We put $d' = d/3$, then we can see that

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

This can be obtained by using an explicit endomorphism given in [46, Theorem 3]. (However, it seems that the multiplication by $(-1 + \sqrt{-11})/2$ endomorphism given in [46, Theorem 3] is actually the multiplication by $(-1 - \sqrt{-11})/2$ endomorphism.)

Let $\overline{p}$ be the conjugate of $p$. Then, $\overline{p}$ is unramified in $F_0$. Moreover, we can see that $\overline{p}$ 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 $\overline{p}$ splits completely in $F_0$.

Hence, by Proposition [2.2.2](ii), we have obtained the following result.

- If $d \equiv 3 \pmod{9}$, then (Q2) has an affirmative answer for $E_0^d$.

Let $L(E_0^d/Q, s)$ be the complex $L$-function of $E_0^d$ over $Q$. We also note that the root number of $E_0^d$ is $-1$ when $d > 0$. (See [22, Theorem 19.1.1].) Recall also that $d$ is assumed to be prime to 11. Then, $L(E_0^d/Q, 1) = 0$ for this case. Hence if $d > 0$ and the Birch and Swinnerton-Dyer conjecture (or the parity conjecture) holds for $E_0^d$, we see that $\text{rank}_E E_0^d(Q) \geq 1$ (and (Q2) has an affirmative answer by Theorem Z (ii)).

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

**Example 3.4.1.** Assume that $d > 0$ and $d \equiv 6 \pmod{9}$. In the range $1 < d < 3000$, the following values satisfy that $|A(F_0)^\chi| \neq 1$. (We note that $A(F_0) = A(F_0)^\chi$ in this situation. Hence, the process of extracting the $\chi$-part is not needed.)

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

Recall that $L(E_0^d/Q, 1) = 0$ in this situation. Hence, if $L'(E_0^d/Q, 1) \neq 0$, we see that $\text{rank}_E E_0^d(Q) = 1$ ([18, Corollary C]). In the above values, the condition $L'(E_0^d/Q, 1) \neq 0$ is satisfied except for the cases when $d = 141, 807, 2121$. Moreover, for all of these three values, the author checked that $\text{rank}_E E_0^d(Q) = 3$. 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 \((\mathcal{U}^1/\mathcal{E}^1)_x\) is not trivial. Hence, Proposition \ref{prop:2.2.2} is also applicable for these
three values.)

**Example 3.4.2.** Assume that \( d < 0 \) and \( d \equiv 6 \) (mod 9). In the range \(-3000 < d < 0\),
the following 48 values of \( d \) satisfy that \(|A(F_0)_x| \neq 1\).

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

(6)

We can see that the 45 values except for \(-2910, -2361, -1731\) satisfy that \((\mathcal{U}^1/\mathcal{E}^1)_x\) is not
trivial, then (Q2) has an affirmative answer for these 45 values. We note that \(L(E_0^d/Q, 1)\)
is approximately 0 for several values in the above list. (Since the root number of \(E_0^d\) is
+1 in this case \([\ref{thm:22} \text{Theorem 19.1.1}]\), if \(L(E_0^d/Q, 1) = 0\) then \(\text{rank}_{\mathbb{Z}} E_0^d(Q) \geq 2\) under
the parity conjecture.) See the following Examples \ref{ex:3.4.4} and \ref{ex:3.4.7}. (For the case when
\( d = -2361 \), we will later see that (Q1) has an affirmative answer, and hence (Q2) also
has an affirmative answer.)

Next, we shall consider (Q1).

**Example 3.4.3.** We shall back to the situation treated in Example \ref{ex:3.4.1}. Assume that
\( d > 0 \) and \( d \equiv 6 \) (mod 9). For the values given in (5), it was checked that \(\text{rank}_{\mathbb{Z}} E_0^d \geq 1\).
Moreover, if \((\mathcal{U}^1/\mathcal{E}^1)_x\) is trivial then (Q1) has an affirmative answer by Proposition \ref{prop:2.3.1}.
For the values stated in (5), the following values satisfy that \((\mathcal{U}^1/\mathcal{E}^1)_x\) is trivial.

\[
d = \begin{array}{c}
78, 87, 186, 195, 213, 285, 393, 447, 501, 510, 537, 609, 699, 717, \\
753, 861, 870, 915, 969, 987, 1005, 1017, 1320, 1293, 1365, 1482, \\
1545, 1635, 1662, 1707, 1779, 1842, 1851, 1887, 1923, 1959, 2085, \\
2139, 2247, 2454, 2463, 2481, 2562, 2571, 2634, 2679, 2715, 2769, \\
2877, 2922, 2967, 2985.
\end{array}
\]

Note that all of these values satisfy \(\text{rank}_{\mathbb{Z}} E_0^d = 1\). In addition, if \(|A(F_0)_x| = 3\), then
\(X(F_\infty)_x\) is non-trivial and finite by Corollary \ref{cor:2.3.2}. In the above list, the condition
\(|A(F_0)_x| = 3\) is satisfied except for the cases when \(d = 1167, 1482, 2247\).

The above are the affirmative examples for (Q1). We can also find many negative
examples (that is, \(X(F_\infty)_x\) is infinite and \(X(F_\infty)_\text{fin}\) is trivial).

**Example 3.4.4.** As noted in Example \ref{ex:3.4.2}, several values of \( d \) stated in (6) satisfy that
\(L(E_0^d/Q, 1)\) is approximately 0. Such values are the following:

\[
d = \begin{array}{c}
-2874, -2847, -2730, -2703, -2649, -2514, -2361, -2271, -2154, -1974, \\
-1965, -1758, -1119, -1002, -651, -489, -399, -390, -255, -174, -93, -21.
\end{array}
\]

The author checked that \(\text{rank}_{\mathbb{Z}} E_0^d(Q) = 2\) for all of the above values. Hence, for these
values, we see that \(X(F_\infty)_x\) is infinite by Theorem Z (i). Moreover, if \(|A(F_0)_x| = 3\), then
\(X(F_\infty)_\text{fin}\) is trivial (and \(\text{Char}_{\Lambda} X(F_\infty)_x = (T + 1 - \kappa(\gamma_0))\Lambda\) by Proposition \ref{prop:2.3.3}.
In the above list, we can check that \(|A(F_0)_x| = 3\) except for the cases when \(d = -2703, -2361.\)
Example 3.4.5. We shall consider the cases when \( d = 141, 807, 2121 \). Recall that \( \text{rank}_{E_0^d}(\Q) = 3 \) for these values (see Example 3.4.4). Moreover, it can be checked that \( |A(F_0)^\chi| = 9 \) for all of these values. Then we see that \( X(F_\infty)^\chi \) is trivial and \( \text{Char}_{\Lambda} X(F_\infty)^\chi = (T + 1 - \kappa(\gamma_0))^{\text{fin}} \) by Proposition 2.3.3.

The above Example 3.4.5 gives examples of rank 3 elliptic curves such that Conjecture 1.2 of [13] is valid.

Remark 3.4.6. We can also find examples satisfying \( X(F_\infty)^\chi \) is infinite and \( X(F_\infty)^\chi_{\text{fin}} \) is trivial for the case when \( d \equiv 3 \pmod 9 \). For instance, \( d = -159, -114, -51 \) are such values.

The following is an example such that \( X(F_\infty)^\chi \) is infinite and \( X(F_\infty)^\chi_{\text{fin}} \) is not trivial.

Example 3.4.7. We shall consider the case when \( d = -2361 \). Recall that \( \text{rank}_{E_0} E_0^{-2361}(\Q) = 2 \), and hence \( X(F_\infty)^\chi \) is infinite (Example 3.4.4). In this case, we also see that \( (\mathcal{U}/\mathcal{E})^\chi \) is trivial (Example 3.4.2). Thus, by Proposition 2.3.1, we see that \( X(F_\infty)^\chi_{\text{fin}} \) is not trivial.

As a conclusion of this subsection, for the case of \( E_0^d \) 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 when \( d = -2910, -1731 \).
- Similar to the situation treated in Section 3.2, both affirmative and negative examples exist for (Q1).

A.1. Questions and results. In this Appendix B, we fix \( K = \Q(\sqrt{-7}) \) and \( p = 2 \). For a non-zero square free integer \( d \), let \( E_0^d \) be the elliptic curve over \( \Q \) defined by the following equation

\[
y^2 = x^3 + 21dx^2 + 112d^2x.
\]

It is well known that \( E_0^d \) has complex multiplication by \( O_K \). This situation is well studied, and we shall recall several facts. Note that \( E_0^d \) has good reduction at 2 if and only if \( d \equiv 1 \pmod 4 \) (see, e.g., [23]). Moreover, if \( d \) is prime to 7, then \( E_0^d \) is isomorphic to \( E_0^{-7d} \) over \( K \) (see, e.g., [55], Chapter X], [16], Section 7], [32], Section 2]). Hence, it is sufficient to consider \( E_0^d \) such that \( d \) satisfies the following condition.

(D2) \( d \) is a square-free integer satisfying \( d \equiv 1 \pmod 4 \) and \( d \neq 0 \pmod 7 \).

(See also, e.g., [16], Section 7], [6], [7].) Note 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 put \( \pi = \psi(\mathfrak{p}) \) (where \( \psi \) is the Grössencharacter of \( E_0^d \) over \( K \)), and \( F_n = K(E_0^d[\pi^{n+2}]) \) for all \( n \geq 0 \) (this definition is slightly different from the case when \( p \geq 3 \)). Note that \( F_0/K \) is a quadratic extension (see, e.g., [16], Section 2], [6]). It is known that \( F_n/K \) is totally ramified at \( \mathfrak{p} \) (see, e.g., [48] (3.6)Proposition (i)], [6]). We denote by \( \mathfrak{q} \) the unique prime of \( F_0 \) lying above \( \mathfrak{p} \). We put \( F_\infty = \bigcup_n F_n \), then \( F_\infty/F_0 \) is a \( \Z_2 \)-extension unramified outside \( \mathfrak{q} \).

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

\[
F_0 = K(\sqrt{d\sqrt{-7}}).
\]

(See [6], Lemma 2.2], however, notice the difference of the choice of \( \mathfrak{p} \).)

We define the notation \( \Gamma, \Lambda, X(F_\infty), X(F_\infty), M(F_\infty), L(F_\infty), \) etc. as similar to Section 1. In this appendix, we shall consider the following:
Questions. Let the notation be as in the previous paragraphs, and assume that \(d\) satisfies (D2).

(Q1t) When \(X(F_\infty)\) is not trivial, is \(X(F_\infty)_{\text{fin}}\) not trivial?

(Q2t) When \(X(F_\infty)\) is not trivial, is \(\text{Gal}(M(F_\infty)/L(F_\infty))\) not trivial?

Concerning the above questions, we shall show the following:

Theorem A.1.1. Assume that \(d\) satisfies (D2).

(i) If \(d \equiv 5 \pmod{8}\), then (Q1t) has an affirmative answer for \(E^d_\ast\).

(ii) Suppose that \(d \equiv 1 \pmod{8}\). If \(\text{Gal}(M(F_\infty)/L(F_\infty))\) is not trivial, then \(X(F_\infty)_{\text{fin}}\) not trivial.

Hence, in this situation, if (Q2t) has an affirmative answer then (Q1t) also has, and vice versa. (Note that a similar assertion to that of stated in Remark A.1.2 also holds.)

One can also show an analog of Theorem Y for this situation (see Section A.3). Thus, (Q2t) has an affirmative answer when \(\text{rank}_\mathbb{Z} E^d_\ast(\mathbb{Q}) \geq 1\). By combining this fact and Theorem A.1.1, we obtain the following:

Corollary A.1.2. Assume that \(d\) satisfies (D2). If \(\text{rank}_\mathbb{Z} E^d_\ast(\mathbb{Q}) \geq 1\), then (Q1t) has an affirmative answer for \(E^d_\ast\).

Furthermore, we can also show an analog of Theorem X. That is, If \(\text{rank}_\mathbb{Z} E^d_\ast(\mathbb{Q}) \geq 2\), then \(X(F_\infty)\) is infinite (see Section A.3).

A.2. Proof of Theorem A.1.1. Let the notation be as in Section A.1. Recall that \(F_0/K\) is totally ramified at \(p\), and \(\mathfrak{P}\) is the unique prime of \(F_0\) lying above \(p\). Let \(\text{cl}(\mathfrak{P})\) be the ideal class of \(F_0\) containing \(\mathfrak{P}\). We note that the order of \(\text{cl}(\mathfrak{P})\) is equal to 1 or 2 because the class number of \(K\) is 1.

Lemma A.2.1. Assume that \(d\) satisfies (D2). If \(\text{cl}(\mathfrak{P})\) is not trivial (i.e., \(\mathfrak{P}\) is not principal), then \(X(F_\infty)_{\text{fin}}\) is not trivial.

Proof. This assertion is essentially well known, and this can be shown by using the arguments given in the papers treating original Greenberg’s conjecture. (See also [12, Corollary 3.5] which treats a similar situation to ours.)

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 \(A(F_n)\) consists of the classes containing a power of the prime lying above \(\mathfrak{P}\). Assume that \(\text{cl}(\mathfrak{P})\) is not trivial. As noted above, the order of \(\text{cl}(\mathfrak{P})\) is 2.

In our situation, we can see that \(|A(F_n)^{\text{Gal}(F_n/F_0)}|\) is bounded with respect to \(n\) (cf. the proof of [18, Theorem 1]), and then \(|D_n|\) is also bounded. From this, we can show that \(\text{cl}(\mathfrak{P})\) capitolates in \(F_n\) if \(n\) is sufficiently large (cf. [18, p.267]). Thus, by using [38, p.218, Proposition], we see that \(X(F_\infty)_{\text{fin}}\) is not trivial. \(\square\)

We also show the following lemma. (A similar result for the case of real quadratic fields is known. See [12, Lemma 2].)

Lemma A.2.2. Assume that \(d\) satisfies (D2). If \(d\) has a rational prime divisor \(\ell\) which satisfies \(\ell \equiv \pm 3 \pmod{8}\), then \(\text{cl}(\mathfrak{P})\) is not trivial.

Proof. We put \(\ell^* = \ell\) or \(-\ell\) so that \(\ell^*\) satisfies \(\ell^* \equiv 1 \pmod{4}\). Then \(K(\sqrt{\ell^*})/K\) is unramified outside the primes lying above \(\ell^*\), and every prime of \(K\) lying above \(\ell^*\) is totally ramified in \(K(\sqrt{\ell^*})\).
We note that every prime of $K$ lying above $\ell$ also ramifies in $F_0$. Since the prime of $K$ lying above 7 is ramified in $F_0$, $K(\sqrt[4]{\ell})$ and $F_0$ are disjoint. (See \[7\]).

Note that every prime of $K$ lying above $\ell$ is tamely ramified in $F_0(\sqrt[4]{\ell})$. Then, we can see that $F_0(\sqrt[4]{\ell^*})/F_0$ is an unramified extension by combining the above results.

On the other hand, the rational prime 2 is inert in $\mathbb{Q}(\sqrt[4]{\ell})$. Since 2 splits in $K$ and $p$ ramifies in $F_0$, we see that $\mathfrak{P}$ is inert in $F_0(\sqrt[4]{\ell^*})$. This implies the assertion of the lemma.

\begin{proof}[Proof of Theorem \ref{thm:A.1.1} (i)]
Since $d \equiv 5 \pmod{8}$, there is a rational prime divisor $\ell$ of $d$ which satisfies $\ell \equiv \pm 3 \pmod{8}$. Then the theorem follows from Lemmas \ref{lem:A.2.1} and \ref{lem:A.2.2}.
\end{proof}

We shall give a significant lemma to prove (ii). Similar to the case when $p \geq 3$, we denote by $(F_0)_{\mathfrak{P}}$ the completion of $F_0$ at $\mathfrak{P}$. We also define $\mathcal{U}^1$, $E(F_0)^1$, and $\mathcal{E}^1$ similarly (see Section \ref{section:2.3}).

\begin{lemma}
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.
\end{lemma}

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

By taking a suitable generator $\gamma$ 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 \cite{Li} Lemma 5]). Let $\text{ord}_{\mathfrak{P}}(\cdot)$ be the normalized (additive) valuation at $\mathfrak{P}$. By using a similar argument given in the proof of \cite{Li} Lemma 5], we see that $\text{ord}_{\mathfrak{P}}(\eta^2 - 1) = 2$. Hence, we also see that

$$\text{ord}_{\mathfrak{P}}(\eta - 1) = 1 \quad \text{and} \quad \text{ord}_{\mathfrak{P}}(-\eta - 1) = 1.$$ 

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 \cite{Li}.) From these facts, we can see that $\mathcal{U}^1/\mathcal{E}^1$ has no non-trivial $\mathbb{Z}_2$-torsion element.
\end{proof}

\begin{proof}[Proof of Theorem \ref{thm:A.1.1} (ii)]
If $\text{cl}(\mathfrak{P})$ is not trivial, then $X(F_\infty)_{\text{fin}}$ is not trivial by Lemma \ref{lem:A.2.1}. Hence, in the following, we assume that $\text{cl}(\mathfrak{P})$ is trivial.

Similar to the proof of Proposition \ref{prop:2.3.1}, we use the argument given in \cite{19} 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 \ref{lem:A.2.3}. From this, we see that $\mathfrak{X}(F_\infty)_{\Gamma} \cong X(F_\infty)_{\Gamma}$, and then

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

(We used the validity of the $\{\mathfrak{P}\}$-adic analog of Leopoldt’s conjecture and the fact that $\mathfrak{X}(F_\infty)$ does not have a non-trivial finite $\Lambda$-submodule. See \cite{19}.) The assertion follows from this.
\end{proof}

\subsection{Remarks}
Assume that $d$ satisfies (D2). In our situation of this Appendix \ref{appendix:A}, we can obtain an analog of Theorem Y. That is, if $\text{rank}_\mathbb{Z} E^4_{\eta}(\mathbb{Q}) \geq 1$ then $\text{Gal}(M(F_\infty)/L(F_\infty))$ is not trivial. This can be shown by using a similar method (see the proofs of Theorem 11 (p.231) and Lemmas 33, 35 of \cite{8}). Note that the main difference from the case when $p \geq 3$ seems that certain cohomology groups (corresponding to $H^1(G_\infty, \mathcal{E}_{\infty + 1})$ in \cite{8}) are
non-trivial (cf. also the proof of [16, Lemma 2.7]). However, by using Sah’s lemma, we can see that the orders of these groups are bounded with respect to \( n \), and hence this does not give an essential difficulty. (See, e.g., [33, Lemma A.2]. See also [48, (2.2) Lemma].) We can also obtain an analog of Theorem X by using the known method for the case when \( p \geq 3 \). (See [48, p.551, Remark], [21, pp.364–366]. See also [14] for a more detailed argument.)

As noted in [16, 7] (see also [22, Theorem 19.1.1]), it is known that \( L(E_d^s, 1) = 0 \) when \( d < 0 \) (recall that \( d \not\equiv 0 \pmod 7 \)). Hence, \( \operatorname{rank}_\mathbb{Z} E_d^s(\mathbb{Q}) \) is expected to be positive for this case. We also mention that a sufficient condition to satisfy \( \operatorname{rank}_\mathbb{Z} E_d^s(\mathbb{Q}) = 1 \) is given in [7, Theorem 1.4].

We shall give another remark. The \( \mathbb{Z}_2 \)-rank of \( \mathfrak{X}(F_\infty) \) was considered in [6]. See also the recently announced preprint [30]. These results seem helpful for future research on our questions (Q1t), (Q2t).

Acknowledgments. This research was born out of the discussions with Satoshi Fujii. In particular, informing the ideas concerning the results of [11] from him was one of the motivations to start this study. (See also Remark 2.1.1, the proofs of Proposition 2.3.1 and Theorem A.1.1(ii).) The author would express thanks to him. The author also would 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 express thanks to Christian Maire for giving comments on an earlier manuscript (Remark 2.1.1) and to Jianing Li for sending a manuscript of a stronger version of [29] 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. This work was partly supported by JSPS KAKENHI Grant Number JP15K04791.

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 ceraines formes faibles de la conjecture de Greenberg*, manuscripta math. 116 (2005), 323–340.
[3] M. H. Baker and K. A. Ribet: *Galois theory and torsion points on curves*, J. Théor. Nombres Bordeaux 15 (2003), 11–32.
[4] D. Bernardi, C. Goldstein, and N. Stephens: *Notes p-adiques sur les courbes elliptiques*, J. Reine Angew. Math. 351 (1984), 129–170.
[5] A. Brumer: *On the units of algebraic number fields*, Mathematika 14 (1967), 121–124.
[6] J. Choi and J. Coates: *Iwasawa theory of quadratic twists of \( X_0(49) \)*, Acta Math. Sin. (Engl. Ser.) 34 (2018), 19–28.
[7] J. Coates, Y. Li, and Y. Tian: *Quadratic twists of elliptic curves*, Proc. Lond. Math. Soc. 110 (2015), 357–394.
[8] J. Coates and A. Wiles : On the conjecture of Birch and Swinnerton-Dyer, Invent. Math. 39 (1977), 223–251.
[9] J. E. Cremona : mwrank and eclib.
http://homepages.warwick.ac.uk/staff/J.E.Cremona/mwrank/index.html.
[10] B. Ferrero and L. C. Washington : The Iwasawa invariant $\mu_p$ vanishes for abelian number fields, Ann. of Math. (2) 109 (1979), 377–395.
[11] 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.
[12] S. Fujii and T. Itoh : Some remarks on pseudo-null submodules of tamely ramified Iwasawa modules, J. Théor. Nombres Bordeaux 30 (2018), 533–555.
[13] 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.
[14] T. Fukuda, K. Komatsu, and S. Yamagata : Iwasawa $\lambda$-invariants and Mordell-Weil ranks of abelian varieties with complex multiplication, J. Théor. Nombres Bordeaux 30 (2018), 533–555.
[15] R. Gillard : Transformation de Mellin-Leopoldt des fonctions elliptiques, J. Number Theory 25 (1987), 379–393.
[16] C. D. Gonzalez-Avilés : On the conjecture of Birch and Swinnerton-Dyer, Trans. Amer. Math. Soc. 349 (1997), 4181–4200.
[17] G. Gras : The $p$-adic Kummer-Leopoldt constant: Normalized $p$-adic regulator, Int. J. Number Theory 14 (2018), 329–337.
[18] R. Greenberg : On the structure of certain Galois groups, Invent. Math. 47 (1978), 85–99.
[19] R. Greenberg : On the structure of certain Galois groups, Invent. Math. 72 (1983), 241–265.
[20] R. Greenberg : Iwasawa theory – past and present, Class field theory – its centenary and prospect (Tokyo, 1998), 335–385, Adv. Stud. Pure. Math. 30, Math. Soc. Japan, Tokyo, 2001.
[21] B. H. Gross : Arithmetic on elliptic curves with complex multiplication, With an appendix by B. Mazur, Lecture Notes in Mathematics 776, Springer-Verlag, Berlin, Heidelberg, 1980.
[22] T. Hadano : Conductor of elliptic curves with complex multiplication and elliptic curves of prime conductor, Proc. Japan Acad. Ser. A Math. Sci. 51 (1975), 92–95.
[23] H. Ichimura : A note on the Iwasawa $\lambda$-invariants of real quadratic fields, Proc. Japan Acad. Ser. A Math. Sci. 72 (1996), 28–30.
[24] T. Itoh : Tamely ramified Iwasawa modules having no non-trivial pseudo-null submodules, J. Théor. Nombres Bordeaux 30 (2018), 859–872.
[25] I. Kimura : Suron kenkyusha no tameno Sage (Sage for number theorists) (in Japanese), Algebraic number theory and related topics 2010, 125–114, RIMS Kôkyûroku Bessatsu, B32, Res. Inst. Math. Sci., Kyoto, 2012.
[26] J. S. Kraft : Iwasawa invariants of CM fields, J. Number Theory 32 (1989), 65–77.
[27] S. Lang : Cyclotomic fields I and II. Combined second edition, With an appendix by K. Rubin, Graduate Texts in Math. 121, Springer-Verlag, New York, 1990.
[28] J. Li : On the 2-adic logarithm of units if certain totally imaginary quartic fields, Asian J. Math. 25 (2021), 177–182.
[29] J. Li : On the $\lambda$-invariant of Selmer groups arising from certain quadratic twists of Gross curves, preprint, arXiv:2107.03027.
[30] B. Mazur and A. Wiles : Class fields of abelian extensions of $\mathbb{Q}$, Invent. Math. 76 (1984), 179–330.
[31] 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.
[32] T. Nguyen Quang Do : Sur la conjecture faible de Greenberg dans le cas abélien p-décomposé, Int. J. Number Theory 2 (2006), 49–64.
[33] T. Nguyen Quang Do : Sur une forme faible de la conjecture de Greenberg II, Int. J. Number Theory 13 (2017), 1061–1070.
[34] T. Nguyen Quang Do : Formules de genres et conjecture de Greenberg, Ann. Math. Qué. 42 (2018), 267–280.
[36] K. Ono and M. A. Papanikolas: Quadratic twists of modular forms and elliptic curves, Number\ntheory for the millennium, III (Urbana, IL, 2000), 73–85, A K Peters, Natick, MA, 2002.

[37] H. Oukhaba and S. Viguié: On the \( \mu \)-invariant of Katz \( p \)-adic \( L \) functions attached to imaginary\nquadratic fields and applications, Forum Math. 28 (2016), 507–525.

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

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

[40] M. Ozaki: The class group of \( \mathbb{Z}_p \)-extensions over totally real number fields, Tôhoku Math. J. (2)\n49 (1997), 431–435.

[41] M. Ozaki and H. Taya: A note on Greenberg’s conjecture for real abelian number fields, manuscripta\nmath. 88 (1995), 311–320.

[42] M. Ozaki and H. Taya: On the Iwasawa \( \lambda \)-invariants of certain families of real quadratic fields,\nmanuscripta math. 94 (1997), 437–444.

[43] M. Ozaki and H. Taya: A note on the Iwasawa \( \lambda \)-invariants of real abelian number fields, Interdiscip.\nInform. Sci. 4 (1998), 109–116.

[44] The PARI-Group: PARI/GP version 2.13.1, Univ. Bordeaux, 2021, \texttt{http://pari.math.u-bordeaux.fr/}.

[45] B. Perrin-Riou: Arithmétique des courbes elliptiques et théorie d’Iwasawa, Mém. Soc. Math. France\n17 (1984), 1–130.

[46] A. R. Rajwade: Some formulae for elliptic curves with complex multiplication, Indian J. Pure Appl.\nMath. 8 (1977), 379–387.

[47] M. J. Razar: The non-vanishing of \( L(1) \) for certain elliptic curves with no first descents, Amer. J.\nMath. 96 (1974), 104–126.

[48] K. Rubin: Tate–Shafarevich groups and \( L \)-functions of elliptic curves with complex multiplication,\nInvent. Math. 89 (1987), 527–560.

[49] K. Rubin: The “main conjectures” of Iwasawa theory for imaginary quadratic fields, Invent. Math.\n103 (1991), 25–68.

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

[51] K. Rubin: Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-\nDyer, Arithmetic theory of elliptic curves (Cetraro, Italy, 1997), 167–234, Lecture Notes in Math.\n1716, Springer-Verlag, Berlin, Heidelberg, New York, 1999.

[52] The Sage Developers: SageMath, the Sage Mathematics Software System (Version 9.2), 2020, \texttt{https://www.sagemath.org}.

[53] C.-H. Sah: Automorphism of finite groups, J. Algebra 10 (1968), 47–68.

[54] L. Schneps: On the \( \mu \)-invariant of \( p \)-adic \( L \)-functions attached to elliptic curves with complex mul-
tiplication, J. Number Theory 25 (1987), 20–33.

[55] J. H. Silverman: The arithmetic of elliptic curves, Graduate Texts in Math. 106, Springer-Verlag,\r
New York, 1986. (corrected 2nd printing, 1992.)

[56] J. H. Silverman: Advanced topics in the arithmetic of elliptic curves, Graduate Texts in Math. 151,\r
Springer-Verlag, New York, 1994. (corrected second printing, 1999.)

[57] L. C. Washington: Introduction to cyclotomic fields, Second edition, Graduate Texts in Math. 83,\r
Springer-Verlag, New York, Berlin, Heidelberg, 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